Allestimento di collegamenti on-line nel settore della polizia

Rapporto della Commissione della gestione del Consiglio degli Stati del 19 novembre 1998

Rapporto

1 Introduzione

11 Problematica

La progressiva dotazione di mezzi informatici a disposizione delle autorità federali affinché esse possano adempiere i loro compiti legali ha comportato l'allestimento di un numero sempre maggiore di collegamenti on-line, in particolare nel settore della polizia. Questi collegamenti consentono a molti servizi pubblici l'accesso diretto (on-line) a diverse banche dati.

Nell'intento di illustrare questa problematica in modo più esplicito, è stato elaborato uno schema che rappresenta diversi sistemi informatici della polizia (*fonte:* primo rapporto d'attività 93/94 dell'Incaricato federale della protezione dei dati, aggiornato dall'OPCA, gennaio 1998). Questo schema, che comprende solo una parte di tutti i sistemi dell'Amministrazione federale, mostra chiaramente la quantità di collegamenti on-line esistenti o previsti di cui possono beneficiare diverse autorità.

Non tutti i collegamenti on-line riportati sullo schema consentono l'accesso all'insieme dei dati di un sistema. In realtà, è possibile accedere soltanto a una parte dei dati, a seconda della matrice d'accesso. Fra tutti i collegamenti rappresentati, alcuni sono già operativi, altri possono essere autorizzati sulla base delle leggi o delle ordinanze vigenti, e altri ancora sono previsti nel quadro di progetti legislativi.

La legge federale sulla protezione dei dati prescrive che gli organi federali hanno il diritto di elaborare dati personali soltanto se ne esistono i fondamenti giuridici. Essa prescrive inoltre che gli organi federali possono permettere l'accesso a dati personali solo mediante una procedura di richiamo (on-line) qualora ciò sia previsto esplicitamente. Dati personali degni di particolare protezione come pure profili della personalità possono essere resi accessibili mediante una procedura di richiamo soltanto qualora lo preveda esplicitamente una legge in senso formale.

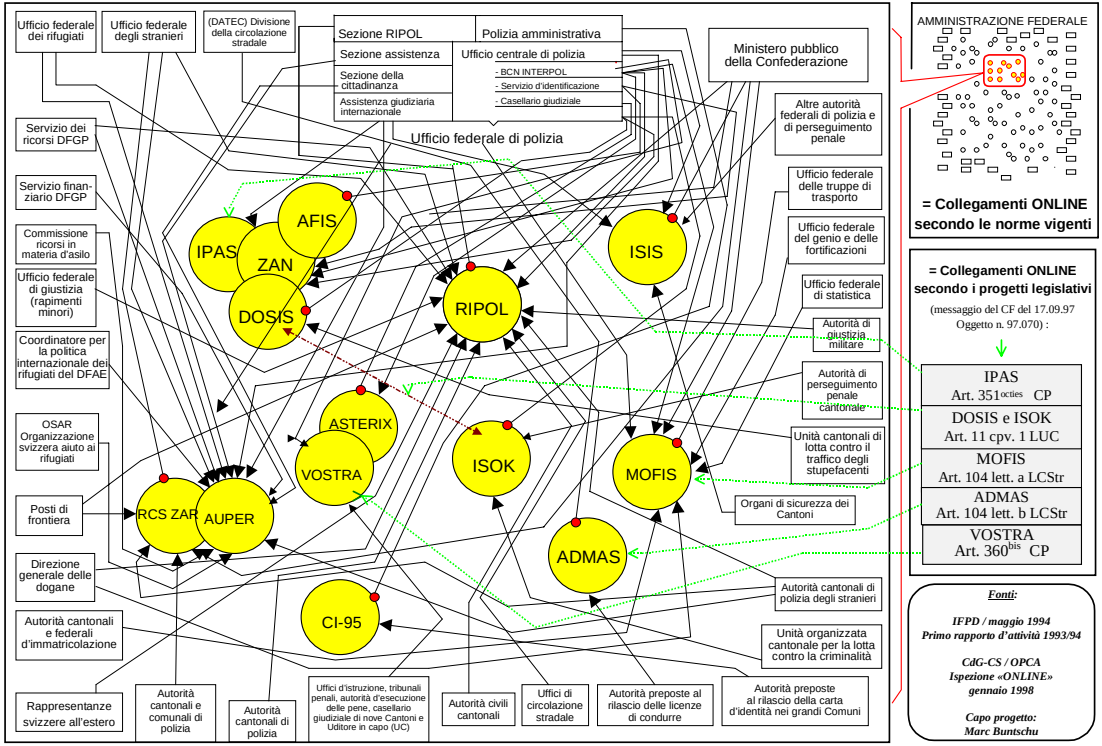
L'Ufficio federale di giustizia e l'Incaricato federale della protezione dei dati (IFPD), prendendo posizione in occasione di audizioni, comunicazioni o conferenze stampa, hanno ripetutamente ricordato che queste esigenze vanno soddisfatte per qualsiasi trattamento di dati personali. In questi ultimi anni molte autorità federali hanno chiesto di accedere a un numero crescente di sistemi informativi. Questa tendenza ha avuto quale conseguenza l'istituzione di basi legali che permettono ogni possibile accesso, in particolare nel settore della polizia.

Il principio di legalità mira innanzitutto a garantire la trasparenza e, da solo, non basta a legittimare un accesso on-line. Prima di allestire un collegamento on-line occorre procedere a un esame della necessità, dei costi e della conformità ai principi

di proporzionalità, finalità e opportunità. In altre parole, una procedura di richiamo dev'essere conforme anche a questi principi e non può essere prevista o giustificata soltanto con l'esistenza di una base legale. Questa problematica è stata sollevata anche a livello cantonale[1].

[1] «Questo impegno si registra in particolare nell'ambito della procedura di richiamo: di fronte all'attuale tendenza a introdurre tali procedure in tutta l'Amministrazione, la Commissione auspica che si intraprenda una riflessione generalizzata e che il Governo non si limiti unicamente a proporre al Gran Consiglio di adottare una base legale ogni volta che viene allestito un nuovo collegamento on-line» (cfr. Rapport sur l'activité de l'Autorité cantonale fribourgeoise de surveillance en matière de protection des données, luglio 95 - dicembre 96, pag.7).

Ispezione ON-LINE / (Allestimento di collegamenti on-line nel settore della polizia)
Ispezione della Commissione della gestione del Consiglio degli Stati e dell'Organo parlamentare di controllo dell'Amministrazione



ADMAS registro automatizzato delle misure amministrative dei conducenti di veicoli / **AFIS** sistema automatico d'identificazione delle impronte digitali / **ASTERIX** indice automatizzato del casellario giudiziale / **AUPER** sistema automatizzato di registrazione delle persone / **CI-95** banca di dati della nuova carta d'identità / **IPAS** sistema informatizzato di gestione e indice informatizzato delle persone e dei fascicoli / **ISIS** sistema per il trattamento dei dati relativi alla protezione dello Stato / **ISOK** sistema di trattamento dei dati in materia di lotta contro la criminalità organizzata / **DOSIS** sistema di trattamento dei dati in materia di lotta contro il traffico illegale di stupefacenti / **MOFIS** registro dei veicoli e detentori di veicoli / **RCS-ZAR** registro centrale degli stranieri / **RIPOL** sistema di ricerca informatizzato di persone e oggetti / **VOSTRA** casellario giudiziale informatizzato / **ZAN** indice centrale delle pratiche

12 Mandato delle commissioni della gestione

Le Commissioni della gestione hanno deciso, nell'ambito del loro programma annuale 1998, di svolgere un'ispezione relativa all'allestimento di collegamenti on-line nel settore della polizia.

La Sezione «Autorità» della Commissione della gestione del Consiglio degli Stati, incaricata dell'ispezione, si è posta diversi obiettivi da perseguire nell'ambito della sua inchiesta, fra cui un esame sul piano concettuale e una valutazione della prassi attualmente in vigore (cfr. rapporto peritale, allegato 1[2]).

L'ispezione intende innanzitutto enucleare le esigenze legali e concettuali attualmente in vigore nel quadro dell'allestimento di collegamenti on-line. Questa parte ha pertanto carattere teorico ed esamina le esigenze concettuali, le questioni relative alla protezione dei dati e al rispetto, fin dalla sua concezione, della proporzionalità, della finalità e dell'opportunità da un punto di vista generale.

Il rapporto peritale esamina la prassi adottata dall'Amministrazione federale nell'allestimento di procedure di richiamo di dati fin dalla pianificazione di un sistema, come pure l'attribuzione di nuove possibilità di accesso on-line alle autorità federali e cantonali.

13 Organizzazione e svolgimento dei lavori della Commissione

131 Organizzazione

La Sezione è organizzata nel seguente modo:

Presidente:	CS Pierre Aeby
Membri:	CS Hans Danioth; CS Bruno Frick (fino alla fine del 1997); CS Hans Hess (dal giugno 1998), CS Andreas Iten; CS Franz Wicki; CS Kaspar Rhyner (fino a fine maggio 1998)
Segreteria:	Mariangela Wallimann-Bornatico, segretaria della CdG

Organo parlamentare di controllo dell'amministrazione (OPCA): Marc Buntschu

Esperto incaricato: Lukas Fässler, avvocato ed esperto di informatica.

132 Svolgimento dei lavori

La Sezione «Autorità», riunitasi l'8 aprile 1997, ha esaminato questa problematica sulla base di un documento di lavoro redatto dall'Organo parlamentare di controllo dell'Amministrazione (OPCA). La Sezione ha riconosciuto la necessità di continuare le sue indagini e, in una lettera del 10 aprile 1997, ha informato al riguardo il Consiglio federale.

[2] L'allegato 1 può essere ottenuto (in tedesco e in francese) presso la Segreteria della Commissione della gestione del Consiglio degli Stati.

Dopo aver preso atto, il 27 giugno 1997, dell'abbozzo di progetto dell'OPCA, la Sezione ha stabilito, nell'ambito di uno studio di fattibilità, il settore, le scadenze e gli aspetti organizzativi dell'indagine, definendo i temi che intendeva trattare.

A fine marzo 1998, l'OPCA ha depositato un documento di lavoro. Il 6 maggio 1998 l'esperto incaricato ha presentato oralmente le sue prime conclusioni alla Sezione, la quale, nella seduta plenaria del 25 e 26 maggio 1998, ha informato la Commissione della gestione del Consiglio degli Stati sui primi risultati dell'ispezione. Dopo aver consultato gli uffici interessati, l'esperto incaricato ha presentato il suo rapporto definitivo il 31 luglio 1998.

La Sezione ha esaminato per la prima volta il 2 settembre 1998 i risultati dell'inchiesta. Dopo un secondo esame, ha fatto pervenire al capo del DFGP e a quello del DFF il progetto di rapporto per una presa di posizione. Essa ha in seguito discusso, nella seduta del 5 novembre 1998, le posizioni di detti Dipartimenti in presenza del consigliere federale Arnold Koller. La Sezione ha altresì sentito il parere dell'Incaricato federale della protezione dei dati.

Il rapporto finale è stato presentato alla Commissione della gestione del Consiglio degli Stati, che l'ha approvato il 19 novembre 1998.

133 Collaborazione con l'Amministrazione federale

Sia l'OPCA sia l'esperto incaricato hanno rilevato che la collaborazione con gli uffici interessati del Dipartimento di giustizia e polizia è stata interessante e costruttiva. Alcuni dei miglioramenti che l'esperto aveva proposto nel suo primo documento di lavoro hanno già potuto essere in parte realizzati.

134 Indipendenza dei membri della Sezione

I membri della Sezione confermano di non avere alcun legame, né di natura privata né di natura professionale, che possa interferire con le questioni sollevate nel presente rapporto.

14 Metodologia

141 Modo di procedere

L'OPCA e l'esperto hanno in un primo tempo proceduto all'esame della situazione. Su richiesta degli esperti, i servizi interessati hanno messo a disposizione la seguente documentazione:

- tutte le disposizioni vigenti che trovano applicazione nell'allestimento di collegamenti on-line (leggi formali, ordinanze d'esecuzione, istruzioni tecniche, direttive di sicurezza, manuali di applicazione, regolamenti d'utilizzazione, standard per la gestione e l'attuazione di progetti d'informatica, misure di controlling ecc.);
- tutti i documenti relativi allo sviluppo dei sistemi informatici esaminati (*documenti di inizializzazione, analisi preliminari, concetti, realizzazioni, messa in funzione, nuovi sviluppi*);

– le basi legali appositamente istituite per questi sistemi e le possibilità di richiamare dati da questi sistemi (*leggi, ordinanze, direttive, regolamenti, matrici d'accesso*).

Gli uffici interessati sono inoltre stati invitati a presentare per iscritto l'elenco di tutti i collegamenti on-line del loro sistema informatico con le autorità autorizzate ad accedervi come pure un'elencazione cronologica dello sviluppo del sistema e dell'allestimento dei relativi collegamenti on-line; sono inoltre stati chiamati a esprimere il loro parere in merito ai problemi sorti al momento dell'allestimento dei diversi collegamenti on-line dei rispettivi sistemi informatici.

Dopo aver proceduto a un'analisi di tali documenti, sono stati sentiti i rappresentanti dei diversi servizi ai quali è stato chiesto un parere scritto complementare.

142 Interlocutori

Gli interlocutori scelti nell'ambito della presente ispezione erano soprattutto gli organi e gli uffici coinvolti nell'allestimento di collegamenti on-line esistenti o in fase di pianificazione per i sistemi informatici scelti dalla Sezione. Si tratta in particolare:

– dell'Ufficio federale di polizia,
– del Ministero pubblico della Confederazione,
– dell'Ufficio federale degli stranieri,
– delle autorità cantonali collegate (o che prevedono di collegarsi) ai sistemi informatici scelti,
– dell'Ufficio federale dell'informatica,
– delle segreterie generali del DFGP e del DFF,
– del Centro di calcolo del DFGP,
– del Consulente per la protezione dei dati del DFGP,
– dell'Incaricato federale della protezione dei dati.

È stata inoltre stabilita una stretta collaborazione con il Controllo amministrativo del Consiglio federale (CCF), che nel rapporto pubblicato il 16 marzo 1998 aveva esaminato lo scambio di dati on-line tra i Cantoni e la Confederazione.[3]

143 Contenuto del rapporto

Il presente rapporto non ha la pretesa di trattare in modo esaustivo i problemi connessi con l'allestimento di collegamenti on-line, giacché si tratta di un campo assai vasto e complesso. Si concentra piuttosto sugli aspetti concettuali e giuridici, nonché sulle questioni relative alla protezione dei dati.

I risultati delle ricerche su cui si basano le raccomandazioni della Commissione dovrebbero consentire un allestimento adeguato dei collegamenti on-line in generale e in particolare nel settore delle polizia.

3 Cfr. Rapporto del controllo amministrativo del Consiglio federale del 16 marzo 1998 «On-line-Datenaustausch zwischen Bund und Kantonen».

15 Scelta dei sistemi informatici

La Sezione ha esaminato svariati sistemi suscettibili di essere oggetto dell'indagine [RIPOL, DOSIS, ISIS, ZAN, AFIS, RCS, AUPER]. Essa ha stabilito vari criteri che andavano presi in considerazione per la scelta, fra cui in particolare: *i pericoli, le interferenze e i potenziali abusi* cui sono sottoposti i collegamenti on-line; il *numero di autorità autorizzate a servirsi* di un sistema informatico mediante la procedura di richiamo; infine, il criterio della distinzione tra le *norme legali esistenti* (de lege lata) e le *basi legali in via d'elaborazione* (de lege ferenda), che permetterà di valutare la tendenza in atto nel processo legislativo. La Sezione ha inoltre rilevato che occorre tener conto dei risultati delle ricerche condotte dalla *Delegazione* della CdG sugli «Eventi in seno al DMF (EBG 95)».

Sulla base di questi criteri, la Sezione ha deciso di concentrare l'attenzione sui seguenti sistemi informatici:

- **RIPOL** (Sistema di ricerca informatizzato di persone e oggetti)
- **DOSIS** (Sistema di trattamento dei dati in materia di lotta contro il traffico illegale di stupefacenti)
- **ISIS**-[Plus] (Sistema per il trattamento provvisorio dei dati relativi alla protezione dello Stato)
- **RCS** (Registro centrale degli stranieri) [=**ZAR** Zentrales Ausländerregister].

La Sezione ha tenuto conto anche del sistema ZAN (Indice centrale delle pratiche), in cui si possono importare dati dal sistema DOSIS, e di ISOK (Sistema di trattamento dei dati in materia di lotta contro la criminalità organizzata), la cui elaborazione è direttamente legata allo sviluppo di DOSIS in fase di attuazione.

16 Delimitazione del campo dell'indagine

Le discussioni in seno alla Sezione e alla Commissione hanno mostrato che l'esame dell'allestimento di collegamenti on-line nel settore della polizia è opportuno e necessario. Inoltre, accanto ai numerosi collegamenti già allestiti negli ultimi anni, questo settore è in costante evoluzione e vengono attuati regolarmente nuovi progetti e sviluppi.

La Commissione ribadisce la necessità di stabilire collegamenti on-line, riconoscendo l'importanza dell'efficienza e della coordinazione nel settore della polizia e della compatibilità dei sistemi.

Essa richiama tuttavia l'attenzione sui pericoli insiti in tali collegamenti e auspica maggiore trasparenza. Ha pertanto messo in evidenza l'assoluta necessità di analizzare le precise condizioni d'allestimento di tali collegamenti, tenendo conto del loro numero in costante aumento e dei rischi di potenziali interferenze o abusi.

La Sezione non ha voluto porre gli aspetti tecnici al centro della sua indagine, anche se tali aspetti non sono stati trascurati, segnatamente nell'ambito dell'analisi dei concetti informatici, delle misure di sicurezza o dei meccanismi di controllo. Per quest'ultimo punto è stato posto l'accento sugli aspetti riguardanti la protezione dei dati.

Ciò ha consentito di proseguire le indagini avviate dalla CdG del Consiglio nazionale nel quadro dell'*introduzione dell'informatica nell'Amministrazione federale* (FF 1988 II 565). In effetti, nonostante le numerose lacune[4] relative alla protezione dei dati rilevati a tal fine, non è mai stato intrapreso un esame approfondito del *controllo dei progetti di trattamento automatizzato*. La CdG del Consiglio nazionale aveva concluso questa ispezione nel maggio 1997 in vista della presente indagine svolta dalla CdG del Consiglio degli Stati.

2 Esame sul piano concettuale

21 Campo d'analisi

La presente ispezione è imperniata sulla seguente questione principale:

Quali sono le regole applicabili in sede di pianificazione e di allestimento di collegamenti on-line nel settore della polizia?

Sempre intorno a questo tema, la Commissione si è inoltre posta i seguenti interrogativi:

- esistono nell'Amministrazione federale, segnatamente in seno al DFGP, *disposizioni* che disciplinano l'allestimento di collegamenti on-line?
- le numerose *istruzioni e direttive dell'UFI* sono applicabili a questa problematica?
- quali *esigenze* occorre soddisfare in materia di *protezione dei dati*?
- quali sono le *basi legali* applicabili in materia di protezione dei dati?
- nell'elaborazione dei concetti informatici si tiene conto dei principi di *proporzionalità*, *finalità*, *opportunità* e *necessità?*
- nell'allestimento di collegamenti on-line nel quadro dell'elaborazione dei concetti informatici è previsto anche l'esame dei costi?
- esistono regolamentazioni relative alla *sorveglianza* e al *controllo* dell'allestimento di collegamenti on-line?
- qual è il ruolo della *procedura HERMES* quale strumento e standard per la gestione e l'attuazione di progetti d'informatica in seno all'Amministrazione federale?
- *chi autorizza*, secondo le norme attualmente vigenti, l'allestimento di collegamenti on-line?
- quali sono i ruoli e le competenze dei *gruppi di progetto* o dei *gruppi tecnici* incaricati dell'allestimento di collegamenti on-line?

[4] Evoluzione dei cosiddetti sistemi interconnessi; imbricazione dei sistemi d'informazione dell'Amministrazione (FF **1988** II 582, 605). Il ruolo e i mezzi dell'Incaricato federale della protezione dei dati in materia di sorveglianza (cfr. lettera della CdG-CN del 23 maggio 1995 al CF).

22 Introduzione

La Commissione ha constatato che le banche di dati e i collegamenti che permettono di accedervi, sono disciplinati come segue:

RIPOL
- Art. 351bis Codice penale svizzero
- Ordinanza RIPOL del 19 giugno 1995
- Modifica dell'ordinanza RIPOL dell'11 settembre 1996

DOSIS
- Legge federale del 7 ottobre 1994 sugli Uffici centrali della polizia giudiziaria della Confederazione
- Ordinanza DOSIS del 26 giugno 1996

ISOK
- Legge federale del 7 ottobre 1994 sugli Uffici centrali della polizia giudiziaria della Confederazione
- Ordinanza ISOK del 19 novembre 1997

ISIS
- Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (entrata in vigore il 1° luglio 1998)
- Ordinanza ISIS del 31 agosto 1992
- Modifica dell'ordinanza ISIS del 2 dicembre 1996
- Direttive ISIS del 31 agosto 1992

ZAN
- Ordinanza del 1° dicembre 1986 concernente il Servizio d'identificazione dell'Ufficio federale di polizia
- Modifica dell'ordinanza del 2 dicembre 1996

RCS
- Ordinanza RCS del 23 novembre 1994
- Modifica dell'ordinanza RCS del 4 dicembre 1995
- Legge federale concernente la dimora e il domicilio degli stranieri (LDDS)

Benché il principio di legalità miri principalmente alla trasparenza, da solo non basta per legittimare l'allestimento di collegamenti on-line. L'allestimento di un collegamento on-line deve infatti essere preceduto da una serie di passi preliminari (inizializzazione, pianificazione, esame della necessità, dei costi e della conformità con i principi di proporzionalità, finalità e opportunità, esame delle misure di sicurezza, valutazione globale dei rischi ecc.). Una procedura di richiamo dei dati non può quindi essere pianificata o giustificata unicamente dall'esistenza di una base legale, ma deve seguire determinate procedure preliminari e rispettare alcune regole o principi in sede di pianificazione.

L'esame della questione principale e del campo d'analisi ad essa connesso ha l'obiettivo di determinare quali sono le tappe che precedono qualsiasi allestimento di un collegamento on-line e di appurare se in questo ambito vi sono lacune. In altri termini, occorre chiarire quali sono le norme da applicare in sede di pianificazione di collegamenti on-line prima che vengano allestiti e istituite le basi legali su cui poggiano.

23 Esame delle questioni complementari

231 Le direttive dell'UFI

Le numerose direttive dell'UFI disciplinano questa problematica?

231.1 Elenco delle direttive dell'UFI[5]

Le principali basi legali che disciplinano le questioni inerenti l'informatica a livello federale sono:

- l'ordinanza dell'11 dicembre 1989 concernente l'allestimento di un Ufficio federale dell'informatica e disciplinante il coordinamento dell'informatica presso l'Amministrazione federale (RS *172.010.58*).
- l'ordinanza del 10 giugno 1991 concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale (RS *172.010.59*).
- il piano direttore informatico della Confederazione dell'8 luglio 1994 (FF 1994 III 1435).

Sulla base di tali norme, l'Ufficio federale dell'informatica ha pubblicato diverse *istruzioni tecniche* (IT), *direttive concernenti la sicurezza informatica* (DS) e *strategie* (questa documentazione è disponibile solo in francese e tedesco):

A Elenco delle istruzioni tecniche

(Articolo 3 dell'ordinanza del CF concernente l'istituzione di un UFI e disciplinante il coordinamento dell'informatica presso l'Amministrazione federale; RS 172.010.58):

IT 01 Aggiudicazione dei mandati di servizi informatici a imprese esterne, del 15 gennaio 1997
- Allegato 1 Criteri di classificazione, edizione 1994
- Allegato 2 Tariffa oraria per prestazioni informatiche, edizione 1998
- Allegato 3 Modello di contratto per l'acquisto di sistemi informatici completi e l'elaborazione di programmi specifici (contratto d'appalto), edizione del 15 gennaio 1997
- Allegato 4 Modello di contratto per le prestazioni informatiche (mandato), edizione del 15 gennaio 1997
- Allegato 5 Condizioni generali per l'acquisto di sistemi informatici com pleti e l'elaborazione di programmi specifici (foglio giallo), edi zione luglio 1997
- Allegato 6 Condizioni generali per le prestazioni informatiche (foglio verde), edizione luglio 1994
- Allegato 7 Manuale d'uso, in preparazione

IT 02 Modalità di finanziamento e d'acquisto nel settore dell'informatica, del 15 gennaio 1997
- Allegato 1 Lista di controllo per un acquisto conformemente alla LAPub e all'OAPub, gennaio 1997

5 Cfr. pubblicazione dell'UFI «UFI News 1997», pag. 39-47 e lettera dell'UFI del 9 gen. 1998, punto 4, «On-line Verbindungen allgemein», pag. 5-6.

IT 03 Annuncio di progetti d'informatica all'UFI, del 22 agosto 1990

IT 04 Concezione dell'informatizzazione dei servizi di registrazione, dell'11 dicembre 1990
Allegato 1 Catalogo dei criteri di valutazione dei sistemi di registrazione

IT 05 Rapporti annuali dei servizi sull'effettivo del personale, le spese e i costi nel settore dell'informatica, del 16 settembre 1992

IT 06 MANUALE PC, soppresso il 18 ottobre 1995

IT 07 Indirizzamento della posta elettronica in seno all'Amministrazione federale, del 17 gennaio 1996
Allegato 1 Transizione dalla IT 07 del 1991 alla IT 07 del 1996, del 17 gennaio 1996

IT 08 Manuale per responsabili di progetto LAN, del 16 ottobre 1996
Allegati 1-15 (disponibili solo in tedesco)

IT 09 Convenzioni di nomi SNA / SNI - 92, del 16 settembre 1992

IT 10 Riutilizzazione di materiale informatico in disuso, del 15 giugno 1994

IT 11 Domain Name System (DNS), del 13 novembre 1996

IT 12 Coordinamento e standardizzazione di sistemi di gestione degli affari amministrativi (GEVER), del 18 gennaio 1995
Allegato 1 Modello di dati GEVER (disponibile solo in tedesco)
Allegato 2 Profilo d'uso (disponibile solo in tedesco)

IT 13 Introduzione e uso del programma SAP R/3, del 17 settembre 1997
Allegato 1 Architettura SAP R/3
Allegato 2 Coordinamento SAP

IT 14 Interfaccia per la consegna di dati all'Archivio federale, del 21 agosto 1996

IT 15 Sistemi di registrazione del tempo di presenza basata sull'informatica nell'Amministrazione federale, del 17 maggio 1995
Allegato 1 Foglio di registrazione del tempo basata sull'informatica ad uso dell'Amministrazione federale, del 17 maggio 1995

IT 16 Gestione di progetti e sviluppo di sistemi nel quadro di progetti d'informatica, del 19 aprile 1995
Allegato 1 Documentazione supplementare
Allegato 2 Compiti e prestazioni dell'Ufficio federale dell'informatica
Allegato 3 Organi di coordinamento e di controllo
Allegato 4 Standard

Ristampa a parte: Direttive per la gestione di progetti e lo sviluppo di sistemi nel quadro di progetti d'informatica, del 19 aprile 1995

IT 17 Indirizzamento NSAP (Network Service Access Point), del 18 ottobre 1995
Allegato 1 Modulo di richiesta per lo spazio degli indirizzi NSAP Administrativ-Domain
Allegato 2 Modulo di richiesta per lo spazio degli indirizzi NSAP Routing-Domain
Allegato 3 Modulo di richiesta per lo spazio degli indirizzi NSAP Routing-Area

IT 18 World Wide Web (WWW) nell'Amministrazione federale, del 15 gennaio 1997

Allegato 1 Modulo di richiesta per un http-Proxy proprio
Allegato 2 Modulo di richiesta per l'accesso WWW via Internet a partire da un server Proxy
Allegato 3 Modulo di richiesta per il server WWW Public su Internet.

IT 19 Controlling e calcolo dell'economicità nel settore dell'informatica in seno all'Amministrazione federale, del 14 gennaio 1998.

B Elenco delle direttive relative alla sicurezza nell'ambito dell'informatica (DS)

(Articolo 8 dell'ordinanza del 10 giugno 1991 concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale; RS 172.010.59)

DS S01 Gestione dell'identificazione degli utenti e delle parole d'ordine, del 18 agosto 1993
Scheda tecnica sull'uso delle parole d'ordine nell'Amministrazione federale, del dicembre 1993

DS S02 Protezione di base di sistemi e applicazioni informatici, del 19 aprile 1995

Allegato 1 Istruzione relativa al rilevamento e alla classificazione degli oggetti da proteggere
Allegato 2 Catalogo delle misure di protezione fondamentali
Allegato 3 Moduli di rilevamento (moduli colorati ottenibili presso l'UFI)

MANUALE n. 1 relativo alla DS S02: Procedura per l'elaborazione delle liste di controllo e catalogo completo delle misure di protezione fondamentali, del 1° ottobre 1996

DS S03 Applicazione della Network Security Policy (NSP), del 25 giugno 1997

C Elenco delle strategie

Secondo il numero 3 del Piano direttore informatico della Confederazione (PDIC), le strategie d'applicazione valide a livello federale vengono elaborate dall'UFI d'intesa con la Conferenza informatica della Confederazione (CIC) ed emanate conformemente all'ordinanza concernente l'istituzione di un Ufficio federale dell'informatica e disciplinante il coordinamento dell'informatica presso l'Amministrazione federale.

Strategia GEVER Strategia in materia di coordinazione e di standardizzazione di sistemi di gestione degli affari correnti nell'Amministrazione federale generale, del 18 gennaio 1995
Allegato 1: Glossario
Allegato 2: Bibliografia
Allegato 3: Illustrazioni

Strategia di telecomunicazione Strategia in materia di telecomunicazioni dell'Amministrazione federale generale, del 12 giugno 1996
Allegato: Spiegazione delle abbreviazioni

Network Security Policy (NSP), del 25 giugno 1997

231.2 Queste istruzioni prevedono disposizioni specifiche per l'allestimento di collegamenti on-line?

Per l'allestimento di collegamenti on-line, l'Ufficio federale dell'informatica ha il compito di pianificare e gestire le *infrastrutture di comunicazione* nell'ambito di tutta l'Amministrazione federale. Sul piano fisico, i collegamenti on-line nel settore della polizia avvengono, laddove esiste, mediante l'infrastruttura per la comunicazione dei dati della Confederazione, mentre sul piano logico le reti sono separate per motivi di sicurezza.

Come detto, l'Ufficio federale dell'informatica ha elaborato e pubblicato numerose istruzioni. Le applicazioni quali RIPOL, DOSIS, ISOK, ZAN, RCS e ISIS sono unità organizzative che sottostanno alle direttive di sicurezza dell'UFI. A tali sistemi si applicano quindi i principi e le disposizioni di sicurezza dell'Amministrazione federale, in particolare:

- la legge federale sulla protezione dei dati e la relativa ordinanza (RS *235.1* e RS *235.11*),
- l'ordinanza concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale (RS *172.010.59*),
- la direttiva di sicurezza DS S01: Gestione dell'identificazione degli utenti e delle parole d'ordine,
- la direttiva di sicurezza DS S02: Protezione di base di sistemi e applicazioni informatici,
- la direttiva di sicurezza DS S03: Applicazione della Network Security Policy (NSP).

Concretamente, ciò significa che:

- in virtù della direttiva di sicurezza DS S02 sulla protezione di base di sistemi e applicazioni informatici, queste applicazioni devono essere rilevate e classificate quali oggetti da proteggere e in ogni caso vanno sottoposte a una valutazione dei rischi;
- per queste applicazioni occorre adottare misure di sicurezza conformemente alle direttive DS S01 e DS S02;
- conformemente alla direttiva di sicurezza DS S02 vanno adottate misure di carattere organizzativo (responsabili delle applicazioni, incaricati dei servizi di sicurezza, organi di controllo ecc.):
- dal 1997, i nuovi accessi a queste applicazioni devono soddisfare le esigenze della *Network Security Policy (NSP)* e della *direttiva di sicurezza DS S03* : Applicazione della *Network Security Policy*.

L'importanza di queste misure di sicurezza è stata altresì rilevata nel rapporto del Dipartimento federale delle finanze «*Rapporto DFF (UFI) al Consiglio federale rispettivamente del 14 aprile 1997 e del 13 giugno 1997 conc. a) lo stato dell'applicazione dell'ordinanza concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale b) la sicurezza nel campo della burotica e delle possibilità di verifiche casuali di funzionalità degli accessi a banche dati*

sensibili»[6] (p. es. valutazione dei rischi, nomina di responsabili della sicurezza nell'ambito dell'informatica, codifica dei dati, autenticazione, registrazione quotidiana degli accessi ecc.).

Nonostante le numerose direttive e disposizioni summenzionate, applicabili ai sistemi informatici scelti dalla Sezione «Autorità», si constata che tali direttive non contengono disposizioni specifiche circa l'allestimento di collegamenti on-line, segnatamente per quanto riguarda l'esame dei principi di opportunità, finalità e proporzionalità. In effetti, dalla documentazione e dalle prese di posizione dell'UFI, nonché dalle spiegazioni del consulente per la protezione dei dati del DFGP, risulta che le suddette direttive disciplinano piuttosto le questioni relative alle misure di sicurezza, alla procedura di autenticazione e di accesso, alle operazioni crittografiche, alle misure di carattere organizzativo, alla valutazione dei rischi, a diversi livelli di protezione (da 1 a 3) e alla protezione dei sistemi e delle applicazioni ad essi connesse (Network Security Policy / NSP).

L'allegato 2 della direttiva DS S02 concernente la sicurezza informatica, che contiene un «Catalogo delle misure di protezione fondamentali», prevede nel capitolo 8 «Confidenzialità e integrità» tutta una serie di disposizioni dettagliate in merito agli accessi ai sistemi informatici, anche se queste vigono principalmente per gli *accessi individuali*. Oltre alla descrizione delle misure relative all'identificazione degli utenti o alle parole d'ordine, l'allegato 2 formula determinati criteri, quali ad esempio l'interruzione di collegamenti inattivi, il blocco di diritti di accesso non rivendicati, il controllo di soggetti, oggetti, frequenza e durata dei diritti di accesso, l'attribuzione degli accessi caso per caso a dipendenza dei compiti individuali e delle funzioni delle persone interessate, l'attribuzione o la modifica dei privilegi.

Per contro, *la procedura* d'allestimento dei sistemi informatici e dei collegamenti on-line che permettono di accedervi non è disciplinata da queste direttive, bensì da una particolare procedura di gestione dei progetti: la procedura HERMES.

232 Procedura e competenze

Esistono nell'Amministrazione federale, in particolare in seno al DFGP, disposizioni che disciplinano l'allestimento di collegamenti on-line ?

Qual è il ruolo della procedura HERMES quale strumento e standard per la gestione e l'attuazione di progetti d'informatica in seno all'Amministrazione federale?

Chi, secondo le norme in vigore, autorizza gli accessi on-line?

Che ruolo e quali competenze hanno i gruppi di progetto o i gruppi tecnici incaricati di allestire i collegamenti on-line?

Il consulente per la protezione dei dati del DFGP, che la Sezione «Autorità» ha interrogato in merito a questa problematica, ha fornito numerose precisazioni sia sulle disposizioni legali applicate dal DFGP per l'allestimento di collegamenti on-line sia

6 Cfr. Bericht EFD (BFI) an den Bundesrat vom 14. April 97, resp. vom 13. Juni 97 und Bundesratbeschluss vom 16. Juni 97 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken.

sull'impiego della procedura HERMES quale strumento e standard per la gestione e l'attuazione dei progetti d'informatica in seno al DFGP.

232.1 Le disposizioni legali

In questo contesto, il DFGP applica le seguenti disposizioni legali:

– l'ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (RS *235.11*);

  L'articolo 20 capoverso 2 di questa ordinanza sancisce che gli organi federali responsabili annunciano dall'inizio all'Incaricato federale della protezione dei dati ogni progetto di trattamento automatizzato di dati personali. Di regola, l'annuncio all'Incaricato federale si svolge per il tramite dell'Ufficio federale dell'informatica.

– l'ordinanza del 10 giugno 1991 concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale (RS *172.010.59*)

  L'articolo 7 di questa ordinanza prevede che le unità organizzative responsabili dei sistemi informatici annuncino all'UFI la pianificazione dei sistemi conformemente alle istruzioni tecniche della Conferenza informatica della Confederazione (CIC). In virtù di tale ordinanza, l'annuncio è fatto all'UFI e allo stesso tempo ne viene trasmessa una copia all'Incaricato federale della protezione dei dati.

– l'istruzione tecnica IT 03 del 22 agosto 1990: Annuncio dei progetti d'informatica all'UFI

  L'articolo 1 di questa istruzione stabilisce che ogni nuovo progetto informatico dev'essere annunciato sotto forma di proposta conformemente alla procedura HERMES.

232.2 La procedura HERMES in generale

La procedura HERMES è un metodo di gestione e di attuazione dei progetti d'informatica in forma di strumento d'organizzazione, di pianificazione, d'esecuzione, di comando e di controllo dei progetti d'informatica[7].

Questo strumento di gestione dei progetti è utilizzato nell'Amministrazione federale dal 1975. Nel 1986, la procedura HERMES è stata oggetto di un'importante revisione e ne è stata resa obbligatoria l'applicazione per tutti i progetti d'informatica.

232.3 La procedura HERMES in seno al DFGP

Secondo il consulente per la protezione dei dati del DFGP, la procedura HERMES è utilizzata in seno al Dipartimento di giustizia e polizia quale strumento e standard per la gestione e l'attuazione dei progetti d'informatica del DFGP. Questo metodo si

[7] Cfr. manuale HERMES, gestione e attuazione di progetti d'informatica, UFI, edizione 1995.

articola in diverse fasi successive ognuna delle quali non può essere autorizzata prima che sia stata approvata la fase precedente. Le principali fasi sono:

a) l'avvio del progetto (proposta): documento di una decina di pagine che spiega le intenzioni del progetto, i mezzi necessari per attuarlo ecc.;

b) l'analisi preliminare: elaborazione e verifica degli aspetti principali del progetto; esame e approntamento di eventuali basi legali;

c) la concezione: specificazione della proposta di soluzione scelta;

d) l'attuazione: programmazione e test;

e) l'introduzione: formazione degli utenti, esercizio del sistema.

Il metodo HERMES cita inoltre i punti che devono essere esaminati in ogni fase. Prima di prendere una decisione, vanno quindi chiarite diverse questioni che stabiliscono le grandi linee dell'organizzazione di un progetto.

I ruoli e le competenze dei gruppi di progetto o di altri organi tecnici sono precisati nel manuale HERMES[8]:

– istanza di approvazione;

– mandante del progetto;

– comitato di progetto;

– direzione del progetto;

– ecc.

Secondo il consulente per la protezione dei dati del DFGP, diverse istanze accompagnano i progetti d'informatica a livello del DFGP, come previsto dalla procedura HERMES.

a) L'istanza di approvazione

Autorizza il passaggio alla fase successiva.

Nel DFGP, per i progetti di grande entità la decisione in merito al passaggio alla fase successiva spetta al segretario generale o al suo sostituto.

b) Il comitato di progetto

È composto, a seconda del progetto, da un numero variabile di membri, fra cui il responsabile del progetto, il capo dell'informatica del Dipartimento, un consulente per la protezione dei dati (quello dell'Ufficio o quello del Dipartimento; per alcuni progetti vi partecipano entrambi) e i rappresentanti degli utenti (Uffici e Cantoni). Talvolta vi partecipa anche l'Incaricato federale della protezione dei dati, ma solo in via eccezionale. Questo comitato si riunisce da due a quattro volte l'anno e assiste ogni progetto informatico durante tutta la sua durata. Fanno parte del comitato di progetto un rappresentante degli utenti e, per i progetti di grande entità, un rappresentante cantonale.

Va inoltre rilevato che i progetti d'informatica non sono mai conclusi. Infatti, nella maggior parte dei progetti non appena una versione funziona si inizia subito ad elaborare la versione successiva (RIPOL-4, RCS-3, AUPER-2 ecc.). È questa la ragione per cui un comitato accompagna un progetto per tutta la sua durata. Qualsiasi

8 Cfr. manuale HERMES, UFI, edizione 1995, pagg. 6-3 a 6-13.

modifica di un sistema informatico dev'essere approvata dal comitato di progetto, e in caso di modifica importante è necessario ripercorrere il processo delle cinque fasi (inizializzazione, analisi preliminare, concezione, attuazione, introduzione).

c) La direzione del progetto

Si tratta dei compiti della direzione operativa del progetto, ossia della pianificazione, della coordinazione, del controllo e del comando delle attività legate al progetto entro i limiti dei costi e delle scadenze previsti. Il capo del progetto assume la responsabilità della direzione operativa del progetto.

Per l'approvazione delle fasi del progetto viene utilizzato un modulo che nel DFGP dev'essere firmato segnatamente dalla direzione dell'Ufficio interessato, dal capo del Centro di calcolo, dal consulente per la protezione dei dati del Dipartimento e dal capo dell'informatica del Dipartimento. Il consulente per la protezione dei dati del DFGP riceve un modulo da firmare per ogni fase. Egli può porre alcune riserve, che verranno in seguito considerate nella fase successiva.

L'acquisto di materiale informatico non è possibile se non è stato approvato in una delle fasi del progetto. Al di fuori di un progetto funzionante secondo il metodo HERMES, non si può acquistare ne programmi né materiali.

232.4 Da dove viene l'impulso iniziale per allestire collegamenti on-line o sviluppare un sistema d'informazione nel settore della polizia?

La Commissione ha constatato che l'impulso iniziale proviene soprattutto dalla Commissione tecnica svizzera della polizia o da altri organi tecnici di polizia, segnatamente in seno all'lNTERPOL. *L'Ufficio federale di polizia* e il *Centro di calcolo del DFGP* sono rappresentati in questi gruppi di lavoro e i collaboratori traggono da queste riunioni nuove idee per migliorare l'efficienza degli strumenti informatici. Queste proposte sono esaminate dalla direzione del progetto e sottoposte al comitato.

232.5 Applicazione della procedura HERMES da parte del DFGP per i collegamenti on-line

Se il comitato di progetto approva la proposta di allestire un collegamento on-line, si procede all'esame delle basi legali e, se del caso, a una modifica della legge. Nel contempo nasce un nuovo progetto conforme a HERMES per l'eventuale realizzazione di questo collegamento on-line (occorre tuttavia rispettare le cinque fasi della procedura HERMES).

Le indagini intraprese presso il consulente per la protezione dei dati del DFGP hanno rivelato che l'allestimento di un collegamento on-line impone un nuovo ciclo di fasi secondo HERMES, qualora l'allestimento del collegamento implichi una modifica dell'applicazione (nuove funzionalità). La decisione di principio di realizzare e di istituire collegamenti on-line costituisce infatti una modifica essenziale del progetto, ragione per cui occorre ripercorrere le diverse fasi del progetto. A prescindere da queste fasi, la decisione di istituire collegamenti on-line spetta quindi al Comitato di progetto, con l'approvazione del segretario generale del Dipartimento.

Lo stesso vale quando il Comitato di progetto decide in merito al collegamento di un determinato Cantone. In questo caso tuttavia accade spesso che il Cantone disponga già delle basi legali necessarie al collegamento e che sia già stato realizzato un progetto pilota con la partecipazione di quattro o cinque Cantoni. Il collegamento di un nuovo Cantone non richiede né una nuova base legale né nuovi programmi, poiché è già stato fatto tutto il necessario per il collegamento del primo Cantone. Per contro, per quanto riguarda l'esercizio, il DFGP, prima del collegamento di nuovi Cantoni, deve accertarsi che esistano le linee e le periferiche necessarie.

232.6 I limiti della procedura HERMES

Come abbiamo esposto in precedenza, *la procedura* per l'allestimento di sistemi informatici e i relativi collegamenti on-line non è disciplinata da direttive, bensì mediante un particolare sistema di gestione dei progetti, la procedura HERMES. Se tale procedura è applicata correttamente dal DFGP, occorre tuttavia rilevare che HERMES rimane soprattutto un «metodo» di gestione di progetti d'informatica che prevede diverse fasi obbligatorie.

In altri termini, HERMES prevede sì le fasi che si impongono per decidere in merito all'allestimento di nuovi collegamenti on-line, ma non contiene alcuna disposizione specifica in materia, soprattutto per quanto attiene all'esame dei principi di opportunità, proporzionalità e finalità. Vi è solo qualche accenno o interrogativo, per esempio nella fase dell'analisi preliminare (la sicurezza e la protezione dei dati sono state analizzate e valutate tenendo conto della situazione?)[9], della concezione (le esigenze in materia di sicurezza e di protezione dei dati sono soddisfatte?)[10] o in relazione ai tipi di sistemi che HERMES distingue: «...infrastrutture informatiche, per esempio l'acquisto e l'allestimento di reti di comunicazione)»[11].

La procedura HERMES applicata dal DFGP costituisce dunque uno strumento fondamentale per allestire i collegamenti on-line nel settore della polizia. Ancora una volta, HERMES è un semplice «metodo» per la gestione e l'attuazione di progetti d'informatica, e non prevede norme specifiche in merito ai collegamenti on-line.

Secondo quanto spiegato dal consulente per la protezione dei dati del DFGP e dall'Incaricato federale della protezione dei dati, risulta che la mancanza di disposizioni specifiche relative ai collegamenti on-line nella procedura HERMES può comportare problemi a livello di analisi delle necessità degli utenti, dell'efficienza del controllo e della sorveglianza degli sviluppi informatici da parte dei servizi competenti.

233 Questioni relative alla protezione dei dati e controllo dell'allestimento di collegamenti on-line

Quali sono le basi legali vigenti in materia di protezione dei dati?

Quali esigenze devono essere soddisfatte in materia di protezione dei dati?

I principi di proporzionalità, di finalità, d'opportunità e di necessità sono considerati nell'elaborazione di concetti informatici?

9 Cfr. manuale HERMES, UFI, edizione 1995, pag. 2-7.
10 Cfr. manuale HERMES, UFI, edizione 1995, pag. 3-9.
11 Cfr. manuale HERMES, UFI, edizione 1995, pag. 11-14.

Esistono regolamentazioni relative alla sorveglianza e al controllo per l'allestimento di collegamenti on-line?

233.1 Basi legali ed esigenze in materia di protezione dei dati concernenti l'allestimento di collegamenti on-line

Le basi legali applicabili in materia di protezione dei dati sono la legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS *235.1*) e l'ordinanza del Consiglio federale del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD; RS *235.11*).

Queste basi legali disciplinano non solo gli aspetti legati all'osservanza, per esempio dei principi di proporzionalità e di finalità (art. 4 LPD), ma anche le misure di sicurezza (art. 7 LPD) e le misure tecniche e organizzative (art. 20 segg. OLPD) da adottare in sede di trattamento dei dati personali.

Va rilevato che le esigenze poste alla protezione dei dati per l'allestimento di collegamenti on-line sono state descritte in modo dettagliato ed esaustivo in un capitolo speciale di un rapporto del Dipartimento federale delle finanze[12], di cui presentiamo gli elementi principali:

A Principi relativi alla protezione dei dati

Legalità

Gli organi federali hanno il diritto di trattare dati personali solo se esiste una base legale che lo consenta (art. 4 cpv. 1, art. 17 cpv. 1 LPD).

Gli organi federali hanno il diritto di comunicare dati personali se ne esistono i fondamenti giuridici che lo consentano (art. 17 e 19 LPD). Essi possono permettere l'accesso a dati personali mediante una procedura di richiamo, qualora ciò sia previsto esplicitamente. Dati personali degni di particolare protezione come pure profili della personalità possono essere accessibili mediante una procedura di richiamo soltanto qualora lo preveda esplicitamente una legge in senso formale (art. 19 cpv. 3 LPD).

Proporzionalità

Il trattamento dei dati personali deve essere conforme al principio di proporzionalità (art. 4 cpv. 2 LPD).

Finalità

I dati personali possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge (art. 4 cpv. 3 LPD).

Un'autorità che desidera consultare certi dati persegue sovente diversi scopi, motivo per cui esiste un interesse fattuale a utilizzare i dati richiesti anche per altri scopi.

12 Cfr. Bericht EFD (BFI) an den Bundesrat vom 14 April 97, resp. vom 13 Juni 1997 und Bundesratbeschluss vom 16 Juni 97 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken (cap. 4 Büroautomation und Datenbankzugriffe / 4.2 Anforderungen des EDSB, pag. 22-26).

Un'autorità può tuttavia consultare certi dati soltanto per adempiere i propri compiti o per scopi definiti nelle basi legali. I dati personali di terzi non interessati non devono, di regola, essere consultabili, e in nessun caso devono essere trattati ulteriormente (cfr. p. es. art. 7 cpv. 3 ordinanza RCS, RS *142.215*; RU *1994* 2859).

Esattezza

Chi tratta dati personali deve accertarsi della loro esattezza (art. 5 cpv. 1 LPD). Qualsiasi modifica di dati dev'essere soggetta a meccanismi di controllo (segnatamente le misure d'organizzazione) che ne garantiscono l'esattezza (in relazione allo scopo prefissato).

Sicurezza dei dati

I dati personali devono essere protetti contro ogni trattamento non autorizzato, mediante provvedimenti tecnici ed organizzativi adeguati (art. 7 cpv. 1 LPD).

B Applicazione / misure

Identificazione

Dev'essere garantita la possibilità di identificare l'autore e le operazioni di trattamento dei dati, segnatamente la raccolta, la modifica, la comunicazione e la distruzione (cfr. criteri relativi all'aggiornamento, art. 10 OLPD).

Autorizzazione per modificare i dati

Mediante controlli di memoria occorre garantire che nessuna persona non autorizzata possa introdurre dati personali nella memoria, consultare dati memorizzati, modificarli o cancellarli.

Accesso solo alle persone autorizzate

I controlli d'accesso sono volti a garantire che le persone interessate abbiano accesso soltanto ai dati di cui hanno bisogno per adempiere i loro compiti.

Controllo del collegamento dei dati

Occorre verificare se mediante la burotica sia possibile procurarsi da diverse fonti dati concernenti uno stesso oggetto, in modo da stabilire per esempio profili della personalità (mancanza di base legale, trattamento dei dati non proporzionale, sicurezza insufficiente e insufficiente controllo dell'esattezza). Se l'adempimento dei compiti non esige una messa in relazione dei dati (base legale), occorre rendere tecnicamente impossibile un collegamento di dati automatizzato.

C Stato della sicurezza

Occorre operare una distinzione tra la correttezza dei dati (legalità, proporzionalità, finalità ed esattezza) e la sicurezza dei dati (protezione di carattere confidenziale, integrità, disponibilità e autenticità).

Esempio di misure tecniche ai fini della protezione dei dati: aggiornamento (controllo finalità); esempi di misure tecniche ai fini della sicurezza dei dati: codifica della rete, codifica della memoria.

233.2 Esame dei principi di proporzionalità, finalità e opportunità (necessità) a livello di elaborazione dei concetti informatici

Il consulente per la protezione dei dati del DFGP ha precisato che in seno al DFGP è stata effettuata un'analisi dei bisogni degli utenti nel quadro della procedura HERMES, poiché la necessità di un collegamento on-line risulta da esigenze che sono state espresse.

Tuttavia, come già accennato, né le direttive dell'UFI né la procedura HERMES contengono, a parte qualche accenno generico, norme specifiche riguardanti l'allestimento di collegamenti on-line, segnatamente per quanto riguarda l'esame dei principi di opportunità, proporzionalità o finalità.

Quando nell'ambito di un progetto informatico del DFGP vengono esaminati questi principi nell'ambito delle fasi della procedura HERMES, può accadere che gli aspetti legati allo sviluppo di nuovi collegamenti on-line non siano ancora chiaramente definiti, e talvolta è addirittura impossibile sapere quali possibilità di consultazione sono previste, perché il progetto non è ancora sufficientemente avanzato. Ciò rende più difficile sia la valutazione della necessità, della proporzionalità e della finalità di un futuro collegamento on-line, sia l'esercizio dei compiti di controllo spettanti in particolare all'Incaricato federale della protezione dei dati.

233.3 Sorveglianza e controllo dell'allestimento di collegamenti on-line

In virtù dell'articolo 20 OLPD, gli organi federali annunciano dall'inizio all'Incaricato federale della protezione dei dati ogni progetto di trattamento automatizzato di dati personali, affinché le esigenze poste alla protezione dei dati siano immediatamente prese in considerazione. L'annuncio all'Incaricato federale avviene per il tramite dell'Ufficio federale dell'informatica quando un progetto dev'essere annunciato anche a quest'ultimo. L'Incaricato federale e l'UFI collaborano nel quadro delle loro attività relative alle misure tecniche.

Per l'allestimento di collegamenti on-line, l'Ufficio federale dell'informatica ha il compito di pianificare e gestire le *infrastrutture di comunicazione* nell'ambito di tutta l'Amministrazione federale. Sul piano fisico, i collegamenti on-line nel settore della polizia avvengono, laddove esiste, attraverso l'infrastruttura per la comunicazione dei dati della Confederazione, mentre sul piano logico le reti sono separate per motivi di sicurezza. Nel quadro delle sue competenze, l'Ufficio prende posizione sui progetti d'informatica sviluppati ed elaborati, ed emana numerose direttive.

In virtù dell'articolo 27 LPD, spetta all'Incaricato federale della protezione dei dati sorvegliare l'osservanza da parte degli organi federali della legge federale sulla protezione dei dati. Nel quadro dell'allestimento di nuovi collegamenti on-line, egli deve quindi far rispettare i principi di proporzionalità, finalità e necessità. Le indagini hanno tuttavia appurato che l'esercizio di tale controllo pone due difficoltà principali:

a) innanzitutto, l'Incaricato rileva che per adempiere adeguatamente i suoi compiti legali di controllo gli mancano i mezzi necessari, segnatamente il personale. Questo problema è già stato sollevato in occasione delle indagini avviate dalla CdG del Consiglio nazionale nel quadro dell'ispezione sull'in-

troduzione dell'informatica nell'Amministrazione federale (esame del ruolo e dei mezzi dell'Incaricato federale della protezione dei dati in materia di sorveglianza; assenza di misure concrete e, data la mancanza di mezzi, impossibilità per l'Incaricato federale di procedere a una sorveglianza sistematica e dettagliata di tutti i progetti di trattamento automatizzato di dati personali in seno all'Amministrazione federale).

b) d'altra parte, all'Incaricato federale si pone, nel quadro dei suoi compiti di controllo, un altro problema: benché venga consultato durante le diverse fasi di un progetto secondo HERMES e sebbene sia grosso modo al corrente delle necessità degli utenti, ha difficoltà a esprimersi sugli aspetti che concernono lo sviluppo di nuovi collegamenti on-line, poiché nella maggioranza dei casi tali collegamenti non sono ancora chiaramente definiti nei concetti che gli sono sottoposti nel corso delle diverse fasi della procedura HERMES. Le precisazioni vengono generalmente fornite quando occorre istituire le basi legali per l'accesso in questione.

A questo punto sorge un altro problema, quello della legislazione «a titolo preventivo»: il consulente per la protezione dei dati del DFGP ammette che, considerata la lentezza del processo legislativo, si ha la tendenza a proporre emendamenti di leggi per collegamenti on-line che non sono ancora stati definiti in modo preciso e la cui necessità, proporzionalità, ecc. non sono state dimostrate. Occorrerà quindi accertarsi che per eventuali futuri collegamenti on-line esistano le basi legali.

L'Incaricato federale della protezione dei dati si trova quindi di fronte a diverse difficoltà nel quadro dei compiti di controllo da lui assunti nell'ambito dell'allestimento di collegamenti on-line:

- la mancanza di mezzi, segnatamente di personale, gli impedisce di effettuare gli adeguati controlli previsti dal suo mandato legale;
- lo stato di avanzamento di un progetto nel quadro di HERMES non è sempre sufficiente per valutare la necessità o la proporzionalità di un accesso;
- si può pertanto procedere a un esame durante l'elaborazione delle basi legali. Alcuni uffici non sanno tuttavia di che cosa hanno realmente bisogno e hanno la tendenza a prevedere «a titolo preventivo» l'allestimento di collegamenti di cui non è stata verificata la necessità;
- altri uffici, invece, non vedono l'utilità di istituire taluni collegamenti e quindi non li prevedono nei loro progetti legislativi. Se una volta adottata la legge si rende necessario allestire un collegamento, gli uffici si rivolgono all'Incaricato federale per ottenere l'autorizzazione di tali collegamenti privi di basi legali.

233.4 Il controllo degli accessi ai Cantoni

La concessione ai Cantoni di collegamenti on-line a sistemi informatici della polizia solleva un certo numero di problemi, segnatamente per quanto concerne il potere decisionale per l'attribuzione di tali collegamenti e il controllo del rispetto delle esigenze in materia di protezione dei dati o delle misure di sicurezza.

Le procedure decisionali di domanda di collegamento variano da Cantone a Cantone. Il processo decisionale spazia da una procedura estremamente minuziosa per

l'allestimento di collegamenti on-line, così com'è praticata per esempio nel Cantone di Lucerna, a procedure meno trasparenti vigenti in altri Cantoni, in cui le autorità federali devono badare a che la gerarchia e le competenze decisionali cantonali siano state rispettate.

Si aggiunge inoltre il fatto che le leggi cantonali sulla protezione dei dati non possono essere controllate a livello federale. La LPD non conferisce ai servizi dell'Amministrazione federale la competenza d'intraprendere controlli nei Cantoni. L'Incaricato federale ha, nei confronti dei Cantoni, unicamente una funzione di consulente. Dato che i Cantoni hanno l'obbligo di avere un organo di controllo proprio, l'Incaricato federale non può intraprendervi alcun controllo, il che può comportare problemi, soprattutto nell'ambito dell'allestimento di collegamenti on-line. Egli può sì intervenire al momento in cui l'attribuzione di un collegamento è definito, ma in seguito non ha più alcun mezzo di controllare se tali collegamenti sono rispettati e se non sono stati estesi ad altri servizi. Tale controllo è di competenza delle autorità cantonali e il livello può variare in notevole misura da Cantone a Cantone.

Inoltre, l'esame della necessità o della proporzionalità dei collegamenti on-line concessi ai Cantoni è relativo. Il DFGP prende in considerazione un bisogno generale espresso dalle autorità cantonali non appena la gerarchia cantonale si è pronunciata in questo senso. In seguito vengono messe a punto misure di sicurezza al fine di garantire, segnatamente a livello di Centro di calcolo del DFGP, un controllo globale dei collegamenti dei Cantoni (parole d'ordine, registrazione degli utenti ecc.). Per contro, se un servizio cantonale di polizia chiede un collegamento per cinque persone perché ne hanno bisogno, il DFGP non verifica se questa necessità sia reale.

233.5 Il caso particolare del Centro di calcolo del DFGP

Le indagini intraprese sia dalla Sezione «Autorità» nell'ambito di questa ispezione on-line, sia dalla delegazione della CdG nel quadro dei controlli relativi ai sistemi ISIS e DOSIS hanno permesso di evidenziare una problematica derivante dall'inesistenza di un esame relativo alla sicurezza dei collaboratori del Centro di calcolo del DFGP.

Contrariamente ai collaboratori della polizia federale, gli informatici che lavorano presso il Centro di calcolo di Zollikofen non sono sottoposti ad alcun controllo sulla sicurezza, benché abbiano accesso a dati estremamente delicati, sia nel settore della polizia sia nell'ambito della protezione dello Stato.

Questa situazione può comportare problemi nell'ambito delle misure di sicurezza. Inoltre, il caso sollevato nel rapporto del servizio di controllo amministrativo del Consiglio federale "On-line-Datenaustausch zwischen Bund und Kantonen", secondo cui ex collaboratori del Centro di calcolo del DFGP hanno sviluppato un sistema cantonale (ABI) parallelo ai sistemi DOSIS e ISOK, mostra quanto sia attuale questa problematica.

234 Esame dei costi

Nel quadro dell'elaborazione dei concetti informatici, è previsto anche l'esame dei costi per l'allestimento di collegamenti on-line?

Secondo le spiegazioni fornite dal consulente per la protezione dei dati del DFGP, la ripartizione dei costi tra la Confederazione e i Cantoni per l'allestimento di collegamenti «on-line» è all'incirca la seguente.

L'allestimento e l'esercizio della rete fino al punto di collegamento nel Cantone spetta alla Confederazione; i Cantoni sono incaricati dell'esercizio della rete interna (LAN) e dell'acquisto delle periferiche (PC, stampanti ecc.).

Oltre al principio della ripartizione dei costi tra Confederazione e Cantoni, si pongono per l'allestimento di collegamenti on-line numerose altre questioni concernenti i costi. Al fine di occuparsi più concretamente di questi aspetti, tale questione è stata trattata nel quadro dell'esame del blocco 2. Considerati i numerosi collegamenti dei Cantoni ai sistemi informatici delle autorità di polizia della Confederazione, è stato in particolare trattato l'aspetto della ripartizione dei costi tra la Confederazione e i Cantoni, e questo per ciascuno dei sistemi scelti dalla Sezione «Autorità» (RIPOL, DOSIS, ISOK, ZAN, RCS e ISIS), ma anche gli aspetti relativi al preventivo, ai costi d'investimento, d'esercizio ecc.

La problematica dei costi è trattata in modo approfondito nel rapporto peritale.

24 Esame della questione principale

Quali regole si applicano in sede di pianificazione e allestimento di collegamenti on-line nel settore della polizia?

Date le risposte e le precisazioni relative alle questioni complementari, si può dare alla questione principale la seguente risposta riassuntiva.

241 Norme tecniche e norme di sicurezza

Sulla base di disposizioni quadro, quali l'ordinanza dell'11 dicembre 1989 *concernente l'istituzione di un Ufficio federale dell'informatica e disciplinante il coordinamento dell'informatica presso l'Amministrazione federale e l'ordinanza del 10 giugno 1991 concernente la protezione delle applicazioni e dei sistemi informatici nell'Amministrazione federale*, l'Ufficio federale dell'informatica ha emanato diverse istruzioni tecniche (IT), direttive concernenti la sicurezza informatica (DS) e le strategie.

Le applicazioni quali RIPOL, DOSIS, ISOK, ZAN, RCS e ISIS scelte nel quadro della presente ispezione appartengono a unità organizzative a cui si applicano le direttive di sicurezza dell'UFI. Per questi sistemi vigono pertanto i principi e le disposizioni in materia di sicurezza dell'Amministrazione federale (v. elenco n. 231.2).

L'applicazione di queste disposizioni implica, da una parte, che i suddetti sistemi informatici siano rilevati e classificati quali oggetti di protezione e che siano in ogni caso sottoposti anche a una valutazione dei rischi. D'altra parte, per queste applicazioni occorre adottare misure di sicurezza e organizzative (responsabili dell'applica-

zione, incaricati della sicurezza, organi di controllo ecc.) e le nuove autorizzazioni per l'accesso a queste applicazioni devono soddisfare le esigenze della *Network Security Policy (NSP)* e della *direttiva di sicurezza DS S03.*

242 Norme di procedura (metodo)

La procedura per l'allestimento di sistemi informatici e dei relativi collegamenti on-line avviene secondo un particolare sistema di gestione dei progetti: la procedura HERMES. Questa procedura trova applicazione quale strumento di gestione e standard per l'attuazione di progetti d'informatica in seno al DFGP. HERMES è articolata in diverse fasi e determina i ruoli e le competenze dei diversi gruppi di progetto o di altri organi (*istanza d'autorizzazione, mandante del progetto, comitato di progetto, direzione del progetto ecc.*).

L'indagine svolta presso il consulente per la protezione dei dati del DFGP ha rilevato che l'allestimento di un collegamento on-line deve ripercorrere ogni volta le cinque fasi secondo la procedura HERMES. Questa procedura non vale però quando uno o più Cantoni sono già collegati a un sistema, per esempio nel quadro di un progetto pilota, e se si decide in seguito di collegarvi altri Cantoni.

La procedura HERMES applicata dal DFGP è uno strumento fondamentale per l'allestimento di collegamenti on-line nel settore della polizia. Tale procedura disciplina la gestione e l'attuazione di progetti d'informatica, ma non prevede norme specifiche per i collegamenti on-line, segnatamente per quanto riguarda il rispetto dei principi di opportunità, proporzionalità e finalità.

243 Norme relative alla protezione dei dati

La legge federale del 19 giugno 1992 sulla protezione dei dati e l'ordinanza del Consiglio federale del 14 giugno 1993 ad essa relativa disciplinano non solo le questioni concernenti il rispetto dei principi di proporzionalità e di finalità (art. 4 LPD), bensì anche le misure di sicurezza (art. 7 LPD) e le misure tecniche e organizzative (art. 20 segg. OLPD) che occorre adottare in caso di trattamento di dati personali come pure le modalità per l'annuncio di progetti d'informatica.

In virtù dell'articolo 27 LPD, spetta all'Incaricato federale della protezione dei dati controllare il rispetto della legge federale sulla protezione dei dati da parte degli organi federali. Per l'allestimento di collegamenti on-line, gli incombe quindi il compito di far rispettare i principi di proporzionalità, finalità e necessità. La Commissione della gestione condivide l'opinione dell'Incaricato federale della protezione dei dati, secondo cui per adempiere i suoi compiti legali di controllo gli mancherebbero i mezzi, segnatamente a livello di personale. Questo problema era già stato sollevato nel quadro dell'ispezione sull'introduzione dell'informatica nell'Amministrazione federale. La commissione constata che questa situazione è ancora attuale.

È inoltre rimessa in questione l'efficacia dei controlli per il fatto che l'Incaricato federale può difficilmente pronunciarsi in merito allo sviluppo di nuovi collegamenti on-line, poiché spesso questi ultimi gli vengono sottoposti allo stadio di concetto, quando non sono ancora stati chiaramente definiti. Queste lacune del controllo si ripercuotono anche sul processo legislativo, nel senso che vengono proposte modifi-

che di leggi per i collegamenti on-line non ancora definiti con precisione, e la cui necessità, proporzionalità ecc. non sono ancora state esaminate.

244 Norme e prassi cantonali

Per l'allestimento di collegamenti on-line occorre anche tener conto delle *disposizioni* e delle *procedure decisionali* che variano in notevole misura da Cantone a Cantone. L'Incaricato federale della protezione dei dati ha nei confronti dei Cantoni una semplice funzione consultiva. Egli può intervenire al momento in cui viene allestito il collegamento, ma in seguito non ha più alcuna possibilità di controllare che i Cantoni rispettino tali collegamenti o che questi ultimi non siano stati estesi ad altri organi. Questo controllo è di competenza delle autorità cantonali e il livello dello stesso può essere molto diverso da un Cantone all'altro.

Inoltre l'esame della necessità o della proporzionalità dei collegamenti on-line allestiti con i Cantoni è relativo. Se le autorità cantonali esprimono il bisogno di un collegamento, vengono adottate misure di sicurezza che consentono, soprattutto a livello di Centro di calcolo del DFGP, un certo controllo globale dei collegamenti dei Cantoni (parole d'ordine, registrazione degli utenti ecc.). Se invece un servizio cantonale di polizia chiede di collegare cinque persone perché ne ha bisogno, il DFGP non controlla se questa necessità esiste realmente.

25 Conclusioni della Commissione

Esame a livello concettuale

Tenuto conto delle indagini condotte, che si basavano essenzialmente sui lavori preparatori dell'OPCA, la Commissione rileva alcuni aspetti positivi e diverse lacune.

251 Le basi legali per l'allestimento di sistemi informatici (*legge e ordinanza sulla protezione dei dati, ordinanza sull'UFI, istruzioni tecniche e direttive di sicurezza dell'UFI*) e la procedura HERMES costituiscono, quale strumento e standard per la gestione e l'attuazione di progetti d'informatica in seno all'Amministrazione federale, un quadro giuridico preciso e completo.

252 Per la pianificazione e l'allestimento di collegamenti on-line, vigono diverse disposizioni, che derivano dalle suddette prescrizioni, sul piano delle diverse fasi secondo la procedura HERMES, sia su quello delle misure di sicurezza e organizzative, delle direttive di sicurezza o dei principi di protezione dei dati. A questo proposito è tuttavia necessario fare due considerazioni:

– da una parte, le diverse direttive summenzionate prevedono innanzitutto numerose disposizioni relative alle misure di sicurezza, di codifica e di autenticazione, ai livelli di protezione, alle misure organizzative, alla valutazione dei rischi o alla protezione dei sistemi e delle applicazioni ad essi connessi (Network Security Policy / NSP). Esse non contengono tuttavia disposizioni specifiche ai fini dell'allestimento di collegamenti on-line, in particolare per quanto riguarda l'esame preliminare dei principi di necessità, finalità e proporzionalità di un nuovo collegamento. L'allegato 2 della direttiva sulla sicurezza informatica DS S02 prevede alcune disposizioni più precise; essa non mira tuttavia

all'esame di detti principi per i collegamenti previsti per le autorità federali o cantonali, ma disciplina piuttosto gli aspetti che riguardano il collegamento individuale di un utente a un sistema (identificazione degli utenti, parole d'ordine, interruzione di connessioni inattive o inutilizzate, controllo dei soggetti, frequenza e durata dei diritti di collegamento, attribuzione dei diritti di accesso caso per caso o modifica dei privilegi);

– d'altra parte, la procedura HERMES, quale metodo di gestione e di attuazione di progetti d'informatica, prevede di ripercorrere le fasi per decidere in merito all'allestimento di nuovi collegamenti on-line, ma a parte qualche accenno di carattere generale (p. es. in merito all'adempimento delle misure di sicurezza e delle esigenze nell'ambito della protezione dei dati), essa non contiene prescrizioni o disposizioni specifiche per i collegamenti on-line, segnatamente per quanto riguarda l'esame dei principi di opportunità, proporzionalità o finalità. La procedura HERMES applicata in seno al DFGP rappresenta quindi uno strumento fondamentale nel quadro dell'allestimento di collegamenti on-line nel settore della polizia; essa è comunque soltanto il "metodo" per la gestione e l'attuazione di progetti d'informatica.

253 L'esame di questi principi è previsto nelle disposizioni relative alla protezione dei dati, le quali sanciscono non solo i *principi di opportunità, proporzionalità e finalità*, ma disciplinano altresì *le modalità di annuncio* dei progetti relativi al trattamento automatizzato di dati personali all'IFPD tramite l'UFI, nonché *le competenze di controllo* ad essi relative.

Come già accennato, l'esame e il controllo del rispetto dei principi relativi alla protezione dei dati nell'ambito dell'allestimento di collegamenti on-line è tuttavia difficile da realizzare per il fatto che mancano i mezzi necessari, che l'allestimento di certi collegamenti è previsto «a titolo preventivo» senza che ne sia stata dimostrata la necessità, e che talvolta si inoltrano domande di allestimento di accessi senza che esista una base legale.

254 Il collegamento on-line dei Cantoni a sistemi informatici della Confederazione solleva diversi problemi, segnatamente per quanto concerne le numerose disposizioni cantonali tra loro diverse (p. es. in materia di protezione dei dati), le procedure decisionali che variano in notevole misura da Cantone a Cantone, l'esame della necessità o della proporzionalità oppure il controllo dei collegamenti attribuiti.

255 La seguente tabella illustra i principi o le fasi più importanti dell'allestimento di collegamenti on-line, rilevandone gli aspetti soddisfacenti [✓] o le lacune ancora esistenti[✘]:

a)	Disposizioni quadro per la pianificazione di collegamenti on-line sotto forma di istruzioni tecniche (IT), di direttive concernenti la sicurezza informatica (DS) o di strategie	✓
b)	Standard e metodi di gestione e attuazione di progetti d'informatica in quanto strumento d'organizzazione, di pianificazione, d'esecuzione e di comando	✓
c)	Modalità di annuncio dei progetti d'informatica	✓

d)	Valutazione dei rischi	*da esaminare sulla base dei risultati*
e)	Pianificazione delle misure di sicurezza	*dell'indagine rapporto peritale*
f)	Esame precedente l'allestimento di collegamenti on-line	
g)	Necessità	✘
h)	Proporzionalità	
i)	Finalità	
j)	Concessione di collegamenti on-line ai Cantoni (procedure decisionali, disposizioni, controllo) Controllo dei collegamenti on-line (esame a posteriori, controllo della portata dei collegamenti ecc.)	✘ ✘
k)	Basi legali su cui si fondano i sistemi informatici	✓
l)	Disposizioni di leggi formali che prevedono esplicitamente la possibilità di consultazione on-line di dati degni di particolare protezione	✓

Analisi della prassi in seno all'Amministrazione

I risultati esposti nel rapporto peritale (v. allegato I) relativi alla prassi dell'Amministrazione federale nell'ambito dell'allestimento di collegamenti on-line nel settore della polizia confermano in gran parte e completano le conclusioni della Commissione.

L'esperto insiste soprattutto sulla necessità di sensibilizzare il legislatore sulle questioni delle norme di delega, e di raccomandargli una scelta esatta delle nozioni. La Commissione condivide il parere dell'esperto, secondo cui è necessaria una regolamentazione generale di un livello superiore per la concessione di collegamenti on-line. La prassi attualmente in vigore consiste nel delegare le competenze fino alle unità amministrative gerarchicamente inferiori senza tener conto dell'importanza dell'informazione nel settore della polizia, né del carattere riservato dei dati trattati. Quale istanza indipendente incaricata di rilasciare le autorizzazioni relative ai collegamenti on-line, un'unità amministrativa gerarchicamente superiore è più adeguata che non un'unità che fa capo a sua volta a un servizio d'informazione e che potrebbe pertanto avere un interesse a che questo sistema sia più ampiamente utilizzato. Un esame delle severe condizioni legali per l'uso dei sistemi d'informazione della polizia (necessità, proporzionalità e opportunità) dev'essere garantito nell'ambito di una procedura chiaramente definita.

L'esperto propone nel suo rapporto in particolare le seguenti misure:

- emanare in seno al DFGP precise prescrizioni sulla procedura di autorizzazione dei collegamenti on-line. La trasparenza così creata permette di garantire che la procedura avvenga in modo unificato;
- istituire basi legali anche per i progetti pilota;

– definire standard minimi per la collaborazione tra Confederazione e Cantoni nel quadro della domanda e dell'allestimento di collegamenti on-line a sistemi d'informazione della Confederazione;
– coinvolgere i responsabili politici (Confederazione e Cantoni) per decidere in merito alla realizzazione e all'ammissibilità dei collegamenti on-line;
– trovare un'ubicazione più appropriata per il Centro di calcolo del DFGP;
– introdurre un controllo di sicurezza per i collaboratori del Centro di calcolo del DFGP
– procedere a una rapida fusione delle reti parallele KOMBV-KTV e DFGP-WAN.

26 Mozione e raccomandazioni della Commissione

Alla luce di queste considerazioni, la Commissione presenta al suo Consiglio una mozione e al Consiglio federale une serie di raccomandazioni, invitandolo a esaminare anche le altre proposte dell'esperto, e se le ritiene opportune ad attuarle il più presto possibile.

Mozione della Commissione della gestione del Consiglio degli Stati

Maggiore protezione dei dati personali nei collegamenti on-line

Il Consiglio federale propone una revisione della legge federale del 19 giugno 1992 sulla protezione dei dati. La revisione ha i seguenti obiettivi:

a) per l'istituzione di collegamenti on-line occorre prevedere una base legale anche per i progetti pilota;
b) per le domande e l'istituzione di collegamenti on-line ai sistemi informatici della Confederazione, quest'ultima definisce standard minimi riguardo alla collaborazione tra Confederazione e Cantoni. Essa stabilisce l'accesso, l'utilizzazione, la protezione e il controllo delle sue banche di dati.

Raccomandazioni della Commissione

261 Esame di opportunità, proporzionalità e finalità

La crescente dotazione di mezzi informatici comporta l'allestimento di un numero sempre maggiore di collegamenti on-line che consentono a numerose autorità federali e cantonali di consultare direttamente diverse banche di dati. Prima di regolamentare questi collegamenti mediante disposizioni legali in senso formale, il Consiglio federale li esamina dal punto di vista dell'opportunità (necessità), della proporzionalità e della finalità.

262 Controllo da parte dell'istanza competente

Il Consiglio federale si impegna affinché l'Incaricato federale della protezione dei dati possa controllare in modo più adeguato questi collegamenti on-line. Tale controllo deve garantire che vengano allestiti soltanto i collegamenti di cui sia stato dimostrato il bisogno, l'obiettivo sia conosciuto, i costi siano stati previsti e i cui rischi di abuso o di lesione della personalità siano stati oggetto di un'attenta valutazione.

263 Collegamenti on-line: trasparenza nei messaggi del Consiglio federale

Il Consiglio federale fa sì che i suoi messaggi contengano tutte le indicazioni necessarie sui collegamenti previsti, sia per quanto riguarda la loro necessità, finalità, proporzionalità e volume, sia in relazione alle autorità che devono concederne la possibilità di collegamento.

264 Collaborazione e coordinamento tra Confederazione e Cantoni

Il Consiglio federale si premura affinché vi sia un miglior coordinamento e una migliore collaborazione tra Confederazione e Cantoni. Occorre pertanto istituire a livello cantonale procedure decisionali che, se non identiche, siano quanto meno unificate o comparabili e che tengano conto del federalismo e delle norme cantonali vigenti.

265 Principi per le procedure di concessione dei collegamenti on-line

Il Consiglio federale fissa i principi per tutte le procedure di concessione per l'allestimento di collegamenti on-line nel settore della polizia, disciplinando in particolare i compiti, le competenze e le responsabilità nell'ambito della procedura.

266 Controllo delle norme di delega

Il Consiglio federale controlla la delega generale delle competenze fino ai gradini inferiori della scala gerarchica e in tutti i settori interessati. Esso fa sì che le autorizzazioni di collegamento on-line siano rilasciate da un'istanza adeguata e indipendente che sia consapevole dell'importanza e della portata della sua decisione come pure del carattere riservato dei dati trattati.

267 Controllo del rispetto dei principi di sicurezza e di collegamento da parte degli utenti cantonali/comunali

Il Consiglio federale offre ai gestori di sistemi informatici la possibilità di controllo (ispezioni di sicurezza) allo scopo di garantire che gli utenti cantonali e comunali rispettino i principi di sicurezza e le regole fissate per i collegamenti.

268 Norme per le domande d'autorizzazione

Il Consiglio federale fissa gli standard che devono soddisfare le domande volte a ottenere la concessione di collegamenti on-line nel settore della polizia.

269 Controllo della frequenza d'uso dei collegamenti on-line

Il Consiglio federale procede a controlli regolari per stabilire la frequenza d'uso dei collegamenti on-line nel settore della polizia.

2610 Controlli di sicurezza dei collaboratori del Centro di calcolo del DFGP

Il Consiglio federale provvede a un controllo di sicurezza dei collaboratori del Centro di calcolo del DFGP. Contrariamente ai collaboratori della polizia federale, attualmente queste persone non sono sottoposte ad alcun controllo di sicurezza, benché abbiano accesso a dati degni di particolare protezione (informazioni sulle persone, dati concernenti la polizia o la sicurezza dello Stato ecc.) o a informazioni relative alle misure di sicurezza o agli sviluppi informatici delle applicazioni in seno alla Confederazione.

2611 Ubicazione del Centro di calcolo del DFGP

Il Consiglio federale provvede affinché il Centro di calcolo del DFGP sia installato in un luogo più appropriato.

2612 Decisione in merito alla fusione di KOMBV-KTV e DFGP-WAN

Il Consiglio federale decide il più presto possibile se è opportuno operare una fusione tra KOMBV-KTV e DFGP-WAN.

27 Seguito della procedura

La Commissione invita il Consiglio federale a prendere posizione sul presente rapporto e sulle raccomandazioni ivi contenute entro la fine di giugno 1999.

19 novembre 1998

In nome della Commissione della gestione del Consiglio degli Stati:

Il presidente, Peter Bieri

In nome della Sezione «Autorità»:

Il presidente, Pierre Aeby

La segretaria delle Commissioni della gestione:

Mariangela Wallimannn-Bornatico

Allegato 1: Rapporto peritale e risultati della procedura di consultazione (non pubblicati sul Foglio federale)

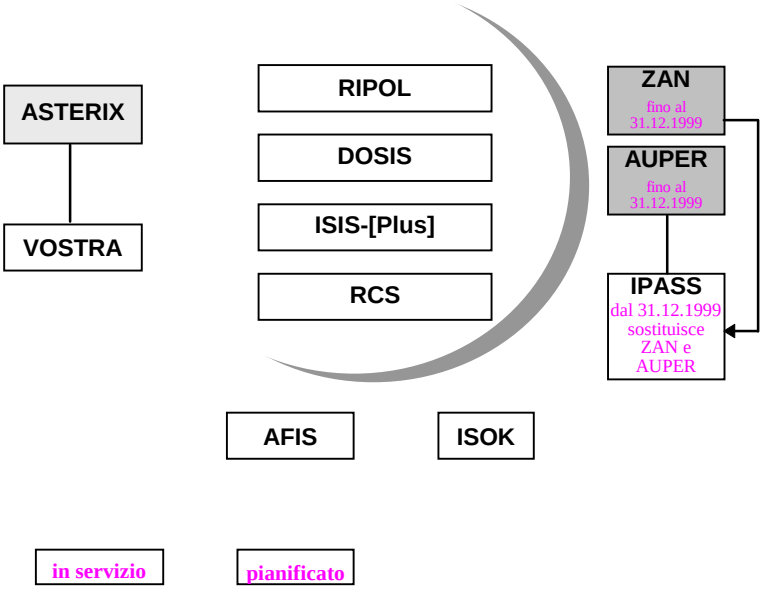
Allegato 2: Elenco delle abbreviazioni

Allegato 3: Panoramica dei sistemi

Elenco delle abbreviazioni

ABI	«Automation Büro Innendienst»
AFIS	Sistema automatico d'identificazione delle impronte digitali (Automatic Fingerprints Identification System)
AUPER	Sistema automatizzato di registrazione delle persone
CCF	Controllo amministrativo del Consiglio federale
CIC	Conferenza informatica della Confederazione
CdG-CN	Commissione della gestione del Consiglio nazionale
CdG-CS	Commissione della gestione del Consiglio degli Stati
CF	Consiglio federale
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
DFGP-WAN	Dipartimento federale di giustizia e polizia «Wide-Area-Network»
DOSIS	Sistema di trattamento dei dati in materia di lotta contro il traffico illegale di stupefacenti
GPDel	Delegazione delle Commissioni della gestione
HERMES	(Procedura HERMES) Gestione e attuazione di progetti d'informatica / Standard dell'Ufficio federale dell'informatica
IFPD	Incaricato federale della protezione dei dati
ISIS	Sistema per il trattamento provvisorio dei dati relativi alla protezione dello Stato
ISIS-Plus	Progetto di sistema provvisorio di trattamento dei dati relativi alla protezione dello Stato con collegamento on-line da parte delle autorità cantonali
ISOK	Sistema di trattamento dei dati in materia di lotta contro la criminalità organizzata
KOMBV-KTV	«Kommunikation der Bundesverwaltung - Kantonalverbund»
LMSI	Progetto di legge federale sulle misure per la salvaguardia della sicurezza interna
LDDS	Legge federale concernente la dimora e il domicilio degli stranieri
LPD	Legge federale sulla protezione dei dati del 19 giugno 1992 [RS 235.1]
MPC	Ministero pubblico della Confederazione
OLPD	Ordinanza relativa alla legge sulla protezione dei dati del 14 giugno 1993
On-line	Collegamenti on-line; procedura di richiamo; collegamento diretto a sistemi informatici
OPCA	Organo parlamentare di controllo dell'Amministrazione
RCS	Registro centrale degli stranieri (= ZAR: Zentrales Ausländerregister)
RIPOL	Sistema di ricerca informatizzato di persone e oggetti
UFI	Ufficio federale dell'informatica
UFP	Ufficio federale di polizia
ZAN	Indice centrale delle pratiche (Zentraler Aktennachweis)

Panoramica dei sistemi



Sistema	Nome	Competenze e responsabilità
RIPOL Art. 1 e 4 ordinanza RIPOL	**Sistema di ricerca informatizzato di persone e oggetti**	*Ufficio federale di polizia*
DOSIS Art. 19 ordinanza DOSIS	**Sistema di trattamento dei dati in materia di lotta contro il traffico illegale di stupefacenti**	*Ufficio federale di polizia*
ISIS-[PLUS] Art. 1 e 23 cpv. 1 ordinanza ISIS	**Sistema provvisorio di trattamento dei dati relativi alla protezione dello Stato**	*Ministero pubblico della Confederazione* Capo della polizia federale
RCS Art. 1 ordinanza RCS	**REGISTRO CENTRALE DEGLI STRANIERI**	*Ufficio federale degli stranieri*

Sistema	Nome	Competenze e responsabilità
ZAN	**INDICE CENTRALE DEI DATI**	*Ufficio federale di polizia* – Sezione d'identificazione – Sezione servizi centrali *Ufficio centrale svizzero di polizia* INTERPOL
AUPER Art. 3 ordinanza AUPER	**Sistema automatizzato di registrazione delle persone**	*Ufficio federale dei rifugiati* *Ufficio federale di polizia* – Divisione Affari internazionali, dell'assistenza giudiziaria internazionale e della polizia – Ufficio centrale di polizia – Sezione assistenza degli Svizzeri all'estero – Sezione della cittadinanza *Ufficio federale degli stranieri* *Servizio dei ricorsi e Servizio finanziario del DFGP* *Commissione dei ricorsi in materia d'asilo*
IPAS Nuovo art. 351^{octies} cpv. 1 CP	**Sistema informatizzato di gestione e indice informatizzato delle persone e dei fascicoli**	*Ufficio federale di polizia*
AFIS Art. 6 ordinanza conc. il Servizio d'identificazione dell'UFP	**Sistema automatico d'identificazione delle impronte digitali**	*Ufficio federale di polizia* Servizio d'identificazione
ISOK Art. 21 cpv. 1. ordinanza ISOK	**Sistema di trattamento dei dati in materia di lotta contro la criminalità organizzata**	*Ufficio federale di polizia*
VOSTRA Art.1 cpv.1bis, 1ter, 1^{quater} O sul casellario giudiziale		