88.032

Messaggio concernente la legge federale sulla protezione dei dati (LPD)

del 23 marzo 1988

Onorevoli presidenti e consiglieri,

Vi presentiamo, con proposta d'approvazione, il disegno di legge federale sulla protezione dei dati.

Contemporaneamente vi proponiamo di togliere di ruolo i seguenti interventi parlamentari:

1971 P 10 898	Legislazione sugli ordinatori (N 11.12.72, Bussey)
1977 P 77.381	Centri d'informazione pubblici e privati (N 17.1.78, Carobbio)
1982 P 82.336	Offerte d'impiego e protezione della personalità (N 8.10.82, Crevoisier)
1984 P 84.598	Protezione della personalità dell'assuntore dell'opera (N 22.3.85, Reimann)
1984 P 84.909	Protezione dei dati, regime transitorio (N, non ancora trattato, Leuenberger)

Vi proponiamo inoltre di non dar seguito alle iniziative seguenti:

1977	77.223	Protezione della personalità e dei dati, Costituzione federale (non ancora trattata, Gerwig)
1977	77.224	Legge sulla protezione della personalità e dei dati (non ancora trattata, Gerwig).

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

23 marzo 1988

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Stich
Il cancelliere della Confederazione, Buser

Compendio

L'impiego dell'informatica e delle moderne tecnologie delle telecomunicazioni in quasi tutti i settori della vita e l'enorme intensificazione del trattamento e della diffusione dei dati personali in seno alla società, all'economia e allo Stato hanno fatto aumentare in modo considerevole il rischio di lesioni della personalità. Il diritto privato e il diritto amministrativo, nella forma attuale, non sono in grado di garantire adeguatamente la protezione della personalità contro lesioni basate sulle attività in ordine all'informatica. La presente legislazione intende colmare questa lacuna e creare una protezione efficace per le persone interessate dal trattamento dei dati.

Il disegno di legge contiene nella parte generale i principi materiali applicabili al trattamento dei dati che valgono sia per gli organi della Confederazione, sia anche per gli elaboratori privati di dati. Esso prevede che ogni persona abbia il diritto di esigere dal proprietario di una collezione di dati le informazioni raccolte sulla propria persona. A tale scopo, le banche di dati devono essere registrate. L'obbligo di registrazione è esteso per gli organi federali, mentre le persone private devono annunciare soltanto le collezioni di dati che presentano rischi particolari nell'ottica della protezione della personalità. Infine anche determinati tipi di comunicazioni di dati all'estero, rilevanti per la loro portata o per la natura delle informazioni protette trasmesse, soggiacciono all'obbligo di essere dichiarati.

Nella misura in cui il presente disegno disciplina l'elaborazione dei dati da parte di privati, esso costituisce un completamento e una concretizzazione della protezione della personalità del Codice civile. Esso fissa ad esempio le condizioni alle quali un trattamento di dati può portare a una lesione della personalità. Esso indica d'altro canto al giudice determinati elementi che gli permettono di valutare in quali casi possa essere giustificata una lesione della personalità, poiché sono dati interessi preponderanti privati o pubblici a quella certa elaborazione dei dati. In tale contesto il progetto tiene soprattutto conto dei bisogni d'informazione dell'economia. Rileviamo infine che spetta al giudice civile pronunciarsi sui litigi concernenti i trattamenti di dati effettuati da privati.

Le legge disciplina in seguito, nei dettagli, il trattamento di dati da parte dell'amministrazione federale e di altri organi federali. Essa stabilisce le responsabilità in materia di protezione dei dati e determina le esigenze legali alle quali devono rispondere le diverse elaborazioni. La legge impartisce inoltre agli organi federali le indicazioni concernenti la ricerca e la comunicazione dei dati personali e altre forme di trattamento. Degli interessi specifici di segretezza degli organi incaricati della sicurezza dello Stato e della sicurezza militare è stato debitamente tenuto conto.

Un Preposto federale alla protezione dei dati è chiamato a sorvegliare l'applicazione della legge. Egli potrà procedere a chiarimenti e rilasciare raccomandazioni; allorquando si tratta di persone private, tuttavia, egli potrà intervenire

soltanto in casi particolari. Egli non è tuttavia autorizzato a prendere misure vincolanti, ma ha invece il diritto di sottoporre una determinata pratica per decisione alla Commissione federale della protezione dei dati. Tale commissione giudica inoltre le controversie in materia di protezione dei dati tra cittadini e organi dell'amministrazione. Le sue decisioni possono essere impugnate con ricorso al Tribunale federale.

Il progetto regola anche la comunicazione di dati per scopi della ricerca medica. I dati soggiacenti al segreto professionale, quali il segreto medico possono essere comunicati per uso nella ricerca soltanto dietro consenso delle persone interessate o in base all'autorizzazione di una Commissione peritale nominata a tale scopo dal Consiglio federale. Questa commissione può tuttavia rilasciare un'autorizzazione del genere soltanto se la ricerca non può essere attuata con dati resi anonimi e se per i ricercatori sarebbe impossibile o particolarmente difficile ottenere il consenso delle persone interessate; gli interessi della ricerca devono inoltre essere preponderanti per rapporto agli interessi del mantenimento del segreto. Con questa regolamentazione, concepita essenzialmente come complemento del Codice penale, si intendono conciliare tra loro la protezione del paziente e l'interesse pubblico a una ricerca efficiente nel campo della medicina.

Con la revisione della procedura penale federale e della legge sull'assistenza internazionale in materia penale sono inoltre ancorati nella legislazione determinati principi del diritto della protezione dei dati, in particolare per quanto concerne la procedura delle indagini preliminari della polizia giudiziaria e lo scambio d'informazioni con INTERPOL.

Con questa legislazione la Svizzera segue l'evoluzione di quasi tutti gli Stati industrializzati. Il disegno di legge precisa inoltre principi di diritto internazionale pubblico in materia di protezione dei dati e fornisce così un valido contributo alla creazione di condizioni quadro per lo scambio internazionale d'informazioni.

1 Parte generale

11 Bisogno di una legislazione sulla protezione dei dati

111 Considerazioni generali

La raccolta e l'elaborazione di informazioni sulle persone ledono la loro personalità in misura più o meno grave e sono all'origine di reazioni positive o negative. L'attività d'informazione può favorire una comunicazione, auspicata, tra le persone, ma d'altro canto anche fare in modo che un individuo abbia a ritenere limitate o pregiudicate le proprie facoltà d'evolvere.

Il trattamento dei dati personali può pregiudicare o ledere la persona interessata in diversa maniera. Le persone divengono insicure se non sono più in grado di sapere chi attorno a loro raccoglie dati che le concernono e in che misura il loro ambiente sia informato su quanto le interessa[1]. Molte persone si risentono che qualcuno abbia l'ardire di raccogliere segretamente informazioni e indiscrezioni sul loro conto[2]. A causa delle decisioni prese sulla base di dati inveritieri, incompleti o non più attuali da parte di privati o di autorità, le persone interessate possono essere svantaggiate o trattate in modo ingiusto[3]. Un individuo può patire tutta una vita se i dati con un'informazione negativa sulla sua persona sono conservati illimitatamente e costantemente riutilizzati. Violazioni dei diritti della personalità sono possibili anche se le informazioni sono oggetto di eccessivo trattamento, come nel caso di un fatto compromettente reso noto senza bisogno[4], di dati raccolti in numero non necessario per lo svolgimento di un contratto, di informazioni sugli amministrati, raccolti o scambiati senza discrezione dai servizi pubblici tra loro[5]. Nessuno poi apprezza l'uso di dati per uno scopo diverso da quello per il quale sono stati raccolti: ad esempio, se le informazioni concernenti il rapporto di lavoro o misure d'ordine sociale siano riutilizzate in un altro contesto.

112 Crescente flusso d'informazioni grazie alle nuove tecnologie

Dalla Seconda guerra mondiale, l'utilizzazione sistematica delle informazioni sulle persone si è sviluppata in modo eccezionale ed ha acquistato nuove forme. L'incremento delle relazioni economiche, l'impiego di nuove strategie di vendita e di nuovi metodi della gestione aziendale, l'aumento e la diversificazione delle operazioni di credito esigono che quantità sempre più importanti di informazioni personali vengano elaborate con tecniche sempre più complesse. Nel settore pubblico, la moltiplicazione dei compiti statali e le crescenti esigenze poste alla qualità delle prestazioni dello Stato sono pure all'origine di un aumento rilevante dei trattamenti d'informazioni.

Questa evoluzione fino all'avvento della società d'informazione è stata resa possibile dalle nuove tecnologie dell'informazione e delle comunicazioni. L'impiego del trattamento automatizzato dei dati permette di sfruttare le informazioni in maniera di gran lunga più sistematica ed efficiente di quanto non sia possibile con i metodi di lavoro tradizionali. La tecnologia moderna permette di raccogliere, riunire, trattare e diffondere le informazioni praticamente senza

[1] La nota [1] e tutte le altre note figurano alla fine del messaggio.

limite alcuno. Essa rende possibile la connessione e il frazionamento mirati di collezioni di dati, la loro valutazione e trasmissione a terzi. Le possibilità di trattamento sono aumentate ancora dall'unione tra elaborazione automatizzata dei dati e nuove tecniche delle comunicazioni. L'evoluzione va nel senso della creazione di reti locali, regionali e internazionali che connettono tra loro centri di calcolo e raccolte di dati geograficamente lontani.

Le nuove tecnologie permettono una vigilanza più stretta sul comportamento delle persone. In tale contesto vanno elencate non soltanto le registrazioni video, bensì anche i mezzi sempre più quotidiani dei controlli automatici dell'accesso, del tempo di presenza, delle prestazioni e delle comunicazioni. L'uso di apparecchi e impianti elettronici, il passaggio di recinti di sicurezza o la lettura automatizzata delle carte d'identità e di credito permettono di raccogliere tutta una serie d'informazioni. Nuove informazioni sono rilevate anche grazie ai sistemi di comunicazione bidirezionali automatizzati quali il videotex. Al rilevamento tradizionale con la tastatura si sostituisce in misura sempre maggiore la lettura ottica di immagini, testi, o altri segni o la registrazione dei suoni.

Parallelamente all'evoluzione descritta è cresciuto anche il potenziale di violazioni dei diritti della personalità. In particolare l'individuo non è spesso più in grado di rilevare, neppure in maniera approssimativa quali dati che lo concernono sono trattati, da chi, dove e quando; egli ha in ampia misura perduto la padronanza sui dati che lo concernono e, con questo, la facoltà di scegliere di persona a chi intende fornire quali informazioni. Spesso l'individuo non è neppure più in grado di riconoscere gli errori e gli abusi causati dai trattamenti delle informazioni e di scoprirne i colpevoli.

Nell'ottica della protezione dei dati il trattamento elettronico dei dati presenta tuttavia anche aspetti positivi. Esso permette in particolare di rendere anonimi i dati personali con un esborso sensato.

113 Obiettivi generali della legge sulla protezione dei dati

Una legge sulla protezione dei dati non ha lo scopo di impedire lo sviluppo delle tecnologie dell'informazione o di limitarne le possibilità. I successi nel campo delle scienze, dell'economia e dell'amministrazione resi possibili grazie a queste tecnologie non possono e non devono essere rimessi in questione e devono essere possibili anche in avvenire. Occorre tuttavia fissare determinati principi direttori per il trattamento dei dati che garantiscano che lo sviluppo della personalità degli individui non abbia ad essere intralciato da trattamenti inutili o indesiderabili dei dati. Nella misura in cui l'ordinamento giuridico non preveda altrimenti, ognuno deve potere determinare da sé se rivelare e lasciare utilizzare i propri dati personali e d'altro canto decidere liberamente su la scelta e l'assetto delle relazioni alle quali fornire informazioni e con le quali entrate in comunicazione[6].

Ciò significa in primo luogo che la vita privata e familiare deve essere protetta dalle ingerenze. Così soltanto le persone o i servizi statali che vantano interessi preponderanti in materia d'informazione dovranno potere raccogliere i dati relativi alla sfera privata di una persona[7]. Inoltre le informazioni sull'esercizio

di diritti protetti dalla Costituzione quali la libertà di culto e di coscienza, la libertà d'opinione o il diritto di voto e di petizione devono essere oggetto di particolare protezione, considerato che proprio tali diritti garantiscono in modo particolare lo sviluppo delle personalità. Una legge sulla protezione dei dati deve inoltre impedire che il singolo divenga semplice oggetto d'informazione. L'individuo deve invece potere contribuire a determinare l'immagine e le conoscenze che l'ambiente circostante si fa di lui. Per tale ragione egli ha ottenuto il diritto di sapere chi sa qualcosa su di lui e a quali scopi i dati relativi vengono trattati. Soltanto così gli è dato di decidere in ogni caso adeguatamente nella sua vita privata, professionale e sociale. Egli deve però anche avere la possibilità di fare correggere o distruggere informazioni che lo concernono o di esigere da coloro che trattano tali informazioni il rispetto del segreto.

114 Stato del diritto in Svizzera

114.1 Nel settore privato

Nelle relazioni private la protezione dei dati è retta attualmente dai soli principi della protezione generale della personalità, ancorata negli articoli 28 e seguenti del Codice civile (CC). Giusta i termini dell'articolo 28 capoverso 1 CC, entrato in vigore il 1° luglio 1985, «Chi è illecitamente leso nella sua personalità può, a sua tutela, chiedere l'intervento del giudice contro chiunque partecipi all'offesa». La nozione di personalità deve essere intesa in senso lato, comprendente l'insieme dei valori fisici, psichici, morali e sociali legati all'esistenza della persona[8]. Questa definizione estensiva della protezione della personalità nella legge lascia tuttavia aperta una questione fondamentale; a sapere cioè in quali situazioni vi sia effettivamente una lesione illecita della personalità. La legge neppure fornisce indicazioni che permettano di rilevare a quali condizioni trattamenti dei dati siano giustificati.

La *giurisprudenza,* da parte sua ha definito soltanto pochi criteri e punti di riferimento in merito alla questione a sapere in quali casi un trattamento dei dati sfoci in una lesione della personalità. Una lesione della personalità può essere data se l'attività d'informazione lede la sfera privata o intima della persona[9]. La sfera intima comprende i fatti ed avvenimenti della vita a conoscenza del solo individuo o delle persone che godono della sua particolare fiducia, mentre alla sfera privata appartengono gli altri fatti della vita privata ai quali non dovrebbe avere accesso un vasto pubblico. Sono lesioni della personalità anche i pregiudizi causati all'onore e alla reputazione sociale, come pure i trattamenti di dati personali inesatti che facciano apparire in «una luce falsa» l'interessato[10]. Riassumendo si può rilevare che la giurisprudenza ritiene un trattamento dei dati illecito se pregiudica uno degli aspetti della vita dell'individuo, la sua indipendenza morale o il suo credito sociale.

In considerazione di questa regolamentazione sommaria del trattamento dei dati nel diritto vigente, iniziative per norme di protezione dei dati sono partite singolarmente da *organizzazioni private.* La Conferenza degli istituti svizzeri d'indagine di mercato e di pareri, in collaborazione con l'Associazione svizzera dei periti in studi di mercato, l'Associazione delle agenzie d'informazioni com-

merciali in Svizzera e l'Associazione svizzera di vendita per corrispondenza hanno elaborato regole deontologiche applicabili al trattamento dei dati personali che esse effettuano. Di particolare importanza sono anche i «Nuovi principi per i medici di fiducia» e i «Principi per i medici aziendali» adottati dalla Camera dei medici svizzeri nel 1981. Menzioniamo infine l'accordo conchiuso nel 1983 tra l'Associazione svizzera degli industriali della metalmeccanica (ASM) e la Federazione svizzera dei lavoratori metallurgici e orologiai (FOMO), come pure la convenzione modello del 1984 della Commissione degli impiegati dell'Unione sindacale svizzera su «Nuove tecniche e protezione dei dati nell'azienda»; ambedue le convenzioni fissano importanti principi della protezione dei dati.

114.2 In diritto pubblico

Quasi riflesso della protezione della personalità in diritto civile è data anche una certa protezione di diritto costituzionale contro i trattamenti di dati illeciti ed eccessivi. La Costituzione federale in effetti non garantisce esplicitamente una siffatta protezione contro le ingerenze dello Stato per mezzo del trattamento dei dati. Le persone lese sono bensì protette dal diritto fondamentale non scritto della libertà personale e dall'articolo 8 della Convenzione europea dei diritti dell'uomo (CEDU). La libertà personale garantisce non soltanto «il diritto di spostarsi e il rispetto dell'integrità fisica», ma anche «tutte le libertà elementari, il cui esercizio è necessario allo sviluppo della persona umana»[11]. Ai sensi dell'articolo 8 della CEDU «Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza». Il segreto di voto e il diritto di petizione, inoltre, impongono determinati limiti al trattamento delle informazioni, soprattutto nel caso le firme di iniziative, referendum o petizioni siano usate per scopi politici o di polizia[12]. Importante è infine l'articolo 4 della Costituzione federale che garantisce all'interessato la partecipazione al trattamento dei dati[13].

Onde concretizzare tali principi, il Consiglio federale ha emanato, il 16 marzo 1981 le «Direttive concernenti l'elaborazione dei dati personali nell'Amministrazione federale»[14], a titolo provvisorio e allorquando erano già in atto i lavori preparatori relativi alla legge sulla protezione dei dati. Tali direttive contengono: principi giuridici che devono disciplinare il trattamento dei dati e statuiscono a carico dei servizi dell'amministrazione l'obbligo d'informare le persone interessate. Le direttive hanno lo scopo di familiarizzare l'amministrazione con gli imperativi fondamentali della protezione dei dati e di preparare l'introduzione della legge federale sulla protezione dei dati. Per i grandi sistemi d'informazione, il Consiglio federale ha inoltre emanato, pure in certo modo quale avvio alla creanda legge sulla protezione dei dati, ordinamenti specifici di protezione dei dati relativi a determinati settori. Ricordiamo in questa sede l'ordinanza del 20 ottobre 1982 sul Registro centrale degli stranieri (RS *142.215*), l'ordinanza del 16 dicembre 1985 sul sistema informativo per le indagini di polizia (RIPOL) (RS *172.213.61*), l'ordinanza del 29 ottobre 1986 sui controlli militari (RS *511.22*), l'ordinanza del 27 settembre 1982 sulla sperimentazione di un sistema d'informazione in materia di servizio di collocamento e

di statistica del mercato del lavoro (RS *823.114*), come pure una serie di ordinanze sulla statistica federale[15].

Diversi Cantoni dispongono già di leggi sulla protezione dei dati per il loro settore pubblico. Il primo è stato il Cantone di Ginevra che nel 1976 ha emanato la «Loi sur la protection des informations traitées automatiquement par ordinateur», sottoposta poi, nel 1981, a revisione totale e ampliata. Seguirono altri Cantoni: Vaud, Neuchâtel, Vallese, Berna, Giura, Ticino e Turgovia. I Cantoni di Basilea Città, Basilea Campagna, Soletta, Zurigo, Lucerna, San Gallo e Glarona, stanno attualmente approntando i loro progetti di legge. In altri Cantoni, ancora, ci si contenta per il momento con ordinanze o semplici direttive.

114.3 Carenze del diritto vigente

Come testé rilevato, il nostro ordinamento giuridico attuale già contiene determinate regole sul trattamento dei dati. Tuttavia, nonostante singole decisioni giudiziali importanti, siamo ancora sprovvisti di protezione efficace contro i pregiudizi causati dai trattamenti d'informazioni. Né il diritto privato, né il diritto pubblico sono in grado di tenere sufficientemente conto dei bisogni di protezione sorti in relazione all'elaborazione automatizzata dei dati.

In materia di diritto privato ciò è in relazione soprattutto al fatto che agli interessati torna spesso difficile rilevare chi tratta dati sulla loro persona. Ma anche nei casi nei quali questo risulta possibile, spesso essi non ottengono informazioni in merito alle collezioni di dati che li concernono e ai dati che vi sono memorizzati. Essi sono inoltre difficilmente in grado d'identificare i rischi che corrono o le lesioni subite in ragione di trattamenti di dati. L'articolo 28 del Codice civile, dal tenore molto generalizzato non offre criteri in base ai quali appurare se un trattamento sia ammesso o meno. Spesso è per tali persone difficile provare il nesso di causalità tra un trattamento d'informazioni e il pregiudizio causato ai loro diritti personali. In tali condizioni è chiaro che per le persone interessate qualsiasi valutazione giudiziale di un trattamento di dati è esposta a rischi processuali rilevanti.

Nel settore pubblico, la protezione giudiziale dei diritti fondamentali ha influito in misura soltanto limitata e puntuale sulle attività informative dello Stato[16]. Si aggiunga poi che i compiti dell'amministrazione implicanti il trattamento di informazioni sono in generale definiti in modo molto frammentario. Esistono invero innumerevoli prescrizioni sui compiti d'informazione del cittadino, come pure varie regole sull'uso dei dati oppure sugli obblighi di comunicazione delle autorità, tuttavia sono con queste perseguiti obiettivi specifici dell'esecuzione della legge, non invece la protezione della persona lesa. Gli obblighi di segretezza imposti dalla legislazione sui funzionari garantiscono certo una protezione importante contro la comunicazione di informazioni ai privati: essi non costituiscono però una regolamentazione generale adatta per sbrigare domande d'assistenza amministrativa o giudiziaria di altri servizi dell'amministrazione. Inoltre, fino ad oggi nessuna regola vieta all'amministrazione pubblica di utilizzare i dati per scopi diversi da quelli previsti. In parte non risolta è anche la questione a sapere come debbano presentarsi le informa-

zioni conformi alle esigenze della protezione dei dati. In diritto pubblico mancano inoltre anche procedure amministrative o giudiziarie che permettano alle persone di informarsi sui dati che le concernono, di controllare l'uso e la comunicazione e di difendersi contro errori del trattamento[17].

115 Discrepanza tra il diritto vigente e la prassi nella ricerca medica

115.1 Protezione della personalità del paziente e interesse pubblico alla ricerca medica: interessi divergenti

Le informazioni concernenti lo stato di salute di una persona fanno parte dei dati delicati e sensibili che possono toccare il centro della sfera intima. Questo è soprattutto il caso dei dati sulla malattie gravi e le infermità. Molte persone esitano a fornire ai terzi dettagli sullo stato di salute. Esse temono che la loro situazione sociale o professionale ne abbia a soffrire. L'aspetto è diverso per la persona che si affida alle cure mediche. Al personale medico il paziente in genere comunica molti dati intimi sul suo stato fisico e psichico, poiché soltanto disponendo di questi è possibile una terapia efficace. Il paziente è tuttavia pronto a fornire senza riserve informazioni sullo stato di salute soltanto quando ha fiducia nel personale trattante e, in particolare, nel medico. La fiducia è data anche dalla certezza che i rilevamenti fatti nel corso della cura siano coperti dalla più grande discrezione.

Queste correlazioni sono note da tempo. Non meraviglia quindi che proprio il settore attinente alla salute conosca una delle più antiche regole sulla protezione dei dati: il segreto professionale che trova la sua più remota espressione già nel giuramento d'Ippocrate. La violazione del segreto professionale del medico si configura nella maggior parte dei Paesi come fattispecie d'ordine penale. Secondo l'articolo 321 del Codice penale, medici, dentisti, farmacisti, levatrici come pure gli ausiliari di questi professionisti che rivelano un segreto professionale sono puniti, a querela di parte, con la detenzione o con la multa. La rivelazione non è punibile quando sia fatta col consenso dell'interessato o con l'autorizzazione scritta data dall'autorità superiore o dall'autorità di vigilanza.

La ricerca medica, d'altro canto, opera in ampia misura con dati personali. Molto più spesso che non in altri settori della ricerca è dato qui il bisogno di disporre di dati in base ai quali sia possibile identificare le persone interessate (soprattutto in materia di malattie ereditarie, insorgenza del cancro, influssi patogeni dell'ambiente ecc.). Soltanto dati personali diretti permettono, ad esempio, di far beneficiare immediatamente una persona in trattamento medico dei frutti di una ricerca, di riconoscere delle registrazioni ripetute di un dato soggetto, di costituire gruppi di confronto, di attuare esami di lunga durata o di procedere a domande suppletive. Questa attività di ricerca medica risponde a un interesse pubblico e/o privato importante, soprattutto allorquando serve a lottare più efficacemente contro le affezioni particolarmente gravi o molto diffuse. In molti casi singoli, la ricerca medica può creare le premesse per un'efficace terapia o un'adeguata prevenzione ed è quindi al servizio della sanità pubblica.

115.2 Regolamentazione insoddisfacente nel Codice penale

Le disposizioni penali sul segreto professionale (art. 321 CP) non sono in pratica più rispettate: esse non tengono in effetto conto degli sviluppi recenti della ricerca medica.

Secondo il diritto vigente, i ricercatori devono ottenere il consenso di tutti i pazienti, direttamente o tramite il medico trattante, prima di consultare i dossier degli stessi[18]. Vi sono però spesso casi nei quali non è sempre facile ottenere tale accordo: sia perché i pazienti sono scomparsi senza lasciar tracce o sono morti, oppure sono andati a risiedere a grandi distanze gli uni dagli altri. Anche la comunicazione di dati a persone esse stesse sottoposte a un segreto professionale costituisce violazione del segreto professionale. Questo vale anche per la comunicazione di dati tra i medici. Il segreto medico deve di per sé essere rispettato anche nell'ambito di un nosocomio, a meno che il trattamento dei dati avvenga tra persone tutte direttamente interessate alla cura di un determinato paziente. In questo caso si può partire dal presupposto di un consenso tacito del paziente alla rivelazione di un segreto medico[19]. Se il paziente sin dall'inizio della sua ospitalizzazione deve contare sul fatto che il suo dossier medico, nel corso del trattamento, giungerà a conoscenza di diverse persone, non è in genere in grado di determinare l'identità di tutti quanti partecipano al trattamento della sua malattia. Tuttavia, in considerazione dell'organizzazione e delle strutture di uno stabilimento ospedaliero, la comunicazione dei dati concernenti i pazienti tra il personale curante sottoposto alla stessa direzione terapeutica - vale a dire, di regola, entro una determinata divisione dell'ospedale - dovrebbe essere ammessa.

116 Sviluppo del diritto sulla protezione dei dati all'estero

Verso la fine degli anni Sessanta presero avvio negli Stati industriali occidentali gli sforzi per attuare una regolamentazione legislativa del trattamento dei dati. Il primo atto legislativo fu la legge sulla protezione dei dati del 1970 nel Land dell'Assia. In questo Land fu creata la prima istanza di controllo del tutto indipendente dall'amministrazione e responsabile unicamente davanti al Parlamento. Nel 1973 fu la volta della Svezia che emanò una legge sulla protezione dei dati che per la creazione e la tenuta di un «registro automatizzato delle persone», esige l'approvazione dell'ispettorato dei dati. Nella Repubblica federale di Germania la legge sulla protezione dei dati fu adottata nel 1977 e a questa seguirono, in rapida serie, le leggi sulla protezione dei dati dei Länder federali. In Francia fu licenziata, all'inizio del 1978, la «Loi relative à l'informatique, aux fichiers et aux libertés». Nel 1978 una legge del genere adottò l'Austria, terzo Stato vicino ad agire in tal senso. Lo stesso anno videro la luce una legge in Norvegia e due leggi in Danimarca (una ciascuna per il settore privato e pubblico). Nel 1979 fu la volta del Lussemburgo, nel 1981 dell'Islanda, di Israele e - con un decreto - dell'Ungheria. Gli ultimi grandi atti legislativi sono stati attuati nel 1984 in Gran Bretagna e, nel 1987, in Finlandia e Irlanda.

Interessante è pure l'evoluzione legislativa oltre-oceano. Nel 1974, gli Stati Uniti d'America crearono una legge sulla protezione dei dati che permette, alle persone interessate, accesso ai propri dati, concede rimedi di diritto più ampi e pone alle autorità federali chiari limiti nel trattamento dei dati. Gli Stati Uniti hanno poi completato la loro legge per l'amministrazione federale sulla protezione dei dati con una serie di leggi speciali, ad es., sulla protezione dei dati in materia di concessione di crediti, nel settore dell'educazione e della formazione, nei mezzi elettronici di pagamento e nei sistemi di telecomunicazioni. Gli Stati federali americani, ispirandosi a leggi modello si sono dotati in parte di decreti sulla protezione dei dati per le loro amministrazioni pubbliche e di regolamenti per il settore privato. Analogo andamento ha conosciuto la legislazione in Canada e in Australia. In ambedue i Paesi, lo Stato centrale dispone, come è il caso per gli USA, di competenze soltanto limitate in merito alla legislazione di diritto privato. Caratteristica comune a questi tre Stati: essi hanno coordinato in parte già anteriormente il diritto della personalità e il diritto sulla protezione dei dati con le prescrizioni concernenti la pubblicità dell'amministrazione e sull'accesso alle informazioni statali, onde ponderare l'interesse di conservare il segreto con i bisogni di trasparenza dell'informazione. Questo è avvenuto negli USA con il «Freedom of Information Act» del 1966. Nel Canada realizza tale obiettivo la legge del 1982 che emana la legge sull'accesso all'informazione e la legge sulla protezione delle informazioni personali.

117 Protezione internazionale dei dati

Lo sviluppo dell'informatica e delle telecomunicazioni ha permesso un forte sviluppo delle relazioni commerciali e una più stretta cooperazione tra gli Stati e le organizzazioni internazionali. In molti settori privati e pubblici il trattamento dei dati non si arresta più alle frontiere dello Stato. Diverse organizzazioni internazionali si sono quindi premurate di disciplinare i flussi transfrontalieri di dati con norme di diritto internazionale pubblico[20].

La regolamentazione più estesa in materia di protezione internazionale dei dati è stata sviluppata dal *Consiglio d'Europa* con la «Convenzione n. 108 del 28 gennaio 1981 sulla protezione delle persone nei confronti del trattamento automatizzato dei dati di carattere personale». La convenzione è già stata ratificata da Austria, Repubblica federale di Germania, Francia, Gran Bretagna, Lussemburgo, Norvegia, Spagna e Svezia e firmata da 10 altri Paesi.

Obiettivo della Convenzione n. 8 è la protezione delle libertà fondamentali, in particolare della vita privata delle persone fisiche per rapporto all'elaborazione automatizzata di dati personali. Gli Stati contraenti si impegnano a istituire nel loro diritto interno certe garanzie minime di protezione dei dati (art. 4-11). L'armonizzazione tra gli ordinamenti di protezione dei dati nei singoli Paesi membri dovrebbe da parte sua facilitare il flusso transfrontaliero delle informazioni tra gli Stati contraenti (art. 12). La convenzione disciplina inoltre la collaborazione e la reciproca assistenza degli Stati contraenti in pratiche di protezione dei dati (art. 13-17). Il Consiglio d'Europa ha inoltre elaborato, nel corso degli ultimi anni, diverse *raccomandazioni* atte a disciplinare la prote-

zione dei dati in certi settori particolari. Esse concernono la protezione dei dati delle banche di dati medici automatizzati, della ricerca e della statistica, della vendita diretta, della sicurezza sociale e della polizia.

Da parte sua, l'*Organizzazione di cooperazione e di sviluppo economico* (OCSE) ha elaborato, praticamente contemporanee alle raccomandazioni del Consiglio d'Europa, «Linee direttive per la protezione della vita privata e il flusso transfrontaliero di dati di carattere personale». Il Consiglio dell'OCSE ha rimesso, il 23 settembre 1980, le linee direttive, accompagnate da una raccomandazione, ai Governi dei Paesi membri: ad eccezione di uno solo, tutti gli Stati le hanno accettate. Le linee direttive formulano principi generali applicabili ai flussi internazionali di dati e alla protezione dei dati e disciplinano in particolare la collaborazione degli Stati membri in materia di scambio internazionale di dati. L'importanza delle direttive dell'OCSE risiede soprattutto nel fatto che vi hanno aderito anche Paesi d'oltre oceano (in particolare Stati Uniti d'America, Canada, Giappone e Australia) e che in tali Paesi un gran numero di aziende multinazionali si sono pubblicamente impegnate a rispettarle.

12 Condizioni di diritto costituzionale

Non esiste una disposizione speciale, nella Costituzione federale, che autorizzi la Confederazione a emanare prescrizioni sulla protezione dei dati. Con la protezione dei dati si intende invero concretizzare in maniera sostanziale i diritti fondamentali tradizionali e rafforzarne l'efficacia: i diritti fondamentali soli non sono tuttavia in grado, secondo la dottrina dominante, di costituire la competenza specifica della Confederazione. Diverse competenze federali comprendono tuttavia anche la facoltà di emanare regole di protezione dei dati.

121 Nel settore del diritto privato

L'articolo 64 della Costituzione federale autorizza la Confederazione a legiferare in materia di diritto civile. Sulla base di tale norma, il legislatore federale *può estendere e rafforzare* la protezione della personalità, finora disciplinata soltanto in principio, *con disposizioni di diritto privato che reggono in modo specifico la protezione dei dati.* Ciò facendo egli può anche emanare disposizioni che pure rivestono carattere di diritto pubblico - ad esempio l'obbligo di registrare determinate collezioni di dati - sempre che siano necessarie per l'esecuzione e l'applicazione uniformi del diritto civile federale o per evitare conflitti di legge[21].

Inoltre, sulla base dell'articolo 31bis capoverso 2 della Costituzione federale, la Confederazione ha la facoltà generale di «... *emanare disposizioni sull'esercizio del commercio e dell'industria*». In virtù di tale norma, all'attività lucrativa privata possono essere imposte limitazioni di polizia economica, il bene centrale protetto da pertinenti prescrizioni dovendo essere la *lealtà in affari.* Questa esigenza di lealtà nell'attività economica privata dev'essere garantita anche per quanto concerne l'uso d'informazioni personali. In tale contesto non si deve trattare unicamente di attività d'ordine economico nelle quali - come nei

centri di calcolo - scopo principale è il trattamento dei dati in quanto tale, bensì qualsiasi attività economica nell'ambito della quale sono usati dati personali. I trattamenti di dati per uso unicamente personale oppure per scopi scientifici o ideali non possono invece essere disciplinati sulla base dell'articolo 37bis capoverso 2 Cost.

Altre disposizioni costituzionali completano queste due competenze principali ed autorizzano la Confederazione a legiferare sulla protezione dei dati in settori specifici. L'articolo 34ter capoverso 1 Cost. permette di emanare disposizioni sui sistemi d'informazione relativi al personale, onde proteggere i lavoratori. La Confederazione ha anche la competenza di legiferare, sulla base dell'articolo 31^{quater} Cost., sui sistemi d'informazione delle banche e degli istituti di credito oppure, giusta l'articolo 34 capoverso 2 Cost., di prevedere speciali regole in merito alle attività d'informazione effettuate dalle assicurazioni private.

122 Nel settore del diritto pubblico

Il legislatore federale può appoggiarsi sul *potere d'organizzazione* che gli conferisce l'articolo 85 numero 1 della Costituzione federale per emanare disposizioni di protezione dei dati applicabili alle autorità e ai servizi dell'amministrazione. Questa norma costituzionale permette di disciplinare l'impiego legale del trattamento dei dati come strumento di lavoro e d'organizzazione nei servizi federali e di creare meccanismi di controllo che assicurino una protezione efficace dei dati. La Confederazione può inoltre, in base alla competenza di legiferare in materia penale dell'articolo 64bis Cost., rafforzare la protezione dei dati con i mezzi del diritto penale, sia emanando nuove disposizioni penali, sia estendendo l'applicazione del segreto di funzione e del segreto professionale.

Sulla base della piena autonomia in materia d'organizzazione garantita dalla Costituzione federale ai Cantoni, quest'ultimi sono legittimati a legiferare sulla protezione dei dati nei *settori pubblici cantonali.* Il diritto costituzionale e legislativo cantonale decide anche a sapere in quale misura l'ordinamento cantonale sulla protezione dei dati sia applicabile anche alle amministrazioni comunali. La Confederazione invece può soltanto emanare disposizioni di protezione dei dati applicabili ai settori pubblici cantonali e comunali nei quali i Cantoni sono incaricati d'eseguire prescrizioni federali: quest'ultime devono essere fondate su un disposto costituzionale attributivo di competenza e l'esecuzione deferita ai Cantoni (ad es., lotta contro le malattie trasmissibili art. 69 Cost.). Anche in tali casi, la Confederazione deve tuttavia rispettare il diritto cantonale in materia d'organizzazione.

13 Procedura preliminare alla legislazione

131 Diritto generale della protezione dei dati

La prima mozione volta all'adozione di una legge sulla protezione dei dati fu deposta il 17 marzo 1971 dal consigliere nazionale Bussey. Egli chiedeva una legislazione «che assicuri la protezione del cittadino e della sua sfera privata

contro l'utilizzazione abusiva dell'ordinatore e che permetta, d'altro canto, uno sviluppo normale dell'uso degli ordinatori»[22]. Questa mozione fu trasformata in postulato[23]. Il 22 marzo 1977, il consigliere nazionale Gerwig depose due iniziative parlamentari sulla protezione dei dati. Con la prima, presentata come proposta formulata, Gerwig chiedeva di inserire nella Costituzione federale un articolo sulla protezione dei dati. La seconda iniziativa, mantenuta nella forma di una proposta generale, enumerava le esigenze poste a una legge sulla protezione dei dati.

Pure nell'anno 1977, prima ancora che la commissione del Nazionale che trattava l'iniziativa Gerwig decidesse del seguito da dare alla stessa, il capo del Dipartimento federale di giustizia e polizia decise di affidare a periti i lavori preliminari per una legge sulla protezione dei dati. In tale contesto il capo del DFGP prese due decisioni di principio: il progetto di legge doveva attenersi alle basi costituzionali esistenti e quindi rilevare soltanto il settore privato e il settore pubblico della Confederazione; occorreva quindi rinunciare a una revisione costituzionale che avrebbe permesso una legislazione completiva inglobante anche il settore di diritto pubblico cantonale. I lavori preliminari relativi al settore privato e quelli relativi al settore pubblico federale dovevano essere impresi separatamente, almeno nella fase preliminare.

In tale ottica, una prima commissione fu incaricata, nel 1977, di elaborare le disposizioni di protezione dei dati per l'amministrazione federale; affidata alla presidenza del professor Mario M. Pedrazzini di San Gallo, la commissione era composta di rappresentanti della scienza, dell'economia privata e dell'amministrazione pubblica. Dopo aver rilevato le collezioni di dati esistenti e steso l'inventario delle questioni sollevate dalla protezione dei dati, tale commissione rimise, nel 1981, al capo del Dipartimento federale di giustizia e polizia un avamprogetto di legge federale sulla protezione dei dati nell'amministrazione federale.

Nel frattempo, nel mese di settembre del 1979, il capo del DFGP aveva incaricato una seconda commissione di approntare un progetto di regolamentazione per il settore privato. Anche questa commissione era affidata alla direzione del prof. Pedrazzini. Presso oltre 100 imprese, associazioni e organizzazioni, questa procedette a rilevamenti sulla portata e l'utilizzazione di collezioni di dati e su specifici problemi concernenti la protezione dei dati. Nel mese d'ottobre del 1982 questa commissione licenziò un disegno di legge sul settore del diritto privato.

Nel mese di novembre del 1982, il capo del DFGP affidò a un piccolo comitato composto di rappresentanti delle due commissioni l'incarico di raccogliere i due avamprogetti in un unico disegno di legge. Con questo s'intendeva evitare in particolare, a favore degli interessati, una dispersione del diritto ed apportare una semplificazione della procedura legislativa. Questi lavori redazionali sfociarono, a fine 1983, nel *disegno per la procedura di consultazione.*

Il disegno per la procedura di consultazione cercava, in primo luogo, di indicare i criteri secondo i quali le necessità d'informazione delle persone private e degli organi statali siano da ponderare nei confronti dei bisogni di protezione delle persone interessate. Nel settore privato, la legge istituiva regole differen-

ziate per quanto concerne l'onere della prova da una parte a beneficio delle persone interessate, dall'altra a favore di certi trattamenti di dati. Per quanto concerne il settore pubblico, il progetto prevedeva disposizioni dettagliate sul trattamento dei dati personali eseguiti dagli organi federali. Le persone private, come pure gli organi della Confederazione che tenevano una collezione di dati avrebbero poi, a determinate condizioni, dovuto fare registrare tali collezioni di dati. Il progetto accordava inoltre alle persone interessate il diritto a ottenere informazioni sui dati che le concernevano a creava i rimedi giuridici che permettevano di difendersi contro i pregiudizi causati alla personalità dal trattamento dei dati. Come istanza di controllo era prevista una commissione sulla protezione dei dati, concepita nel settore privato sull'esempio della Commissione dei cartelli, mentre i suoi compiti nel settore dell'amministrazione federale potevano essere equiparati a quelli del Controllo federale delle finanze. Il progetto prevedeva infine diverse disposizioni penali destinate a punire la violazione di importanti principi della protezione dei dati.

132 Protezione dei dati nel settore della medicina

Oltre alle regole generali sulla protezione dei dati, occorrono disposizioni complementari valevoli per determinati settori particolari, quali soprattutto quello della medicina e delle assicurazioni sociali. In questa materia sono spesso trattati dati degni di particolare protezione che possono toccare la sfera privata dell'interessato. D'altro canto è dato un provato interesse pubblico allo sfruttamento dei dati concernenti la salute.

Nel 1980, l'Ufficio federale di giustizia incaricò quindi una commissione speciale ad hoc, affidata alla direzione della signora Yvette Jaggi, consigliere nazionale di Losanna, di chiarire le questioni in ordine al diritto di protezione dei dati nel settore medico. Il rapporto di questa commissione fu pubblicato nel 1984; questo stende un inventario dei trattamenti di dati caratteristici del settore sanitario e di quello delle assicurazioni sociali, che tali trattamenti vengano effettuati da persone private o da organi pubblici. Il rapporto fissa le basi legali di tali trattamenti e definisce le diverse questioni attuali di protezione dei dati. Il rapporto conchiude poi con una serie di raccomandazioni che in parte hanno trovato realizzazione nel presente disegno di legge generale sulla protezione dei dati, in parte sono state oggetto di rielaborazione approfondita all'interno dell'amministrazione.

Nel mese di ottobre del 1983, il capo del DFGP affidò a un nuovo gruppo di lavoro, presieduto dal professore Günter Stratenwerth di Basilea, l'incarico di studiare i problemi di protezione dei dati inerenti alla ricerca medica. Essa doveva in particolare ricercare un equilibrio tra gli interessi dei ricercatori al trattamento dei dati e gli interessi dei pazienti al rispetto del segreto medico. Nel suo rapporto del mese di dicembre del 1985 il gruppo di lavoro presentò un catalogo di proposte, giungendo essenzialmente alla conclusione che la ricerca con dati personali che soggiacciono al segreto professionale medico è in principio possibile soltanto con l'approvazione degli interessati. Sempre che un interessato non sollevi esplicitamente opposizione, l'approvazione deve potere essere sostituita all'autorizzazione rilasciata da una commissione di periti.

Fondandosi su questi lavori preliminari, il Dipartimento federale di giustizia e polizia, in collaborazione con il Dipartimento federale dell'interno ha elaborato un progetto di legge federale sulla rivelazione del segreto professionale in favore della ricerca medica. Nell'estate del 1987 fu aperta una procedura di consultazione in merito a questo progetto. Il disegno di legge riprendeva essenzialmente i principi elaborati dal gruppo di lavoro Stratenwerth, limitandosi tuttavia a disciplinare *la comunicazione,* rispettivamente la ricerca dei dati. Esso definiva le condizioni alle quali un segreto professionale può essere rivelato per scopi della ricerca medica, costituendo così, in parte preponderante, diritto d'applicazione dell'articolo 321 del Codice penale sul segreto professionale. Il suo campo d'applicazione si estende a ogni attività di ricerca, indipendentemente dal fatto che questa avvenga in istituti privati di ricerca, in servizi federali di ricerca, in università cantonali, come pure in ospedali cantonali, regionali o comunali.

14 Risultati della procedura di consultazione

141 Procedura di consultazione relativa alla legge generale sulla protezione dei dati

Il 25 gennaio 1984 fu avviata la procedura di consultazione sul progetto peritale di «Legge federale sulla protezione dei dati (LPD)». Fino all'autunno 1984 giunsero 156 risposte, in parte molto ponderose. Delle 141 istanze invitate ufficialmente, 107 si sono espresse in merito al progetto, fra le quali tutti i Cantoni. Oltre alle istanze invitate ufficialmente, altre 49 persone e organizzazioni hanno spontaneamente preso parte alla consultazione.

I risultati più importanti della consultazione sono i seguenti: una maggioranza preponderante delle risposte riconosce la necessità e l'urgenza di una legislazione sulla protezione dei dati. Il progetto - nella misura in cui esso si riferisce al trattamento dei dati nell'amministrazione federale - è stato definito tra utile e buono. Molto più contestate sono state, invece, le disposizioni sulla protezione dei dati per il settore privato e per questa materia il giudizio è risultato in complesso sfavorevole. Queste disposizioni hanno invero trovato approvazione quasi unanime tra i sindacati, le istituzioni di diritto pubblico, le organizzazioni scientifiche e culturali e le chiese. In maggioranza positive sono state anche le risposte dei Cantoni, dei partiti politici e delle organizzazioni professionali e femminili. Di parere diviso sono stati gli informatici; le disposizioni per il settore privato sono state del tutto respinte dalle organizzazioni padronali ed economiche (ad eccezione delle associazioni dei consumatori), come pure dai rappresentanti delle professioni sociali. Controverso è stato anche il principio di una legge comune per il settore pubblico e il settore privato. L'idea di una «legge unitaria» è stata accolta da certi Cantoni, partiti politici e organizzazioni, mentre altri Cantoni e soprattutto le associazioni padronali erano contrari.

Tutta una serie di proposte fondamentali del progetto sono state chiaramente approvate. Ciò vale per la parità di trattamento automatizzato e trattamento manuale dei dati e per l'introduzione di una categoria di dati degni di

speciale protezione. Hanno trovato approvazione anche l'obbligo di registrare determinate categorie di collezioni di dati e il diritto d'accesso e di rettificazione riconosciuto alle persone interessate. È inoltre stata accolta, almeno come principio, la necessità di un controllo efficace e indipendente della protezione dei dati come pure l'inserimento di disposizioni di diritto penale nel progetto.

La critica del progetto verteva soprattutto sull'ampiezza e la complessità della legge che contava 69 articoli. Certi tratti della legge erano inoltre giudicati troppo astratti e avulsi dalla realtà. Presentava difficoltà anche il fatto che nello stesso articolo c'erano spesso disposizioni sia per il settore pubblico sia per il settore privato. Le presunzioni e le finzioni della violazione della personalità, come pure i motivi giustificativi previsti nella parte del settore privato sono stati ritenuti di difficile comprensione. L'applicabilità della legge alle autorità cantonali incaricate di applicare il diritto federale è pure stata criticata. Diversi partecipanti alla procedura di consultazione hanno chiesto un regime giuridico differente per le persone fisiche e le persone giuridiche. Sono inoltre state chieste certe facilitazioni per determinate attività economiche, quali ad esempio la ricerca d'informazioni sull'affidabilità nel caso di concessione di crediti. Da più parti è stato inoltre avanzato il desiderio che le disposizioni specifiche applicabili ai mass media, alla ricerca e alla statistica, agli organi incaricati della sicurezza dello Stato e alle autorità fiscali siano riesaminate per essere completate o precisate. L'istituzione di una Commissione della protezione dei dati in quanto organo indipendente di controllo ha raccolto l'approvazione di un gruppo rilevante di organismi interpellati, mentre un altro gruppo, praticamente dello stesso peso avrebbe preferito un Preposto alla protezione dei dati, una sorta di ombudsmann della protezione dei dati.

142 Protezione dei dati nella ricerca medica

Il disegno di «legge federale sulla rivelazione del segreto professionale a favore della ricerca medica» è stato inviato in consultazione il 27 maggio 1987. Nell'autunno dello stesso anno erano pervenute al Dipartimento 54 risposte. Dei 61 organismi consultati soltanto 47 si sono pronunciati in merito al progetto, fra questi tutti i Cantoni. Oltre alle cerchie ufficialmente adite, hanno preso parte alla consultazione altre 7 organizzazioni.

Il progetto è stato complessivamente bene accolto. Da una maggioranza rilevante dei Cantoni e quasi all'unanimità dalle università e dalle organizzazioni mediche e della ricerca medica esso è stato riconosciuto fondamento adeguato per una futura legge. Di parere divergente tra loro sono stati i partiti politici: i tre maggiori si sono tuttavia espressi in favore del progetto. Piuttosto per il rigetto sono state le organizzazioni che rappresentano gli interessi dei pazienti.

Nel senso di una critica è stata da più parti avanzata l'esigenza di dovere tenere ancora meglio conto dei diritti dei pazienti e sottolineare con maggiore evidenza il carattere del progetto come atto legislativo per la protezione dei dati. Una minoranza ha messo in dubbio che sia effettivamente data la base

costituzionale per disciplinare a livello federale la protezione dei dati nella ricerca medica. In risposte isolate è stata respinta anche l'idea della creazione di una commissione federale centrale preposta alle autorizzazioni della comunicazione di dati per scopi di ricerca medica. Non è rimasto incontestato il fatto che il Preposto alla protezione dei dati dovrebbe assumere funzioni di controllo.

Molti organismi consultati si sono inoltre espressi a favore di una regolamentazione della protezione dei dati nel settore della ricerca medica non in una legge speciale, bensì in una legge generale sulla protezione dei dati e poiché si tratta di una nuova regolamentazione di un segreto professionale definito dalle disposizioni penali - nel Codice penale.

15 Messa a punto del progetto

Il Consiglio federale prese conoscenza, nella primavera del 1985, dei risultati della procedura di consultazione concernente la legge generale sulla protezione dei dati e incaricò un piccolo gruppo di lavoro sotto la presidenza del professore Pedrazzini di rielaborare ancora una volta il progetto alla luce dei risultati della procedura di consultazione. Il gruppo di lavoro stese nuovi progetti e fornì occasione ai rappresentanti delle organizzazioni padronali e dei sindacati, come pure di importanti rami dell'economia - banche, assicurazioni, mediatori di indirizzi - come pure dei mass media e degli uffici federali particolarmente interessati, di esprimersi in occasione di «hearings» tenutisi nel mese di maggio del 1986 in merito a tali progetti. La commissione intendeva con questo offrire a persone e servizi specialmente obbligati dalla legge l'occasione di presentare i loro concreti desiderata nei confronti della nuova versione della legge. Negli «hearings» è stata accolta favorevolmente la separazione netta delle prescrizioni attinenti al settore privato e al settore pubblico, come pure la maggiore concisione e migliore trasparenza del progetto. Per quanto concerne l'aspetto materiale, il disegno è stato in parte approvato, in parte ha invece riscontrato analoghe riserve come già in sede di procedura di consultazione. Nel mese di febbraio del 1987, il gruppo di lavoro presentò al capo del DFGP un nuovo disegno di legge con commento.

Per incarico del capo del Dipartimento, il progetto fu ancora una volta rielaborato, soprattutto nell'aspetto sistematico e redazionale, di molto semplificato e ulteriormente raccorciato a cura di un gruppo di lavoro interno all'amministrazione, presieduto dal dott. iur. Christoph Steinlin, vicedirettore dell'Ufficio federale di giustizia. Contemporaneamente - soprattutto mediante un complemento del Codice penale - le disposizioni del progetto di legge federale sulla rivelazione del segreto professionale per la ricerca medica furono integrate nella legge sulla protezione dei dati. Infine la procedura penale federale e la legge sull'assistenza internazionale in materia penale sono state completate con disposizioni di protezione dei dati applicabili rispettivamente alla procedura delle indagini preliminari della polizia giudiziaria e allo scambio d'informazioni con INTERPOL.

2 Parte speciale: Commento del disegno di legge federale sulla protezione dei dati, della regolamentazione della protezione dei dati nella ricerca medica e della revisione della procedura penale federale e della legge sull'assistenza internazionale in materia penale

21 Fondamenti del disegno di legge generale sulla protezione dei dati

211 Una legge comune per il settore pubblico e il settore privato

Dalla consultazione è risultata una forte opposizione a una legge unica che regga in uno il settore privato e anche l'amministrazione federale. L'opposizione è motivata essenzialmente dal fatto che la protezione dei dati nell'amministrazione federale e quella del settore privato sono di concezione talmente diversa che una normativa unica complicherebbe la legge. Secondo il nostro parere, tuttavia, il primo di questi argomenti non è fondato, e del secondo può essere tenuto conto senza che per questo si debba rinunciare ai vantaggi dovuti a una regolamentazione comune dei due settori. Una legge unica ha dalla sua parte il fatto che lo scopo di politica legislativa - proteggere la personalità dalle violazioni dovute all'elaborazione di dati personali - è lo stesso per il settore dell'amministrazione federale e per il settore privato. I principali fondamenti del diritto sulla protezione dei dati devono poi essere applicabili sia al settore privato che a quello pubblico. È quindi auspicabile che per la valutazione delle questioni in ordine al diritto sulla protezione dei dati siano competenti, in ambedue i settori, le stesse autorità - vale a dire lo stesso Preposto alla protezione dei dati e la stessa Commissione per la protezione dei dati -, osservando tuttavia che le rispettive competenze dovrebbero, nel settore privato, essere molto meno estese. In questo modo si potrà garantire meglio uno sviluppo armonico e reciprocamente coordinato della protezione dei dati nei settori privato e pubblico. Una legge unica può anche essere giustificata proprio perché il settore privato e il settore pubblico vi possono essere mantenuti distintivamente separati tra loro. Inoltre il progetto stabilisce chiaramente che le regolamentazioni applicabili al settore privato s'iscrivono nel quadro delle regole generali sulla protezione della personalità del Codice civile. Un ulteriore argomento per la legge unica è infine il fatto che questa permette di evitare interferenze reciproche e di ridurre al minimo il numero delle norme.

212 Campo d'applicazione

Il legislatore che intenda emanare una legge generale sulla protezione dei dati si vede confrontato dapprima a due difficoltà capitali. Il diritto sulla protezione dei dati è materia inglobante che proprio all'insegna della crescente informatizzazione tocca quasi tutti i settori dell'attività privata e pubblica. Considerata la grande varietà di mezzi ausiliari tecnici di cui disponiamo oggi, il trattamento di informazioni quale oggetto di una legge sulla protezione dei dati assume esso stesso le forme più diverse. Una legge generale sulla protezione dei

dati non può tuttavia tenere conto di tutte le probabili configurazioni del trattamento dei dati; essa deve piuttosto contenere norme fondamentali e generali che permettano almeno di abbozzare una soluzione per la maggior parte dei problemi, lasciando spazio per l'ulteriore sviluppo della protezione dei dati. Il disegno non può quindi disciplinare già in partenza tutti gli aspetti specifici al settore.

Di conseguenza il progetto rinuncia, come fanno anche numerose leggi straniere[24)] a distinguere fra il trattamento manuale e il trattamento automatizzato dei dati. Il progetto non intende basarsi su condizioni tecniche concrete, bensì resta il più possibile neutrale nei confronti della tecnica e del suo sviluppo. Al carattere generale della legge corrisponde anche la circostanza che essa comprende tutti i dati personali. Si è rinunciato a prevedere «dati liberamente disponibili» che non sottostanno alla legge, poiché una tale categoria è difficilmente delimitabile, in seguito perché qualsiasi informazione si presta, a seconda del contesto, ad attuare una violazione della personalità. La legge vuole inoltre proteggere la *persona fisica* e la *persona giuridica,* poiché entrambe possono da un trattamento di dati essere pregiudicate nei loro diritti. In contropartita le prescrizioni sul trattamento delle informazioni sono le stesse per le persone fisiche e le persone giuridiche. Il progetto vale infine per il settore del diritto privato come anche per quello del diritto pubblico.

All'applicabilità della legge generale sulla protezione dei dati sono tuttavia posti *determinati limiti.* Essa non si applica in effetti alle procedure giurisdizionali davanti alle autorità giudiziarie, alle procedure penali, alle procedure ricorsuali amministrative, alle procedure d'assistenza giudiziaria e ai registri pubblici. Il motivo va ricercato principalmente nel fatto che le leggi di procedura già prevedono garanzie a protezione della personalità che non devono essere doppiate in seguito dalla legge sulla protezione dei dati, che costituisce in parte anche diritto procedurale. Durante i lavori preliminari per il disegno di legge è stato rilevato che la *procedura delle indagini preliminari della polizia giudiziaria* regolate dalla legge federale sulla procedura penale necessita di ulteriori garanzie in ordine alla protezione dei dati. In allegato al progetto proponiamo quindi una modificazione della legge federale sulla procedura penale federale introducendo disposizioni speciali sulla protezione dei dati. Nella stessa ottica vengono create, con una modificazione della legge federale sull'assistenza internazionale in materia penale, le basi legali per lo scambio dei dati nell'ambito dell'Organizzazione internazionale di polizia criminale (INTERPOL) e in pari tempo diritto specifico sulla protezione dei dati inerente a tale attività d'informazione in materia di polizia criminale.

Il progetto che era stato inviato in consultazione nel 1983 aveva previsto che la legge della Confederazione sulla protezione dei dati sarebbe stata applicata anche nel caso un Cantone, per l'esecuzione del diritto federale, non disponesse di una sufficiente legislazione propria sulla protezione dei dati. Con una siffatta regolamentazione si sarebbe potuto promuovere l'armonizzazione del diritto svizzero sulla protezione dei dati ed evitare, d'altro canto, l'insorgere di «oasi dei dati» nel settore dell'esecuzione del diritto federale. Il presente progetto non contiene tuttavia una norma del genere. Il motivo è dovuto al fatto che la definizione della «sufficiente legislazione cantonale in materia di prote-

zione dei dati» solleverebbe importanti problemi, soprattutto perché dovrebbe essere attuata nel rispetto che s'impone delle diversità federalistiche. Se la Confederazione dovesse accontentarsi della semplice presenza di una legge cantonale, questo potrebbe portare a soluzioni non eque. Se d'altro canto la Confederazione non volesse semplicemente accettare qualsiasi diritto cantonale sulla protezione dei dati, dovrebbe istituire un obbligo per l'approvazione degli atti legislativi cantonali, unito a un ordinamento sostitutivo a livello federale per tutti i casi di diritto cantonale carente. Sarebbe allora possibile che nello stesso Cantone varrebbero diritti sulla protezione dei dati diversificati, per l'esecuzione del diritto federale e per il settore cantonale autonomo. Riteniamo quindi che la legge federale sulla protezione dei dati non dovrebbe trovare applicazione in materia d'esecuzione del diritto federale da parte dei Cantoni.

213 Legge federale sulla protezione dei dati

213.1 Principi materiali e organizzatori della protezione dei dati

Le *disposizioni generali* della prima sezione contengono i principi direttori più importanti e le premesse organizzatorie per attuare una protezione efficace dei dati. Le disposizioni generali si applicano ai privati che trattano dati come pure agli organi della Confederazione. L'articolo 4 fondamentale stipula che i dati personali possono essere raccolti soltanto con *mezzi legali* e che *non violino il principio della buona fede.* I dati trattati devono poi essere *esatti.* Il trattamento dei dati deve avvenire conformemente al principio della proporzionalità. È inoltre vietato, salvo disposizione legale contraria, trattare dati per *uno scopo diverso* da quello che è stato indicato alla persona interessata al momento della raccolta dei dati. Chi tratta dati deve *proteggerli* con mezzi tecnici o organizzatori adeguati *contro ingerenze illecite di terzi.* – Queste disposizioni costituiscono insieme al principio che regge la comunicazione dei dati all'estero (cfr. n. 213.5), il *nucleo materiale* della protezione dei dati.

Affinché i principi menzionati possano anche essere attuati nella realtà legale, occorre creare adeguate premesse d'organizzazione e di procedura. Essi devono garantire che il trattamento dei dati abbia ad essere per le persone interessate fino ad un certo punto trasparente. A tale scopo i detentori delle collezioni sono *obbligati a informare ogni persona che ne fa richiesta sui dati che la concernono e che sono contenuti nella collezione e sull'utilizzazione della collezione stessa.* Poiché però può fare uso del *diritto d'essere informato* soltanto chi è al corrente dell'esistenza di una collezione di dati, tutti i servizi federali sono obbligati a far registrare le loro collezioni di dati presso il Preposto alla protezione dei dati. Le persone private sono sottoposte a un obbligo di registrare meno esteso: esse devono notificare le collezioni di dati in merito alle quali esiste un pericolo rilevante di lesione della personalità. Occorre infine, a determinate condizioni dichiarare le comunicazioni di dati all'estero (cfr. n. 213.5).

213.2 Protezione dei dati nel settore del diritto privato

La seconda sezione del progetto si limita a quattro articoli e contiene prescrizioni all'attenzione di persone fisiche e persone giuridiche che agiscono nell'ambito del diritto privato. Una proposta di normativa per questo settore era già stata discussa durante i preparativi della revisione degli articoli 28 CC e 49 CO, decisa il 16 dicembre 1982, ed era tuttavia poi stata accantonata e rinviata per un esame più approfondito nel quadro della legislazione sulla protezione dei dati. Nella sua parte consacrata al diritto privato, il diritto sulla protezione dei dati completa e concretizza le regole sulla protezione della personalità del Codice civile. Il presente progetto si conforma quindi alla terminologia e alla sistematica del Codice civile. La nuova legge dovrebbe fornire a quanti elaborano dati e ai giudici gli elementi che permettano loro di giudicare in quale caso un trattamento dei dati può ledere illecitamente i diritti della personalità. Determinate attività d'informazione, soprattutto quelle che infrangono i principi generali fissati dalla legge e applicabili al trattamento dei dati sono nel progetto considerate quindi violazioni illecite della personalità. D'altro canto il progetto indica anche a quali condizioni possa essere dato un interesse all'attività d'informazione, tale da giustificare persino una lesione della personalità. In tale contesto possiamo ricordare che la raccolta e l'elaborazione dei dati rivestono importanza nodale in materia di concorrenza economica. In determinate occasioni l'interesse a ottenere informazioni sulla concorrenza oppure ai dati in relazione a contrattazioni o a ricerche sul credito di cui gode una persona può essere d'importanza tale che la persona interessata deve accettare un pregiudizio dei suoi diritti della personalità. Le complicate finzioni e presunzioni - tanto criticate - del progetto sottoposto a consultazione sono state abbandonate a favore di un sistema più flessibile che permette di tenere conto delle particolarità del caso singolo. Per quanto concerne la protezione giuridica, infine, il progetto rinvia per l'essenziale agli articoli 28-28*f* del Codice civile.

213.3 La protezione dei dati nel settore pubblico

Il disegno disciplina nella sezione dedicata al settore pubblico il trattamento dei dati da parte dell'amministrazione federale come pure delle persone e organizzazioni incaricate di eseguire compiti pubblici. Il progetto parte dall'idea che l'amministrazione, trattando i dati personali può in principio - anche se con diversa intensità - pregiudicare i diritti fondamentali delle persone interessate. La futura legge sulla protezione dei dati deve quindi garantire che anche nel trattamento dei dati sia rispettato il principio della legalità e della proporzionalità. Di conseguenza, gli organi federali saranno quindi in grado di trattare i dati personali soltanto se è data a tal proposito una base legale. Al trattamento di dati degni di speciale protezione e alla stesura di profili della personalità saranno poste condizioni più severe quanto alla base legale, rispettivamente verrà chiesta un'autorizzazione del Consiglio federale o il consenso delle persone interessate. Certe forme particolari di trattamento, in particolare la raccolta, la comunicazione, l'obbligo di rendere anonimi i dati e la distruzione dei dati saranno oggetto di *disposizioni speciali* all'indirizzo degli organi federali. Per il

trattamento dei dati nei settori della statistica, della ricerca e della pianificazione sono previste facilitazioni, nella misura in cui lo scopo del trattamento non si riferisce a persone. Il Consiglio federale è infine autorizzato a emanare regole di trattamento divergenti dai principi della presente legge in materia di protezione dello Stato e di sicurezza militare. Il progetto contiene inoltre disposizioni di diritto procedurale che in parte servono a precisare il diritto vigente, in parte però anche contengono innovazioni, quali ad esempio la possibilità di apporre la menzione del carattere contestato di un dato la cui esattezza è stata messa in dubbio dalla persona interessata.

213.4 Disposizioni penali e organizzative

Per il rispetto della legge, il progetto prevede l'istituzione di un Preposto federale alla protezione dei dati e di una Commissione federale della protezione dei dati.

Il Preposto alla protezione dei dati ha anzitutto funzione di mediatore tra elaboratori di dati e persone interessate. Nel caso di trattamenti di dati controversi egli può procedere a indagini. Le sue competenze di controllo nel settore pubblico son in tale contesto molto estese. Nel settore privato, invece, spetta in primo luogo alla persona interessata fare valere davanti al giudice civile i propri diritti in ordine alla protezione dei dati; il Preposto alla protezione dei dati può in tali casi intervenire soltanto se, in ragione di determinati metodi o sistemi di trattamento dei dati, insorge pericolo di lesione della personalità per un numero rilevante di persone. Se anche constata irregolarità, il Preposto non può giuridicamente obbligare gli organi e i privati interessati ad accantonarle, ma può soltanto rilasciare raccomandazioni. Se quest'ultime non sono rispettate, egli può allora sottoporre la pratica per decisione alla Commissione federale della protezione dei dati.

La *Commissione federale della protezione dei dati* deve garantire nel settore pubblico un'ampia protezione giuridica; nel settore privato, invece, anche la commissione può intervenire soltanto nei trattamenti di dati che costituiscono un pericolo importante per un grande numero di persone. Essa decide in prima istanza sulle raccomandazioni rilasciate dal Preposto alla protezione dei dati e tratta i ricorsi contro decisioni degli organi della Confederazione in questioni di protezione dei dati e gravami contro le decisioni delle ultime istanze cantonali che si fondano sulle prescrizioni della protezione dei dati di diritto pubblico federale. Le decisioni della Commissione della protezione dei dati possono essere deferite al Tribunale federale.

Il dispositivo di protezione istituito dalla legge è inoltre rafforzato da *disposizioni penali.* Sono punibili la raccolta illegale di dati personali, come pure la comunicazione di dati personali segreti dei quali qualcuno è venuto a conoscenza nell'esercizio della professione. Infine è punibile anche il privato detentore di una collezione di dati che viola l'obbligo d'informazione nei confronti della persona interessata, non notifica una collezione che soggiace all'obbligo di registrazione o rifiuta di collaborare a un'inchiesta del Preposto alla protezione dei dati.

213.5 Protezione transfrontaliera dei dati

In contrapposizione al flusso d'informazioni tra amministrazione federale e Cantoni, lo scambio di dati dalla Svizzera all'estero deve essere disciplinato specificamente. Il diritto della protezione dei dati non può ignorare l'importanza considerevole dei flussi transfrontalieri d'informazioni. E se già è difficile nel diritto interno rispondere alle esigenze di protezione delle persone interessate, le difficoltà divengono quasi insormontabili quando si tratta di trattamenti di dati transfrontalieri, nel caso il legislatore non preveda particolari provvedimenti. Le misure di protezione dal canto loro devono avere una conformazione tale da non intralciare in principio la circolazione internazionale delle informazioni.

Per il flusso transfrontaliero di dati, il progetto prevede una disciplina articolata su tre aspetti. In primo luogo né gli organi pubblici né gli elaboratori privati hanno il diritto di comunicare informazioni all'estero, se con questo la personalità della persona interessata è minacciata in modo grave. Tale è il caso se dati delicati sono trasmessi a uno Stato sprovvisto di legislazione sulla protezione dei dati comparabile a quella svizzera. In secondo, gli organi della Confederazione devono sottostare alle regole generali sulla comunicazione quando trasmettono dati all'estero. Questo significa principalmente che i dati possono essere trasmessi all'estero soltanto se esiste una base giuridica o se il destinatario all'estero ha bisogno di tali dati per l'adempimento dei suoi compiti legali. Infine, gli elaboratori privati o pubblici che, all'insaputa delle persone interessate, comunicano all'estero dati, regolarmente o in gran numero, devono informarne il Preposto alla protezione dei dati, affinché questi, se del caso, possa attirare la loro attenzione sugli eventuali danni che essi causano alle persone interessate.

214 Protezione dei dati nella ricerca medica

La rivelazione del segreto professionale per scopi di ricerca medica deve poter avvenire non soltanto con l'approvazione della persona interessata, bensì anche grazie all'autorizzazione rilasciata da una Commissione peritale nominata dal Consiglio federale. La commissione può concedere l'autorizzazione soltanto se la ricerca non può essere eseguita con dati resi anonimi e se per il ricercatore è particolarmente difficile ottenere il consenso delle persone interessate. Ulteriore premessa dell'autorizzazione della commissione è inoltre il prevalere degli interessi della ricerca su quelli delle persone interessate – i pazienti – a vedere salvaguardate la segretezza dei loro dati. Sono con questo poste altre esigenze qualitative al progetto di ricerca, a favore del quale deve essere permessa la rivelazione del segreto professionale. In determinati casi, la procedura d'autorizzazione potrà tuttavia essere semplificata. La commissione peritale deve tra l'altro poter rilasciare a una clinica o a un istituto un'autorizzazione generale, ad esempio, per la ricerca interna, tesi di laurea in medicina o registri medici. Tali semplificazioni sono tuttavia possibili soltanto se nessun interesse degno di protezione della persona interessata è leso e se i dati personali delle persone interessate sono resi anonimi all'inizio del procedimento di ricerca. Indipen-

dentemente dall'autorizzazione della commissione, ogni persona interessata ha tuttavia anche la possibilità di vietare la comunicazione dei dati che la concernono.

La Commissione peritale è un'autorità federale indipendente. Essa è consigliata dal Preposto alla protezione dei dati. Questi vigila anche sul rispetto delle autorizzazioni. Il Preposto può impugnare la decisione della Commissione peritale davanti alla Commissione generale della protezione dei dati.

La prevista rivelazione del segreto professionale per scopi della ricerca medica esige in primo luogo la revisione del Codice penale (art. 321 CP). La protezione dei dati nella ricerca medica deve quindi essere disciplinata direttamente nel Codice penale e nella legge sulla protezione dei dati. Dovendo tenere conto dei risultati della procedura di consultazione abbiamo rinunciato a creare una legge speciale.

215 Revisione della legge sulla procedura penale federale e della legge sull'assistenza internazionale in materia penale

La procedura penale federale non soggiace alla legge sulla protezione dei dati. Con questo verrebbero però a mancare in ampia misura i principi per il trattamento dei dati anche per la procedura delle indagini preliminari della polizia giudiziaria. Tale lacuna dovrebbe ora essere colmata con la revisione della legge federale sulla procedura penale federale. Occorre a tale proposito trovare un equilibrio tra due interessi: l'esigenza della persona interessata a salvaguardare la propria sfera privata e gli interessi del perseguimento penale. È quindi prevista una regolamentazione speciale per le *riprese d'immagini* in caso di *manifestazioni pubbliche* da parte della polizia giudiziaria. Poiché i partecipanti a tali manifestazioni possono in principio appellarsi alla libertà di manifestare il pensiero, la polizia può fotografarli e filmarli soltanto se ci sono indicazioni che, in relazione alla manifestazione sono previsti crimini o delitti, la cui gravità o particolarità giustifichino tali misure. Sono inoltre disciplinati il *diritto d'accesso e di rettificazione* delle persone interessate a proposito dei dati contenuti negli atti della polizia giudiziaria, come pure la comunicazione ad altre autorità dei dati risultanti dalla procedura delle indagini. Se gli organi della polizia giudiziaria rifiutano l'informazione, l'interessato può fare intervenire il Preposto alla protezione dei dati che rilascia raccomandazioni all'indirizzo del Procuratore generale della Confederazione, in quanto responsabile della polizia giudiziaria. Se Procuratore generale e Preposto non si accordano, possono deferire la pratica alla Camera d'accusa del Tribunale federale. Questa soluzione è stata scelta poiché già attualmente la Camera d'accusa adempie un compito analogo in materia di ascolto telefonico.

Proponiamo infine le basi legali per la perquisizione, la visita medica e le misure d'identificazione. Queste ultime disposizioni non sono invero propriamente disposizioni sulla protezione dei dati: una regolamentazione anche di tali questioni s'impone tuttavia, considerato che la personalità delle persone interessate può da tali atti d'ufficio degli organi di polizia giudiziaria essere lesa alla stessa stregua di quanto lo è in ragione del trattamento dei dati.

La legge federale sull'assistenza internazionale in materia penale crea la premessa legale dello scambio d'informazioni tra il Ministero pubblico della Confederazione e l'Organizzazione internazionale di polizia criminale INTERPOL. La protezione dei dati in questo settore è retta in principio dagli statuti e dai regolamenti d'INTERPOL, nella misura in cui siano dal Consiglio federale dichiarati applicabili. Il Preposto alla protezione dei dati può consigliare i competenti servizi amministrativi sulle questioni relative alla protezione dei dati. Esso non ha tuttavia il diritto di portare una pratica davanti alla Commissione della protezione dei dati; è invece autorizzato nei casi nei quali INTERPOL trasmette informazioni di natura non criminale - come ad esempio nella ricerca di persone scomparse o nell'identificazione di persone sconosciute - a esercitare tutti i diritti che gli competono in base alla legge generale sulla protezione dei dati.

22 Commento del progetto

221 Legge generale sulla protezione dei dati

221.1 Sezione 1: Obiettivo, campo d'applicazione e definizioni

Articolo 1 Obiettivo

L'articolo 1 del progetto richiama i punti di riferimento e le fonti di tutto il diritto sulla protezione dei dati. Tra questi, in primo luogo, in materia di scambio d'informazioni tra privati la protezione della personalità e in materia di trattamento dei dati da parte delle autorità dello Stato, i diritti fondamentali, soprattutto il diritto costituzionale non scritto della libertà personale. Obiettivo della protezione dei dati è da un canto precisare l'importanza di questi beni giuridici e dall'altro proteggerli contro determinati tipi di trattamento dei dati. L'articolo sull'obiettivo della legge, in quanto norma direttrice per l'interpretazione delle singole disposizioni di protezione dei dati, intende quindi sottolineare la congiunzione con la protezione dei dati e con i diritti fondamentali.

Possono avanzare pretese sulla protezione dei dati ai sensi della presente legge sia le persone fisiche, sia le persone giuridiche. Secondo le regole della protezione della personalità del Codice civile, fanno parte delle persone giuridiche non soltanto le persone giuridiche del diritto privato e quelle del diritto pubblico della Confederazione e dei Cantoni, bensì anche le persone giuridiche straniere di diritto pubblico, se è loro riconosciuta la capacità giuridica. Non sono invece protetti, pure per analogia con il diritto della personalità, i gruppi di persone ai quali il diritto svizzero disconosce personalità giuridica. Le società di persone che, pure non godendo di personalità giuridica, hanno tuttavia capacità giuridica già in base al diritto vigente - come ad esempio le società in accomandita e le società collettive - possono esigere la protezione della legge. Questo non vale invece per i gruppi di persone che, secondo il diritto svizzero, non possiedono alcun elemento di personalità giuridica, quali gruppi etnici o società semplici a proposito dei quali vengono trattati dati. Si potrebbe invero immaginare che anche siffatti gruppi di persone abbiano un bisogno di protezione dei dati; la loro sottomissione alla legge sarebbe quindi per tale ragione

giustificata nell'ottica materiale. Contro una soluzione del genere si oppone tuttavia in ultima analisi il fatto che con la legge sulla protezione dei dati – concepita, nella parte afferente al diritto privato, come un complemento del Codice civile – non si vogliono creare, per determinati casi singoli, nuove forme di persone giuridiche. Nei casi del genere, ogni singolo appartenente al gruppo di persone deve far valere a proprio nome le pretese risultanti dalla protezione dei dati.

In sede d'approntamento del disegno e in special modo nella procedura di consultazione si era discusso a sapere se le persone giuridiche, nel settore del diritto privato, siano protette alla stessa stregua delle persone fisiche: si era posta anche la questione a sapere in quale misura le persone giuridiche possano far valere, nel settore del diritto pubblico – nel quale la protezione dei dati costituisce una concretizzazione dei diritti fondamentali –, una protezione corrispondente. Da più parti era stato richiesto che le persone giuridiche dovessero essere escluse dalla protezione della legge (come è il caso, ad esempio, nella Repubblica federale di Germania e in Francia), o che, almeno, fosse accordata loro una protezione attenuata. Tali esigenze furono motivate nel senso che, per le persone giuridiche con attività commerciale, sarebbe auspicabile una maggiore trasparenza, soprattutto allorquando si tratta di tutelare gli interessi dei creditori. In effetti le persone e le imprese che prendono parte alla lotta della concorrenza economica, sono esposte a un maggiore interesse del pubblico; anche devono accettare di essere oggetto di sorveglianza da parte degli altri concorrenti, più stretta di quella esercitata sulle persone private. Anche in materia di corporazioni o di aziende di diritto pubblico, un preponderante interesse pubblico alla pubblicità della loro attività può essere contrapposto a un eventuale interesse di segretezza. In considerazione di questi casi, sarebbe eventualmente giustificato non porre a disposizione delle persone giuridiche tutti i rimedi giuridici offerti dalla legge sulla protezione dei dati. Una (parziale) esclusione delle persone giuridiche dalla sfera di protezione offerta dalla legge sulla protezione dei dati sarebbe tuttavia stata la rottura con la tradizione giuridica svizzera. Già sulla base dell'articolo 53 del Codice civile le persone giuridiche sono in effetti protette contro i trattamenti illeciti d'informazioni, in particolare quando esse sono lese nell'onore o nella sfera privata (di particolare importanza nella concorrenza economica)[25]. Ma anche nel merito, la non sottomissione delle persone giuridiche darebbe risultati insoddisfacenti. Addirittura urtanti sarebbero poi le conseguenze per le piccole imprese, nelle quali spesso sui dati relativi alla persona giuridica s'innestano quelli concernenti le persone fisiche. D'altro canto anche le persone giuridiche con scopi non economici, quali partiti politici, organizzazioni caritative o chiese non avrebbero diritto a esigere la protezione dei dati. Ove si volessero tuttavia escludere dall'applicazione della legge soltanto le persone giuridiche attive nel campo economico, ciò avrebbe come conseguenza un trattamento di *privilegio delle persone fisiche* che operano nella concorrenza economica. Per questi motivi, la legge sulla protezione dei dati deve, nel settore privato, assicurare la *stessa protezione* alle persone fisiche e alle persone giuridiche. Occorre accordare a pieno alle persone giuridiche la protezione dei dati nei confronti del trattamento dei dati da parte delle autorità, nonostante per la dottrina dominante le persone giuridiche non pos-

sano invocare tutti i diritti fondamentali rilevanti per la protezione dei dati nel settore pubblico, in particolare non la libertà personale[26]. Poiché però in materia di protezione dei dati, persone fisiche e persone giuridiche hanno bisogno di protezione molto analoghi, una persona giuridica deve, in relazione al trattamento dei dati, potersi appellare anche alla libertà personale. E poiché altre massime di diritto costituzionale, determinanti in materia di protezione dei dati, quali il principio della legalità e della proporzionalità proteggono incontestabilmente anche le persone giuridiche, non s'impone, neppure nel settore pubblico, una disciplina differenziata per le persone fisiche e le persone giuridiche.

Per contro, il progetto di legge non si applica alle organizzazioni internazionali. In quanto soggetti del diritto internazionale pubblico, esse non possono senz'altro venire sottoposte al diritto interno. La regolamentazione di protezione dei dati nel caso di tali organizzazioni deve essere prevista nei relativi accordi di sede. Lo stesso vale anche per il Comitato internazionale della Croce Rossa (CICR). Nonostante il CICR sia un'associazione ai sensi del Codice civile, in pratica esso è considerato sempre più un soggetto di diritto internazionale ed equiparato alle organizzazioni internazionali[27]. Questa pratica risulta adeguata anche nell'ottica della legislazione sulla protezione dei dati. Il CICR può in effetti adempiere il suo compito soltanto se la sua attività non è controllata da un'autorità statale e neppure da un Preposto alla protezione dei dati ai sensi della presente legge. Il CICR stesso ha sottoposto la propria agenzia centrale di ricerca a severe regole interne di protezione dei dati.

Articolo 2 Campo d'applicazione

Secondo il *capoverso 1,* la legge impone obblighi a due categorie di elaboratori di dati, vale a dire alle cosiddette persone private e agli organi federali. *Persone private* (lett. a) sono quelle che trattano i dati nel quadro di un rapporto regolato dal diritto privato. La categoria degli *organi federali* (lett. b), comprende in primo luogo tutte le unità amministrative della Confederazione che trattano in maniera indipendente un determinato settore di compiti, ma anche persone alle quali sono affidati compiti pubblici (cfr. art. 3 lett. c e d e relative esplicazioni).

La questione a sapere se colui che tratta i dati debba essere considerato persona privata o organo pubblico non sarà, nel caso concreto, sempre di facile risposta. Criterio determinante è la natura giuridica dell'attività alla base del trattamento: prevalentemente improntata sul diritto pubblico o sul diritto privato. Aziende indipendenti come l'INSAI, ma anche le casse di compensazione delle assicurazioni private che adempiono compiti in materia d'assicurazione per la vecchiaia e i superstiti e d'assicurazione contro la disoccupazione, sono organi federali poiché la loro attività è in ampia misura disciplinata dal diritto amministrativo federale. Più difficile da valutare è la situazione delle casse malati. Nella misura in cui queste sono sottoposte alla legge sull'assicurazione contro le malattie, sono riconosciute dalla Confederazione e possono decidere autonomamente, sono esse pure esecutrici di compiti pubblici della Confederazione e soggiacciono quindi alle prescrizioni valide per gli organi federali. La distinzione è importante, considerato che per gli organi pubblici valgono regole di protezione dei dati più severe e più dettagliate che non per le persone private.

Il *capoverso 2* prevede diverse limitazioni del campo d'applicazione:

Lettera a: Trattamento per uso esclusivamente personale

Gli obblighi legali che occorre osservare da parte di chi tratta i dati, come pure i diritti delle persone interessate, devono trovare un limite nel ristretto ambito della persona stessa che tratta i dati. Là dove una *persona fisica* tratta dati per uso *esclusivamente personale,* la legge sulla protezione dei dati non può comunque trovare applicazione. L'idea che l'uso personale privato di un dato debba essere rispettato appare del resto anche nella legislazione sul diritto d'autore[28]. Per uso esclusivamente personale si intende soprattutto l'utilizzazione di informazioni nella ristretta cerchia privata e familiare. Nessuno deve, per esempio, essere obbligato a permettere la consultazione della sua agenda personale. Devono pure restare sottratte alla legge sulla protezione dei dati colloqui privati nella cerchia dei familiari e degli amici, raccolte private di lettere e analoghe. Anche le note che una persona fa durante l'esercizio della professione, ma unicamente per scopo personale a titolo di promemoria o di aiuto per il proprio lavoro, non cadono nel campo d'applicazione della legge. Ove nell'ambito del trattamento dei dati per uso personale dovessero ugualmente aversi lesioni della personalità - ad esempio se una lettera personale andata perduta, giunge a conoscenza di terzi - la persona lesa può tuttavia far valere le pretese legali risultanti dalla protezione generale della personalità, prevista dall'articolo 28 CC. Spetta del resto alla giurisprudenza vegliare affinché chi tratta i dati non si appelli abusivamente alla presente disposizione per sottrarsi, in particolare, all'obbligo che gli incombe di informare.

Lettera b: Eccezione a favore dei mezzi di comunicazione sociale

Con la revisione dell'articolo 28 del Codice civile del 16 dicembre 1983, la protezione della personalità nei rapporti dei mezzi di comunicazione sociale è stata migliorata in modo molto rilevante. Nella misura in cui le informazioni sono pubblicate nei mezzi di comunicazione sociale di carattere periodico quali la stampa, la radio, la televisione, la persona lesa può, sulla base dell'articolo 28*g* e seguenti del Codice civile, esercitare il diritto di risposta. Questo mezzo di difesa specificamente improntato sulle particolarità di una violazione della personalità, causata da un mezzo di comunicazione sociale, non deve anche essere completato con disposizioni generali di protezione dei dati; la legge non deve quindi trovare applicazione in questo settore. Le disposizioni della legge valgono invece per i mezzi di comunicazione sociale di carattere periodico fintanto che *non è ancora avvenuta la pubblicazione dei dati.* Per i trattamenti dei dati in questa *fase antecedente alla pubblicazione,* il progetto prevede tuttavia determinante facilitazioni (cfr. a tal proposito art. 10 cpv. 2 lett. d).

Lettera c: Assemblea federale

Sono pure eccettuati dal campo d'applicazione della legge sulla protezione dei dati gli *affari dell'Assemblea federale.* Il Parlamento non sarebbe più in grado di esercitare adeguatamente la vigilanza, prevista dal diritto costituzionale, sull'amministrazione e sui tribunali (art. 85 n. 11 Cost.), se, in ogni caso, dovesse conformarsi ai principi della protezione dei dati, in particolare alla disposizione concernente la comunicazione dei dati personali. Si aggiunga poi che per i

dibattiti delle Camere federali vale per Costituzione il principio dell'ufficialità (art. 94 Cost.). La legge sui rapporti tra i Consigli e i regolamenti dei due Consigli, come pure i regolamenti delle Commissioni, inoltre, contengono disposizioni in parte molto dettagliate sul trattamento delle informazioni del Parlamento nella procedura legislativa preliminare[29]. Le commissioni di gestione delle Camere federali hanno diritto, sulla base dell'articolo 47quater della legge sui rapporti tra i Consigli (RS *171.11*), di chiedere informazioni necessarie a tutte le autorità e a tutti i servizi, indipendentemente dal segreto di funzione. Il Consiglio federale, tuttavia, può in luogo della produzione dei documenti ufficiali, presentare un rapporto speciale, tra l'altro onde tutelare interessi degni d'essere protetti. L'applicabilità della legge sulla protezione dei dati anche a questo settore sfocerebbe in situazioni problematiche, poiché non sarebbe sempre chiaro quale atto legislativo sia da applicare. La clausola d'eccezione si riferisce a tutta l'attività parlamentare e si estende anche ai Servizi del Parlamento, nella misura in cui essi siano direttamente attivi per il Parlamento. Trattamenti di dati che non sono in relazione diretta con il Parlamento, quali ad esempio la tenuta degli atti personali dei collaboratori di tali Servizi, devono tuttavia soggiacere alla legge.

Contrariamente al progetto del 1983, il campo d'applicazione della presente legge si estende alle *attività governative del Consiglio federale.* Anche il Consiglio federale dovrà quindi rispettare i principi della presente legge. I dibattiti del Consiglio federale resteranno tuttavia segreti come nel passato, affinché questi possa trattare gli affari di governo con la necessaria imparzialità. A tale unico scopo non è però necessario escludere il Consiglio federale dal campo d'applicazione della legge sulla protezione dei dati, poiché l'articolo 13 della legge federale sull'organizzazione dell'amministrazione già prevede che le deliberazioni del Consiglio federale non sono pubbliche. Questa disposizione dev'essere interpretata nel senso che anche una persona interessata, analogamente a quanto avviene per i dibattiti di molti tribunali, non ha diritto d'accesso alle deliberazioni del Consiglio federale. In quanto norma speciale, essa sopravvanza la legge sulla protezione dei dati. Si tratta di una restrizione legale del diritto d'accesso ai sensi dell'articolo 6 della presente legge. L'articolo 24 capoverso 1 della legge stipula del resto che il Consiglio federale non soggiace alla sorveglianza del Preposto alla protezione dei dati.

Lettera d: Procedura giurisdizionale

Le procedure giurisdizionali seguono regole precise, fissate nelle leggi di procedura. Lo scopo delle diverse disposizioni procedurali è la protezione della personalità delle persone implicate nella procedura. Ciò vale soprattutto per le disposizioni sul diritto d'essere inteso, sul diritto di consultazione degli atti e sul diritto di partecipare al rilevamento delle prove. Le leggi di procedura contengono anche disposizioni sul trattamento delle informazioni, ad esempio là dove fissano come il materiale per la procedura debba essere raccolto e valutato. Le leggi di procedura ponderano anche l'interesse del giudice e delle parti a ottenere un'informazione, contrapposto all'interesse del mantenimento del segreto della persona che potrebbe fornire i dati, così ad esempio per quanto concerne le regole sul rifiuto di testimoniare. In questo senso il diritto procedurale è an-

che sempre diritto sulla protezione dei dati. Se la legge sulla protezione dei dati dovesse applicarsi anche alle procedure giurisdizionali, si sarebbe in presenza di due leggi con, in parte, uguale obiettivo. Questa dualità potrebbe tuttavia portare a insicurezze giuridiche, causare problemi di coordinazione e, infine, ritardi procedurali. La clausola d'eccezione di questo capoverso intende evitare tutto questo.

Sono eccettuate dall'applicazione della legge anche le procedure davanti al Tribunale federale e davanti alle commissioni federali di ricorso e d'arbitrato, indipendentemente dal fatto che si tratti di procedure di prima istanza o di procedure ricorsuali. La clausola d'eccezione vale però soltanto per il periodo durante il quale una procedura è *pendente*. La legge è quindi applicabile a qualsiasi trattamento di dati posteriore alla chiusura della procedura, quando si tratta di conservazione o di distruzione di dati, come pure della loro comunicazione a terzi. Anche i trattamenti dei dati da parte dei *servizi amministrativi dei tribunali (ad es. delle cancellerie) soggiacciono alla presente legge.*

Lettera e: Procedure penali

L'eccezione dell'applicazione della legge sulla protezione dei dati, relativa alle procedure penali risponde agli stessi motivi di quella concernente le procedure giurisdizionali davanti alle autorità giudiziarie (lett. d). Per procedura penale si intendono le cause secondo la procedura penale federale, la procedura penale amministrativa e la procedura penale militare. Queste procedure non vengono menzionate alla lettera d (procedure giurisdizionali), poiché vi sono contenute anche disposizioni sulla procedura delle indagini preliminari. Il procuratore generale della Confederazione che dirige le indagini della polizia giudiziaria è invero un organo giurisdizionale; vista la sua appartenenza al potere esecutivo, il Ministero pubblico della Confederazione è però un'autorità amministrativa. Sotto la clausola d'eccezione cadono anche le autorizzazioni date dal Dipartimento federale di giustizia e polizia sull'apertura di un perseguimento penale contro funzionari ai sensi dell'articolo 15 della legge federale sulla responsabilità (RS *170.32*).

Lettera f: Procedure d'assistenza giudiziaria internazionale in materia civile e penale

La legge sulla protezione dei dati non si applicherà neppure alle procedure d'assistenza giudiziaria internazionale in materia civile e penale. Il motivo è da ricercare nel fatto che il punto di partenza di una domanda d'assistenza giudiziaria è sempre una procedura giurisdizionale o penale e che la legge sull'assistenza giudiziaria in materia penale contiene da parte sua determinate disposizioni sulla protezione della personalità (cfr. a questo proposito più dettagliato il n. 224). L'assistenza giudiziaria in materia civile è inoltre in ampia misura di competenza dei tribunali cantonali; la Confederazione (Ufficio federale di polizia) ha in questo campo soltanto funzione di mediatore.

Lettera g: Procedure ricorsuali in materia di diritto pubblico e di diritto amministrativo

Le procedure di ricorso amministrativo sono procedure giurisdizionali dell'*amministrazione federale e del Consiglio federale.* Esse sono regolate dettagliata-

mente nella legge amministrativa (RS *172.021*), ed è per questa ragione che la legge sulla protezione dei dati non trova applicazione neppure in questa materia. La clausola d'eccezione vale tuttavia soltanto per la *procedura amministrativa di seconda istanza*. Se anche l'attività amministrativa di prima istanza ai sensi della legge sulla procedura amministrativa dovesse non essere sottoposta alla legge sula protezione dei dati, sarebbe dato il pericolo che in ampi settori dell'attività amministrativa non esisterebbero garanzia di protezione dei dati per le persone interessate. La legge sulla procedura amministrativa trova in effetti applicazione in tutte le cause amministrative che vengono liquidate con una decisione. Poiché la maggior parte delle attività d'ordine amministrativo possono sfociare in una decisione, gli organi della Confederazione potrebbero troppo facilmente sottrarsi agli obblighi che incombono loro in virtù della legge sulla protezione dei dati. Per ragioni analoghe sono sottratte dall'applicazione della legge sulla protezione dei dati i rari casi di un ricorso di diritto pubblico al Consiglio federale (art. 73 della legge sulla procedura amministrativa).

Lettera h: Registri pubblici

L'esclusione dei registri pubblici relativi ai rapporti giuridici di diritto privato risponde a considerazioni analoghe a quelle che hanno improntato l'esclusione delle procedure giurisdizionali pendenti. L'eccezione introdotta dalla lettera h concerne il registro fondiario, i registri dello stato civile, i registri dei regimi matrimoniali, il registro di commercio, il registro dei natanti, il registro delle aeronavi, i registri concernenti l'esecuzione e il fallimento, il registro delle riserve di proprietà, come pure i registri dei brevetti d'invenzione della protezione delle varietà vegetali, delle marche, dei disegni e dei modelli industriali. Questi registri sono effettivamente «sistemi d'informazione» tenuti e garantiti dallo Stato; essi contengono determinati dati sulla costituzione, lo stato, la modificazione e l'esercizio dei diritti privati. Il trattamento dei dati nell'ambito di questi registri si svolge per lo più secondo prescrizioni formali molto dettagliate. Quest'ultime, pure per motivi in ordine alla sicurezza del diritto, non devono venire modificate dalla legge sulla protezione dei dati.

Oltre ai casi enunciati nelle lettere c-h, esistono in molti altri atti legislativi, pure disposizioni specifiche sul trattamento dei dati e sulla protezione dei dati. Se queste regole sono in contrasto con la legge sulla protezione dei dati, chi applica il diritto dovrà decidere come debba essere risolto tale conflitto. Egli dovrà procedere secondo le regole generali d'interpretazione. In generale questo significherà la supremazia della legge sulla protezione dei dati su altre prescrizioni relative al trattamento dei dati, poiché, in quanto legge generale, contiene norme che valgono in principio per tutte le attività d'informazione private e pubbliche. Se però il diritto speciale contiene norme più severe di protezione dei dati oppure una concezione completa sulla protezione dei dati, queste ultime disposizioni prevarranno su quelle della legge generale sulla protezione dei dati.

Articolo 3 Nozioni

Lettera a: Dati personali

Dati personali (dati) sono tutte le informazioni relative a una persona fisica o giuridica identificata o identificabile. I dati personali possono prendere forma

di parola, immagine o segno. Una persona è identificata se dai dati risulta che essi si riferiscono a questa persona e unicamente a questa persona (ad es. un documento d'identità). *Identificabile* è la persona che in effetti non identificata in modo univoco grazie ai dati, lo è tuttavia in base alle circostanze, vale a dire al contesto di un'informazione (ad es. se a partire dai dati concernenti beni immobiliari è possibile risalire al proprietario). Per l'identificazione non basta tuttavia una qualsiasi possibilità teorica. Se l'identificazione delle persone interessate richiede mezzi tali che, secondo l'esperienza generale della vita non si può prevedere che un interessato vorrà farsene carico (ad es., perché dovrebbe procedere a un'analisi complessa di una statistica) non si può parlare di possibilità d'identificazione[30].

Lettera b: Persone interessate

La persona interessata è una persona i cui dati sono trattati. Le persone interessate sono coloro per la cui protezione dev'essere creata la legge. Persona interessata può essere ogni persona fisica e ogni persona giuridica del diritto privato e del diritto pubblico (cfr. a questo proposito il nostro commento dell'art. 1).

Lettera c: Persone private

Sono persone private ai sensi della legge presente in primo luogo le persone fisiche e giuridiche del diritto privato che trattano dati. Sono tuttavia considerate persone private anche le persone del diritto pubblico in quanto agiscano entro l'ambito del diritto privato.

Per quanto concerne gli organi ancorati nel diritto privato occorre chiedersi se il loro statuto giuridico è, per l'aspetto materiale, da ascrivere al diritto privato o al diritto pubblico. Se l'organo in questione è essenzialmente considerato d'assetto pubblico, il responsabile soggiace non alla parte di diritto privato della legge sulla protezione dei dati, bensì al diritto cantonale di protezione dei dati eventualmente esistente. Questa considerazione vale in particolare per il tutore. I suoi compiti sono invero disciplinati dal Codice civile, in modo che, in accordo con la giurisprudenza del Tribunale federale[31], egli potrebbe anche essere considerato come persona privata. Poiché tuttavia il suo rapporto con il pupillo è essenzialmente un atto d'autorità, e considerato che egli soggiace a una sorveglianza statale e che i suoi atti possono essere impugnati con ricorso, il tutore dev'essere considerato un organo pubblico nell'ottica della legge sulla protezione dei dati[32]. Ne consegue che il tutore deve essere sottoposto al diritto della protezione dei dati del Cantone che determina il suo statuto giuridico. La Confederazione, basandosi sulla sua competenza di diritto privato potrebbe certo disciplinare la protezione dei dati in maniera uniforme per la materia relativa alla tutela. L'opportunità di una tale revisione sarà tuttavia esaminata nel quadro della revisione del diritto sulla tutela.

Lettera d: Organi federali

Sono considerati organi federali in primo luogo i Dipartimenti e gli Uffici federali, come pure le loro divisioni e sezioni. Sono inoltre considerati tali le aziende e le regìe federali (in particolare le FFS e le PTT), come pure i comandi militari. Organi federali sono tuttavia anche tutte le persone fisiche e giuridi-

che, in primo luogo le organizzazioni economiche e le corporazioni di diritto pubblico che, nell'adempimento dei compiti pubblici, trattano dati per la Confederazione. Gli organi dei Cantoni e dei Comuni non sono per contro, secondo il diritto pubblico svizzero, organi della Confederazione, anche se eseguono compiti federali.

Lettera e: Dati degni di particolare protezione

Dipende non soltanto dallo scopo, dalla portata e dal tipo del trattamento, bensì anche dalla qualità delle informazioni elaborate, se il trattamento dei dati possa ledere la personalità e i diritti fondamentali di una persona. Vi sono certi dati che come tali hanno importanti ripercussioni sulla personalità della persona interessata, soprattutto se tali dati provengono dalla sfera intima o dalla vita privata, oppure se possono influire in modo rilevante sulla reputazione e sul credito sociale di una persona. Il progetto di legge prevede quindi per questi tipi di dati in parte prescrizioni speciali (cfr. art. 7 cpv. 2, 9 cpv. 2, 14 cpv. 2, 16 cpv. 1, 29).

Il *numero 1* comprende non soltanto le opinioni e le attività religiose, filosofiche, politiche e sindacali ma bensì anche l'appartenenza alle relative associazioni. Il *numero 2* elenca tra i dati degni di particolare protezione le informazioni concernenti la salute, la sfera intima o l'appartenenza a una razza. Con l'uso del termine di «*salute*». il cerchio dei dati degni di particolare protezione viene qualche po' ristretto per rapporto a quello che figurava nel disegno di legge inviato in procedura di consultazione nel 1983, secondo il quale ogni dato sullo *stato fisico* sarebbe stato degno di particolare protezione. Lo «stato fisico» avrebbe, ad esempio, compreso anche l'altezza e il colore dei capelli e degli occhi, mentre con la nozione più ristretta di «salute», del presente disegno, si intendono tutte le informazioni d'ordine medico che possono dare un'immagine negativa della persona interessata. La sfera intima dev'essere intesa nel senso della «sphère intime» francese (ted. Intimsphäre); essa comprende i dati che una persona comunica soltanto a poche persone scelte e che sono per lei di grande importanza emozionale. La sfera intima va ben oltre il senso tedesco di vita sessuale, senza tuttavia estendersi anche alla situazione finanziaria. L'inclusione dell'*appartenenza alla razza* nella cerchia dei dati degni di particolare protezione è avvenuta soprattutto in considerazione della Convenzione del Consiglio d'Europa, rispettivamente in vista dello scambio internazionale di dati. Con le *misure d'ordine sociale* menzionate nel *numero 3* sono intese prestazioni dell'assicurazione sociale in rapporto a malattie o incidenti, come pure misure quali la tutela e l'assistenza sociale. Infine tra i *procedimenti e le sanzioni amministrative e penali del numero 4,* oltre ai procedimenti e alle sanzioni penali secondo il diritto penale comune, sono da intendere anche i procedimenti e le sanzioni secondo le procedure disciplinari, le procedure di ritiro del permesso di circolare e misure d'esecuzione delle pene.

Di regola, i numeri da 1 a 3 concernono soltanto le persone fisiche. Un'eccezione è costituita ad esempio dal dato concernente le società con scopi ideali che esercitano un'attività economica accessoria o persone giuridiche che sono state condannate penalmente[33)].

L'enumerazione dei dati degni di particolare protezione è completa.

Lettera f: Profilo della personalità

La costituzione, la valutazione e la comunicazione a terzi di profili della personalità richiedono una protezione speciale. Il profilo della personalità è l'insieme di un numero rilevante di dati sulla struttura della personalità, sulle conoscenze e attività professionali e sulle attività extraprofessionali, dai quali risulta un'*immagine globale* o un'*immagine parziale importante* dell'interessato. Profili della personalità possono ad esempio essere elaborati in occasione di controlli di sicurezza o di procedure del personale. Anche collezioni di dati sulle abitudini d'acquisto o sulle qualifiche scolastiche o professionali sono adeguate a fornire almeno un'immagine parziale dell'interessato. Determinante è il fatto che con la raccolta sistematica di dati di per sé non degni di particolare protezione (ad es. sulle abitudini di lettura, di viaggio, sulle attività del tempo libero) possa essere dato l'accesso ad aspetti segreti di una personalità, ad esempio, della sua visione del mondo. Attraverso le possibilità di valutazione dell'elaborazione automatica dei dati e l'interconnessione di banche di dati automatizzate, la stesura di profili della personalità è divenuta più facile e più rapida. Gli interessati spesso non hanno conoscenza dell'esistenza di un profilo e non sono quindi in grado di controllarne l'esattezza e l'utilizzazione. Una volta compilati, i profili della personalità possono però privare gli interessati della libertà di fornire essi stessi l'immagine da loro auspicata. I profili della personalità possono quindi pregiudicare in modo determinante lo sviluppo della personalità. Per tale ragione, esattamente come avviene per i dati degni di particolare protezione, i profili della personalità dovranno poter essere compilati e trattati soltanto a determinate condizioni.

Lettera g e h: Trattamento e comunicazione

La nozione di trattamento è molto ampia: essa comprende *ogni operazione* relativa ai *dati,* in particolare *ognuna delle fasi del trattamento.* Essa ingloba persino la semplice conservazione o archiviazione dei dati, poiché anche in questo stadio del trattamento, ad esempio, in ragione di lacune nella sicurezza dei dati, sono ancora possibili lesioni della personalità. Nella misura in cui tuttavia gli atti sono archiviati nell'Archivio federale, possono per gli stessi essere previsti regolamenti speciali (cfr. art. 30 cpv. 2). La lettera h definisce la *comunicazione* dei dati come forma speciale di trattamento, poiché si tratta senz'altro della fase più delicata del trattamento e considerato che la comunicazione può avvenire in forme molteplici. Comunica dati chi concede di consultare gli atti, ad esempio con l'accesso a una collezione di dati per mezzo di un collegamento in linea, chi lascia copiare nastri magnetici o, semplicemente trasmette dati estratti da una collezione di dati. Il disegno prevede per la comunicazione prescrizioni suppletive (cfr. art. 7 cpv. 2 lett. b, 8, 16). Là dove accenna unicamente al trattamento, la comunicazione è pure sempre compresa. La nozione di trattamento è usata del resto non soltanto per l'elaborazione automatica, bensì anche per l'elaborazione manuale dei dati, come pure per tutte le forme intermedie.

Lettera i: Collezione di dati

Nelle collezioni di dati si concentrano di regola i dati personali trattati e nelle collezioni di dati essi sono per lo più conservati a lungo termine. All'esistenza

di una collezione di dati sono per questo vincolate due disposizioni specifiche di tutela del diritto di protezione dei dati, il diritto d'accesso e l'obbligo di registrare (art. 5 e 7).

Una collezione di dati ai sensi della legge è un complesso di dati che fa riferimento a più di una persona. Essa può essere organizzata e strutturata nel più diverso dei modi. Determinante in merito alla protezione dei dati è il fatto che i dati concernenti una determinata persona siano reperibili. Nelle collezioni di dati tenute automaticamente, con le loro molteplici possibilità di interrogazione, tale è quasi sempre il caso, indipendentemente dal fatto che i nomi delle persone siano previsti o meno come vere e proprie chiavi d'accesso. Nelle categorie di collezioni di dati personali tenute manualmente, cadono sotto la nozione di collezione di dati non soltanto gli schedari e le collezioni ordinati per persona, bensì anche i registri, l'accesso ai quali è possibile soltanto per mezzo di un indice di ricerca. Per contro, non sono considerati collezioni di dati i registri nei quali possono essere in effetti rinvenuti ancora dati personali, tuttavia soltanto con un dispendio disproporzionato. Tale è il caso ad esempio dei milioni di dichiarazioni doganali che sono conservate per un certo tempo presso tutti gli uffici doganali della Svizzera, ma che non sono classificate nominalmente.

Lettera k: Detentore della collezione di dati

La nozione definisce una persona fisica o una persona giuridica o un organo federale che nell'ottica del diritto sulla protezione dei dati sono responsabili del trattamento dei dati personali di una collezione di dati e che sottostanno in particolare all'obbligo d'informare e di dichiarare la collezione dei dati. Detentore della collezione di dati è chi, senza disporre necessariamente di persona dei singoli dati, fissa l'obiettivo, i mezzi e i metodi di trattamento (ad es. hardware e software).

La legge designa nel *settore del diritto privato* accanto alle persone fisiche anche le persone giuridiche quali detentori di collezioni di dati, fra queste anche grandi imprese fortemente strutturate. In quest'ultimo caso non sarà sempre facile rilevare chi sia il detentore *effettivo*. Le grandi imprese devono per questa ragione garantire che la persona interessata sia sempre in grado di ottenere informazioni su tutti i dati memorizzati su di lei. Per ragioni pratiche tuttavia, esse dovranno in parte interessarsi per sapere se il richiedente intenda limitarsi a una determinata filiale, oppure a un determinato settore dell'azienda. Per quanto attiene agli organi della Confederazione il problema non si pone negli stessi termini, poiché questi sono obbligati a far registrare tutte le collezioni di dati. In occasione della notificazione per la registrazione essi possono anche comunicare a chi una persona interessata debba rivolgere la sua richiesta d'informazione. Lo stesso vale anche per le collezioni di dati del diritto privato in merito alle quali è dato l'obbligo di registrazione.

Se qualcuno fa trattare dati da un terzo, quale detentore della collezione di dati entra in considerazione il mandante, come pure il terzo. È determinante chi dei due possa in ultima istanza assumere la responsabilità del trattamento dei dati. Tale è di regola colui che appronta i dati. Se il compito di un centro di calcolo si limita a mettere a disposizione l'infrastruttura tecnica che permette di far subire a un complesso precostituito di dati un trattamento preciso, il mandante

resta allora detentore della collezione di dati. Tale è il caso del medico che affida la gestione degli onorari a un servizio d'incasso. L'istituto che, su mandato, procede a studi di mercato per il producente di un prodotto, resterà invece responsabile dei dati raccolti. Lo stesso vale per l'investigatore privato che ha il mandato di raccogliere informazioni su una determinata persona, poiché il mandante stesso non dispone dei dati.

Lettera l: Partecipanti alla collezione di dati

Partecipanti alla collezione di dati sono le persone e gli organi della Confederazione che in effetti non possono decidere in merito allo scopo o alla struttura della collezione di dati, ma che hanno però il diritto di trattare autonomamente singoli dati della collezione. Quale esempio sia menzionato il Registro centrale degli stranieri, la cui responsabilità è portata dall'Ufficio federale di polizia, ma i cui dati possono tuttavia essere modificati a volontà dai diversi servizi di controllo degli abitanti e di polizia degli stranieri, servizi che dispongono tutti di un collegamento in linea diretta con il Registro. Dalla categoria dei partecipanti occorre distinguere quella dei *destinatari dei dati* che prendono unicamente conoscenza dei dati e che non possono per contro modificare o cancellare i dati.

221.2 Sezione 2: Disposizioni generali di protezione dei dati

Articolo 4 Principi

L'articolo 4 definisce succintamente i principi fondamentali materiali della protezione dei dati; si tratta delle vere e proprie idee direttrici della legge. L'articolo vale sia per l'elaboratore privato di dati, sia per l'elaboratore pubblico dei dati. Ogni persona che *tratta i dati a titolo privato* violando i principi senza poter fare valere un giusto motivo commette una violazione della personalità (cfr. art. 9 cpv. 2 lett. a). I principi fondamentali precisano quindi a quali condizioni un trattamento effettuato da una persona privata viola la personalità. Per gli *organi pubblici,* l'efficacia dei principi è ancora più diretta; essi costituiscono in effetti norme di comportamento direttamente applicabili, la cui violazione la persona interessata può censurare sulla via ricorsuale.

Capoverso 1: Modalità di raccolta dei dati

Coloro che trattano i dati a titolo privato o gli organi della Confederazione possono rilevare dati se ciò è previsto da un trattato di diritto internazionale pubblico, da una legge, da un decreto federale di portata generale o se del caso da un'ordinanza. Nel settore privato la raccolta dei dati personali non è altrimenti definita. In questo campo, accanto alle norme generali che si oppongono alla raccolta e che possono se del caso trovare applicazione, riveste importanza particolare il principio giusta il quale i dati devono essere trattati secondo la buona fede, I dati non devono essere raccolti all'insaputa della persona interessata o contro la sua volontà. Colui che raccoglie dati ingannando intenzionalmente (cfr. art. 28 CO) la persona interessata, ad esempio presentandosi sotto mentite spoglie o fornendo false indicazioni in merito allo scopo del trattamento, agisce contro il principio della buona fede. Viola il principio della

buona fede, sempre che non adempia già i limiti di una fattispecie penale, anche la *raccolta clandestina* di dati, ad esempio, chi ascolta le conversazioni o spia le persone interessate[34)], oppure manipola i programmi di un sistema di comunicazione interattivo (videotex). Chiaramente illecita, poiché avviene in violazione di norme del Codice penale, è poi la raccolta di dati che avvenga con la forza, l'astuzia o la minaccia nei confronti della persona interessata.

Per gli organi della Confederazione, nella quarta sezione della presente legge si fissa ancora che il rilevamento dei dati deve in principio essere riconoscibile per la persona interessata (art. 15).

Capoverso 2: Esattezza dei dati

Il trattamento di dati inesatti può arrecare grave pregiudizio alla persona colpita. Errori minimi possono già causare danni rilevanti. Se ad esempio qualcuno è ingiustamente perseguito da un ufficio d'incasso poiché abita nella stessa strada di una persona che porta lo stesso nome, ma il servizio incassi ha notato il numero civico errato, allora questi ne risentirà le conseguenze del tutto sgradite. Esattezza ai sensi della presente legge non significa tuttavia solo che i dati non possono contenere affermazioni inesatte, bensì anche che, nella misura permessa dalle circostanze, essi devono essere aggiornati e completi. Va senza detto che un capo del personale che, ad esempio, rimuova o congedi un lavoratore sulla base di un certificato medico superato può ledere la personalità di quest'ultimo. La valutazione del credito di una persona può inoltre essere falsata se i documenti prodotti a tale scopo, mettono in evidenza il fatto che la persona è effettivamente stata condannata al pagamento di alimenti sulla base di una sentenza di divorzio, senza poi rilevare che l'obbligo di versamento degli alimenti della persona interessata è estinto in ragione del nuovo vincolo coniugale stretto dal coniuge anteriore. Questi esempi mostrano come la questione a sapere se un dato sia esatto non è astratta, ma che però può trovare risposta soltanto nel caso d'applicazione pratica.

Capoverso 3: Proporzionalità del trattamento

Con l'obbligo di rispettare la proporzionalità sancito in questo capoverso, il principio della proporzionalità che comunque vige nel settore del diritto pubblico viene dichiarato applicabile anche al settore del diritto privato. In conseguenza, chiunque tratta i dati è obbligato a raccogliere e a trattare soltanto i dati che sono necessari per un determinato scopo e che gli sono effettivamente necessari, Chi ad esempio ha un'agenzia di autonoleggio ha il diritto di rilevare l'identità e l'indirizzo del noleggiatore; sarebbe tuttavia eccessivo esigere ulteriori informazioni sullo stato familiare o sui rapporti dello stesso con altre terze persone. Queste informazioni possono per contro essere indispensabili in merito alla situazione patrimoniale e alla valutazione del credito di una persona. Resta che, anche in questo caso, sarebbe esagerato fornire le informazioni sull'appartenenza religiosa o sull'atteggiamento politico della persona interessata.

Inoltre occorre procedere a una ponderazione adeguata degli interessi, tra lo scopo del trattamento e il necessario pregiudizio causato per questo fatto alla personalità. Non si giustifica in effetti in vista di una battaglia elettorale, svelare a fondo e sistematicamente la vita privata di un avversario politico.

Capoverso 4: Modificazione dello scopo iniziale

Visto che i moderni sistemi d'informazione hanno fortemente aumentato le possibilità multifunzionali di utilizzare e di comunicare i dati, è molto aumentato il pericolo che i dati siano utilizzati per scopi diversi da quello previsto in origine. Il principio della buona fede nei negozi giuridici esige tuttavia che le persone interessate dal trattamento delle informazioni abbiano a sapere a quale scopo sono trattati i dati che le concernono. In molti casi esse non forniscono senza condizioni i loro dati, bensì in vista di un determinato scopo di trattamento e probabilmente per quello soltanto. Per tale ragione i dati devono essere in principio usati soltanto per lo scopo denunciato al momento della raccolta oppure per quello che risulta dalle circostanze. Ciò significa ad esempio che gli indirizzi raccolti in relazione a un'iniziativa non abbiano in seguito ad essere usati dal proponenti per usi commerciali, quali l'invio di materiale pubblicitario. E neppure sarebbe ammissibile che i servizi del personale dell'amministrazione federale comunicassero a organizzazioni di vendita gli indirizzi dei funzionari federali che dispongono di un determinato reddito. Sarebbe anche inaccettabile che i dati registrati nel sistema Videotex venissero analizzati sistematicamente per acquisire un'opinione sulle abitudini d'acquisto e su altri interessi di una determinata persona.

È tuttavia possibile modificare lo scopo iniziale se *lo prevede una norma giuridica.* Un'autorità può ad esempio essere da una disposizione legale autorizzata ad accedere alle informazioni detenute da un'altra autorità. Questa eccezione appare giustificata poiché, in primo luogo esiste alla base la decisione di un legislatore democraticamente legittimato e, in secondo luogo, la persona interessata, in ragione della pubblicità del testo di legge ha in principio conoscenza di un tale cambiamento dello scopo.

Capoverso 5: Comunicazione dei dati all'estero

I dati, il cui trattamento in Svizzera non pone problemi di sorta, possono divenire pericolosi per la persona interessata, se vengono fatti conoscere all'estero. Si pensi, per esempio, alle informazioni fornite a Stati esteri sugli stranieri in Svizzera, nel caso il governo del Paese d'origine degli stranieri di cui si tratta non rispetta il diritto dell'uomo. Ma anche le informazioni personali fornite da un'impresa svizzera alla sua filiale estera possono risultare pregiudizievoli per la persona interessata nel caso si venga, ad esempio, a sapere all'estero che tale persona fa parte in Svizzera di una comunità religiosa perseguitata in tale Paese[35]. Per tale ragione, chi intende trasferire dati all'estero deve conoscere tali pericoli e tirarne le debite conseguenze. Analoga cautela può in determinate circostanze imporsi anche per le comunicazioni a *organizzazioni internazionali.* In molti casi, tuttavia potrebbe essere molto difficile per un elaboratore valutare la situazione di pericolo. Per tale ragione sono vietate soltanto le comunicazioni di dati che potrebbero avere per conseguenza un *pregiudizio grave della personalità.* Con siffatta definizione si vuole garantire che lo scambio transfrontaliero dei dati non venga da un lato reso arduo oltre misura e che, dall'altro, soprattutto non comprenda comunicazioni che hanno un carattere preponderante personale o familiare.

Una lesione grave della personalità è realizzata se i dati sono trasmessi a un Paese che non li protegge in misura analoga a quella del diritto svizzero. Un carattere analogo della protezione offerta è dato se nello Stato in questione vengono rispettati i principi materiali ai sensi dell'articolo 4 della presente legge e se l'interessato può ottenere informazioni sui suoi dati e se li può, se del caso, rettificare o distruggere. Tale dovrebbe praticamente essere sempre il caso per i Paesi che dispongono di una legge sulla protezione dei dati e per quelli che hanno ratificato la Convenzione n. 108 del Consiglio d'Europa. Tuttavia, poiché la grande maggioranza degli Stati non dispone di legislazione sulla protezione dei dati, tale criterio non è l'unico adeguato. In molti casi l'ordinamento giuridico e la prassi legale, come pure l'organizzazione amministrativa dello Stato in questione potrebbero essere oggetto di una valutazione globale. Nei casi nei quali l'assetto statale estero non offre sufficienti garanzie in materia di protezione dei dati, agli elaboratori di dati resta la possibilità di prendere le misure di sicurezza necessarie su base contrattuale.

Capoverso 6: Sicurezza dei dati

Determinati problemi di protezione dei dati possono essere evitati se chi tratta i dati prende tempestivamente i necessari provvedimenti di sicurezza. I sistemi informatici moderni, in particolare, esigono *misure edilizie* che impediscono a tutti i terzi non autorizzati l'accesso all'ordinatore. Nel caso di determinati trattamenti di dati sono necessarie *misure tecniche* atte ad impedire che in caso di un guasto (ad es., interruzione del funzionamento in ragione di caduta di corrente) i dati abbiano a risultare irrimediabilmente perduti. Infine, grazie a *misure d'ordine organizzativo* (codice d'identificazione per gli utenti, valutazione periodica delle misure di sicurezza, nomina di un responsabile della protezione dei dati all'interno dell'azienda) è possibile garantire che i dati non abbiano ad essere messi a disposizione di qualsivoglia persona e che i principi della protezione dei dati siano rispettati.

La legge rinuncia a regolare in dettaglio le misure di sicurezza. In considerazione della molteplicità dei tipi di trattamento dei dati, spetta a quanti trattano i dati o alle loro associazioni professionali o di categoria, definire i bisogni di sicurezza per il loro settore e di ordinare le necessarie misure di sicurezza. Ove risultassero difficoltà a tal proposito, il Consiglio federale, sulla base della competenza riconosciutagli di emanare la legislazione d'esecuzione (art. 30 cpv. 1) potrà fissare alcune esigenze minime. Nell'amministrazione federale saranno emanate prescrizioni di sicurezza specifiche.

Articolo 5 Diritto d'accesso

Il diritto d'accesso è l'istituto più importante della legge sulla protezione dei dati. Esso permette alla persona interessata di far valere effettivamente le proprie esigenze in materia di protezione dei dati. Soltanto colui che sa se e quali dati che sono trattati su di lui, può se del caso rettificarli o farli distruggere o almeno impugnarne l'esattezza (cfr. art. 12 e 22).

Autorizzata a chiedere l'accesso alla collezione di dati è, giusta il *capoverso 1,* ogni persona. Il diritto d'accesso è un diritto soggettivo, strettamente personale; anche un minore o un interdetto capace di discernimento può esercitare

da solo, senza il consenso del rappresentante (art. 19 cpv. 2 CC). Dal carattere del diritto strettamente personale consegue anche che non è possibile rinunciare preventivamente al diritto d'accesso (cpv. 6). Destinatario della richiesta d'accesso non è chiunque tratti i dati, bensì *il detentore di una collezione di dati.* Poiché questo ha ordinato sistematicamente i propri dati, le possibilità di lesione della personalità sono presso di lui molto più grandi che non presso qualcuno, i cui dati non sono accessibili secondo le persone interessate. Un obbligo generale d'accesso a tutte le collezioni di dati che non avvenga nell'ambito di una determinata collezione di dati non è possibile, poiché chi tratta i dati dovrebbe spesso attuare ricerche dispendiose, soltanto per poter reperire i dati. Un persona può esigere informazioni unicamente sui propri dati; se potesse richiedere anche i dati concernenti terze persone, sarebbero realizzati i presupposti di nuove lesioni della personalità.

Il *capoverso 2* definisce in che cosa consiste l'accesso. Il detentore della collezione di dati rileverà dapprima se esistono, nella propria collezione, dati relativi al richiedente. Se tale non è il caso, il detentore lo comunica al richiedente e la faccenda è liquidata. Se esistono dati, il detentore deve comunicarne il contenuto al richiedente (lett. a). In tale contesto egli deve curare che l'informazione sia *completa e esatta.* Un'informazione parziale è ammissibile soltanto se la legge prevede un'eccezione, rispettivamente una limitazione dell'informazione (cfr. art. 6), oppure se la persona interessata ha esplicitamente richiesto soltanto un'informazione parziale. Il richiedente deve inoltre essere informato sullo *scopo del trattamento,* poiché soltanto così egli è in grado di valutare in modo esatto gli eventuali rischi che possono risultare dal trattamento dei dati. Allo stesso deve essere comunicato anche il fondamento giuridico del trattamento. Quest'ultima disposizione è rivolta in primo luogo agli organi federali; essa può però essere di rilievo anche per rapporto ai privati, poiché in parte sulla base di impegni legali essi procedono a trattamenti dei dati (il datore di lavoro, ad es., che tratta dati relativi ai lavoratori per i calcoli dell'AVS). Al richiedente devono essere comunicate anche le *categorie dei dati trattati,* dei *partecipanti* alla *collezione di dati* e dei *destinatari dei dati* (lett. b). I detentori della collezione dei dati non sono invece obbligati ad elencare *singolarmente i partecipanti e i destinatari.* Questo causerebbe un dispendio eccessivo di lavoro e potrebbe obbligare i privati a svelare le relazioni d'affari e a far conoscere i loro soci in affari. Il presente progetto non obbliga neppure il detentore della collezione a rivelare la *fonte* dei suoi dati. L'esperienza mostra che la rivelazione della fonte causa in molti casi un dispendio rilevante di lavoro, oppure che la conoscenza delle fonti di un dato non porta molto lontano. È del resto giustificato non obbligare i mezzi di comunicazione sociale a far conoscere l'origine, poiché altrimenti i giornalisti sarebbero tenuti, già prima di una pubblicazione, a fornire delucidazioni sui propri informatori. Questo non significa però che una persona interessata non possa venire a sapere qualcosa in merito alla fonte dei dati. Secondo la giurisprudenza del Tribunale federale essa può – certo soltanto nei confronti degli organi dello Stato, non nei confronti dei privati –, sulla base dell'articolo 4 della Costituzione federale, e non soltanto nell'ambito di una procedura pendente, bensì anche, in principio, fuori di qualsiasi procedura formale, esigere la consultazione degli atti, a meno che si op-

ponga un interesse pubblico dello Stato o interessi giustificati di un terzo al mantenimento del segreto[36].

Il *capoverso 3* tratta il cosiddetto *danno da informazione,* nozione conosciuta soprattutto in medicina. Un danno siffatto è dato allorquando un paziente è confrontato, impreparato, con la verità sul suo stato di salute che in seguito per tale ragione peggiora. Il progetto parte invero dal principio che non il detentore della collezione dei dati deve decidere se un'informazione possa avere o meno effetti negativi per l'interessato. Il richiedente stesso deve ponderare gli eventuali rischi di un'informazione. Per quanto concerne le informazioni relative allo stato di salute s'impone tuttavia un'eccezione. Il detentore di una collezione di dati, ad esempio una cassa malati non deve tuttavia poter negare l'informazione, invocando, in casi del genere, il rischio di un danno dovuto alla rivelazione sullo stato di salute. Esso deve però poter rilasciare l'informazione tramite un medico, perché questi, in base alla formazione e all'esperienza è meglio in grado di orientare l'interessato, in modo che questi non abbia a riportarne un danno ancora maggiore. Il capoverso 3 è quindi una disposizione di protezione della personalità a favore della persona interessata. Nell'ottica del diritto sulla protezione dei dati e nella misura in cui il detentore della collezione dei dati è un organo federale, si tratta quindi di un'eccezione per rapporto alle disposizioni sulla comunicazione dell'articolo 16.

Il *capoverso 4* intende garantire che il detentore di una collezione di dati non abbia a potersi svincolare dall'obbligo d'informare che gli compete, facendo trattare i dati da un terzo. Egli può tuttavia anche incaricare il suo mandatario, ad esempio, un centro di calcolo, di fornire l'informazione in sua vece. Il terzo è da parte sua obbligato a fornire l'informazione se non fa conoscere il nome del detentore della collezione dei dati oppure se questi è domiciliato all'estero. Con questo è garantito che ci sia sempre qualcuno in grado di fornire informazioni in merito a una collezione di dati. L'interessato che desidera informazioni sui suoi dati contenuti in una collezione di dati non deve essere costretto a lunghe ricerche sull'identità del detentore della collezione dei dati oppure a intentare azione all'estero.

Secondo il *capoverso 3,* l'informazione dev'essere scritta e gratuita. Nell'ordinanza d'esecuzione il Consiglio federale può tuttavia prevedere eccezioni del principio del carattere scritto e gratuito dell'informazione. In principio si può ipotizzare che in determinati casi il richiedente possa prendere direttamente conoscenza dei suoi dati su uno schermo. In determinate condizioni può anche essere adeguato permettere al richiedente di consultare un fascicolo completo. Onde evitare un aggravio eccessivo del detentore di una collezione di dati, l'ordinanza prevederà presumibilmente che colui che entro un determinato tempo, ad esempio un anno, solleciti più di un'informazione, abbia a dovere versare un emolumento. Il detentore potrà molto probabilmente richiedere un compenso anche nel caso l'informazione sia fonte di dispendio eccessivo di tempo, ad esempio se gli atti sono già stati archiviati.

Articolo 6 Restrizione del diritto d'accesso

Tanto importante ed essenziale per la protezione dei dati della personalità e dei dati possa essere il diritto d'accesso, questo non è tuttavia illimitato. Interessi

pubblici preponderanti, come pure interessi di protezione di un terzo o della persona che tratta i dati possono opporsi al rilascio di un'informazione. Poiché questo articolo costituisce un'eccezione, con la quale si viene a limitare il diritto altamente personale che è quello d'essere informati, l'elenco dei motivi della sua limitazione dev'essere completo. E in conformità anche la disposizione deve essere interpretata restrittivamente e l'informazione deve poter essere limitata soltanto nei casi ciò sia assolutamente necessario. Il genere di restrizione del diritto d'accesso può del resto essere del tutto diversificato. È possibile rifiutare del tutto o in parte l'informazione, oppure differirla nel tempo. Sono date diverse possibilità: occorre scegliere la soluzione più favorevole per l'interessato. La disposizione nel presente disegno ricalca in gran parte la regolamentazione del rifiuto di testimoniare istituita dalla legge sulla procedura amministrativa (art. 27; RS *172.021*).

A proposito dei diversi motivi di restrizione elencati nel *capoverso 1* rileviamo quanto segue:

Le facoltà del detentore di una collezione di dati di rifiutare l'informazione (lett. a), previste in una legge formale (vale a dire in un trattato internazionale o in un decreto federale di portata generale sottoposto all'obbligo del referendum), sono in primo luogo ipotizzabili nel settore del diritto pubblico. Da menzionare in questo contesto è in particolare l'articolo 13 della legge sull'organizzazione dell'amministrazione (RS *172.010*), giusta il quale i dibattiti del Consiglio federale non sono pubblici. Sulla base di questa disposizione, il Consiglio federale ha la possibilità di respingere una richiesta d'informazione con la quale si esige la consultazione dei verbali delle sedute. Nel settore privato tali facoltà del detentore della collezione dei dati di rifiutare l'informazione, se mai, dovrebbero essere date raramente.

Interessi pubblici preponderanti che giustificano una restrizione dell'accesso (lett. b) sono possibili soprattutto in materia di sicurezza interna ed esterna del Paese, la nozione di sicurezza esterna dovendo comprendere, oltre al rispetto degli obblighi di diritto internazionale pubblico, anche il mantenimento di buone relazioni con l'estero. Questa disposizione permetterà, ad esempio, di rifiutare l'accesso alle collezioni di dati del Ministero pubblico della Confederazione, ove l'autorizzazione di fornire informazioni rischiasse di svelare metodi o risultati d'indagini. Il rifiuto di dare informazioni è possibile anche per rapporto alle collezioni di dati del Dipartimento federale degli affari esteri, se negoziati in corso con Stati esteri risultassero compromessi, oppure se fossero richieste informazioni su persone la protezione delle quali la Svizzera ha assunto in virtù del diritto internazionale.

L'accesso può anche essere negato se l'informazione fornita rischia di compromettere lo scopo di un'*istruzione penale* o di un'altra procedura ufficiale d'istruzione, quale una procedura disciplinare (lett. c). Questa disposizione non dovrebbe avere un'importanza pratica rilevante: la presente legge non si applica in effetti a procedure disciplinate in leggi di procedura (cfr. art. 2). Si può tuttavia immaginare che anche le informazioni rilasciate al di fuori di una procedura d'indagine possono influire negativamente su quest'ultima, nel caso, per esempio, una persona incolpata desideri avere accesso alla collezione di dati che contenga il nome dei suoi denuncianti.

Anche *interessi preponderanti del detentore della collezione di dati* possono giustificare una restrizione dell'informazione (lett. d). Si tratta in primo luogo di casi attinenti al diritto privato. Così, ad esempio, un grande emporio può negare l'accesso al registro dei clienti sospettati di furto. Una restrizione è anche ammessa nel caso il detentore della collezione dei dati debba temere che il richiedente faccia dello spionaggio economico.

È infine possibile limitare il diritto d'accesso ove si debba temere che il richiedente, accedendo ai dati che lo concernono abbia in pari tempo a ottenere informazioni anche su terzi e con questo possano essere *lesi gli interessi di tali terze persone* (lett. e). Un contraente d'assicurazione, ad esempio, potrebbe avere interesse a che il terzo beneficiario dell'assicurazione, non abbia conoscenza di tale fatto.

Ogni restrizione del diritto d'accesso, limitazione o differimento di un'informazione dev'essere, giusta il capoverso 2, motivata. Gli organi della Confederazione devono farlo, secondo i principi della procedura amministrativa, nella forma di una decisione impugnabile. Per i privati che trattano dati non esistono prescrizioni sulla forma; sarà tuttavia utile comunicare per scritto al richiedente i motivi della restrizione del diritto d'accesso. La motivazione dev'essere fatta in modo tale che la persona interessata sia posta in condizione di giudicare se la limitazione dell'informazione avviene a giusto titolo. In determinati casi, nel settore della sicurezza interna ed esterna del Paese, in particolare, non possono essere poste esigenze troppo severe all'obbligo di motivare il diniego, perché altrimenti l'organo federale competente dovrebbe svelare proprio quanto dovrebbe essere tenuto segreto grazie al rifiuto di fornire l'informazione.

Articolo 7 Registro delle collezioni di dati

Il registro delle collezioni di dati è la chiave per potere esercitare il diritto d'accesso. Esso è tenuto, giusta il *capoverso 1,* dal Preposto alla protezione dei dati e può essere consultato da chiunque.

Secondo il *capoverso 2,* la portata dell'obbligo di notificare una collezione di dati è diversa a seconda che si tratti di collezione di dati del settore pubblico o del settore privato. Le collezioni di dati tenute dagli organi federali devono in principio essere notificate. Fanno eccezione a tale obbligo, se del caso le collezioni di dati nel settore della protezione dello Stato e della sicurezza militare (art. 21). Nel settore privato, invece, non esiste in principio l'obbligo di registrare le collezioni di dati. L'eccezione vale per le collezioni nell'ambito delle quali vengono trattati dati degni di particolare protezione o profili della personalità (lett. a), oppure se i dati relativi sono comunicati a terzi (lett. b). Tuttavia anche queste collezioni di dati, sensibili nell'ottica della protezione dei dati, sottostanno all'obbligo della registrazione soltanto se il detentore della collezione non è obbligato, giusta una legge, a tenerla oppure se le persone interessate non ne hanno conoscenza. Il datore di lavoro, ad esempio, che sulla base della legislazione dell'AVS tiene uno schedario sul salario dei suoi impiegati e che sulla base di questa collezione comunica i dati all'AVS, non soggiace all'obbligo della registrazione. Non è possibile determinare in modo completo in quale modo le persone interessate debbano avere conoscenza che una collezione di dati contiene dati sensibili su di loro o che i dati sono comunicati a terzi.

Non sarà necessario in ogni caso che il detentore di una collezione di dati abbia ad orientare personalmente tutti coloro che vi figurano. Se si tratta di collezioni di dati di un imprenditore sui suoi collaboratori, basterà una circolare o un avviso affisso. Possiamo anche immaginare che venga fatta una pertinente comunicazione a ogni nuova persona in occasione dell'assunzione. La comunicazione deve tuttavia in ogni caso essere, per l'interessato, chiaramente riconoscibile. Sottostanno all'obbligo della registrazione soltanto i trattamenti e le comunicazioni regolari, vale a dire quelli che avvengono periodicamente. Sulla base della regolamentazione proposta, il detentore privato di una collezione di dati può decidere liberamente se intende far registrare una collezione di dati, oppure se invece preferisce orientare direttamente le persone interessate sull'esistenza della sua collezione. Grandi collezioni però, quali quelle di organizzazioni di pubblicità diretta, oppure le agenzie d'informazione, devono di regola essere registrate poiché l'informazione di tutti gli interessati è praticamente impossibile.

Giusta il *capoverso 3,* le collezioni di dati devono essere notificate, prima di divenire operazionali. Il Preposto sarà così in grado di attirare l'attenzione su eventuali problemi già all'inizio dell'attività d'informazione.

Il *capoverso 4* rileva che il Consiglio federale regolerà, in un'ordinanza d'esecuzione, i dettagli della registrazione. Esso dovrà in particolare prevedere quali indicazioni debbano essere fornite in occasione della registrazione. Dovrebbe essenzialmente trattarsi delle stesse che, sulla base dell'articolo 5 capoverso 2 lettera b devono essere rese note al momento che si inoltra una domanda d'accesso. Il Consiglio federale deciderà inoltre in quale modo il registro deve essere pubblicato, rispettivamente come può essere consultato. L'ordinanza prevederà inoltre che il registro dev'essere aggiornato periodicamente. Il Consiglio federale, per le collezioni di dati dal cui trattamento non si devono temere pregiudizi per le persone interessate, potrà prevedere procedure di notifica semplificate oppure eccezioni dell'obbligo di notificazione o di registrazione.

Infine occorre rilevare che le persone private che non notificano le collezioni di dati sottoposte all'obbligo di registrazione si rendono punibili ai sensi dell'articolo 28 del disegno di legge.

Articolo 8 Comunicazione all'estero

Come già indicato più sopra (cfr. le osservazioni a proposito dell'art. 4 cpv. 5), la comunicazione dei dati all'estero non è sprovvista di rischi gravi di lesione della personalità. Il *capoverso 1* prevede quindi che determinati trasferimenti di dati all'estero devono essere comunicati al Preposto alla protezione dei dati affinché questi, appoggiandosi all'articolo 24 possa, in casi difficili, procedere a chiarimenti. Estero ai sensi della presente legge non sono soltanto altri Stati, bensì anche organizzazioni internazionali. Determinante è unicamente che i dati siano sottoposti a un ordinamento giuridico straniero. Anche una trasmissione di dati all'interno di un'impresa multinazionale costituisce una comunicazione all'estero. L'obbligo di notificare le comunicazioni di dati è tuttavia molto limitato. Esso insorge soltanto se la comunicazione di dati avviene *regolarmente* oppure in *numero rilevante.* Esso decade inoltre in tutti i casi nei quali la comunicazione dei dati è prescritta per legge (lett. a) o se le

persone interessate sono a conoscenza (lett. b). Per determinare se vi ha conoscenza o meno, si applicano gli stessi criteri validi in materia d'eccezioni dell'obbligo di registrare (cfr. art. 7).

Giusta il *capoverso 2,* spetta al Consiglio federale di regolare le modalità della notificazione. Esso preciserà in particolare quando la comunicazione all'estero è di «grande rilievo». Occorre partire dal presupposto che la nozione di «grande rilievo» ha una componente quantitativa e una componente qualitativa. Nell'ordinanza occorrerà quindi distinguere tra i dati personali degni di particolare protezione e gli altri dati, in modo tale che nella prima categoria il numero che fa insorgere un obbligo di notificare è minore di quello della seconda categoria. Il Consiglio federale può inoltre prevedere notificazioni semplificate per i trasferimenti di dati che, nonostante non siano noti alle persone interessate, non ledono la loro personalità. La comunicazione di dati non degni di particolare protezione per scopi di ricerca o di statistica potrà, per esempio beneficiare di tale eccezione. Questo sarà il caso anche quando vengono comunicati dati all'interno di imprese attive in diversi Paesi, quale ad esempio una società di navigazione aerea. In casi del genere dovrebbe già bastare una notificazione globale.

Infine occorre rilevare che le persone private si rendono punibili ai sensi dell'articolo 28 se violano intenzionalmente l'obbligo di notificare.

221.3 Sezione 3: Trattamento di dati personali da parte di persone private

Articolo 9 Lesioni della personalità

Nella parte dedicata al diritto privato, la legge sulla protezione dei dati costituisce un complemento e una concretizzazione della protezione della personalità del Codice civile. Punto di partenza è la disposizione dell'articolo 28 capoverso 1 del Codice civile che recita fra l'altro che chi è leso illecitamente nella sua personalità può adire al giudice. La terza sezione del progetto di legge concretizza tale clausola generale per il settore del trattamento dei dati. L'articolo 9 quale prima disposizione della sezione elenca fattispecie, vale a dire tipi di trattamento che devono valere quali lesioni della personalità e sono quindi in principio illecite, ove la persona che tratta tali dati non possa appellarsi a un motivo giustificativo.

Il *capoverso 1* costituisce la correlazione con l'articolo 28 capoverso 1 del Codice civile. Esso rende in questo modo evidente che la legge sulla protezione dei dati, nella misura in cui si riferisce a trattamenti privati di dati, segue i principi della protezione della personalità del Codice civile. Ambedue le leggi hanno in ultima istanza lo stesso obiettivo, proteggere l'autonomia e la libertà delle persone interessate a decidere liberamente.

Nel *capoverso 2* sono enunciati trattamenti di dati che possono sfociare in lesioni della personalità. Una lesione della personalità commette chi non rispetta i *principi generali della protezione dei dati* fissati dall'*articolo 4* (lett. a). Tali principi costituiscono il fondamento etico, giuridico e politico della legge sulla

protezione dei dati e non devono quindi essere violati senza un motivo impellente. Una lesione della personalità è inoltre data quando la persona che tratta i dati *agisce contro l'esplicita volontà della persona interessata* (lett. b). Si tratta in effetti di una vera novità introdotta nel diritto privato: il diritto di autodeterminazione della persona interessata in merito ai propri dati è garantito e protetto. La persona interessata può vietare il trattamento dei dati che la concernono, senza condizioni e senza dover provare un interesse particolare. Essa non può tuttavia vietare in globo il trattamento dei dati; il divieto si riferisce tuttavia soltanto a determinati elaboratori e concerne unicamente determinati tipi di trattamento. Una violazione della personalità è inoltre data soltanto se la persona interessata ha *esplicitamente* vietato il trattamento dei dati. Se un elaboratore di dati ha unicamente omesso di chiarire se una persona sia d'accordo con il trattamento dei dati che la concernono, tale fatto non vale ancora, per legge, come lesione della personalità. In tale contesto va rilevato che già oggi i mercanti d'indirizzi hanno creato la cosiddetta lista «Robinson», censimento delle persone che hanno esplicitamente manifestato il desiderio di non ricevere invii di carattere pubblicitario. È del resto evidente che una persona interessata può ritirare il divieto di trattamento, se del caso con una tacita accettazione del trattamento dei dati. Una lesione della personalità è infine data quando sono *comunicati a terzi dati personali degni di particolare protezione o profili di personalità* (lett. c). Queste indicazioni possono danneggiare in modo rilevante la persona interessata oppure costituire una completa descrizione dell'individuo. Egli deve quindi potere esigere da colui al quale ha comunicato i dati o che è giunto a conoscenza degli stessi, che abbia a rispettare la segretezza. Dati del genere non devono essere comunicati senza che sia realizzato un motivo giustificativo, ad esempio non senza l'autorizzazione della persona interessata. Anche questa disposizione riflette, come quella della lettera b, l'idea direttrice della legge, secondo la quale le persone interessate devono potere determinare quali dati che le concernono possono essere trattati.

L'elenco delle lesioni della personalità non è *esauriente*. E ove siano soddisfatte le rispettive fattispecie, una persona interessata può procedere contro trattamenti illeciti di dati, suppletivamente appellandosi ad altre leggi che servono alla protezione della personalità, quale ad esempio alla legge sulla concorrenza sleale[37].

Articolo 10 Motivi giustificativi

Il *capoverso 1* riprende, chiarendo, il principio già enunciato nell'articolo 28 capoverso 2 del Codice civile, secondo il quale una lesione della personalità non è illecita, non coinvolgendo così alcuna conseguenza giuridica, se la persona lesa ha dato il proprio consenso oppure se l'elaboratore di dati può far valere un interesse privato o pubblico preponderante o se fa valere una disposizione legale come motivo giustificativo. Anche nei confronti di lesioni della personalità, commesse con il trattamento di dati, la protezione non è globale. Essa deve in particolare ritrarsi se gli interessi - privati o pubblici - al trattamento dei dati sono superiori all'interesse a essere informato che riviene alla persona interessata. Diversamente da quanto fatto nell'avamprogetto, il disegno attuale rinuncia a procedere a una ponderazione degli interessi in modo tale che, per

determinati tipi di trattamento dei dati, venga previsto per legge un motivo giustificativo, rispettivamente la presunzione legale di interessi superiori. Un tale sistema appare troppo rigido e non permetterebbe di tenere conto adeguatamente del caso singolo. Anche nella procedura di consultazione, esso è stato criticato come troppo complicato. In ultima istanza soltanto il giudice può decidere, tenendo debitamente in considerazione i fatti concreti, se una lesione della personalità è giustificata o meno.

Il *capoverso 2* propone tuttavia al giudice determinati *punti di riferimento*. Il legislatore non può certo alleviare il giudice della sua responsabilità. Egli è però in grado di fornirgli, per determinati settori - nei quali interessi al trattamento dei dati e interessi di protezione si trovano in uno speciale rapporto di tensione - elementi che lo assistano nella valutazione. I motivi giustificativi elencati nel capoverso 2 possono in principio essere applicati a tutte le violazioni della personalità previste dall'articolo 9, come pure ad altre violazioni della personalità non descritte nel disegno di legge. Il giudice tuttavia sarà incline ad ammettere l'esistenza di un motivo giustificativo nel caso di determinate lesioni della personalità che non per altre lesioni. Una raccolta di dati avvenuta con mezzi illeciti sarà soltanto raramente giustificata, certamente mai giustificata sarà invece la raccolta di dati avvenuta contro il principio della buona fede: sarà per contro possibile trovare un motivo giustificativo per una lesione della personalità avvenuta in ragione di un trattamento inesatto di dati.

Il disegno prevede tre categorie di motivi giustificativi: quelli per determinate attività economiche (conclusione di contratto, concorrenza economica, valutazione del credito), quelli per i mezzi di comunicazione sociale e quelli per i trattamenti di dati il cui scopo non si riferisce a persone:

Secondo la *lettera a,* una lesione della personalità può essere giustificata se la persona interessata è l'altra parte del contratto con la persona che tratta i dati, indipendentemente dalla forma del contratto. L'espressione «in relazione diretta con la conclusione di un contratto» copre anche le attività d'informazione avvenute nella fase pre-contrattuale. Questo motivo giustificativo potrebbe, ad esempio, entrare in considerazione se qualcuno, in vista dei negoziati per la conclusione di un contratto, raccoglie referenze su un potenziale acquirente o su un possibile inquilino. Non più in relazione diretta con la conclusione del contratto sono invece le campagne pubblicitarie, nonostante debbano portare, in ultima analisi, alla conclusione di un contratto. Il motivo giustificativo vale per ogni forma di trattamento, per la raccolta, come anche per la valutazione dei dati. Può essere fatto appello al motivo giustificativo anche per le comunicazioni a terzi, allorquando l'elaboratore fa proseguire i dati del suo socio in affari a una filiale, a un fornitore o a uno speditore.

La *lettera b* istituisce un motivo giustificativo nel campo della *concorrenza economica.* Chi vuole affermarsi sul mercato, deve continuamente rielaborare i propri dati economici e in particolare informarsi sui concorrenti. Viceversa egli deve accettare che i suoi concorrenti abbiano a raccogliere su di lui le più diverse informazioni. Il *registro di commercio* già assicura una certa pubblicità nella concorrenza economica. Le persone iscritte nel Registro informano di inserirsi nella concorrenza economica; esse svelano fino a un certo punto gli estremi della loro attività commerciale, in particolare quelle per apparire degne

di fiducia e di credito. Se qualcuno tratta dati di tali persone, in qualche modo «pubbliche», dovrebbe poter invocare un motivo giustificativo, ove fosse accusato di lesioni della personalità. Della cerchia di queste persone fanno parte in primo luogo le società di capitali e le società cooperative, come pure ditte individuali e società di persone sottoposte all'obbligo dell'iscrizione[38]. Non fanno invece parte le persone fisiche che sono iscritte al Registro di commercio nella loro qualità di organi di persone giuridiche. Il motivo giustificativo della lettera b entra tuttavia in considerazione soltanto se i dati sono trattati esclusivamente per scopi interni, vale a dire che non sono comunicati a terzi. In quale misura lo scambio di informazioni all'interno di un consorzio debba essere considerato ancora come trattamento interno, dovrà essere deciso dalla pratica. Sarà determinante a tale proposito se le informazioni, nel caso singolo, restano limitate a un'impresa in quanto unità economica. Il motivo giustificativo può inoltre essere invocato soltanto quando i dati in questione e il tipo del loro trattamento sono rilevanti per la concorrenza economica.

Per motivi analoghi a quelli validi per le attività d'informazione nell'ambito della concorrenza economica, la *lettera c* istituisce un motivo giustificativo a favore di quanti trattano dati per la valutazione del credito di un'azienda commerciale. Nell'economia di mercato, il credito è un fattore essenziale. Quando si è iscritti nel Registro di commercio ci si deve attendere di fare oggetto di valutazione del credito e tollerare, quindi, più che altri, eventuali violazioni della personalità. Si può tuttavia invocare il motivo giustificativo nel caso, in occasione del controllo del credito, vengano trattati dati non degni di particolare protezione. Questa limitazione appare necessaria poiché, diversamente da quanto avviene nel caso contemplato dalla lettera b, nella valutazione del credito i dati sono, in molti casi, comunicati a terzi. Questo avviene, ad esempio, quando un'agenzia d'informazione, dopo aver appurato la solvibilità di un'impresa, comunica al mandante i risultati delle proprie indagini. Il motivo giustificativo trova inoltre applicazione soltanto se è evidente che l'informazione sulla solvibilità è necessaria per la conclusione e lo svolgimento di un contratto. Sono con questo escluse comunicazioni globali fatte secondo una lista di informazioni concernenti la solvibilità o risposte a richieste generali non vincolate a un caso specifico.

La *lettera d* riconosce un motivo giustificativo a favore di quanti trattano dati in vista della pubblicazione in *mezzi di comunicazione sociale periodici.* Si tratta in questo caso di un trattamento di dati nella fase precedente alla pubblicazione. Una volta pubblicati i dati, secondo l'articolo 2 capoverso 2 lettera b non trova più applicazione la legge sulla protezione dei dati, bensì gli articoli 28 e seguenti del Codice civile. Con questa regolamentazione ci si addentra in un campo oggetto di controversie. L'attività d'informazione dei mezzi di comunicazione sociale, nella quale si tratta sempre anche di dati relativi a persone, può, nell'ottica della protezione dei dati, essere problematica per più d'un aspetto. I responsabili e le imprese dei mezzi di comunicazione sociale dispongono di molteplici metodi per la raccolta dei dati. Essi intendono sempre ottenere proprio indicazioni sensibili su determinate persone. Essi devono spesso operare sotto l'incalzare del tempo e riferendosi a fonti insicure: ed è per tale ragione che l'esattezza dei dati, in questa fase della loro attività, pure

con la maggiore coscienza professionale possibile, non sempre può essere garantita a pieno. Spesso essi raccolgono dati a futura memoria, in parte in banche di dati ben fornite e per un lungo lasso di tempo, onde poter disporre, al momento giusto, del materiale necessario per la pubblicazione. D'altro canto il funzionamento dell'opera dei mass media è importante per una democrazia. I mass media possono esplicare il loro compito soltanto se anche nel trattamento di dati sensibili, essi godono di una certa libertà e se le fonti d'informazione restano fino a un certo grado protette. Per questa ragione l'interesse pubblico a disporre di mass media indipendenti e autonomi può in determinati casi essere preponderante per rispetto all'interesse di protezione della personalità del singolo. La disposizione presente dovrebbe creare equilibrio tra protezione della personalità e libertà dei mezzi di comunicazione sociale. Al motivo giustificativo legale può tuttavia appellarsi soltanto chi tratta dati per un *mezzo di comunicazione sociale di carattere periodico*. Libro e pellicola non sono protetti. La limitazione ai mass media periodici appare indicata perché tali media rivestono il ruolo più importante nella formazione dell'opinione pubblica. Certo, non si può negare che anche pellicole e libri possono in tale contesto fornire contributi essenziali. L'inclusione anche di questi mezzi nella regolamentazione presente pregiudicherebbe tuttavia oltre misura la protezione della personalità, poiché chi tratta i dati potrebbe quasi sempre, in caso di lesione della personalità, affermare di raccogliere dati e di valutarli poi in vista di una pubblicazione. Che cosa si debba intendere per mezzi di comunicazione sociale con carattere periodico risulta dalla prassi relativa alla protezione della personalità in diritto civile (art. 28*c* cpv. 3 e 28*g* CC). Di questa categoria fanno parte non soltanto i prodotti tradizionali della stampa scritta, la radio e la televisione, ma anche le collezioni d'informazioni accessibili a chiunque, a condizione che essi contengano dati personali e che siano costantemente aggiornati. Il motivo giustificativo copre anche *comunicazione a terzi* di dati che sono trattati in vista di una pubblicazione. Con questo si intende tenere conto del fatto che un giornalista deve potere fornire all'editore progetti di articoli a mò di prova. Questa regolamentazione garantisce inoltre la parità di trattamento dei giornalisti che lavorano per la radio, la televisione o la stampa e dei giornalisti attivi per le agenzie di stampa o le agenzie d'immagini. L'obiettivo di tali agenzie consiste proprio nell'approntare informazioni per i terzi, in particolare per media pubblicati periodicamente.

La *lettera e* prevede un motivo giustificativo per i casi nei quali se vengono trattati dati e lo scopo del trattamento non è invece in rapporto alcuno con le persone interessate. Il progetto elenca come più importanti fra questi tipi di trattamento nei quali manca la relazione diretta con la persona, *la ricerca, la pianificazione e la statistica*. Altri simili trattamenti senza relazione diretta con la persona sono ipotizzabili, ad esempio, l'utilizzazione di dati personali per controllare un impianto di EED. Il motivo di tale privilegio consiste nel fatto che ricerca, statistica e pianificazione non soltanto forniscono importanti elementi di decisione per le attività dell'economia privata, ma rispondono anche a numerosi bisogni d'ordine sociale e pubblico. Inoltre, eventuali lesioni della personalità, quali ad esempio violazione dei principi dell'articolo 4 del disegno, risultano, nel contesto di ricerca, pianificazione e statistica, meno gravi, visto

che questi trattamenti di dati non hanno conseguenze dirette per le persone interessate. Ciò significa però inversamente, che non può appellarsi al motivo giustificativo, ad esempio, la persona che esperta in storia o genealogia conduce una ricerca effettivamente improntata sulle persone. Questi ricercatori possono tutt'al più far valere i motivi giustificativi generali dell'articolo 10 capoverso 1 del disegno di legge. Il motivo giustificativo speciale della lettera e entra inoltre in linea di conto soltanto se i risultati della ricerca sono presentati in modo che non sia praticamente più possibile risalire alle persone interessate. Il motivo giustificativo speciale copre anche lo scambio di dati tra ricercatori o gruppi di ricercatori. Si viene con questo a tenere conto del fatto che nella ricerca e in parte anche nella pianificazione e nella statistica esiste una molteplice cooperazione, spesso anche transfrontaliera che merita di essere in certo qual modo privilegiata nell'ottica della protezione dei dati. Infine vogliamo rilevare che eventuali prescrizioni in materia di segretezza dei dati hanno validità piena anche nel settore della ricerca, della statistica e della pianificazione: un ricercatore non può, appellandosi alla lettera e, giustificare la comunicazione di dati segreti a terzi.

Una lesione della personalità può inoltre essere giustificata secondo la *lettera f,* qualora la persona interessata abbia reso i propri dati accessibili a tutti. Chi divulga in un mezzo di comunicazione sociale, dati, anche quelli degni di particolare protezione, deve aspettarsi che un numero indefinito di persone ne prende atto e poi eventualmente reimpiega le indicazioni rispettive. Lo stesso vale per le opinioni espresse in pubblico da una persona, nell'ambito, ad esempio, di un'assemblea comunale. Se per le eventuali lesioni della personalità causate con il trattamento, in particolare con la comunicazione di tali informazioni non vi fosse alcun motivo giustificativo, le relazioni sociali risulterebbero troppo fortemente limitate.

Articolo 11 Trattamento di dati da parte di terzi

Le possibilità organizzatorie e tecniche di affidare a terzi il trattamento dei dati sono numerose. Esse corrispondono alle molteplici necessità di ripartire il lavoro in materia di trattamento e comunicazione delle informazioni. In determinati casi, il trattamento dei dati è completamente deferito a un terzo specializzato, ad esempio, a un istituto di sondaggio d'opinione o a una fiduciaria. La legge non intende intervenire su tali modi di procedere.

Il *capoverso 1* intende però tutelare i diritti delle persone interessate nel caso di trattamenti dei dati affidati a terzi. Chi affida a un terzo il mandato di trattare dati, deve preoccuparsi che il mandatario abbia a rispettare alla stessa stregua i limiti in ordine alla protezione dei dati, come se dovesse farlo lui stesso (lett. a). Ciò vale per tutte le forme di trattamento, dal rilevamento fino all'eventuale comunicazione dei dati a terzi. Nel trasferimento del trattamento a un terzo, il mandante deve, per analogia con l'articolo 55 del Codice delle obbligazioni, usare tutta la diligenza richiesta dalle circostanze, onde evitare violazioni della legge sulla protezione dei dati. Egli deve scegliere il mandatario in modo adeguato, impartirgli le istruzioni adeguate e nella misura del possibile sorvegliarlo. Il trasferimento del trattamento a terzi è tuttavia escluso se il mandante

è obbligato, per legge o per contratto, a tenere segreti i dati (lett. b). Ciò significa, ad esempio, che un medico che faccia stendere la fatture per i clienti da un istituto d'incasso può farlo, sulla base dell'articolo 321 del Codice penale, soltanto con l'accordo dei pazienti oppure deve fare in modo che tale ufficio d'incasso non venga a conoscenza dei dati dei pazienti che soggiacciono al segreto medico. Anche in questo caso le prescrizioni concernenti la segretezza, in quanto disposizioni più limitative in materia di protezione dei dati, scalzano la legge generale sulla protezione dei dati.

D'altro canto, il terzo può, giusta il *capoverso 2,* far valere i motivi giustificativi ai quali può appellarsi anche il mandante. Questa norma è necessaria poiché una persona interessata che ritiene pregiudicati i propri diritti in ordine alla personalità può, sulla base dell'articolo 28 del Codice civile, rivalersi non soltanto nei confronti del mandante, bensì anche del mandatario. In tali casi tuttavia, una parte della dottrina è del parere che, in mancanza di disposizioni specifiche, il mandatario convenuto ha il diritto di far valere unicamente i *mezzi di cui dispone personalmente*[39]. Il presente progetto vuole completare i mezzi di difesa della persona che tratta i dati per un'altra persona, affinché, in caso di eventuali controversie tra il mandatario e la persona interessata, abbiano ad essere chiarite tutte le questioni del diritto di protezione dei dati.

Articolo 12 Azioni e procedura

Poiché la legge sulla protezione dei dati è, nella parte di diritto privato, completamento e concretizzazione del Codice civile, anche la protezione giuridica deve essere la stessa di quella che vale per il diritto civile. Il disegno prevede alcuni complementi che da un canto tengono conto di determinare particolarità del trattamento dei dati e che, d'altro canto, sono destinate ad ancorare il *diritto d'accesso* quale istituto centrale della legge sulla protezione dei dati anche per gli aspetti procedurali. L'allineamento al Codice civile ha per conseguenza che la *legittimazione ad agire* è in gran parte uguale a quella del diritto sulla personalità. Ciò vale completamente per la *legittimazione passiva.* La persona illecitamente lesa può far valere le proprie esigenze di protezione nei confronti di chiunque partecipa alla lesione (cfr. art. 28 cpv. 1 CC). La vittima può agire contro *qualsiasi persona* della quale presuma che sarebbe stata in grado, con una modificazione dell'atteggiamento, di accantonare o di ridurre la lesione o nei confronti della quale egli ha rilevato l'illeicità del trattamento dei propri dati. Poco importa che il convenuto sia il principale responsabile della lesione o che vi abbia avuto una parte soltanto accessoria[40]. Applicata al trattamento automatico dei dati, questa regola significa che la vittima della lesione può citare in azione non soltanto il detentore della collezione dei dati, bensì anche i suoi ausiliari e il suo mandatario. La vittima della lesione può anche rivalersi, ad esempio, sui gestori di un centro di calcolo o di una rete di trasmissione dei dati oppure anche sulle persone che hanno fornito lo software e lo hardware per il trattamento dei dati che è all'origine della lesione, nella misura in cui le loro azioni od omissioni siano all'origine della lesione. Tuttavia, la persona citata a rispondere di una lesione della personalità non è necessariamente identica con quella che deve versare risarcimento. Le pretese di risarcimento si basano su particolari premesse: l'attore deve di regola provare la colpa.

Per quanto concerne la *legittimazione ricorsuale attiva,* il diritto d'agire non spetta a qualsiasi persona lesa per il fatto di un'attività d'informazione, bensì soltanto alla persona i cui dati sono stati oggetto di trattamento. In effetti, la legge sulla protezione dei dati protegge, all'articolo 1 soltanto tale persona. I terzi lesi hanno diritto d'agire soltanto se un tale diritto spetta loro in base al Codice civile[41)].

Contrariamente all'avamprogetto, l'attuale disegno rinuncia a disciplinare esplicitamente il *diritto d'agire delle associazioni.* Per il diritto d'agire delle associazioni valgono di conseguenza, nell'ambito della legge sulla protezione dei dati, le stesse regole sviluppate nella giurisprudenza dal Tribunale federale in merito al diritto generale sulla personalità. Un'associazione potrà da un canto agire, se sarà pregiudicata o messa in pericolo in ragione di un trattamento illecito di dati. Le associazioni professionali possono inoltre agire in nome proprio, ma tuttavia per i loro soci, ove, giusta gli statuti esse abbiano il compito di rappresentare gli interessi dei soci e se quest'ultimi sono essi stessi legittimati a intentare azione[42)].

Il *capoverso 1* rinvia, nella prima frase, unicamente ai rimedi di diritto del Codice civile. Sono quindi a disposizione della persona lesa tre tipi d'azione: con l'*azione negatoria* essa intende impedire una lesione imminente della personalità, con l'*azione di cessazione,* porre termine a una lesione già intervenuta e, con l'*azione d'accertamento,* far riconoscere giudizialmente l'illeicità di un trattamento dei dati. Nell'ambito dell'azione negatoria e dell'azione di cessazione, essa può - come precisato nella seconda frase - esigere in particolare la rettificazione o la distruzione dei dati. Dovrebbero essere queste le due richieste principali nel quadro della protezione della personalità in ordine al diritto sulla protezione dei dati. La persona lesa può giusta l'articolo 28*c* CC esigere *provvedimenti cautelari* per ottenere i quali la lesione illecita della personalità deve unicamente essere resa verosimile.

Il *capoverso 2* istituisce un rimedio di diritto particolare: la possibilità di far menzionare il *carattere contestato* di un dato. È in effetti molto spesso difficile provare l'esattezza o l'inesattezza di fatti legati soprattutto a giudizi di valore. In casi del genere, la persona interessata deve poter esigere che ai dati in questione venga apposta la menzione del carattere contestato. In questo modo, essa può esprimere il proprio parere su un'informazione senza per questo dover ricorrere alla via molto più limitata e per questo assai più ardua, della rettificazione o addirittura della distruzione dei dati. Le premesse concrete dell'accoglimento di una domanda volta a fare apporre una menzione del genere dovranno essere rilevate dalla giurisprudenza. Quest'ultima fisserà portata e contenuto dell'eventuale menzione, a seconda delle circostanze e sempre che ciò possa essere ragionevolmente richiesto alla persona che tratta i dati. Rileviamo infine che la menzione del carattere contestato può essere ottenuta anche nell'ambito di un provvedimento cautelare ai sensi dell'articolo 28*c* del Codice civile.

Il *capoverso 3* stipula che le azioni in vista dell'esecuzione *del diritto d'accesso* devono essere proposte allo stesso foro che l'articolo 28*b* del Codice civile riconosce alle azioni volte a ottenere la protezione della personalità in generale. Il capoverso 3 esige inoltre una procedura semplice e rapida. Una siffatta procedura risulta in particolare necessaria in ragione del fatto che la decisione rela-

tiva al diritto d'accesso può essere d'importanza determinante per la presentazione di azioni di protezione della personalità. Come già nel caso dell'articolo 28*b* capoverso 1 CC, la concretizzazione del diritto materiale implica anche qui l'adozione di norme procedurali federali.

221.4 Sezione 4: Trattamento di dati personali da parte di organi federali

Articolo 13 Organo responsabile

Nel campo dell'amministrazione pubblica, numerose autorità e servizi amministrativi, ma anche privati e organizzazioni private trattano dati per i più diversi compiti legali. Il *capoverso 1* prevede che tutti questi organi federali, nel quadro delle competenze attribuite loro da leggi e ordinanze assumano anche la responsabilità in ordine alla protezione dei dati. In particolare essi devono permettere l'accesso alle collezioni di dati, rispettare le norme che reggono la comunicazione dei dati e prendere le misure di sicurezza necessarie. Questa attribuzione diretta della responsabilità è necessaria; è più sensato riconoscerla soltanto a quel servizio che è effettivamente in grado di applicare le prescrizioni in materia di protezione dei dati, che non attribuirla alla Confederazione in quanto tale o al Consiglio federale quale massima autorità esecutrice. Non è sempre facile determinare concretamente su quale unità amministrativa riposi la responsabilità nel caso singolo, poiché le prescrizioni sull'organizzazione della Confederazione definiscono di regola soltanto i compiti degli *Uffici*. A seconda della materia e dell'organizzazione di un Ufficio, è possibile che la responsabilità per determinati trattamenti di dati sia attribuita ad unità amministrative di rango inferiore, quali la divisione o la sezione. Spetta in ultima analisi al Dipartimento e agli Uffici regolare la questione della responsabilità e farla conoscere poi verso l'esterno. Già attualmente, nel registro delle collezioni di dati, pubblicato dall'Ufficio federale di giustizia, è designata, per ogni collezione di dati, un organo responsabile.

Il *capoverso 2* attribuisce al Consiglio federale la competenza a disciplinare le responsabilità in maniera specifica, ogni volta che un organo federale tratta dati congiuntamente ad altri organi federali o a organi cantonali o ancora a privati. Questa disposizione concerne soprattutto i grandi sistemi decentralizzati d'informazione e i sistemi detti ripartiti. *Sistemi decentralizzati* sono sistemi informatici nei quali il rilevamento dei dati avviene non a cura del gestore stesso del sistema, bensì di partecipanti del sistema situati alla periferia, Tale è ad esempio il caso del sistema d'informazione sul personale dell'amministrazione federale (PERIBU), gestito in effetti dall'Ufficio del personale, ma i cui dati sono introdotti a cura dei servizi del personale dei singoli Uffici. Per sistemi *«ripartiti»* si intendono i sistemi ottenuti con l'interconnessione di ordinatori di per sé indipendenti che con lo sviluppo sempre maggiore degli ordinatori personali dovrebbero in avvenire aumentare ancor più. La questione della responsabilità si pone in modo speciale per rapporto ai sistemi *congiuntamente* gestiti dalla *Confederazione e dai Cantoni*. Proprio in tale contesto la questione della responsabilità potrà essere risolta, in modo sensato, in parte sol-

tanto a livello federale. Per quanto concerne l'aspetto materiale si tratterà soprattutto di attribuire le responsabilità principali per un determinato sistema d'informazioni a un organo determinato. Dovrà inoltre essere stabilito in quale misura ogni partecipante avrà diritto a consultare i dati contenuti nel sistema e dovrà curarne l'esattezza e la sicurezza. Occorrerà infine disciplinare, in dettaglio, le modalità d'accesso delle persone interessate ai loro propri dati. Il Consiglio federale può delegare la responsabilità ai Dipartimenti nei casi siano coinvolte unità amministrative di un solo e unico Dipartimento.

Articolo 14 Fondamenti giuridici

Il *capoverso 1* stipula che, alla stregua di qualsiasi attività amministrativa effettuata da un organo federale, un trattamento dei dati ha bisogno di un fondamento giuridico. Questo vale per tutte le forme e tutte le fasi del trattamento dei dati, nella misura in cui gli articoli seguenti non prevedano un'eccezione. Il fondamento giuridico può essere un trattato di diritto internazionale pubblico, una disposizione costituzionale o legislativa oppure la norma di un'ordinanza emanata sulla base di uno di tali atti legislativi. Occorre giudicare secondo principi generali fino a quale punto il fondamento giuridico debba essere dettagliato. Determinante in materia è sapere se e in quale misura un trattamento di dati possa pregiudicare le libertà fondamentali dei cittadini, conoscere il tipo dei dati trattati, la cerchia delle persone interessate, ma anche l'organizzazione del sistema d'informazione e l'eventuale partecipazione di servizi cantonali o privati al trattamento dei dati. In ogni caso il fondamento giuridico deve definire lo scopo del trattamento, descrivere nelle grandi linee la sua portata e designare gli organi partecipanti. In considerazione della varietà quasi infinita di modi di trattamento dei dati in seno all'amministrazione federale, al fondamento giuridico non devono tuttavia essere poste esigenze troppo severe. Basterà in molti casi che un trattamento d'informazioni sia in relazione evidente con i compiti dell'organo federale pertinente. Del resto, salvo particolare disposizione legale contrastante, gli organi federali devono anche rispettare sempre i principi dell'articolo 4.

Il *capoverso 2* pone esigenze qualificate al trattamento di *dati personali degni di particolare protezione* e ai *profigili della personalità.* Tali dati devono da un canto poter essere trattati se una *legge in senso formale* lo prevede esplicitamente (lett. a): ciò ingloba anche i trattati internazionali e tutti i decreti federali soggiacenti al referendum obbligatorio. Poiché non sarà tuttavia praticamente possibile creare in una legge, per ogni trattamento di dati sensibili, il fondamento giuridico necessario, tali dati devono poter essere trattati, ove il trattamento sia indispensabile per l'adempimento di un compito chiaramente definito in una legge formale (lett. b). Per contro, il semplice fatto che un compito possa essere meglio eseguito grazie all'uso di dati degni di particolare protezione o di profili della personalità non è di per sé sufficiente per permettere il trattamento di tali dati. Onde tenere conto di bisogni insorgenti a breve termine, il Consiglio federale dovrà potere autorizzare, nel caso singolo, il trattamento di dati personali degni di particolare protezione oppure di profili della personalità. Noi possiamo tuttavia agire in tal senso soltanto se ci siamo prima assicurati che i diritti delle persone interessate non ne risultino pregiudicati

(lett. c). Il trattamento di dati degni di particolare protezione e di profili della personalità è quindi ammissibile se la persona interessata è consenziente oppure se ha reso i propri dati accessibili a tutti (lett. d). Il consenso non può tuttavia essere globale, ma deve bensì riferirsi a un determinato caso singolo: soltanto in tale occasione è possibile partire dal presupposto che il consenso è stato rilasciato in conoscenza delle implicazioni. Per quanto attiene all'accessibilità ai dati, rinviamo al commento relativo all'articolo 10 capoverso 2 lettera f. Per i trattamenti effettuati in conformità delle lettere b e c deve essere dato almeno un fondamento giuridico ai sensi del capoverso 1.

Articolo 15 Raccolta di dati personali

Le prescrizioni speciali sulla raccolta dei dati personali costituiscono un *complemento* dei principi enunciati nell'articolo 4 e delle prescrizioni generali sul trattamento dell'articolo 14. Esse devono garantire, in quest'epoca che vede l'amministrazione dover contare su un numero sempre più rilevante di informazioni e in particolare, anche su dati personali, che tali dati siano raccolti in modo che l'interessato possa esprimersi in merito ed opporsi a un trattamento illecito.

Il *capoverso 1* rileva quindi che i dati devono essere raccolti in maniera riconoscibile per le persone interessate. Questo principio può essere rispettato nel migliore dei modi se i dati sono rilevati presso la *persona interessata* stessa. È tuttavia ammissibile anche un rilevamento presso terzi, sempre che la persona interessata sia sufficientemente informata. La raccolta presso terzi, che già dispongono dei dati necessari costituisce per l'amministrazione un'importante possibilità di razionalizzazione che in principio non dovrebbe essere rimessa in questione. Spesso è anche nell'interesse del cittadino che non abbia a dovere ripetere le stesse indicazioni presso i diversi servizi amministrativi.

Visto che per la raccolta sistematica dei dati, in particolare per mezzo di *questionari* permette di riunire una quantità rilevante di dati, il capoverso 2 prevede *obblighi speciali d'informare* la persona interessata. Anche se dai dati raccolti con l'inchiesta non nasce necessariamente una collezione di dati ai sensi del presente disegno, le persone interessate devono tuttavia essere informate in maniera analoga a quella prescritta per le collezioni di dati (cfr. art. 5).

Infine, in base al *capoverso 3* è possibile rinunciare a informare la persona interessata sul trattamento dei dati in tre casi. L'informazione non è obbligatoria se la persona interessata, ad esempio, in un libro, ha reso accessibili a un vasto pubblico dati che la concernono (lett. a), se l'adempimento del compito dell'organo federale ne risulterebbe compromesso (lett. b) o se ne risultasse un dispendio eccessivo di lavoro (lett. c). L'ultimo caso potrebbe essere quello di rilevamenti statistici.

Articolo 16 Comunicazione di dati personali

L'esperienza mostra che la regolamentazione della comunicazione di dati personali ricopre il ruolo più importante in materia di protezione della personalità in diritto pubblico. La disposizione proposta nel disegno di legge parte dal presupposto che il moderno stato sociale e debitore di prestazioni ricorre in misura

sempre maggiore al trattamento di informazioni. Nella misura in cui si tratta di dati personali, il trattamento delle relative informazioni si trova ad essere spesso al centro di un conflitto tra le esigenze di un'attività amministrativa coordinata e razionale e gli imperativi della protezione della personalità. Anche se è incontestabile che le singole unità amministrative devono collaborare all'esecuzione di compiti comuni, occorre d'altro canto garantire che non ogni servizio amministrativo possa accedere a tutti i dati personali che globalmente sono trattati nello Stato. È indispensabile istituire una certa separazione tra le unità amministrative, vale a dire un tipo di «separazione informale dei poteri».

Nel diritto vigente vi sono soltanto alcuni abbozzi di disciplinamento dello scambio d'informazioni tra i diversi servizi amministrativi. Secondo numerose leggi sullo statuto dei funzionari è ancorato il segreto di funzione che vieta a un funzionario, fra l'altro, a comunicare a un'altra autorità fatti sui quali dev'essere rispettata la segretezza[43]. D'altro canto, le prescrizioni dell'assistenza giudiziaria e amministrativa prevedono obblighi reciproci d'informazione delle autorità. Disposizioni di questo genere non sono tuttavia molto numerose[44] e i principi dell'assistenza amministrativa e giudiziaria sono in Svizzera, a prescindere da una sparuta prassi in materia d'assistenza giudiziaria nel perseguimento penale[45], a malapena avviati. Il presente articolo costituisce quindi, in qualche modo, una specie di *disposizione generale sull'assistenza amministrativa e giudiziaria* e una *disposizione d'esecuzione* del *segreto generale di funzione.* In effetti, esso determina le condizioni alle quali gli organi federali possono comunicare dati personali. Esso non prevede tuttavia *alcun obbligo* di comunicare dati poiché anche nei casi nei quali sono soddisfatte le premesse dell'articolo 16, l'organo competente deve ancora esaminare se con la comunicazione dei dati non si violano i principi dell'articolo 4. In particolare i dati non possono essere comunicati all'estero, se con ciò la personalità dell'interessato risultasse gravemente pregiudicata (cfr. art. 4 cpv. 5). Le regole della comunicazione valgono sia per lo scambio di dati tra organi federali sia anche per la comunicazione dei dati ad autorità cantonali, comunali e straniere e a persone private nel Paese e all'estero. Esse costituiscono un completamento dell'articolo 14.

Giusta il *capoverso 1* la comunicazione è ammessa in cinque casi:

I dati possono essere comunicati se è dato un *fondamento giuridico* a tale scopo, vale a dire una legge, un'ordinanza o un contratto che prevedono la comunicazione. Questo fondamento giuridico deve riferirsi esplicitamente al *trasferimento dei dati in quanto tali.* Una competenza generale per trattare i dati ai sensi dell'articolo 14 non basta a tale proposito. Invece non conta chiedersi se l'autorità che comunica i dati eserciti un diritto o rispetti un obbligo o ancora dia seguito a una pretesa dei destinatari dei dati.

Mancando un fondamento giuridico, i dati personali possono tuttavia essere comunicati nel caso singolo se il destinatario non può altrimenti adempiere il proprio compito legale (lett. a). La limitazione al caso singolo significa che senza fondamento giuridico non può, a un altro organo o a un privato essere concesso un accesso permanente a una collezione di dati, come sarebbe invece possibile con l'accesso in linea o la fornitura sistematica di liste. Un caso sin-

golo ai sensi della lettera a è dato se i dati sono comunicati per *uno scopo unico*. Poco importa che si tratta di dati relativi a una persona singola o a più persone.

La mancanza del fondamento giuridico può essere sostituita dal consenso della persona interessata (lett. b) che può essere esplicito o tacito. Il consenso deve poi riferirsi al caso concreto: consensi globali non bastano. Ciò non significa tuttavia che il consenso sia valido soltanto se si riferisce a un'unica comunicazione di dati. La persona interessata può dare il proprio consenso anche per diverse comunicazioni di dati se risultano chiare le circostanze nelle quali la comunicazione può avvenire. È possibile, ad esempio, che una persona autorizzi il proprio datore di lavoro, una volta per tutte, a rilasciare informazioni ad altri datori di lavoro sulle proprie qualifiche professionali (cfr. anche il nuovo art. 328*b* CO proposto, n. 221.1). Se è impossibile, o possibile soltanto con un dispendio eccessivo, ottenere il consenso della persona interessata, rileviamo come basti che le circostanze permettano di presumere che la persona interessata avrebbe approvato la comunicazione.

La comunicazione dei dati è permessa anche quando la persona interessata ha comunque già reso i propri dati accessibili al pubblico, ad esempio con la pubblicazione in un libro o in una rivista (lett. c).

La comunicazione può infine essere possibile anche senza che esista fondamento giuridico o anche senza il consenso della persona interessata, nel caso questa ha negato il proprio consenso in maniera abusiva (lett. d). Questa disposizione dovrebbe trovare applicazione pratica soprattutto nel settore delle pretese risultanti dal diritto di famiglia, se ad esempio un genitore, obbligato a versare alimenti parte all'estero e se il coniuge o il figlio beneficiario degli alimenti vorrebbero conoscere il suo indirizzo presso l'ambasciata di Svizzera. La disposizione può assumere importanza anche in materia di assicurazioni sociali: si pensi ad esempio al lavoratore che vuole venire a sapere se il datore di lavoro abbia o meno versato i contributi. Prima che i dati vengano comunicati, la persona interessata deve in principio avere il diritto di esprimersi a proposito, ai sensi del diritto d'essere inteso. Questo diritto non è tuttavia assoluto; l'organo federale può rinunciare a raccogliere il parere della persona interessata, in due casi: se esiste altrimenti il pericolo che le pretese legali oppure importanti interessi di terzo corrono il rischio d'essere compromessi, oppure se l'interessato non è raggiungibile o non si è pronunciato entro il termine impartito.

La comunicazione di dati degni di particolare protezione o di profili della personalità soggiace, come anche il trattamento di tali dati e profili, a esigenze speciali. Se la persona interessata non ha dato il proprio consenso per la comunicazione, oppure se non ha reso i propri dati accessibili al pubblico, la comunicazione deve essere esplicitamente prevista dalla legge oppure dev'essere indispensabile all'esecuzione di un compito chiaramente definito in una legge. Se queste condizioni non sono adempiute, vi è sempre ancora la possibilità di sollecitare un'autorizzazione del Consiglio federale (cfr. art. 14 cpv. 2).

Giusta il *capoverso 2,* gli organi federali hanno la possibilità di comunicare, su richiesta di un altro organo pubblico o di una persona privata, nome e cognome, indirizzo e data di nascita di una determinata persona. Questa possibi-

lità risponde a un desiderio espresso da più parti in sede di consultazione. Determinati dati di base, necessari all'identificazione di una persona e che comunque sono già più o meno noti, devono poter essere comunicati in maniera semplice. Poiché però il capoverso 2 non statuisce un obbligo di comunicare, l'organo federale deve - anche per questo tipo di comunicazione dei dati - tenere conto di eventuali bisogni di protezione di una persona interessata. Esso può ad esempio rifiutare un'informazione se già il solo fatto che un organo dispone di dati su una persona può dar adito a conclusioni negative a proposito della persona interessata. Ciò vale in particolare a proposito della comunicazione di informazioni da parte delle autorità della Confederazione preposte al perseguimento penale. Il Consiglio federale può se del caso designare i servizi amministrativi autorizzati a fornire le informazioni previste al capoverso 2.

Il *capoverso 3,* infine, elenca casi nei quali un organo federale può e deve limitare una comunicazione di per sé ammissibile sulla base della presente legge. Il primo caso è costituito dall'esistenza di un *importante interesse pubblico o un interesse legittimo manifesto* di una persona interessata (lett. a). Questa disposizione è una sorta di «riserva d'ordine pubblico», valida nei confronti di qualsiasi destinatario. Per interesse pubblico importante si intende in primo luogo la protezione dello Stato o la sicurezza militare. L'espressione «interesse legittimo manifesto della persona interessata» può riferirsi, ad esempio, al bisogno di tenere nascosta l'identità di una persona che è stata coinvolta in un'inchiesta amministrativa. Sono poi riservati altri *obblighi legali di conservare il segreto* oppure *speciali disposizioni di protezione dei dati* (lett. b). In diversi settori, in particolare in quello delle assicurazioni sociali, valgono speciali obblighi di segretezza che soltanto nei casi designati dal Consiglio federale eccezionalmente permettono la comunicazione dei dati[46]. Esiste inoltre già una serie di disposizioni di protezione dei dati per certi settori specifici che fissano la cerchia dei destinatari autorizzati e in parte anche i tipi di dati che possono essere trasmessi[47]. Tali disposizioni sono considerate norme speciali dell'articolo 16 del presente disegno di legge.

L'assetto delle presenti disposizioni sulla comunicazione dei dati (e di quelle sulla raccolta dei dati) rende inutile qualsiasi regolamentazione specifica della *comunicazione dei dati alle autorità fiscali,* diversamente da quanto avveniva nell'avamprogetto. La pratica seguita sinora in materia di trasmissione d'informazioni alle autorità fiscali può essere mantenuta essenzialmente. La maggior parte delle leggi fiscali prevedono obblighi espliciti d'assistenza amministrativa[48], in modo tale che esiste il fondamento giuridico per la comunicazione dei dati, in certi casi anche dei dati degni di particolare protezione. Ove manchi un fondamento giuridico, all'autorità fiscale può essere rilasciata l'informazione auspicata, in un caso particolare, sulla base dell'articolo 16 capoverso 1 lettera a, nella misura in cui l'autorità abbia assolutamente bisogno di tale informazione per l'esecuzione dei suoi compiti. Una siffatta comunicazione dei dati non costituisce una violazione del principio della compatibilità degli scopi dell'articolo 4 capoverso 4, fintanto che all'autorità fiscale siano comunicate soltanto le informazioni effettivamente necessarie per l'accertamento fiscale. Giusta l'articolo 15 del disegno, l'autorità fiscale deve in tali casi far conoscere alla persona interessata il rilevamento dei dati, nel caso le informazioni neces-

sarie non vengono raccolte presso la stessa. Gli obblighi esistenti di fornire informazioni nei confronti delle autorità fiscali sono del resto giustificati poiché questi soggiacciono al segreto fiscale, vale a dire a un obbligo qualificato di segretezza che impegna le autorità fiscali ad osservare il silenzio, nei confronti sia dei privati, sia di altre autorità.

Articolo 17 Blocco dei dati

Questa disposizione prevede per la persona interessata un *diritto limitato* di opporsi, anche nel caso di comunicazioni di dati personali di per sé ammissibili. La possibilità del blocco riveste importanza soprattutto quando si tratta di comunicazione di dati all'estero e a privati. Nel caso di siffatte comunicazioni, l'organo federale responsabile non può prevedere tutte le implicazioni negative possibili. Per tale ragione, la persona interessata deve potere far valere direttamente i propri interessi. Il blocco vale in principio però anche in merito a comunicazioni di dati nei confronti di altre autorità: in questi ultimi casi tale possibilità dovrebbe tuttavia essere di rilievo subordinato, poiché nella maggior parte dei casi si applica la clausola d'eccezione del capoverso 2. Il diritto di bloccare non può essere fatto valere globalmente; la persona interessata deve invece rivolgersi agli organi competenti e designare esattamente i dati che devono essere bloccati.

Il diritto di bloccare non può, secondo il capoverso 1, essere esercitato da chiunque, bensì soltanto dalla persona interessata che rende verosimile un interesse degno di protezione. Un simile interesse è ad esempio dato se la persona interessata, in ragione della comunicazione dei dati, è stata esposta a soprusi, pressioni o addirittura persecuzioni da parte dei destinatari.

Secondo il *capoverso 2,* l'effetto di un blocco è inoltre limitato. La dove è dato un obbligo legale della comunicazione dei dati personali, l'organo responsabile deve comunicare i dati, nonostante il blocco (lett. a). Il blocco è senza rilievo anche nel caso l'organo federale sarebbe altrimenti impedito nell'adempimento dei propri compiti (lett. b).

Articolo 18 Obbligo di rendere i dati personali anomini o di distruggerli

I procedimenti moderni di copia delle informazioni, come anche le misure di sicurezza necessarie in ragione del trattamento automatizzato dei dati favoriscono la costituzione di grandi quantità di dati. Molte di queste non hanno più interesse pratico già dopo breve tempo. Poiché però esse possono tuttavia costituire un certo rischio di possibili lesioni della personalità, la presente disposizione fissa il principio secondo il quale tali dati devono essere distrutti o almeno resi anonimi. Tale prescrizione risponde al principio della proporzionalità del trattamento dei dati, come fissato nell'articolo 4 capoverso 3 del disegno. L'articolo tiene d'altra parte conto del fatto che determinati dati, anche se non sono più necessari per l'attività amministrativa ordinaria, tuttavia non devono essere distrutti o resi anonimi. Si tratta da un canto di atti che servono in vista di una possibile procedura di revisione, a titolo di prova o per misura di sicurezza (lett. a). Dall'altro si tratta di documenti interessanti per il loro valore storico. Quali siano, in particolare, tali documenti viene fissato nelle disposizioni concernenti l'Archivio federale: questi documenti devono essere de-

positati nell'Archivio federale (lett. b). Rileviamo infine che le disposizioni del regolamento dell'Archivio federale devono essere considerate come norme speciali dell'articolo 18 del disegno.

Contrariamente all'avamprogetto, abbiamo rinunciato a disciplinare *l'archiviazione dei dati.* Archiviati ai sensi del presente progetto (cfr. art. 3 lett. g) sono i documenti che vengono separati dagli atti correnti e la cui consultazione è limitata in ragione del fatto che sono stati allontanati o a causa di misure d'ordine organizzatorio (ad es., atti che sono conservati sotto chiave, in armadi e locali ai quali hanno accesso soltanto determinate persone, oppure - se si tratta di elaborazione automatizzata - sono i dati accessibili soltanto per mezzo di un codice speciale). Grazie a un'archiviazione conseguente è invero possibile accogliere molte delle esigenze di protezione dei dati. Non è tuttavia possibile fissare, in una regola generale, come l'archiviazione debba essere attuata. Troppo diverse sono le premesse d'ordine organizzatorio e locale presso i singoli servizi amministrativi dell'amministrazione federale e le organizzazioni che assolvono compiti federali. Bisogna poi distinguere tra i dati che occorrono quotidianamente, dati che servono soltanto all'occasione e dati usati saltuariamente. Ne consegue che occorrerebbe emanare per ogni settore una regolamentazione specifica.

Articolo 19 Trattamento dei dati per scopi della ricerca, della pianificazione e della statistica

L'interesse pubblico alla ricerca, alla pianificazione e alla statistica, ma anche il fatto che i trattamenti dei dati appaiono, in tale contesto, un po' meno pericolosi - in quanto non si riferiscono a persone determinate -, richiedono una regolamentazione speciale anche nel settore del diritto pubblico. L'articolo 19 prevede quindi diverse deroghe ai principi generali del disegno. La disposizione vale sia nel caso un organo responsabile tratti dati propri per scopi non relativi a persone, sia nel caso tale organo comunichi i dati in questione, per scopi della ricerca, della pianificazione o della statistica, ad altri organi della Confederazione, dei Cantoni o a privati. In quest'ultimo caso sono tuttavia riservate speciali prescrizioni relative alla segretezza.

Il *capoverso 1* elenca le *condizioni* che devono essere soddisfatte cumulativamente allorquando un organo federale intende appellarsi al privilegio della ricerca. Prima condizione: l'organo che utilizza dati personali per scopi della ricerca, della pianificazione o della statistica, deve renderli anonimi non appena lo permetta lo scopo del trattamento (lett. a). Per «rendere anonimi» si intende qualsiasi provvedimento volto a impedire l'identificazione delle persone interessate oppure a renderla possibile soltanto a prezzo di un dispendio eccessivo. Capita in pratica spesso che un ricercatore, un pianificatore o uno specialista in statistica, benché usi dati senza riferimento a persone determinate non intenda ancora rendere tali dati anonimi perché eccezionalmente deve conservarsi aperta la possibilità di risalire all'identità di una persona. In siffatte situazioni, egli deve operare con codici o criptogrammi. Egli può, ad esempio, separare le caratteristiche personali dagli altri dati in modo tale che non sia più possibile stabilire una relazione tra i dati e le persone senza passare per il numero di referenza. Si tratta di pratica oggi già molto seguita. L'organo federale che comu-

nica dati per il trattamento (senza riferimento alle persone) per scopi di ricerca, pianificazione o statistica, deve assicurarsi, per mezzo di oneri, istituiti per contratto o per decisione, che il destinatario dei dati non abbia a sua volta a trasmetterli a un terzo senza il suo consenso (lett. b). Occorre vigilare affinché tale terzo riutilizzi i dati soltanto per scopi di ricerca, pianificazione o statistica o per un altro scopo di trattamento che non si riferisca a persone determinate. Le facilitazioni introdotte dall'articolo 19, infine, valgono soltanto se i risultati del trattamento sono pubblicati in una forma che non permetta di identificare le persone interessate (lett. c).

Il *capoverso 2* enumera tutte le disposizioni della presente legge non applicabili al trattamento dei dati che non si riferiscono a persone. Si tratta in primo luogo del principio della compatibilità dello scopo, istituito dall'articolo 4 capoverso 4. Poiché i lavori di ricerca, pianificazione e statistica ai sensi di questa disposizione, non hanno implicazioni dirette sulle persone interessate, deve anche potersi trattare di dati che sono eventualmente stati raccolti in tutt'altro contesto (lett. a). Per la stessa ragione, gli organi federali devono poter trattare dati degni di particolare protezione o profili di personalità (anche se quest'ultima eventualità è praticamente irrilevante) per scopi di statistica, di ricerca o di pianificazione o anche per altri scopi che non si riferiscono a persone determinate, anche se si possono basare a tale proposito soltanto su un fondamento giuridico generale ai sensi dell'articolo 14 capoverso 1 e se le esigenze qualificanti dell'articolo 14 capoverso 2 non sono soddisfatte (lett. b). Inoltre non è necessario che essi rispettino le disposizioni generali relative alla comunicazione dei dati (lett. c). Ne consegue che la comunicazione di dati per scopi che non si riferiscono a persone determinate non ha bisogno di alcun fondamento giuridico suppletivo. La comunicazione può anche avvenire senza che il destinatario abbia bisogno dei dati per l'adempimento di un compito legale e senza che la persona interssata abbia, nel caso singolo, dato il suo consenso. L'organo federale dal quale provengono i dati deve invece, in base al capoverso 1 lettera b, dare il suo consenso alla nuova comunicazione.

Articolo 20 Attività di diritto privato degli organi federali

Determinate unità amministrative della Confederazione, in particolare FFS e PTT, ma anche le centrali d'acquisto dell'amministrazione federale, sono coinvolte, con la loro attività, dalla concorrenza economica. Il *capoverso 1* prevede che esse debbano essere parificate ai concorrenti privati, sempre che siano come queste sottoposte al diritto privato. Tale è il caso allorquando esse non esercitano funzioni di sovrano, vale a dire che le loro relazioni con i terzi non rivestono forma di decisioni, bensì di accordi di diritto privato. A tali condizioni, devono valere per loro gli oneri meno gravi del diritto sulla protezione dei dati, previsti nella sezione 3 della legge. Ciò significa in pratica, ad esempio, che esse possono se del caso respingere le richieste d'accesso semplicemente rilevando di essere in concorrenza economica (art. 6 cpv. 1 lett. d): anche le regole della sezione 4 relative al trattamento non devono essere rispettate.

Il fatto che organi federali siano in concorrenza economica e agiscano secondo il diritto privato non sfocia, secondo il capoverso 2, in un *allentamento della vigilanza sul rispetto delle prescrizioni sulla protezione dei dati.* Il Preposto alla

protezione dei dati deve potere esercitare il controllo sulle attività di diritto privato dell'organo federale come pure su quelle risultanti dalle sue funzioni di sovrano. Questo significa che gli organi federali in concorrenza economica devono rispettare gli stessi obblighi di registrazione e di notificazione (art. 7 e 8) degli altri organi federali.

Articolo 21 Protezione dello Stato e sicurezza militare

Gli organi preposti alla protezione dello Stato e alla sicurezza militare - in particolare la polizia federale e i servizi d'informazione e di sicurezza militari - esercitano i loro compiti soprattutto trattando dati personali. Essi devono poter contare sulle informazioni provenienti dalle più diverse fonti. Il trattamento esige una misura rilevante di segretezza: occorre in particolare proteggere i collaboratori di tali servizi. D'altro canto, la collaborazione con le autorità incaricate della protezione dello Stato e della sicurezza militare dei Paesi esteri è pure necessaria. Date tali circostanze è difficile fissare regole generali valide per l'attività d'informazione delle autorità preposte alla sicurezza dello Stato. La necessità di un'efficace protezione dei dati è evidente proprio in questo settore; tuttavia, in considerazione degli interessi superiori dello Stato, tale protezione può essere soltanto limitata. La presente disposizione attribuisce quindi al Consiglio federale la competenza di prevedere deroghe alla legge generale sulla protezione dei dati in materia di protezione dello Stato e di sicurezza militare. Tali eccezioni il Consiglio federale può disciplinare in un'ordinanza o autorizzare in casi singoli.

Il *capoverso 1* elenca tutte le disposizioni della presente legge in merito alle quali sono ammesse deroghe. Il Consiglio federale può quindi, per gli organi della protezione dello Stato e della sicurezza militare, prevedere eccezioni al principio della compatibilità degli scopi (art. 4 cpv. 4) e alle esigenze poste alle comunicazioni di dati all'estero (art. 4 cpv. 5 lett. a). È proprio della natura dell'attività delle autorità incaricate della protezione dello Stato, che esse debbano poter contare anche su dati che non sono stati raccolti in origine non per scopi della protezione dello Stato. Nello scambio di dati con autorità estere incaricate della protezione dello Stato avviene inoltre che siano, nel superiore interesse dello Stato, comunicate informazioni inerenti alle persone, anche se non è possibile escludere che tali persone abbiano a subire uno svantaggio. L'eccezione dell'articolo 4 capoverso 5 intende rendere possibile che la comunicazione dell'informazione ad autorità straniere, nell'interesse della sicurezza interna ed esterna del Paese, abbia a restare possibile nelle stesse proporzioni, come avviene attualmente sulla base del decreto del Consiglio federale concernente il servizio di polizia del Ministero pubblico della Confederazione, come pure sulla base delle prescrizioni del Dipartimento federale di giustizia e polizia relative[49]. Le autorità della protezione dello Stato, inoltre, raramente possono rinunciare a dati personali degni di particolare protezione. Il Consiglio federale deve potere autorizzare il trattamento di tali dati, anche se non sono rispettate le condizioni speciali introdotte dalla legge sulla protezione dei dati (lett. b). Per motivi di segretezza, le autorità incaricate della protezione dello Stato devono, a determinate condizioni, poter essere liberate dall'obbligo di notificare le loro collezioni di dati come pure le comunicazioni di dati all'estero

(lett. c). Il Consiglio federale può anche prevedere che una collezione di dati sia notificata al Preposto alla protezione dei dati, ma che quest'ultimo non pubblichi tale collezione di dati nel relativo registro. Deve infine essere creata la possibilità di disciplinare la collaborazione tra autorità della protezione dello Stato e della sicurezza militare, da una parte, e il Preposto alla protezione dei dati, dall'altra, in deroga ai principi generali (lett. d). Il Consiglio federale dovrà in particolare decidere se l'obbligo di notificare al Preposto alla protezione dei dati e il suo diritto di consultazione (art. 24 cpv. 3) debbano venire limitati.

Il *capoverso 2* rileva per motivi di chiarezza che il segreto di voto, di petizione e delle statistiche non può in nessun modo essere violato, neppure a favore della protezione dello Stato e della sicurezza militare.

Onde conservare ristretta la cerchia delle persone detentrici di segreti negli affari attinenti alla protezione dello Stato, il *capoverso 3* prevede che spetta al Dipartimento dal quale dipende l'organo interessato (DFGP o DMF), e non alla Commissione federale della protezione dei dati - rispettivamente al suo presidente - di dirimere le controversie in merito alla protezione dei dati, tra i servizi di protezione dello Stato, da un canto, e la persona interessata e il Preposto alla protezione dei dati, dall'altro. In caso di ricorso contro la decisione del Dipartimento da parte della persona interessata o di divergenze di pareri tra le autorità della protezione dello Stato e preposti alla protezione dei dati, decide il Consiglio federale. Questo rimedio di diritto è conforme alla regolamentazione generale della procedura federale applicabile agli affari inerenti alla protezione dello Stato (art. 100 lett. a OG; RS *173.110*).

Articolo 22 Pretese e procedura

Non vi ha soltanto un interesse pubblico a che gli organi federali trattino i dati personali conformemente alle esigenze in ordine alla protezione dei dati bensì anche un interesse della persona di volta in volta interessata. A quest'ultima l'articolo 22 riconosce la *pretesa giuridica* a esigere che i trattamenti dei dati avvengano secondo legge. Inoltre l'articolo regola la procedura che dovrà seguire la persona interessata per far valere le proprie pretese. Il sistema di protezione giuridico proposto è orientato per un verso sulle azioni di diritto civile giusta l'articolo 12 del presente progetto e l'articolo 28*a* del Codice civile e, dall'altro, sulla procedura amministrativa attualmente in vigore.

Secondo il *capoverso 1*, chi ha un *interesse legittimo* può far valere, nei confronti dell'organo responsabile le pretese legali risultanti dal diritto della protezione dei dati. Secondo la giurisprudenza amministrativa vigente non è legittimata soltanto la persona interessata, ma, a determinate condizioni anche un terzo i cui dati personali non sono in causa. La cerchia delle persone legittimate è quindi qualche po' più ampia che non nella parte della presente legge consacrata al diritto privato; occorre tuttavia rilevare che, a determinate condizioni, anche terze persone possono agire contro trattamenti di dati che non concernono direttamente la loro persona, basandosi sulla protezione generale delle personalità introdotta dal Codice civile. Anche la legittimazione delle *associazioni* è retta dai principi generali del diritto amministrativo. Le associazioni possono fare valere le pretese risultanti dal diritto della protezione dei dati a

condizione che esse giustifichino un *interesse proprio:* esse sono inoltre legittimate a *far valere gli interessi di un loro membro,* a condizione che la difesa degli interessi della maggioranza o di un numero rilevante dei loro membri avvenga secondo statuto e che i membri stessi siano legittimati a far valere individualmente la stessa pretesa[50]. Alla stessa stregua di quanto avviene nel settore del diritto privato, le istanze possono vertere sull'*astensione* da un trattamento illecito (lett. a), sull'*accantonamento* delle conseguenze di un siffatto trattamento (lett. b), o sulla *constatazione del carattere illecito* del trattamento (lett. c). Come già rilevato (cfr. a tale proposito le nostre osservazioni ad art. 5), il diritto d'accesso agli atti risultante dall'articolo 4 della Costituzione federale permette, a determinate condizioni, di risalire alla *fonte* dei dati. Eventuali pretese di risarcimento sono rette dalla legge sulla responsabilità della Confederazione.

Il *capoverso 2* precisa che è possibile chiedere la *rettificazione* o la *distruzione* dei dati, nell'ambito dell'azione negatoria e dell'azione di cessazione del danno (lett. a). Inoltre prevede, analogamente all'articolo 28*a* capoverso 2 del Codice civile, la possibilità di pubblicare o di comunicare a terzi la decisione (ad es., la constatazione che un trattamento era illecito o la rettificazione di un dato; lett. b).

Il *capoverso 3* estende al settore pubblico la possibilità di far *menzionare il carattere contestato* di un dato. Questo capoverso introduce una disposizione speciale sull'*onere della prova.* Poiché vige nel diritto amministrativo il principio di officialità, l'organo federale adito di una richiesta fondata sul diritto della protezione dei dati deve d'ufficio chiarire i fatti. Le parti sono tuttavia obbligate a collaborare al rilevamento dei fatti. Se l'inchiesta amministrativa non permette di stabilire l'esattezza o l'inesattezza di un dato e se l'organo rifiuta di rinunciare al dato contestato, esiste la possibilità di apporre la menzione del carattere oggetto di controversia. Tale menzione è il segno che la persona interessata non condivide il parere dell'autorità sulla presentazione dei fatti. Spetterà alla giurisprudenza fissare la forma di questa menzione, o come semplice segno distintivo o piuttosto sul genere del diritto di risposta.

Il *capoverso 4* rileva esplicitamente che le richieste risultanti in ordine alla protezione dei dati ai sensi del presente articolo devono essere trattate secondo i principi della legge sulla procedura amministrativa. Ciò vale anche per i settori ai quali non si applica la legge sulla procedura amministrativa secondo gli articoli 2 e 3 della stessa. In effetti, i motivi di queste eccezioni – esistenza di disposizioni speciali di procedura o necessità di decidere rapidamente, fra gli altri – non valgono in materia di protezione dei dati. L'applicabilità della legge sulla procedura amministrativa significa in primo luogo che le richieste ai sensi dei capoversi 1 e 2 devono essere evase in forma di *decisione.* Dovrà dirimere l'autorità giudicante la questione a sapere se tale decisione sia legata a un'altra procedura (ad es., procedura fiscale) oppure se debba restare separata. Rileviamo infine che anche il diniego o la restrizione devono pure rivestire la forma della decisione.

Il *capoverso 5* prevede un *rimedio di diritto speciale* per le cause in materia di diritto sulla protezione dei dati. Le decisioni pertinenti non possono essere deferite all'autorità di sorveglianza, bensì alla Commissione federale della protezione dei dati (cfr. a tale proposito l'art. 27).

221.5 Sezione 5: Preposto federale alla protezione dei dati

Articolo 23 Nomina e statuto

Le norme di comportamento da sole non permettono di creare una protezione efficace dei dati. Affinché i principi di protezione dei dati introdotti dalla legge abbiano ad essere effettivamente rispettati nella realtà giuridica, è necessaria la vigilanza, ma soprattutto anche la consulenza da parte di un organo competente. La necessità di un controllo non è stata in principio posta in questione neppure nella procedura di consultazione, nonostante i pareri siano poi stati in parte divergenti in merito all'assetto concreto. Il presente disegno cerca di istituire una sorveglianza sulla protezione dei dati che sia efficace, e in pari tempo semplice e vicina al cittadino. In luogo della Commissione della protezione dei dati composta di tredici membri che prevedeva l'avamprogetto, istituzione dall'assetto grave, con un complesso capitolato d'oneri, la presente legge affida la sorveglianza in gran parte al *Preposto alla protezione dei dati.* Le controversie in materia di protezione dei dati saranno di competenza di una *Commissione della protezione dei dati* che funzionerà come istanza di ricorso e d'arbitrato ai sensi del progetto di revisione della legge federale sull'organizzazione giudiziaria. Se le competenze del Preposto e della Commissione sono assai estese nel settore pubblico, esse sono invece molto più ristrette nel settore privato, poiché esse si limitano ai trattamenti di dati che presentano gravi rischi.

Secondo il *capoverso 1,* la nomina è di spettanza del Consiglio federale. Compete inoltre a quest'ultimo di precisare le condizioni d'assunzione, sia in generale, sia nel singolo caso. Il Preposto alla protezione dei dati avrà lo statuto di funzionario, e sarà in ogni caso tenuto al rispetto del segreto di funzione. Egli sarà sottoposto amministrativamente al Dipartimento federale di giustizia e polizia, poiché dovrà trattare in primo luogo *questioni giuridiche.*

Il Preposto dispone, giusta il *capoverso 3,* di un segretariato proprio, al cui finanziamento provvede il Consiglio federale nel quadro del preventivo.

Articolo 24 Sorveglianza

La disposizione definisce le competenze del Preposto alla protezione dei dati e regola il modo di lavoro. Le sue competenze sono rivolte soprattutto ad aprire un'inchiesta se deve presumere un'eventuale lesione della personalità e rivolgere *raccomandazioni* a quanti trattano i dati. Egli può anche informare le persone interessate, che si sono a lui rivolte, sui rilievi fatti. Gli è tuttavia impossibile ordinare misure vincolanti.

Secondo il *capoverso 1,* il Preposto non soltanto vigila sul rispetto della legge, ma deve anche sorvegliare tutti gli atti legislativi federali che contengono disposizioni di protezione dei dati. Si intendono con questi non soltanto la legislazione speciale sulla protezione dei dati, attuale e futura, ma anche i trattati internazionali. Si precisa inoltre che il Consiglio federale è escluso dalla sorveglianza del Preposto alla protezione dei dati: quest'ultimo non può in effetti essere organo di controllo della propria autorità di sorveglianza. Ciò non significa però che il Consiglio federale sia dispensato dal rispetto delle disposizioni sulla protezione dei dati.

Secondo il *capoverso 2,* il Preposto alla protezione dei dati può aprire un'inchiesta, motu proprio o sulla base di un'istanza di terzi, onde procedere ai chiarimenti che gli sembreranno necessari. E poiché egli non sarà mai in grado di inquisire tutti i trattamenti di dati problematici nell'ottica della protezione dei dati, dovrà limitarsi ai casi di portata particolare e di grande rilievo pregiudiziale. Così, anche per le persone che propongono azione contro una violazione effettiva o presunta di prescrizioni sulla protezione dei dati non è dato un diritto al disbrigo. Nel caso di trattamenti di dati da parte di privati, il Preposto alla protezione dei dati può soltanto eccezionalmente procedere a indagini. Conformemente al principio dell'autonomia privata vigente nel diritto civile, spetta in principio all'interessato, e non a un'autorità statale, opporsi alle lesioni della personalità causate da trattamenti privati dei dati. Le pretese che ne conseguono devono essere portate davanti al giudice civile. Un'eccezione è data soltanto in tre casi: il Preposto alla protezione dei dati deve potere intervenire anche nel settore privato allorquando determinati metodi di trattamento portano in sé il pericolo della lesione della personalità di un numero rilevante di persone (lett. a). Si può in tale contesto parlare di *errori nella concezione di un sistema d'informazione* che non è possibile accantonare adeguatamente con i rimedi del diritto della procedura civile. In questo caso il Preposto alla protezione dei dati deve poter essere in grado, per ragione d'interesse praticamente pubblico di procedere a un'inchiesta. Delle stesse facoltà egli dispone anche a proposito delle *collezioni di dati sottoposte all'obbligo della registrazione* e delle *comunicazioni all'estero che devono essere notificate* (lett. b e c). Anche in questi casi i rischi di una lesione della personalità sono molto rilevanti. Se il Preposto, in occasione della notifica di tali trattamenti di dati, constata che un trattamento può mettere in pericolo la personalità, egli deve poter prendere le misure che s'impongono, perché altrimenti l'obbligo di registrare e di notificare non avrebbe efficacia alcuna. Poiché però l'obbligo di registrare a carico di elaboratori privati di dati è molto limitato, l'attività del Preposto alla protezione dei dati in questo campo è costretta in limiti ristretti. Se i dati sono invece trattati da organi federali, il Preposto può in ogni momento procedere a qualsiasi indagine che ritenga utile (lett. d). Un controllo tanto esteso si spiega con il fatto che l'amministrazione soggiace senza restrizione alcuna al principio della legalità.

Il *capoverso 3* riconosce al Preposto alla protezione dei dati il diritto *a raccogliere tutte le informazioni* necessarie per le sue inchieste. Egli ha quindi il diritto d'esigere la produzione di atti e, in particolare, sono soprattutto le concezioni dei sistemi informatici a interessarlo. Egli può anche farsi presentare sul posto i trattamenti dei dati, onde rilevare quali sono le possibilità effettive di trattamento. Oltre a ciò, egli deve poter raccogliere informazioni, non soltanto presso gli elaboratori principali responsabili dei dati o presso i detentori di collezioni di dati, bensì anche presso i loro ausiliari. Le persone coinvolte dalle inchieste devono sostenere il Preposto alla protezione dei dati; essi hanno un obbligo di cooperare analogo a quello previsto all'articolo 13 della legge sulla procedura amministrativa (RS *172.021*). L'obbligo di cooperare non deve, d'altro canto, avere la conseguenza che elaboratori privati o organi della Confederazione debbano gravare sé stessi. Il capoverso 3 prevede quindi che una per-

sona implicata in un'inchiesta condotta dal Preposto alla protezione dei dati può rifiutare di testimoniare; sono applicabili per analogia l'articolo 16 della legge sulla procedura amministrativa e, in parte l'articolo 42 capoversi 1 e 2 della legge di procedura civile federale (RS *273*). Chi tratta i dati o un terzo possono quindi rifiutare di testimoniare, se ciò esponesse loro o parenti prossimi al perseguimento penale, in particolare per violazione degli articoli 28 o 29 del disegno. Le persone interrogate possono opporre al Preposto alla protezione dei dati anche un segreto professionale, tuttavia soltanto finché la persona interessata li svincoli dall'obbligo di rispettare il segreto. Il segreto di funzione non può invece essere opposto al Preposto alla protezione dei dati.

Se il Preposto, nell'ambito dell'inchiesta alla quale procede, giunge alla conclusione che un tipo di trattamento viola le prescrizioni della presente legge, allora emana una *raccomandazione* giusta il *capoverso 4*. Con questa il Preposto invita di regola chi tratta i dati a modificare in avvenire la sua pratica, senza però riferirsi a casi particolari. È però anche possibile che il Preposto abbia a rilasciare una raccomandazione concernente una determinata persona interessata o un gruppo di persone. La raccomandazione non è vincolante, né per gli elaboratori privati di dati, né per gli organi federali. *Non* si tratta quindi di una *decisione* che può essere attuata con i mezzi dell'esecuzione forzata. Ne consegue che la persona privata e gli organi federali sono liberi di conformarsi o meno alla raccomandazione. Nel secondo caso essi corrono tuttavia il rischio che, nel quadro di un'azione fondata sul diritto privato o di una procedura ricorsuale di diritto pubblico, venga rilevato che il trattamento contestato o dichiarato illecito: il che potrebbe avere per conseguenza d'impegnare la loro responsabilità civile o penale. Essi devono inoltre contare sulle possibilità che il Preposto deferisca la pratica alla Commissione della protezione dei dati: quest'ultima può allora constatare il carattere illecito del trattamento in una *decisione vincolante*.

Il Preposto invita il destinatario di una raccomandazione a dichiarare entro un determinato termine se intende conformarvisi o meno. Se il Preposto non riceve alcuna risposta o riceve una risposta negativa o ancora se rileva che il trattamento illecito non è interrotto nonostante sia rilasciata dichiarazione d'accettazione della raccomandazione, egli può, se lo ritiene opportuno, sottoporre la pratica alla Commissione della protezione dei dati, in virtù del *capoverso 5* lettera a. Il Preposto esige una decisione della Commissione se sono in gioco importanti interessi pubblici e se si tratta di questioni d'importanza pregiudiziale. Nei casi nei quali sono colpite soltanto una o poche persone da un trattamento illecito di dati e non sono invece toccati interessi pubblici, il Preposto può rinunciare ad adire la Commissione della protezione dei dati e rinviare le persone che gli si sono rivolte, ai rimedi ordinari di diritto (lett. b). Spetta poi alla persona interessata di rivalersi nei confronti del privato che ha trattato i dati con azione civile giusta l'articolo 12 oppure nei confronti di organi federali con ricorso giusta l'articolo 22. Se l'affare è deferito alla Commissione della protezione dei dati, questa esamina la questione contestata ed emana una decisione. Poiché la raccomandazione del Preposto è in generale rispettata, le persone interessate stesse saranno raramente associate a questa procedura.

Articolo 25 Informazione

Le esperienze fatte all'estero mostrano che la protezione dei dati può imporsi soltanto se gli organi che sono incaricati hanno la possibilità d'informare sulle loro attività e di conferire alle stesse una certa pubblicità. Secondo il *capoverso 1,* il Preposto fa rapporto all'Assemblea federale e al Consiglio federale, periodicamente e secondo i bisogni. I rapporti periodici sono relazioni sull'attività e devono sempre essere pubblicati. In merito ai rapporti su avvenimenti singoli, il Consiglio federale decide di caso in caso in merito alla pubblicazione.

In virtù del *capoverso 2,* il Preposto ha anche la possibilità di rivolgersi direttamente al pubblico, in casi d'interesse generale. Sarà ad esempio il caso quando rilascerà una raccomandazione concernente un sistema informatico d'importanza nazionale. Egli può tuttavia portare alla conoscenza del pubblico dati sottoposti al segreto d'ufficio soltanto con il consenso dell'autorità competente. Affinché quest'ultima non possa tuttavia senz'altro impedire la rivelazione di abusi, è previsto che, in caso di divergenze di parere tra lei e il Preposto alla protezione dei dati, decide definitivamente il presidente della Commissione della protezione dei dati.

Articolo 26 Altri compiti

Oltre alla sorveglianza secondo l'articolo 24 che costituisce il nocciolo dell'attività del Preposto alla protezione dei dati, questi deve adempiere altri compiti che sono fissati nel *capoverso 1.* Poiché, in materia di protezione dei dati egli dispone di vaste conoscenze e di una grande esperienza pratica, il Preposto sarà in grado di informare e di assistere con la consulenza privati, ma anche organi della Confederazione e dei Cantoni e se del caso anche agire da mediatore in questioni attinenti alla protezione dei dati (lett. a). Grazie a tali attività, il Preposto può contribuire in misura rilevante a che non insorgano, in primo luogo, conflitti sul diritto in materia di protezione dei dati. Egli deve inoltre pronunciarsi sui progetti di atti legislativi federali, rilevanti per la protezione dei dati (lett. b). Il Preposto alla protezione dei dati deve inoltre collaborare con le autorità nazionali ed estere alle quali incombe la protezione dei dati (lett. c). Egli può in particolare promuovere lo scambio di informazioni tra i responsabili della protezione dei dati della Confederazione e dei Cantoni. I compiti menzionati sono in parte oggi già eseguiti dal Servizio della protezione dei dati dell'Ufficio federale di giustizia. Il Preposto assicura però anche assistenza giudiziaria ai sensi degli articoli 13 e segg. della Convenzione n. 108 del Consiglio d'Europa per la protezione delle persone nei confronti del trattamento automatizzato dei dati di carattere personale. Egli orienta, su richiesta, le autorità straniere sul diritto e sulla pratica amministrativa svizzera in materia di protezione dei dati; egli fornisce informazioni concrete su determinati trattamenti automatizzati dei dati effettuati nel nostro Paese. Il Preposto è infine la persona più adatta per valutare in quale misura la protezione dei dati sia assicurata in un altro Paese. Gli può infine essere chiesto, da parte di privati e di autorità di fornire pareri sulla misura nella quale un trasferimento di dati all'estero ai sensi dell'articolo 4 capoverso 4 potrebbe minacciare seriamente la personalità della persona interessata (lett. d).

I settori ai quali si applica la presente legge non sono i soli ad avere problemi in ordine alla protezione dei dati. Gli organi dell'amministrazione federale hanno, giusta il *capoverso 2* la possibilità di farsi assistere e consigliare dal Preposto alla protezione dei dati. Questi, da parte sua, può chiedere che gli siano presentati i trattamenti di dati delle autorità che non soggiacciono alla legge sulla protezione dei dati in virtù dell'articolo 2, quali i servizi incaricati di tenere i registri pubblici, di condurre indagini preliminari di polizia, d'assicurare l'assistenza giudiziaria internazionale e di dirigere le procedure penali amministrative. Affinché il Preposto possa farsi un'idea esatta dei problemi esistenti, alle autorità è permesso di concedere accesso ai loro affari. In tale contesto, il presente capoverso 2 dev'essere considerato un'eccezione del principio del segreto di funzione secondo l'articolo 27 degli Statuti dei funzionari e dell'obbligo di testimoniare istituito dall'articolo 26 di tali Statuti.

Il *capoverso 3* regola i compiti del Preposto in relazione all'attività della Commissione del segreto professionale in materia di ricerca medica (cfr. a tale proposito il n. 222.43).

221.6 Commissione federale della protezione dei dati

Articolo 27

Con la creazione della Commissione federale della protezione dei dati, la presente legge garantisce la più ampia protezione giuridica possibile nel settore pubblico. Giusta il *capoverso 1,* questa commissione è una commissione d'arbitrato e di ricorso ai sensi delle disposizioni sulla procedura amministrativa contenute nel disegno di revisione della legge federale sull'organizzazione giudiziaria[51]. Anche nel settore della protezione dei dati, vuol essere attuata la concezione di una riduzione delle procedure ricorsuali interne all'amministrazione e di un alleviamento del Tribunale federale, con la creazione di speciali autorità giudiziarie amministrative: tale concezione è stata prevista nell'ambito della revisione dell'organizzazione giudiziaria federale. Varranno quindi, anche per la Commissione della protezione dei dati le nuove disposizioni della legge sulla procedura amministrativa. La commissione sarà composta di sette membri; il Consiglio federale può prevedere nella legislazione d'esecuzione di questa legge o in una speciale ordinanza sull'organizzazione della commissione, che la stessa abbia a formare una divisione ciascuna per il settore pubblico e per il settore privato. Giusta le regole generali valevoli per le commissioni d'arbitrato e di ricorso, la Commissione della protezione dei dati deciderà delle questioni di rilievo fondamentale nella composizione di cinque membri e delle altre questioni nella composizione di tre membri.

Il *capoverso 2* definisce i compiti della commissione. La commissione statuisce in prima istanza sulle raccomandazioni che il Preposto alla protezione dei dati ha adottato nell'ambito delle sue inchieste (cfr. art. 24) e che il Preposto ha sottoposto alla commissione per decisione (lett. a). In seconda istanza la commissione pronuncia sui ricorsi contro decisioni di organi federali in materia di protezione dei dati (lett. b). Si può a tal proposito trattare, ad esempio, di decisioni concernenti il diritto d'accesso, oppure di decisioni relative a richieste di

rettificazione o distruzione ai sensi dell'articolo 22. Pure in seconda istanza la Commissione di protezione dei dati decide dei ricorsi contro le decisioni della Commissione del segreto professionale in materia di ricerca medica (lett. c; cfr. a tal proposito le nostre osservazioni n. 222.4). Infine, le decisioni cantonali di ultima istanza, prese in applicazione delle disposizioni di diritto pubblico federale relative alla protezione dei dati possono essere deferite alla commissione (lett. d). La legge non si applica invero ai trattamenti di dati eseguiti dagli organi cantonali. Tuttavia valgono anche per questi determinate prescrizioni speciali di protezione dei dati della Confederazione (ad es., nel diritto delle assicurazioni sociali e nel diritto sugli stranieri).

Le regolamentazioni previste dalle lettere b e d hanno per conseguenza che l'istanza che deciderà delle pretese di protezione dei dati basate unicamente sulla legge presente, non è l'autorità di ricorso abitualmente competente nella pertinente materia. Ma poiché, proprio all'inizio dell'esistenza della legge sulla protezione dei dati è importante che abbia a cristallizzarsi un'unità di giurisprudenza sulle questioni di protezione dei dati, può essere ammessa tale suddivisione del rimedio di diritto. Poiché le decisioni della Commissione della protezione dei dati possono essere portate, con il ricorso di diritto amministrativo, davanti al Tribunale federale è inoltre garantito che l'alto Tribunale esaminerà l'applicazione della legge indipendentemente dal contesto. Vi possono però essere casi, nei quali una persona interessata, insieme a una richiesta di protezione dei dati, avanzi anche altre pretese che nulla hanno a che vedere con la legge sulla protezione dei dati. Si potrebbe immaginare, ad esempio, che qualcuno esiga (cfr. art. 22 cpv. 2 lett. a) dagli organi dell'assicurazione invalidità una rettifica di dati che concernono il suo stato di salute, per essere quindi in grado di motivare la richiesta di una rendita d'invalidità maggiorata. La pretesa principale non è di natura della protezione dei dati, ma è volta a ottenere una prestazione assicurativa. Una siffatta domanda dev'essere trattata nella procedura normale, sulla via delle istanze previste all'uopo. La Commissione della protezione dei dati non entrerà nel merito delle questioni di protezione dei dati che sono soltanto richieste pregiudiziali che permettono di far valere prestazioni assicurative.

È possibile che il Preposto alla protezione dei dati, in occasione di un'inchiesta, s'imbatta in un trattamento che deve essere subito abbandonato o modificato, ove si vogliano impedire gravi danni a carico di una persona. In tale caso, il *capoverso 3* permette al Preposto di chiedere al presidente della Commissione della protezione dei dati di adottare *provvedimenti cautelativi.* La persona interessata ha la possibilità di fare una cosa analoga: si baserà sull'articolo 28*c* del Codice civile se si tratta di materia del settore privato, sull'articolo 56 della legge sulla procedura amministrativa se si tratta del settore pubblico.

221.7 Sezione 7: Disposizioni penali

Violazioni delle disposizioni della legge sulla protezione dei dati non dovrebbero in principio essere represse per mezzo di sanzioni penali, bensì con sanzioni di diritto civile o amministrativo. Il presente progetto prevede tuttavia

tre eccezioni a questa regola. Sono punibili in primo luogo la violazione degli obblighi d'informare, di notificare e di collaborare da parte di privati (art. 28), poiché tali obblighi garantiscono una *certa trasparenza* del trattamento dei dati. Ove essi non siano rispettati, la legge sulla protezione dei dati resta in gran parte inefficace. È punibile anche colui che rivela dati personali segreti e sensibili dei quali è venuto a conoscenza nell'ambito della sua attività professionale (art. 29). Facendo appello a uno specialista e affidandogli dei dati, la persona interessata crea un rapporto di fiducia che dev'essere protetto. Infine, anche la sottrazione di dati personali dev'essere dichiarata punibile (art. 179^{novies} CP). Le due prime fattispecie, in quanto semplici infrazioni, possono essere disciplinate nella legge sulla protezione dei dati stessa. La terza fattispecie è invece un delitto che presenta inoltre una certa affinità con il titolo terzo del Codice penale: essa viene introdotta nel Codice penale. Il perseguimento penale è nei tre casi di competenza dei Cantoni.

Articolo 28 Violazione degli obblighi d'informare, di notificare e di collaborare

Secondo il *capoverso 1* il detentore privato di una collezione di dati è punito con l'arresto o con la multa, se viola l'obbligo d'informare istituito dall'articolo 5 o se rifiuta di fornire le informazioni senza indicare i motivi ai sensi dell'articolo 6 capoverso 2. È punita l'informazione inesatta e anche l'informazione incompleta, nella misura di cui colui che tratta i dati lascia credere che l'informazione è completa. Non è invece punibile chi pretende di non essere obbligato a fornire informazioni. In questi casi, dev'essere deciso per la via di un'azione di diritto civile se il rifiuto o la limitazione dell'informazione sia avvenuto a giusto titolo. Si rende invece punibile colui che pretende di non detenere alcuna informazione sulla persona interessata. Agisce *intenzionalmente* ai sensi della disposizione chi conosce il carattere inesatto o incompleto delle informazioni che fornisce. Se chi tratta i dati rilascia un'informazione senza controllarla, nonostante sappia che la stessa è probabilmente inesatta, commette *dolo eventuale*. La violazione dell'obbligo d'informare è un delitto punito a querela di parte; l'autore è punito soltanto se ha proposto azione chi ha chiesto l'informazione.

Il *capoverso 2* prevede che possono essere puniti d'ufficio i privati che al Preposto alla protezione dei dati non notificano collezioni di dati soggiacenti all'obbligo della registrazione o una comunicazione di dati all'estero sottoposta all'obbligo della notificazione oppure che forniscono indicazioni inesatte in occasione della notificazione (lett. a). È punibile chi ha agito intenzionalmente, vale a dire che ha inteso sottrarsi volontariamente a uno di questi obblighi. Se egli non conosce le pertinenti prescrizioni, può appellarsi alla non conoscenza del diritto; in tale caso, il giudice potrà sia ridurre la pena, sia fare astrazione dalla pena[52)]. Infine è punito il privato che fornisce al Preposto alla protezione dei dati, in occasione del chiarimento dei fatti, informazioni inesatte, oppure se rifiuta di collaborare (lett. b). Questa disposizione deve garantire al Preposto alla protezione dei dati di poter raccogliere, in occasione dei suoi chiarimenti, tutte le informazioni necessarie.

Abbiamo rinunciato a sottoporre gli organi federali a queste disposizioni poiché esiste già nell'amministrazione una sorveglianza dei servizi e poiché il funzionario che non adempie il suo obbligo, contrariamente a quanto avviene per le persone private, può, con misure disciplinari, essere chiamato a rispondere. Inoltre la sorveglianza del Preposto alla protezione dei dati nel settore pubblico è più estesa che non nei confronti dei privati che trattano dati. Sarebbe peraltro inabituale permettere all'autorità federale richiedente, il Preposto alla protezione dei dati, di intentare azione penale contro un funzionario o un ufficio per essersi questi rifiutati di fornirgli informazioni e quindi di prestargli l'assistenza amministrativa necessaria. Nel caso di simili controversie spetta all'autorità gerarchicamente superiore, vale a dire in ultima istanza il Consiglio federale, di decidere se debba essere prestata assistenza amministrativa.

Articolo 29 Violazione dell'obbligo di osservare il segreto

In ragione del fatto che le attività professionali si specializzano sempre più, e che i metodi di trattamento dell'informazione divengono sempre più sofisticati, la protezione del segreto professionale introdotta dall'articolo 321 del Codice penale (CP) è ora insufficiente. Questa disposizione si applica unicamente a ecclesiastici, avvocati, difensori, notai, revisori e personale medico, come pure ai loro ausiliari. La presente disposizione intende sottoporre all'obbligo di rispettare il segreto determinate attività professionali alle quali l'articolo 321 CP non è applicabile. Sarebbe stato possibile estendere il campo d'applicazione dell'articolo 321 CP ad altre categorie professionali: questa soluzione è stata tuttavia scartata poiché le professioni menzionate all'articolo 321 beneficiano di regola del diritto di rifiutare la testimonianza, previsto dalle leggi di procedura federale e cantonali; un diritto che non deve essere esteso tramite la legislazione sulla protezione dei dati. Una nuova versione dell'articolo 321 CP sarà tuttavia esaminata nel quadro della revisione della parte generale del Codice penale.

Secondo il *capoverso 1* entrano in linea di conto come autori soltanto persone per le quali la conoscenza di dati personali segreti degni di particolare protezione è indispensabile. Questo è il caso, per esempio, dello psicologo, dell'assistente sociale o del proprietario di un'agenzia matrimoniale, non però dei parrucchieri. Quest'ultimi possono invero, nell'esercizio della loro professione, giungere a conoscenza di dati personali segreti e sensibili, che non sono tuttavia necessari per l'esercizio della professione. Poiché la disposizione penale non si applica a ognuno, bensì soltanto a determinate categorie professionali, la relativa fattispecie costituisce un *delitto di funzione propriamente detto*. Oggetto dell'atto sono *dati personali segreti* che sono inoltre degni di particolare protezione ai sensi dell'articolo 3 lettera e. In merito agli articoli 162 (violazione del segreto di fabbrica o commerciale) e 321 (violazione del segreto professionale) del Codice penale, dottrina e giurisprudenza sono del parere che i dati sono segreti allorquando sono relativamente sconosciuti, vale a dire che essi non sono né noti né accessibili a tutti e che la persona interessata intende, a giusto titolo, mantenere segreti. È punibile soltanto l'atto intenzionale. Chi ignora di essere obbligato a osservare il segreto può invocare l'errore di diritto ai sensi dell'articolo 20 CP. La pena è l'arresto o la multa e l'atto è punito soltanto a querela di parte.

Secondo il *capoverso 2* sono ugualmente punibili gli ausiliari impiegati o apprendisti della persona sottoposta, giusta il capoverso 1, all'obbligo di mantenere il segreto e degni di particolare protezione.

Secondo il *capoverso 3* la protezione penale non si estingue, anche se la persona tenuta alla segretezza ha cessato l'attività professionale o ha concluso la formazione.

221.8 Sezione 8: Disposizioni finali

Articolo 30 Esecuzione

Il *capoverso 1* rinvia alla competenza generale del Consiglio federale relativa alle disposizioni d'esecuzione, date sin qui dalla Costituzione federale.

I capoversi seguenti concedono al Consiglio federale competenze che non sono già contenute nella competenza generale relativa alle disposizioni d'esecuzione. Secondo il *capoverso 2,* il Consiglio federale emana disposizioni specifiche che reggono il trattamento dei dati personali deposti nell'Archivio federale. Esso può prevedere deroghe alle regole sul diritto d'accesso (art. 5 e 6) e sul trattamento di dati degni di particolare protezione (art. 14 cpv. 2 e 16 cpv. 1). Tali deroghe possono divenire necessarie perché con l'archiviazione degli atti nell'Archivio federale può essere limitato il diritto d'accesso. La massa enorme di dati depositati nell'Archivio federale può di regola ancora essere consultata a partire dal nome della persona, tuttavia il dispendio di lavoro necessario a questo scopo è in molti casi eccessivo. Nell'Archivio federale si trovano inoltre dati degni di particolare protezione in grande quantità. Una volta trascorso il termine durante il quale essi non possono essere consultati, il loro trattamento non deve tuttavia necessariamente essere basato su un fondamento giuridico esplicito in una legge formale o su una preveniente autorizzazione del Consiglio federale.

Secondo il *capoverso 3* il Consiglio federale può prevedere deroghe alle regole sul diritto d'accesso per quanto concerne le informazioni fornite dalle rappresentanze diplomatiche e consolari svizzere all'estero. Potrebbe in effetti risultare delicato per le rappresentanze di dover fornire informazioni su uno straniero all'estero, perché tale fatto potrebbe compromettere le relazioni con lo Stato di cui è cittadino la persona interessata.

Il *capoverso 4* contiene tre altre deleghe legislative al Consiglio federale. Esso deve potere determinare le collezioni di dati il cui *trattamento* deve fare oggetto di *regolamento* (lett. a). Occorre in effetti che per ciascuna delle importanti collezioni di dati che servono comtemporaneamente a scopi molteplici, in particolare per quelle che dipendono da sistemi detti «ripartiti», i principi della presente legge siano tradotti in pratica. Ordinamenti per il trattamento creano ulteriore trasparenza e facilitano con questo il controllo. Il Consiglio federale potrà fondarsi sull'attuale registro delle collezioni di dati dell'amministrazione federale per determinare quali collezioni di dati debbano fare oggetto di un regolamento. Inoltre il Consiglio federale può indicare a quali condizioni un *terzo* - in particolare un privato - *possa trattare dati per conto di un organo*

federale e quando un organo federale possa effettuare un trattamento per conto di un altro servizio amministrativo o di un privato (lett. b). Ciò facendo, il Consiglio federale dovrà valutare in quale misura un trattamento di dati personali effettuato in relazione all'esecuzione di un compito pubblico possa essere affidato a un privato e se ne possano risultare problemi specifici di sicurezza dei dati. Il Consiglio federale potrà infine anche determinare secondo quale modo possano essere utilizzati i mezzi d'identificazione delle persone (lett. c). Con la diffusione sempre più rapida dell'elaborazione automatizzata dei dati, diverranno sempre più complesse anche le misure di sicurezza, in particolare il controllo d'accesso ai sistemi. A tale scopo assume un ruolo centrale l'identificazione. Le tecniche d'identificazione delle persone si fanno ogni giorno più numerose. L'identità di una persona può essere rilevata oggi non più soltanto con parole d'ordine, badges, impronte digitali, bensì anche sulla base delle caratteristiche della retina o dei capelli. Siffatte procedure d'identificazione costituiscono anch'esse una lesione della personalità e per tale ragione il Consiglio federale deve avere la facoltà di disciplinare il ricorso a tali mezzi. Del resto, anche l'uso dei mezzi d'identificazione tradizionali, quali il numero AVS deve poter essere indigato. Il numero AVS è utilizzato oggi in settori tanto numerosi che se le relative informazioni venissero interconnesse, si otterrebbe un profilo completo della personalità.

Nel *capoverso 5* al Consiglio federale è riconosciuta la competenza di conchiudere *trattati internazionali* in materia di protezione dei dati, nella misura in cui tali trattati siano conformi ai principi fissati nel disegno. Per la conclusione di trattati in deroga alla presente legge resta competente l'Assemblea federale.

Secondo il *capoverso 6* il Consiglio federale, nel quadro delle misure per la difesa integrata può anche regolare la protezione e la sicurezza delle collezioni di dati. Determinate collezioni di dati, a cominciare dalle liste dei membri dei partiti politici non devono cadere nelle mani dell'eventuale aggressore, perché altrimenti le persone interessate sarebbero esposte a seri pericoli.

Articolo 31 Disposizioni transitorie

Secondo il *capoverso 1* gli organi federali come le persone private che trattano dati devono, al più tardi entro un anno, notificare le collezioni di dati esistenti che devono essere registrate.

Secondo il *capoverso 2* essi devono inoltre, entro lo stesso termine, prendere le misure necessarie a garantire l'esercizio del diritto d'accesso ai sensi dell'articolo 5. Effettivamente i detentori di collezioni di dati hanno a disposizione più di un anno per la preparazione a questa legge poiché dispongono suppletivamente del tempo tra il licenziamento e l'entrata in vigore della legge.

Il *capoverso 3* permette agli organi federali di continuare a trattare durante cinque anni ancora collezioni di dati personali degni di particolare protezione e profili della personalità, anche se non sono soddisfatte le severe condizioni poste ai fondamenti giuridici secondo la presente legge (art. 14 cpv. 2). Il motivo risiede nel fatto che tali fondamenti giuridici non possono essere creati da un giorno all'altro.

222 Allegato: Modificazione di leggi federali

222.1 Protezione dei dati nei rapporti di lavoro

Articolo 328b (nuovo) e 362 CO

Con l'introduzione dell'*articolo 328b* nel Codice delle obbligazioni si intende completare la protezione della personalità del *contratto di lavoro* con una specifica prescrizione sulla protezione dei dati. In corrispondenza a tale nuovo articolo occorre ampliare la lista degli articoli che non possono essere modificati a sfavore dei lavoratori. L'adeguamento del diritto sul contratto di lavoro s'impone poiché nessun altro rapporto giuridico quanto il contratto di lavoro dà l'occasione di rilevare e trattare dati personali dei più diversi tipi in quantità tanto importante e durante un periodo di tempo tanto lungo. È inoltre giustificato accordare una particolare protezione al lavoratore che dipende di fatto e in diritto dal datore di lavoro. L'articolo 328*b* nuovo del Codice delle obbligazioni completa la legge sulla protezione dei dati nel senso che determina la natura delle informazioni che il datore di lavoro ha il diritto di trattare sui suoi impiegati, che specifica in quali casi questi possa fornire a terzi informazioni che li concernono e, infine, che accorda ai lavoratori un diritto d'accesso.

L'*articolo 328b capoverso 1* limita l'ammissibilità del trattamento di dati personali ad informazioni che si riferiscono alle attitudini del lavoratore concernenti il rapporto di lavoro o sono necessari all'esecuzione del contratto di lavoro. Esso costituisce quindi una concretizzazione del principio generale della proporzionalità dell'articolo 4 capoverso 3 della legge sulla protezione dei dati. L'obiettività delle decisioni relativa al personale, come pure la protezione della personalità dei lavoratori hanno certo tutto da guadagnare dalla razionalizzazione della gestione del personale attuata grazie a metodi moderni di trattamento dei dati. Tali metodi portano tuttavia in sé il pericolo di un'esteso rilevamento di tutte le informazioni concernenti la persona fino a una trasparenza quasi totale della personalità del lavoratore e in nessun caso sono giustificati dei bisogni reali dell'impresa.

Il *capoverso 2 dell'articolo 328b* fissa che il datore di lavoro non può fornire a terzi informazioni sul lavoratore se non lo autorizza una disposizione legale o se il lavoratore non vi acconsente. Nel vigente diritto del lavoro, l'obbligo del datore di lavoro di rispettare il segreto non è disciplinato esplicitamente. Dalla regolamentazione sull'attestato di lavoro si può in effetti dedurre l'esistenza di un tale obbligo, visto che il lavoratore, se deve attendersi un attestato di lavoro sfavorevole può esigere una semplice conferma (art. 330*a* cpv. 2 CO)[53]. In pratica tuttavia un datore di lavoro s'informa su un candidato presso i datori di lavoro precedenti. Le considerazioni d'ordine legislativo a proposito dell'attestato di lavoro non hanno quindi trovato attuazione e del diritto del lavoratore all'autodeterminazione a proposito della propria data non è stato tenuto sufficientemente conto. È quindi necessario creare ora nel diritto sul contratto di lavoro una regolamentazione adeguata.

Il *capoverso 3* rinvia, per quanto concerne il diritto d'accesso, alla legge sulla protezione dei dati e riconosce inoltre al lavoratore il diritto di *consultare* i dati

che lo concernono. La consultazione di un fascicolo personale è in molti casi più semplice della comunicazione di informazioni da parte del datore di lavoro ed assicura inoltre la completezza dell'informazione. Il datore di lavoro che si sottrae all'obbligo di accordare la consultazione perché, ad esempio, tiene un fascicolo personale «nero», è punibile in virtù dell'articolo 28 capoverso 1 della legge sulla protezione dei dati. Il datore di lavoro ha invece il diritto di richiamarsi ai motivi elencati nell'articolo 6 per limitare l'accesso.

222.2 Diritto internazionale privato: Competenza e diritto applicabile

Articolo 130 capoverso 3 e 139 capoverso 3 LDIP

Le norme sui conflitti di legge previste dalla legge federale sul diritto internazionale privato non bastano per risolvere in modo soddisfacente tutte le questioni inerenti alla competenza e alla scelta di diritto che possono sorgere in relazione alle controversie di diritto internazionale privato in materia[54] di protezione dei dati: la prima concerne la *competenza dei tribunali svizzeri* a pronunciarsi sulle azioni in esecuzione del diritto d'accesso; la seconda, il *diritto applicabile.*

Secondo l'articolo 130 capoverso 3, le azioni in esecuzione del diritto d'accesso contro il detentore di una collezione di dati possono essere proposte ai tribunali svizzeri del suo domicilio, oppure, se del caso, ai tribunali del suo luogo di soggiorno o di domicilio. Non si può tuttavia obbligare la persona interessata, a citare in giudizio il detentore della collezione dei dati davanti a un giudice straniero onde ottenere il diritto d'accesso soltanto perché il detentore vive all'estero. È quindi giustificato permettere alla persona interessata d'intentare azione anche presso il tribunale svizzero del luogo nel quale la collezione dei dati è gestita o utilizzata.

Secondo l'*articolo 139 capoverso 3* LDIP, la persona interessata dispone del diritto di scelta anche per quanto concerne il diritto applicabile. Essa può fare valere le pretese derivanti da una lesione della personalità causata dal trattamento di dati personali, o le pretese derivanti dagli intralci del diritto d'accesso, sulla base sia del diritto dello Stato di soggiorno abituale, sia del diritto dello Stato nel quale si è prodotto il risultato della lesione o dell'intralcio, nella misura in cui l'autore del danno doveva contare sul fatto che il risultato si producesse in questo Stato. La persona interessata può anche far valere le sue pretese secondo il diritto dello Stato nel quale l'autore della lesione o dell'intralcio ha il domicilio o il soggiorno abituale. Chi tratta i dati non ha quindi più la possibilità di arrecare pregiudizio alla persona interessata, scegliendo un domicilio vantaggioso per quanto concerne la protezione dei dati. D'altro canto, la libertà di scelta del diritto non deve permettere a colui che tratta dati, di speculare sul regime giuridico applicabile. Questo non è tuttavia un problema specifico del diritto sulla protezione dei dati: esso si fa tuttavia sempre più acuto anche in molti altri settori, in ragione dell'internazionalizzazione crescente dell'economia.

222.3 Sottrazione di dati personali

Articolo 179^{novies} (nuovo) del Codice penale

La fattispecie di questo articolo si avvicina a quella dell'articolo 143 CP, nel nuovo tenore proposto dalla commissione peritale nell'avamprogetto di revisione delle disposizioni del Codice penale sui reati patrimoniali, inviato in consultazione negli anni 1985 e 1986. Il progetto di un articolo 143 protegge però, in primo luogo, il patrimonio di colui che tratta i dati e non la personalità delle persone interessate. Per tale ragione è stato chiesto, in sede di procedura di consultazione sull'avamprogetto di modificazione delle disposizioni sui reati patrimoniali, che venga disciplinata la sottrazione di dati personali in genere, soprattutto nell'ottica della protezione della personalità. Per questa ragione occorre quindi, insieme alla creazione della legge sulla protezione dei dati, completare le disposizioni del Codice penale sui reati contro la sfera personale riservata (art. 179 e segg.) con l'introduzione della fattispecie della sottrazione di dati personali degni di particolare protezione.

Oggetto del reato sono, nell'articolo 179^{novies} CP, dati personali degni di particolare protezione che non sono liberamente accessibili. Quali siano i dati degni di particolare protezione risulta dall'articolo 3 lettera e. Non sono liberamente accessibili i dati, se l'autore del reato può averne conoscenza soltanto recandosi in locali o accedendo a impianti, il cui accesso gli è vietato. La raccolta di tali dati può avvenire nelle più diverse forme. Può trattarsi di interi fascicoli o di parte di essi sottratti da archivi, oppure di accesso ai dati di sistemi automatizzati con manipolazioni al loro terminale oppure d'intercettazione di dati trasmessi. Punibile è soltanto chi ha agito intenzionalmente. La fattispecie coperta dall'articolo 179^{novies} CP è punibile soltanto a querela di parte. La relativa azione può essere proposta dalla persona interessata o da chi tratta i dati. La sottrazione illecita di dati personali è un delitto, punito con la detenzione o con la multa.

222.4 Protezione dei dati nella ricerca medica

222.41 Condizioni quadro di diritto costituzionale

La ricerca medica si svolge soprattutto nelle università e negli ospedali (pubblici e privati); l'attività di ricerca della Confederazione è per contro di minore importanza. Il diritto costituzionale vigente non permette di disciplinare il trattamento dei dati in questi diversi settori in maniera soddisfacente. Se la Confederazione può fondarsi sugli articoli 64 e 65 numero 1 della Costituzione federale per disciplinare la protezione dei dati nel quadro delle proprie ricerche e di quelle effettuate dai privati, la Confederazione non ha invece nessuna competenza per emanare regole sulla protezione dei dati per il settore del diritto pubblico cantonale, diritto che regge anche le università e gli ospedali cantonali e comunali. In tali casi è determinante il diritto cantonale sulla protezione dei dati, eventualmente presente. L'articolo costituzionale 27^{sexies} sulla ricerca non muta nulla. Esso conferisce alla Confederazione unicamente la facoltà di promuovere la ricerca scientifica, ma mantiene per contro la ripartizione delle competenze nei settori della formazione universitaria e della ricerca.

La formazione universitaria, ad eccezione di quella delle Scuole politecniche, resta quindi in ampia misura sottratta alla sfera d'influsso della Confederazione[55]. Anche l'articolo 69 della Costituzione federale che dà alla Confederazione la competenza di combattere le malattie trasmissibili o largamente diffuse, o di natura maligna non costituisce una base costituzionale sufficiente per una regolamentazione federale di protezione dei dati per il settore cantonale. Soltanto una parte dei progetti di ricerca concerne queste categorie di malattie.

Una regolamentazione uniforme sulla protezione dei dati nel settore della ricerca medica può tuttavia fondarsi, per una parte rilevante, sull'articolo 64bis della Costituzione federale che attribuisce alla Confederazione la competenza a legiferare in materia di diritto penale. Nella misura in cui si tratta di disciplinare soltanto la *comunicazione dei dati,* esiste uno stretto rapporto materiale con il segreto professionale. Secondo l'articolo 64bis Cost., la Confederazione è competente a fissare le sanzioni penali applicabili in caso di violazione del segreto professionale, rispettivamente per disciplinare il segreto professionale. La Confederazione ha fatto uso di tale competenza emanando l'articolo 321 del Codice penale. Nulla si oppone dal punto di vista del diritto costituzionale, ove si voglia regolare in modo più circostanziato i segreti professionali nell'ottica della protezione dei dati. Appare quindi ammissibile prevedere un nuovo motivo giustificativo che autorizzi, a determinate condizioni, violazioni del segreto professionale. Questo motivo giustificativo troverà applicazione allorquando saranno necessari i dati per la ricerca medica.

Diversa è la situazione per rapporto a un'eventuale regolamentazione della *raccolta e del trattamento* dei dati. In contrapposizione alla comunicazione dei dati, il segreto professionale non è in questi casi necessariamente coinvolto. Se si elaborassero principi per il trattamento dei dati (ad es. norme sulla conservazione dei dati), rispettivamente se si sanzionassero penalmente le violazioni di tali principi, si verrebbe a creare una nuova categoria di atti punibili. In considerazione delle diversità delle possibili violazioni non intendiamo penalizzare la globalità delle violazioni dei principi del trattamento di dati, ma soltanto quelle che sono particolarmente gravi, rispettivamente se rimettono in questione l'attuazione della protezione dei dati nel suo insieme (cfr. art. 28 e 29 LPD, come pure art. 179^{novies} CP). Inoltre la competenza di diritto penale non deve essere la base costituzionale determinante per la regolamentazione generale del trattamento dei dati nella ricerca medica. La Confederazione può invece, fondando sulla competenza a legiferare in materia di diritto penale, emanare anche norme d'ordine organizzativo in merito a una commissione che deve esaminare i progetti di ricerca sotto l'angolo del diritto sulla protezione dei dati. L'organizzazione dell'amministrazione della giustizia penale è compito in principio riservato ai Cantoni e fino ad oggi la Confederazione non ha mai fatto uso delle sue competenze penali per istituire un'istanza di questo genere. Laddove però s'impongono misure organizzatorie affinché una regolamentazione materiale del diritto penale sia applicata in modo corretto e conforme al principio della parità di trattamento, la Confederazione ha il diritto di emanare le norme corrispondenti[56]. Del resto la commissione peritale non funzionerà come un vero e proprio organo dell'amministrazione della giustizia

penale, perché giudicherà unicamente della necessità d'autorizzare la rivelazione di un segreto professionale: anche a questo titolo, la commissione proposta non rimette in causa la ripartizione delle competenze.

222.42 Progetto di regolamentazione in generale

La limitazione della regolamentazione alla comunicazione dei dati, imposta dalle norme costituzionali, risulta sostenibile. Poiché, in occasione della comunicazione dei dati occorrerà decidere a quali condizioni sia possibile svelare un segreto professionale relativo a dati medici. Risulta invece qualche po' meno urgente - anche se auspicabile - di disciplinare il trattamento dei dati medici acquisiti con mezzi altri da quelli della rivelazione del segreto professionale, in particolare nel caso della comunicazione di fascicoli medici da parte dei medici curanti. Questo soprattutto perché tali trattamenti saranno sottoposti - almeno nella misura in cui la ricerca è eseguita da istituzioni della Confederazione o da istituti di ricerca privati - alla legge sulla protezione dei dati. Per quanto concerne gli ospedali cantonali e universitari essi soggiacciono al diritto cantonale sulla protezione dei dati eventualmente in vigore. La regolamentazione proposta dovrebbe quindi, nell'insieme, portare a un sensibile miglioramento della protezione dei dati medici.

L'articolo 19 del disegno di legge federale sulla protezione dei dati contiene una disposizione che privilegia i trattamenti di dati personali per scopi che non si riferiscono a persone, segnatamente per scopi della ricerca, della pianificazione e della statistica. Le condizioni poste alla comunicazione di dati a terzi sono quindi meno restrittive, se questi non li usano per scopi riferentisi a persone. Allorquando la ricerca entra in conflitto con un segreto professionale, le disposizioni speciali della legge sulla protezione dei dati che privilegiano determinate forme di trattamento non si applicheranno. In simili casi troverà applicazione soltanto l'articolo 321bis CP.

222.43 Commento dell'articolo 321bis CP e degli articoli 26 capoverso 3 e 24 capoverso 1 lettera c LPD

Articolo 321bis CP Segreto professionale in materia di ricerca medica

Capoverso 1 Nuovo motivo giustificativo per la rivelazione del segreto professionale

I motivi che giustificano la violazione del segreto professionale, menzionati nell'articolo 321 CP sono completati da un nuovo motivo giustificativo: l'autorizzazione di rivelare il segreto professionale è data da una Commissione peritale. Tale autorizzazione è tuttavia valida soltanto per la ricerca nel settore della medicina o della sanità pubblica. Si tratta in primo luogo della ricerca destinata a combattere efficacemente le malattie gravi o diffuse. Tuttavia anche nel settore della sanità pubblica sono attuati progetti di ricerca il cui interesse pubblico è incontestato. Le inchieste sullo stato di salute della popolazione costituiscono, ad esempio, una base indispensabile di un'adeguata pianificazione ospe-

daliera. La commissione può rilasciare un'autorizzazione anche in merito a indagini scientifiche sugli effetti secondari dei medicamenti oppure per documentazioni e statistiche scientifiche relative agli effetti a lunga scadenza di determinate terapie. La commissione peritale non deve invece potere sospendere l'obbligo del segreto per semplici ricerche di mercato.

La legge si limita a definire in termini generali a quale titolo può essere concessa la rivelazione del segreto professionale. Spetterà alla commissione peritale elaborare principi più circostanziati. Il nuovo motivo giustificativo sarà importante soprattutto per medici e dentisti, come pure per il loro personale ausiliario, in singoli casi anche per farmacisti e ostetriche; non avrà invece praticamente rilievo per gli altri gruppi professionali che soggiacciono all'obbligo di conservare il segreto secondo l'articolo 321 CP.

Un segreto professionale ai sensi dell'articolo 321 CP esiste in principio anche oltre la morte del soggetto del segreto[57]. Se la persona obbligata a osservare il segreto viola il segreto professionale soltanto dopo la morte del soggetto del segreto, allora rimane nella maggior parte dei casi impunito, mancando la persona che possa querelarla (art. 28 CP). L'autorizzazione rilasciata dalla Commissione peritale a rivelare il segreto professionale può essere importante anche in relazione ai dati relativi alle persone decedute, poiché una violazione illecita del segreto medico può avere anche conseguenze disciplinari, civili e, eccezionalmente anche penali[58].

L'autorizzazione a rivelare un segreto professionale per scopi di ricerca medica può rilasciare, oltre all'avente diritto, soltanto la Commissione. La disposizione istituisce una regolamentazione di diritto federale completa che, in quanto regolamentazione speciale, è preminente per rapporto all'articolo 321 numero 2 CP. Secondo tale disposizione, l'autorità superiore o l'autorità di sorveglianza è pure in misura di rilasciare l'autorizzazione a rivelare il segreto professionale.

Anche nei casi nei quali la Commissione peritale potrebbe rilasciare autorizzazione o l'ha già rilasciata, l'opposizione dell'interessato dev'essere rispettata. Un segreto professionale, in particolare il segreto medico non deve essere rivelato contro l'esplicita volontà dell'interessato. Se, sulla base di un'autorizzazione rilasciata della Commissione peritale sono già stati comunicati dati e se la persona interessata in seguito vieta tale comunicazione, i ricercatori non possono più oltre operare con i relativi dati personali.

Secondo l'articolo 29 LPD la persona che esercita un'attività professionale che esige la conoscenza di dati personali degni di particolare protezione è punita se rivela senza autorizzazione tali dati a terzi. Chi però rivela tali dati sulla base di un'autorizzazione della Commissione peritale non è punibile, esattamente come se avesse agito con il consenso della persona interessata.

Capoverso 2 Premesse dell'ottenimento dell'autorizzazione della Commissione peritale

Certe condizioni cumulative devono essere soddisfatte per ottenere un'autorizzazione della Commissione peritale per la rivelazione del segreto professionale.

L'autorizzazione può essere rilasciata soltanto se la ricerca non può essere effettuata con dati anonimi (lett. a). Se un progetto di ricerca non deve contare su dati in base ai quali è possibile l'identificazione della persona interessata, la Commissione non deve autorizzare la rivelazione del segreto. L'autorizzazione della commissione può inoltre essere rilasciata soltanto se è impossibile o particolarmente difficile ottenere il consenso dell'interessato (lett. b). Le difficoltà potrebbero insorgere soprattutto nel caso di indagini retrospettive, quando i pazienti non sono più in vita o non sono reperibili, oppure se, nel caso di progetti di ricerca di una grande clinica i pazienti risiedono sparsi su una grande area che addirittura sorpassa le frontiere. Gli ostacoli non devono essere di natura assoluta. Basta che il tentativo di ottenere il consenso dell'interessato esiga un dispendio eccessivo che potrebbe mettere in forse il progetto. Spetta alla commissione delimitare, in questi casi, le frontiere con maggiore precisione. Occorre anche che gli interessi della ricerca siano preminenti su quelli del rispetto del segreto (lett. c).

Vengono così poste esigenze qualitative al progetto di ricerca, a favore del quale un segreto professionale può essere rivelato. La Commissione soppesa e valuta le circostanze concrete del singolo caso. Essa determina in particolare in quale misura il ricercatore deve poter contare sui dati, quali possibilità di cura e progressi medici favorisce il progetto, per quante persone i risultati della ricerca possono risultare utili, quale valore il progetto riveste per la sanità pubblica. Regole generali più ampie non possono tuttavia essere introdotte a questo proposito. È tuttavia certo che i progetti di ricerca che sono fine a sé stessi o che rispondono esclusivamente a considerazioni di politica commerciale non soddisfano certo a queste esigenze.

Capoverso 3 Oneri e pubblicazione dell'autorizzazione

La Commissione peritale grava l'autorizzazione di oneri atti ad assicurare la protezione dei dati. L'ordinanza d'esecuzione del Consiglio federale (cpv. 5) definirà gli oneri possibili. Entrano in linea di conto oneri concernenti ad esempio lo scopo per il quale i dati possono essere comunicati, il tipo e la portata dei dati, le persone che devono essere svincolate dal segreto professionale, il genere dell'utilizzazione dei dati, come pure la cerchia delle persone che ottengono accesso ai dati.

Con la pubblicazione dell'autorizzazione della Commissione, le persone interessate devono essere rese attente alle comunicazioni previste. Sulla base di tale notificazione, il singolo ottiene ancora una volta il diritto di significare, ad esempio, al medico, di voler vietare la comunicazione dei suoi dati di paziente.

Capoverso 4 Autorizzazioni generali e altre semplificazioni

Nei casi nei quali gli interessi legittimi delle persone interessate non siano compromessi e i dati personali siano stati resi anonimi all'inizio della ricerca, la Commissione peritale deve poter rilasciare *autorizzazioni generali.* È preminente il bisogno delle cliniche e degli istituti universitari di medicina di usare i dati rilevati a scopo di cura anche per la ricerca interna e in particolare per l'istruzione e il perfezionamento del personale. A tale scopo, occorre ricono-

scere un diritto d'accesso ai fascicoli medici concernenti pazienti di altre divisioni ospedaliere. In siffatti casi che soggiacciono in principio al segreto professionale istituito dall'articolo 321 CP, la Commissione peritale deve poter rilasciare un'autorizzazione generale, non alla persona effettivamente sottoposta all'obbligo, bensì alla direzione della clinica o dell'istituto. I dettagli saranno disciplinati in un'ordinanza del Consiglio federale. Nei casi, tuttavia, nei quali l'identità della persona interessata sia riconoscibile non soltanto alla raccolta dei dati, ma debba essere disponibile anche per l'ulteriore trattamento dei dati, occorre richiedere un'autorizzazione ordinaria della Commissione peritale.

L'ordinanza del Consiglio federale può inoltre prevedere anche che tali autorizzazioni generali rilasciate alle cliniche e agli istituti possono valere non soltanto per i ricercatori interni, bensì anche per i *dottorandi.* Quest'ultimi potrebbero quindi avere accesso ai fascicoli medici alle condizioni enunciate - nessun pericolo per gli interessi della persona interessata e obbligo di rendere immediatamente anonimi i dati - senza violare illecitamente il segreto medico. L'autorizzazione generale dovrebbe probabilmente essere completata con un obbligo di notificare i singoli progetti di ricerca, affinché la commissione possa esaminare se sia rispettato il quadro dell'autorizzazione generale.

Una semplificazione della procedura d'autorizzazione s'impone anche per i *registri* medici, in particolare i registri del cancro. Il Consiglio federale può, sulla base del capoverso 4, prevedere un'autorizzazione generale anche per questi casi. Un'autorizzazione del genere potrebbe preventivamente essere rilasciata all'organo responsabile del registro, affinché sia in grado di ricevere comunicazione dei dati che non sono stati resi anonimi. La Commissione peritale dovrebbe vincolare tale autorizzazione a oneri, concernenti in particolare la codificazione e la conservazione dei dati che non sono stati resi anonimi e fissare anche la cerchia delle persone che ottengono accesso a questi dati.

Sulla base del capoverso 4 anche per altri casi il Consiglio federale può prevedere semplificazioni. Egli potrebbe ad esempio, per casi evidenti, prevedere una procedura di decisione presidenziale oppure di lasciar decidere a una sottocommissione.

La legge valutamente lascia aperte diverse possibilità di semplificazione. Essendo difficile prevedere il numero delle domande che saranno rivolte ogni anno alla commissione peritale e conoscere la natura che queste avranno, devono essere possibili soluzioni flessibili. Durante i primi anni, la commissione peritale deve, in fase di prova, poter trovare le forme d'organizzazione più appropriate.

Capoverso 5 Organizzazione della Commissione peritale e procedura

La Commissione peritale è nominata dal Consiglio federale. Essa è un'*autorità federale.* Il disegno rinuncia a prevedere istanze cantonali d'autorizzazione. Una simile soluzione sarebbe in effetti in accordo con la struttura federalista del Paese; essa non sarebbe tuttavia praticamente attuabile, oppure sarebbe accompagnata da svantaggi gravi. La competenza d'autorizzazione non spetterebbe unicamente al Cantone nel quale avviene la ricerca; essa dovrebbe parimenti estendersi ai Cantoni nei quali devono essere raccolti i dati o nei quali

sono domiciliati gli interessati. Uno stesso progetto di ricerca, come quello di una clinica universitaria che interessa un vasto territorio dovrebbe a seconda delle circostanze, essere sottoposto per autorizzazione a numerose commissioni cantonali. Ciò non sarebbe attuabile anche qualora tutti i Cantoni disponessero delle risorse personali necessarie alla costituzione di tale commissione. Infine non si può escludere che diverse commissioni potrebbero pervenire, almeno per quanto concerne le modalità dell'organizzazione, a conclusioni diverse. Questo costituirebbe un intralcio dell'opera di ricerca e porterebbe a insicurezza giuridica. La regolamentazione proposta lascia tuttavia aperta la possibilità di suddividere la Commissione peritale in sottocommissioni competenti ciascuna per una parte del Paese o per una regione linguistica. Dalle esperienze pratiche della Commissione risulterà se la soluzione federalista deve essere attuata per questa via.

L'autorizzazione della Commissione peritale deve essere richiesta indipendentemente da qualsiasi altra procedura in relazione a un progetto di ricerca, ad esempio, una procedura davanti al Fondo nazionale o una commissione d'etica professionale. Onde evitare ritardi, una procedura d'autorizzazione davanti la Commissione peritale deve potersi svolgere contemporaneamente ad altre procedure.

L'*organizzazione* della Commissione sarà disciplinata in un'ordinanza del Consiglio federale. Importanza particolare ha la composizione personale della commissione. Va da sé che deve trattarsi di membri indipendenti e che i bisogni della ricerca medica e gli interessi sia della medicina, sia delle persone interessate e in particolare dei pazienti devono essere rappresentati proporzionatamente. Sarà inoltre necessario un certo numero di membri con pratica giudiziaria.

La procedura davanti alla Commissione peritale è in principio retta dalla legge federale sulla procedura amministrativa. L'ordinanza d'esecuzione del Consiglio federale prevederà inoltre quali informazioni deve contenere la domanda d'autorizzazione.

Capoverso 6 Segreto della ricerca

Chiunque tratta informazioni sottoposte al segreto professionale per scopi della ricerca nel settore medico o della sanità pubblica deve soggiacere a sua volta all'obbligo di mantenere il segreto. Occorre quindi che i destinatari delle informazioni, vale a dire i ricercatori e gli ausiliari che ottengono dal medico curante, grazie alla rivelazione del segreto di funzione, dati personali, si vedono pure imporre un obbligo di rispettare il segreto. Allorquando una decisione di un'autorità autorizza la rivelazione del segreto di funzione a favore di un ricercatore, indipendentemente dal consenso degli interessati, occorre d'altro canto assicurarsi che nessun terzo non autorizzato ottenga comunicazione delle informazioni. A proposito del contenuto dell'obbligo del ricercatore di mantenere il segreto, non viene fatta distinzione alcuna tra le informazioni comunicate dai medici e sulla base di una decisione della Commissione peritale e quelle che sono state rivelate con il consenso dell'interessato. Nei due casi, in effetti, l'utilizzazione dei dati personali nella ricerca aumenta in misura rilevante il rischio di altre divulgazioni. Una distinzione sarebbe in pratica d'altro canto difficilmente applicabile.

Il capoverso 6 allarga quindi la cerchia delle persone sottoposte all'articolo 321 CP. Parallelamente, il nuovo motivo giustificativo si applica anche a questi nuovi detentori del segreto professionale che sono i ricercatori. Con il consenso della persona interessata o l'autorizzazione rilasciata dalla Commissione peritale, questi potranno a loro volta trasmettere i dati medici ad altri ricercatori.

Nella misura in cui i ricercatori raccolgono i dati per i loro progetti di ricerca direttamente presso gli interessati e indipendentemente, ad esempio, da un trattamento medico, non appare giustificato sottoporli al segreto professionale corrispondente. Non esiste in effetti tra il ricercatore e la persona che lo informa il rapporto di fiducia che lega il medico al suo paziente. Si applica quindi, in questo caso, la disposizione concernente la violazione dell'obbligo di osservare il segreto (art. 29 LPD).

Articolo 26 capoverso 3 LPD Preposto alla protezione dei dati

In quanto principale responsabile dell'attuazione della protezione dei dati, il Preposto alla protezione dei dati è in modo particolare predestinato a consigliare la Commissione peritale. Egli può anche contribuire a una certa «unité de doctrine» tra la protezione dei dati in generale e la protezione dei dati nella ricerca medica. Egli deve inoltre assumere funzione di controllo. Il Preposto alla protezione dei dati ha, per quanto concerne la sua attività di consulenza e di controllo, gli stessi diritti d'accesso alle informazioni e ai documenti che egli ha giusta l'articolo 24 capoverso 3 della legge federale sulla protezione dei dati. La misure di controllo dovranno essere precisate sull'ordinanza d'esecuzione del Consiglio federale. Dovrà in primo luogo essere regolata la collaborazione tra la Commissione peritale e il Preposto alla protezione dei dati: la Commissione peritale dovrà informare il Preposto sulle autorizzazioni rilasciate e sugli oneri che la accompagnano. Se il Preposto rileva che gli oneri non sono stati rispettati, può da parte sua attirare l'attenzione della Commissione su tale fatto. Nell'ordinanza d'esecuzione può inoltre essere previsto che il presidente in questi casi solleciti ancora una volta il richiedente a rispettare gli oneri della decisione d'autorizzazione e lo minacci in pari tempo della revoca dell'autorizzazione. È inoltre data la possibilità di comminare la pena prevista (art. 292 CP).

Il Preposto alla protezione dei dati, infine, deve poter impugnare le decisioni della Commissione peritale con ricorso alla Commissione della protezione dei dati. Il Preposto può così difendere gli interessi della persona interessata anche davanti alla Commissione federale della protezione dei dati. Invece non appare necessario riconoscere al Preposto alla protezione dei dati anche la legittimazione a inoltrare ricorso di diritto amministrativo al Tribunale federale.

Articolo 27 capoverso 1 lettera c LPD Rimedi di diritto

Contro le decisioni della Commissione peritale non deve essere ammesso direttamente il ricorso di diritto amministrativo: onde alleviare il Tribunale federale, l'affare dovrà prima essere portato davanti a una commissione di ricorso. Questa soluzione s'impone per due ragioni. In primo luogo essa corrisponde alla concezione della revisione della legge federale sull'organizzazione giudizia-

ria: in secondo luogo, la legge federale sulla protezione dei dati personali dal canto suo pure istituisce una commissione speciale di ricorso per le questioni della protezione dei dati.

222.5 Modificazione della legge federale sulla procedura penale

Giusta l'articolo 2 capoverso 2 lettera e, la legge sulla protezione dei dati non si applica ai trattamenti dei dati effettuati nel quadro di una procedura penale, e con questo neppure alle procedure secondo la legge federale del 15 giugno 1934 sulla procedura penale (PPF). Il motivo è da ricercare nel fatto che, come dianzi rilevato, la procedura penale federale contiene già determinate garanzie concernenti la raccolta, l'uso e la comunicazione dei dati personali (ad es. le disposizioni sull'interrogatorio dell'incolpato, art. 39 segg. PPF). Occorre inoltre regolare specificamente, ad ogni stadio della procedura, l'informazione delle persone implicate. Un'applicazione parallela delle regole generali della protezione dei dati rischierebbe di complicare ed intralciare lo svolgimento della procedura penale.

La procedura penale è stata, nel corso degli ultimi anni, oggetto di parecchie revisioni. Si pensi ad esempio all'introduzione del controllo giudiziario degli atti di procedura penale. I principi generali del diritto di procedura sono tuttavia rimasti gli stessi nel corso degli ultimi 50 anni. Ciò significa che per la procedura delle indagini preliminari della polizia giudiziaria mancano effettivamente, fino ad oggi, norme specifiche sul trattamento dei dati. Poiché le informazioni di polizia contengono spesso dati personali degni di particolare protezione, occorre colmare questa lacuna. Suggeriamo quindi di completare la procedura penale federale con disposizioni sull'assistenza giudiziaria, sulla raccolta dei dati di polizia, la loro comunicazione e distruzione: prevediamo inoltre un diritto d'accesso per le persone interessate.

A queste disposizioni di protezione dei dati s'aggiungono alcune prescrizioni relative a determinate *misure costrittive di polizia,* vale a dire prescrizioni su la perquisizione, l'esame medico e l'identificazione delle persone. Poiché ognuna di queste misure può pregiudicare i diritti della personalità della persona interessata, occorre definire le premesse della loro applicazione e rendere possibile il controllo da parte della Corte d'accusa del Tribunale federale. Ove si vogliano seguire esigenze più strette in materia di legalità di trattamento dei dati, non vi è motivo di essere meno severi per tali operazioni costrittive. Le disposizioni che proponiamo a questo proposito s'ispirano a esempi cantonali.

Tutti gli interventi importanti sulla libertà personale sono quindi elencati e ancorati nella legge. Per i pregiudizi leggeri della personalità vale tuttora la clausola generale dell'articolo 102 della legge. Una riserva dev'essere fatta per l'uso delle armi da fuoco da parte della polizia, in merito al quale esistono regole speciali[59].

Rileviamo infine che s'è rinunciato a una corrispondente modificazione della procedura militare federale. In effetti, nel settore del diritto penale militare, le indagini preliminari non hanno la stessa importanza: esse hanno sin quasi dall'inizio carattere giudiziario, poiché sono affidate a un giudice d'istruzione.

Articolo 26bis

Gli organi della polizia giudiziaria della Confederazione non possono adempiere i loro compiti senza la collaborazione di altri servizi amministrativi della Confederazione, dei Cantoni e dei Comuni. L'assistenza giudiziaria deve quindi essere disciplinata esplicitamente in materia di procedura delle indagini preliminari della polizia giudiziaria. Questa disposizione s'ispira all'articolo 30 della legge federale sul diritto penale amministrativo. In quanto legge speciale, essa è preminente sull'articolo 16 della legge generale sulla protezione dei dati.

Il *capoverso 1* introduce un *obbligo generale d'assistenza giudiziaria* a favore delle autorità federali incaricate del perseguimento penale. Questo obbligo vale per tutti gli organi della Confederazione, dei Cantoni e dei Comuni. Esso comprende la comunicazione di informazioni e la consultazione di atti; occorre aggiungere anche l'edizione di documenti o di oggetti che possono rivestire importanza in quanto mezzi di prova (cfr. art. 65 PPF).

La portata dell'assistenza giudiziaria non è tuttavia assoluta. Giusta il *capoverso 2,* un organo può rifiutare o limitare l'assistenza giudiziaria se lo esigono interessi pobblici importanti o interessi manifestamente legittimi di una persona interessata (lett. a) oppure se si oppone un segreto professionale (lett. b). Questa disposizione corrisponde nell'essenza all'articolo 16 capoverso 3 della legge sulla protezione dei dati.

In conformità della regolamentazione nel diritto penale amministrativo, le organizzazioni incaricate di compiti pubblici sono obbligate, giusta il *capoverso 3, a prestare assistenza alla stessa stregua delle autorità.*

Secondo il capoverso 4, le contestazioni tra autorità amministrative federali sono decise sia dal Dipartimento dal quale tali autorità dipendono, sia dal Consiglio federale, se le autorità rispettive non soggiacciono a uno stesso Dipartimento. Se la contestazione oppone un'autorità federale a un'autorità cantonale, decide la Camera d'accusa del Tribunale federale, che è già competente a dirimere le contestazioni tra le autorità cantonali (art. 357 CP e art. 252 PPF). Nei rari casi, infine, nei quali si tratta di contestazioni tra istanze giudiziarie e istanze amministrative della Confederazione, occorre ricercare una composizione sulla via di uno scambio di pareri tra il Consiglio federale e il Tribunale federale.

Il *capoverso 5* prevede l'applicabilità sussidiaria delle disposizioni sull'assistenza giudiziaria del Codice penale e della legge sull'organizzazione giudiziaria.

Articolo 52

Considerato che il nuovo articolo 105bis regola globalmente il ricorso contro le misure coercitive, il capoverso 2 dell'articolo 52 non è più necessario e può essere abrogato.

Articolo 64bis

La disposizione sottopone l'attività delle autorità penali federali, compresa quella degli organi della polizia giudiziaria, ai principi della protezione dei dati. Sono regolati la raccolta, la rettificazione e la distruzione dei dati. La norma

proposta si estende non soltanto ai dati degni di particolare protezione, bensì anche a tutti i dati personali. Nell'ambito di un'istruzione non è in effetti possibile, quando si tratta di procedere a un interrogatorio, dissociare i dati degni di particolare protezione dagli altri dati.

Ispirandosi all'articolo 15 LPD, il *capoverso 1* stipula che, in occasione dell'istruzione, i dati personali sono raccolti anche presso la persona interessata, in modo per questa riconoscibile. Questa regola non vale tuttavia in modo assoluto. Nell'interesse di un'istruzione penale efficace, gli organi della polizia giudiziaria devono poter fare astrazione da questi principi. Occorre inoltre tenere conto della possibilità che deve avere la polizia criminale di controllare e confermare tutte le informazioni concernenti una persona interessata per mezzo di informazioni fornite da testi o di altre prove. Questo è quanto indicato laddove il testo recita che i dati sono raccolti «anche» presso la persona interessata.

Il *capoverso 2* concretizza un principio generale della protezione dei dati posto dall'articolo 4 capoverso 2 LPD. Nei casi di rettificazione o distruzione, il detentore di una collezione di dati o l'organo responsabile devono avvertire immediatamente le autorità e le persone ai quali tali dati erano stati in precedenza comunicati. Accogliendo questo principio nella sezione sulle disposizioni generali, intendiamo chiarire esplicitamente che la prescrizione è applicabile a *tutte le fasi della procedura penale federale.*

Il *capoverso 3* regola il trattamento dei dati non più necessari per l'istruzione ed è parallelo all'articolo 66 capoverso 1ter PPF secondo il quale le registrazioni d'ascolto non più necessarie per l'istruzione devono essere distrutte alla conclusione della procedura. Non devono invece essere distrutti i dati necessari nel quadro di altre procedure. Le regole sviluppate dalla giurisprudenza disciplinano in questi casi l'uso lecito dei dati[60]. Se gli atti costituiti per le indagini preliminari portano all'apertura di una procedura formale, saranno distrutti o archiviati alla conclusione della procedura penale federale o cantonale (cfr. il nuovo art. 107bis proposto).

Articolo 72bis

Questo articolo regola la sorveglianza delle manifestazioni. La questione a sapere in quale misura la polizia possa filmare o fotografare le dimostrazioni che si svolgono nella legalità è da lungo tempo oggetto di controversie. Nell'ottica della protezione dei dati, tali riprese sono problematiche poiché permettono di rilevare le attività politiche dei partecipanti alle manifestazioni. Secondo la nostra proposta, la polizia sarà ora in grado di filmare o fotografare una manifestazione che si svolge legalmente soltanto se nel corso della stessa vengono compiuti atti punibili o se circostanze concrete permettono di concludere che sono preparati atti punibili. Quest'ultimo è il caso allorquando i manifestanti portano armi o utensili pericolosi oppure sono stati lanciati, prima della manifestazione, inviti a commettere atti di violenza.

Nel progetto attuale abbiamo rinunciato a regolare in modo analogo la sorveglianza acustica. Quanti prendono la parola durante la manifestazione devono tuttavia attendersi che, in un modo o nell'altro, si prenda conoscenza di quanto è stato detto ufficialmente.

Rileviamo infine che non è stata prevista alcuna disposizione sulla *sorveglianza tradizionale e il pedinamento delle persone.* È evidente che l'atteggiamento di una persona viene controllato e sorvegliato soltanto se sono realizzati gli estremi di un forte dubbio. La competenza della polizia si basa sul mandato generale di prevenire e scoprire gli atti punibili. Rileviamo che sorveglianze intense con relativi pregiudizi importanti della personalità sono rare e che richiedono l'impiego di mezzi tecnici speciali. Quest'ultimi possono tuttavia essere impiegati, giusta gli articoli 66 e seguenti della procedura penale federale, soltanto con l'autorizzazione del presidente della Camera d'accusa. Per tali motivi non ci sembra quindi necessario regolare in una norma speciale la sorveglianza e il pedinamento delle persone.

Articolo 73bis

Nel diritto vigente soltanto in relazione alla perquisizione domiciliare è possibile la perquisizione personale (art. 67 cpv. 1 seconda frase PPF). Per il resto la polizia giudiziaria deve basarsi sulla clausola generale dell'articolo 102 PPF, giusta la quale essa è autorizzata a rilevare le tracce dei reati e a provvedere alla loro custodia. Poiché la perquisizione domiciliare può costituire un intervento importante nella libertà di una persona, occorre creare all'uopo una disposizione legale esplicita.

Nel *capoverso 1* sono definite le condizioni alle quali la polizia può procedere alla perquisizione personale. La perquisizione personale è ammessa se sono soddisfatte le premesse di un arresto (lett. a), vale a dire se è stato rilasciato mandato d'arresto o se il fermo provvisorio deve avvenire immediatamente (art. 44 e 62 PPF). Una persona può inoltre essere perquisita personalmente se è dato il sospetto che la persona detiene oggetti che devono essere messi in sicurezza (lett. b), vale a dire oggetti che devono essere confiscati[61]). La perquisizione personale può infine avvenire ove ciò sia indispensabile per l'accertamento della personalità (lett. c) oppure per la protezione delle persone che non godono più delle piene facoltà mentali (lett. d).

Giusta il *capoverso 2* una perquisizione personale può inoltre anche essere necessaria al fine di proteggere funzionari di polizia o terzi. In tale contesto accenniamo in primo luogo alle misure di protezione richieste dal diritto internazionale a favore dei capi di Stato, dei membri di governo e dei diplomatici in occasione di visite di Stato o conferenze internazionali.

Il *capoverso 3,* infine, analogo all'articolo 48 capoverso 2 della legge sul diritto penale amministrativo (RS *313.0*) statuisce che la perquisizione può essere attuata unicamente da una persona dello stesso sesso o da un medico. Sono ammesse eccezioni se dovesse altrimenti insorgere un danno irreparabile.

Articolo 73ter

L'articolo definisce le premesse alle quali soggiacciono, nell'ambito della procedura penale gli esami medici delle persone. Tali esami costituiscono di regola interventi gravi sui diritti della personalità delle persone interessate. Essi sono quindi ammissibili, secondo il *capoverso 1,* soltanto se sono necessari per stabi-

lire i fatti (lett. a) oppure se soltanto in questo modo sia possibile rilevare la capacità di discernimento, l'attitudine a partecipare a discussioni o a sopportare la detenzione da parte di una persona incolpata (lett. b).

Il *capoverso 2* disciplina la competenza a ordinare un esame fisico o psichico. Nella procedura delle indagini preliminari la competenza spetta unicamente al procuratore generale della Confederazione.

Per l'esame fisico o psichico di *persona non incolpata* devono inoltre essere soddisfatte, giusta il *capoverso 3* altre premesse. Tali persone possono essere esaminate contro la loro volontà soltanto se si tratta di appurare un fatto rilevante che non può essere chiarito altrimenti. Le persone che hanno il diritto di rifiutare di testimoniare, hanno, parallelamente alla disciplina in vigore in alcuni ordinamenti procedurali cantonali, il *diritto di opporsi all'esame fisico e psichico.*

Il capoverso 4 garantisce che tali esami possono essere attuati soltanto da persone qualificate. Tali interventi sono del resto sottoposti a una restrizione assoluta: essi sono ammessi soltanto se non si debba temere pregiudizio alcuno per la persona interessata.

Il *capoverso 5,* infine, è fissata la competenza a ordinare un esame del sangue in caso di grave indizio di reato. Il prelievo può essere attuato anche da personale ausiliario perito.

*Articolo 73^quater^*

Le misure d'identificazione e di confronto di persone incolpate fanno parte dei mezzi classici a disposizione della polizia per lottare contro la criminalità. Tra le misure d'identificazione - i metodi necessari all'identificazione delle persone - vi sono le impronte digitali e del palmo delle mani, le tracce sul luogo del reato, fotografie e segnalazioni[62]. Le misure d'identificazione possono tuttavia modificarsi a seconda dei progressi fatti nel settore delal polizia scientifica. Si pensi per esempio alle nuove tecniche di paragone delle voci o dei capelli che hanno assunto rilievo in tempi recenti.

Con questo articolo che può essere inteso come concretizzazione ai sensi dell'articolo 30 capoverso 4 lettera c LPD, è creato il fondamento giuridico per l'applicazione di tale importante mezzo d'investigazione[63]. Possono essere sottoposti a misure d'identificazione in primo luogo un incolpato, se lo esige l'assunzione delle prove (lett. a) e d'altro canto, altre persone, onde chiarire, per questa via, l'origine delle tracce (lett. b). Il materiale che ha servito all'identificazione delle persone prosciolte o di persone i cui dati sono stati trattati unicamente a tale scopo, è distrutto secondo le disposizioni dell'ordinanza sul servizio d'identificazione. Anche gli altri dati d'identificazione saranno a loro volta allontanati dalla collezione dei dati, una volta trascorso un determinato termine[64]. Non occorre regolare in modo speciale il rilevamento di prove di scritture o della voce; in effetti, l'articolo 102 della legge federale sulla procedura penale costituisce a questo scopo il fondamento legale sufficiente, dal momento che in pratica sono inattuali misure coercitive e che l'ammissibilità di tali misure risulta già dall'articolo 102 PPF.

Articolo 101bis

Soltanto un giudice istruttore può procedere a un'audizione formale dei testi. Nella procedura delle indagini di polizia giudiziaria, possono tuttavia essere intesi terzi a scopo d'informazione[65], sempre che questi non possano richiamarsi al diritto di rifiutare di testimoniare. Il presente articolo che corrisponde all'articolo 40 della legge sulla procedura penale (RS *313.0*) è la definizione legale di una pratica già in vigore. È inoltre menzionato l'obbligo della polizia giudiziaria di informare le persone aventi il diritto di rifiutare la testimonianza in occasione dell'istruzione federale che hanno tale diritto anche in fase di procedura delle indagini di polizia giudiziaria.

Articolo 102bis

Il *capoverso 1* – come anche la legge generale sulla protezione dei dati – riconosce ad ognuno il diritto di chiedere al Ministero pubblico della Confederazione che dirige le indagini della procedura di polizia giudiziaria quali dati che lo concernono sono trattati dalla polizia giudiziaria.

Secondo il *capoverso 2,* l'informazione può essere ristretta o rifiutata se questa compromette le indagini (lett. a), se lo esigono interessi pubblici preponderanti, in particolare la sicurezza interna od esterna della Confederazione (lett. b) o interessi preponderanti di un terzo (lett. c). Le restrizioni del diritto sono di conseguenza quasi sempre le stesse di quelle previste dall'articolo 6 della legge sulla protezione dei dati. Il diritto d'accesso non deve in effetti servire a indicare ai delinquenti se la polizia sia già sulle loro tracce. Anche nel settore delle indagini della polizia giudiziaria, il richiedente che s'è visto rifiutare o limitare il diritto d'accesso dispone di rimedi di diritto. Egli può in tale caso ricorrere al Preposto alla protezione dei dati (cfr. nostre osservazioni a proposito dell'art. 102ter).

Nel *capoverso 3* è ancorata l'esigenza dell'interessato a che nessun dato inesatto sia trattato su di lui. La nozione di «dati inesatti» non deve tuttavia essere intesa nel senso che sia inesatto ogni dato di cui non sia ancora data la verità materiale. Tutte le informazioni sono raccolte nello stadio delle indagini preliminari in vista della loro valutazione da parte del giudice. Tuttavia, soltanto in questo secondo momento è dato di rilevare definitivamente se un dato possa essere considerato «esatto» o «inesatto». Per questo motivo in fase di procedura delle indagini della polizia giudiziaria una rettifica di dati ai sensi del diritto sulla protezione dei dati non è sempre possibile. Un dato deve tuttavia essere corretto se erroneamente lasci insorgere l'impressione che sia già provato materialmente in modo univoco e che non vi siano più dubbi in merito alla sua esattezza. Rileviamo infine che la pratica non deve porre esigenze troppo severe alla *valutazione dell'interesse legittimo del richiedente* alla rettifica o alla distruzione dei dati inesatti. Il richiedente deve tuttavia far valere un interesse legittimo. Del resto è evidente che i dati dei quali risulti l'inesattezza devono essere corretti o distrutti d'ufficio.

Poiché la persona interessata non ha normalmente i mezzi per provare l'inesattezza di un dato, secondo il *capoverso 4* spetta alla polizia giudiziaria provare l'esattezza del dato. Nel caso non possa essere provata né l'esattezza né l'ine-

sattezza di un dato può essere fatta *menzione del carattere controverso* del dato. Soluzione analoga esiste già nelle leggi di polizia dei Cantoni Vaud e Vallese. Questa corrisponde anche ai principi generali della procedura penale.

Articolo 102ter

Se il procuratore generale rifiuta o limita l'informazione, il richiedente può, giusta il *capoverso 1,* portare la pratica davanti al Preposto federale alla protezione dei dati. Quest'ultimo può informarsi presso il procuratore generale.

Se il Preposto alla protezione dei dati giunge a un'altra conclusione di quella del procuratore generale, allora raccomanda a quest'ultimo, giusta il *capoverso 2,* di riconsiderare la sua decisione.

Se il procuratore generale non è d'accordo con tale raccomandazione, egli o il Preposto alla protezione dei dati possono, secondo il *capoverso 3,* sottoporre l'affare alla Camera d'accusa del Tribunale federale. Questa regolamentazione è giustificata dal fatto che il Tribunale federale già adempie, in materia di procedura d'indagini preliminari, determinati compiti (detenzione, sorveglianza ufficiale, rimozione dei sigilli): con la presente revisione della procedura penale federale, il Tribunale federale vedrà attribuire in generale più competenze in questa materia. Onde non compromettere lo scopo dell'istruzione, alla persona interessata non sono tuttavia riconosciuti, in questa procedura, diritti di parte. La Camera d'accusa può invece, sempre che sia necessario per la sua decisione, consultare gli atti della polizia giudiziaria.

Articolo 102quater

I dati raccolti dalla polizia sono per la più parte degni di particolare protezione; occorre quindi limitare al massimo la loro comunicazione. A tale scopo, il *capoverso 1,* sul modello di diversi ordinamenti cantonali, elenca quelle autorità alle quali gli organi della polizia giudiziaria possono comunicare i dati da loro raccolti.

Il *capoverso 2* contiene una riserva a favore di altre disposizioni in materia d'assistenza giudiziaria. Si tratta in particolare degli articoli 352 e seguenti del Codice penale che definiscono la procedura d'assistenza giudiziaria, e gli articoli 19 e 30 della legge federale sul diritto penale amministrativo che regolano l'obbligo di denuncia delle autorità e il dovere di prestare assistenza. L'assistenza giudiziaria nei confronti degli organi giudiziari militari è retta dagli articoli 18 e seguenti della procedura penale militare (RS *322.1*).

Articolo 105bis

Attualmente soltanto singole misure del procuratore generale soggiacciono all'esame del giudice, quali il rigetto di una domanda di rimessa in libertà (art. 52 PPF), la sorveglianza della corrispondenza postale, telefonica e telegrafica (art. 66bis) e la perquisizione di carte (art. 69 cpv. 1 PPF). Per le altre misure quali sequestro e perquisizione domiciliare non è finora previsto un controllo giudiziale diretto. Secondo il *capoverso 1,* la persona interessata si vede accordata, come nella procedura penale ammninistrativa (cfr. art. 26 cpv. 1 DPA; RS *313.0*), il diritto di fare esaminare ogni misura coercitiva dalla Camera d'ac-

cusa del Tribunale federale. Si tratta delle misure seguenti: arresto, arresto provvisorio, sequestro, esame medico, perquisizione personale, perquisizione domiciliare e confisca. Questo non significa tuttavia anche che la Camera d'accusa possa sostituire la propria valutazione a quella del giudice d'istruzione o che debba esaminare l'opportunità di ogni misura istruttoria. Una modificazione della pratica vigente della Camera d'accusa[66] non è prevista.

Altre misure di polizia che non incidono in ugual misura sui diritti della personalità possono tuttora essere impugnate soltanto con ricorso all'autorità di sorveglianza, il Dipartimento federale di giustizia e polizia (cfr. art. 17 cpv. 1 PPF).

Articolo 107bis

Secondo il *capoverso 1,* il Ministero pubblico della Confederazione deve distruggere o archiviare gli atti al termine della procedura federale o cantonale. Gli atti della procedura delle indagini preliminari della polizia giudiziaria possono però essere distrutti soltanto in misura limitata, poiché spesso devono essere conservati in vista di un'eventuale procedura di revisione o di risarcimento[67]. Inoltre in parte esiste la necessità di valutarli a scopi di statistica. Inoltre occorre poter conservare, trattare e spogliare su un lungo periodo le informazioni raccolte in occasione d'operazioni d'informazione a lungo termine o nell'ambito della lotta contro il terrorismo; una parte di queste informazioni è in effetti stata ottenuta in occasione di indagini preliminari nel senso della procedura penale federale. La distruzione prematura potrebbe mettere in pericolo la sicurezza interna ed esterna della Svizzera. Sono infine riservate le disposizioni legislative sull'obbligo di conservazione dei documenti. Così, il procuratore generale deve tenere in custodia gli atti dell'istruzione sospesa (art. 124 PPF). Per tutti questi casi il capoverso 1 prevede quindi la possibilità dell'*archiviazione.* Nelle prescrizioni sull'Archivio federale possono inoltre essere previsti obblighi di consegna a favore dell'Archivio federale.

Il *capoverso 2* limita l'uso degli atti archiviati. Questi possono essere usati soltanto in relazione a un'altra procedura o per scopi che non si riferiscono alle persone, vale a dire in particolare per scopi statistici.

Secondo il *capoverso 3,* il Consiglio federale regola i dettagli in un'ordinanza, disciplinando fra l'altro l'organizzazione dell'archiviazione.

222.6 Modificazione della legge federale sull'assistenza internazionale in materia penale

222.61 L'organizzazione internazionale di polizia criminale INTERPOL

La revisione di legge proposta ha lo scopo di disciplinare la collaborazione tra l'organizzazione internazionale di polizia criminale (INTERPOL) e il nostro Paese. Un ordinamento del traffico transfrontaliero delle informazioni in materia di polizia s'impone in ragione della crescente portata di tale scambio di dati. Nell'anno 1986 oltre 100 000 informazioni sono state trasmesse, dall'Uf-

ficio centrale svizzero, organo del Ministero pubblico della Confederazione incaricato d'assicurare i rapporti tra i servizi di polizia svizzeri e stranieri. Con il proposto completamento della legge sull'assistenza penale internazionale è fissato il quadro giuridico della collaborazione con INTERPOL (competenza e compiti dell'organo federale interessato) e sono istituite le misure in materia di protezione dei dati che s'impongono nell'ottica attuale. Adempimento dei compiti ed efficienza di INTERPOL non ne risultano pregiudicati.

Fondata nel 1923, INTERPOL raggruppa le polizie criminali di 146 Stati. La Svizzera è da sempre membro dell'organizzazione. INTERPOL persegue l'obiettivo d'assicurare e sviluppare, entro i limiti degli accordi internazionali e delle leggi nazionali, l'assistenza reciproca più ampia possibile tra le autorità di polizia criminale e, quindi, di contribuire efficacemente alla repressione e alla prevenzione dei reati.

L'attività di INTERPOL s'incentra sullo scambio d'informazioni di polizia tra i diversi Stati membri (mandati d'arresto internazionali, avvisi di ricerca, domande di sorveglianza, d'identificazione, ecc.). Questo scambio d'informazioni si svolge attraverso gli Uffici centrali nazionali. Questi sono la piattaforma girevole tra gli organi nazionali di polizia e il Segretariato generale d'INTERPOL, rispettivamente tra gli Uffici cnetrali nazionali di altri Stati membri. La parte preponderante delle informazioni di polizia tra i singoli Uffici centrali nazionali passa attraverso il Segretariato generale di INTERPOL; gli Uffici centrali nazionali comunicano però anche direttamente tra loro. La comunicazione attraverso il Segretariato generale di INTERPOL è retta dal «Regolamento del 1984 sul trattamento e la comunicazione d'informazioni nel quadro di INTERPOL» (detto di seguito Regolamento 84). In merito allo scambio diretto di informazioni tra gli Uffici centrali nazionali, invece, non esiste ancora alcun regolamento sui dati. Il relativo regolamento è però in preparazione (cfr. art. 11 del Regolamento 84; Allegato dell'ordinanza del 1° dicembre 1986 sull'Ufficio centrale nazionale INTERPOL Svizzera; RS *172.213.56*).

222.62 Necessità della regolamentazione

Gli scambi internazionali d'informazioni di polizia sono retti attualmente dagli Statuti d'INTERPOL che tuttavia riservano esplicitamente le prescrizioni legislative dei Paesi membri. Nessun Ufficio centrale nazionale può trasmettere informazioni che costituiscono una violazione del diritto nazionale. Gli Statuti non stati recentemente accolti nel nostro ordinamento giuridico in base all'ordinanza del 1° dicembre 1986 sull'Ufficio centrale nazionale INTERPOL Svizzera; i fondamenti legali per l'ordinanza non sono tuttavia ancora sufficienti.

Con la presente revisione si intende completare i fondamenti legali della collaborazione con INTERPOL. Si tratta in primo luogo di precisare la comunicazione di informazioni di polizia allo scopo della *prevenzione* dei reati. Diversamente che per la *lotta* contro i reati, si applicano qui i principi della legge federale sull'assistenza internazionale in materia penale (AIMP; RS *351.1*) che

hanno in parte anche carattere di protezione dei dati (ad es. divieto di assistenza giudiziaria in caso di perseguimento penale contro reati d'opinione politica, contro l'appartenenza a una determinata razza, religione o etnia; art. 2 AIMP). Inoltre, per lo scambio di dati tra il Ministero pubblico della Confederazione nella sua qualità di Ufficio centrale nazionale e gli Uffici centrali nazionali di altri Stati dev'essere creato un ordinamento legale, considerato che a proposito di questo tipo di scambio d'informazioni il regolamento INTERPOL è soltanto in preparazione.

Con la proposta modificazione dell'AIMP si viene a tenere conto della particolarità dello scambio di informazioni di polizia. Lo scambio di dati per scopi della prevenzione dei reati dev'essere permesso soltanto se, *sulla base di circostanze concrete, si può prevedere che sarà commesso un crimine o un delitto.* I principi dell'AIMP vengono però dichiarati applicabili anche allo scambio d'informazioni a scopo di prevenzione. È inoltre rilevato che gli scambi di atti d'informazioni tra gli Uffici centrali nazionali dovranno conformarsi al Regolamento 84 di INTERPOL, come pure ad eventuali futuri regolamenti di INTERPOL. In questo modo anche il diritto svizzero garantirà certi principi di protezione dei dati in occasione di scambi d'informazioni nel quadro di INTERPOL.

222.63 Sede delle disposizioni proposte

Gli scambi internazionali d'informazioni di polizia criminale fanno parte di fatto o in diritto del campo dell'assistenza giudiziaria e amministrativa in materia penale. La sede delle disposizioni proposte ci sembra quindi essere l'AIMP e non il CP.

Le regole della collaborazione nel quadro di INTERPOL vengono raccolte in una nuova sezione dell'AIMP. Risulta così evidente che le disposizioni si riferiscono unicamente alla trasmissione di informazioni di polizia e non alla comunicazione di dati effettuata nell'ambito di una procedura d'assistenza giudiziaria; anche se tali informazioni passano per i canali di INTERPOL e con questo per l'Ufficio centrale nazionale (cfr. art. 29 cpv. 2 AIMP). Poiché per le domande d'assistenza giudiziaria valgono severe regole procedurali ed esiste un apparato di protezione giuridica dei dati, la legge sulla protezione dei dati non trova applicazione alle stesse (cfr. art. 2 cpv. 2 lett. f LPD).

222.64 Commento del progetto di legge

Articolo 81a Competenza

Secondo l'articolo 32 degli Statuti di INTERPOL, ogni Stato deve designare un Ufficio centrale nazionale. Tale organismo pubblico ha il compito d'assicurare le relazioni tra le autorità preposte al perseguimento penale del Paese interessato, da un canto, e i servizi di altri Paesi che fanno funzione di Uffici centrali nazionali, come pure con il Segretariato generale dell'Organizzazione dall'altro. L'articolo 81*a* assegna - in corrispondenza all'ordinamento attuale

(art. 81 dell'ordinanza sull'Ufficio centrale nazionale INTERPOL Svizzera) - i compiti dell'Ufficio centrale nazionale al Ministero pubblico della Confederazione.

Articolo 81b Compiti

L'articolo fissa a quale scopo e in quale misura il Ministero pubblico della Confederazione può cooperare con il Segretariato generale di INTERPOL e gli Stati membri. Secondo il *capoverso 1* si può procedere a scambi d'informazioni allo scopo di *perseguire reati e di eseguire pene e misure.* Secondo il *capoverso 2* devono poter essere trasmesse anche informazioni di polizia criminale allo scopo di prevenire reati, tuttavia soltanto se viste le *circostanze concrete* si può prevedere che sarà commesso un crimine o un reato. Nel *capoverso 3* si sottolinea che il Ministero pubblico della Confederazione può comunicare informazioni, tramite INTERPOL, destinate alla ricerca di persone scomparse o all'identificazione di sconosciuti. Fanno parte di questa categoria di informazioni *non di polizia criminale* in particolare le ricerche urgenti destinate alla Centrale d'allarme del Touring Club Svizzero. Il *capoverso 4* costituisce il fondamento dello *scambio d'informazione con i privati* in vista di prevenire o chiarire reati. Si tratta in primo luogo di comunicazioni relative a oggetti rubati, chèques e carte di credito falsificate, ecc.

Nella sua qualità di Ufficio centrale nazionale, il Ministero pubblico della Confederazione si limita alla *comunicazione* di dati, fatto sottolineato dai termini usati «trasmettere» e «fornire». Esso esamina in ogni caso l'ammissibilità di domande e informazioni. L'attuazione di ricerche in proprio sulla base dei dati trasmessi non è invece compito dell'Ufficio centrale nazionale.

Articolo 81c Protezione dei dati

Questo articolo contiene le disposizioni effettive di protezione dei dati applicabili alla collaborazione con INTERPOL. Esso istituisce due sistemi diversi a seconda si tratti di scambio di *informazioni di polizia criminale* oppure di scambio di *informazioni destinate a compiti amministrativi.* Nel primo caso sono applicabili i principi generali dell'AIMP, come pure gli statuti e i regolamenti di INTERPOL, nel secondo caso la legge sulla protezione dei dati. Questa soluzione è giustificata dal fatto che nel secondo caso i dati sono spesso comunicati in una procedura non formale e che quindi non è giustificata un'eccezione ai sensi dell'articolo 2 capoverso 2 lettera f LPD.

Il *capoverso 1* sottolinea che gli statuti e i regolamenti di INTERPOL sono applicabili anche al nostro Paese, nella misura in cui sono stati dichiarati tali dal Consiglio federale. Poiché i regolamenti di INTERPOL non sono trattati internazionali, ma bensì accordi tra le autorità di polizia degli Stati membri, essi non sottostanno all'approvazione del Consiglio federale e del Parlamento. In considerazione della loro grande importanza, il Consiglio federale deve tuttavia pronunciarsi esplicitamente sulla loro applicabilità nel nostro Paese. Se del caso essi saranno pubblicati nella Raccolta ufficiale acquistando così carattere vincolante. Valgono come scambio di *informazioni di polizia criminale* anche trasmissioni di informazioni che non in relazione con una domanda formale d'estradizione. I principi generali della legge sull'assistenza giudiziaria saranno

in avvenire applicabili anche a tali flussi di dati. Il Preposto alla protezione dei dati può tuttavia controllare la conformità degli scambi d'informazione con i principi dell'AIMP e delle disposizioni della protezione dei dati dei regolamenti INTERPOL soltanto nella misura in cui l'articolo 26 capoverso 2 LPD non gli permetta altrimenti, vale a dire se il Ministero pubblico della Confederazione acconsente. Se il Preposto rileva lacune, può informare il procuratore generale e presentargli proposte per il relativo accantonamento. Egli può anche, dopo aver sentito il Procuratore generale, farne menzione nel rapporto d'attività al Parlamento e al Consiglio federale. Per contro, egli non ha il diritto, in caso di disaccordo con il Procuratore generale, di portare la pratica davanti alla Commissione federale della protezione dei dati poiché, in effetti, gli scambi d'informazioni di polizia devono di regola svolgersi molto rapidamente.

Il *capoverso 2* contiene la base per lo scambio di informazioni di tipo amministrativo non di polizia criminale. Questo scambio di dati, diversamente da quanto avviene per lo scambio a scopi di polizia criminale, soggiace alla legge generale sulla protezione dei dati. Ne consegue che in questo settore il Preposto alla protezione dei dati può esercitare a pieno le proprie facoltà. In particolare egli può sottoporre trattamenti contestati alla Commissione federale della protezione dei dati.

Il *capoverso 3* disciplina lo *scambio diretto di informazioni con gli Uffici centrali nazionali degli altri Stati.* Anche per questo traffico di dati valgono i principi dell'AIMP menzionati sopra. Tale scambio di informazioni è inoltre ammissibile se gli Stati interessati offrono una protezione giuridica dei dati che coprono le informazioni ottenute direttamente da un Ufficio centrale nazionale e non tramite la centrale INTERPOL. Ciò significa che lo Stato destinatario deve non soltanto vigilare sulla costante esattezza e attualità dei dati ottenuti, bensì offrire alla persona interessata la possibilità di far distruggere o rettificare i dati inesatti. Può darsi che il regolamento di INTERPOL sugli scambi diretti tra gli Uffici centrali nazionali sia adottato prima dell'entrata in vigore della disposizione presente. Lo scambio diretto d'informazione con tutti gli Stati che saranno sottoposti a tale regolamento sarà allora lecito.

Articolo 81d Aiuti finanziari e indennità

Questa disposizione crea la base legale esplicita per l'erogazione di contributi finanziari a INTERPOL.

3 Conseguenze finanziarie e sull'effettivo del personale

31 Conseguenze per la Confederazione

La legge sulla protezione dei dati causerà da un lato determinati esborsi, d'altro lato essa avrà anche effetti finanziari positivi. Ambedue le conseguenze non possono tuttavia essere indicate con cifre precise. Sicuramente, però, le prescrizioni della legge sulla protezione dei dati avranno incidenza di spese per gli organi che elaborano dati.

Tali spese suppletive saranno causate da ulteriori controlli nel trattamento dei dati, da misure più rigide in materia di sicurezza, dalla necessità di rilasciare

informazioni alle persone registrate e di modificare le applicazioni informatiche non conformi alle nuove esigenze legali. In singoli casi occorrerà forse anche accrescere il personale di un servizio. D'altro canto, tuttavia, la maggiore trasparenza apportata dalla legge sull'attività amministrativa, la fiducia del pubblico rinfrancata a proposito dei sistemi d'informazione degli organi della Confederazione avranno certo anche conseguenze finanziarie positive.

Da tali conseguenze differiscono le conseguenze dovute all'istituzione di *organi di controllo*. A tale scopo occorre menzionare il salario che sarà versato al Preposto legale alla protezione dei dati e ai suoi collaboratori. Il segretariato del Preposto, invece, non causerà nuovi esborsi importanti, poiché l'esistente Servizio della protezione dei dati dell'Ufficio federale di giustizia potrà assumere questo nuovo compito. Tale servizio, creato dalle Direttive del Consiglio federale del 16 marzo 1981 concernenti la protezione dei dati, occupa attualmente cinque collaboratori, senza contare le segretarie. Tale servizio tratta attualmente per la metà compiti d'ordine legislativo. Anche se quest'ultimi venissero a diminuire, il segretariato del Preposto dovrà tuttavia impiegare una decina di persone; la presente legge prevede in effetti la registrazione di determinate collezioni private di dati, come anche controlli nel settore privato e nel settore pubblico. Il costo di un'unità amministrativa di dieci persone ammonta a franchi 850 000 circa annualmente. Rileviamo che i membri della Commissione federale della protezione dei dati e quelli della Commissione peritale in materia di ricerca medica saranno indennizzati sulla base delle tariffe applicabili alle commissioni di ricorso, alle quali s'aggiungeranno le spese per il segretariato di ogni commissione, presumibilmente per due persone per la Commissione di protezione dei dati e per una persona per la Commissione peritale. Occorre poi aggiungere le spese di gestione dei due segretariati. Poiché non è tuttavia ancora possibile prevedere il numero delle decisioni che saranno pronunciate ogni anno dalle due commissioni, non è neppure possibile prevedere esattamente il costo totale di gestione delle stesse. Possiamo indicare che le spese di procedura davanti a una commissione di ricorso composta di giudici occasionali ammonta a 1000 franchi. Meno rilevanti dovrebbero essere i costi di un'autorizzazione concernente la rilevazione di un segreto professionale per scopi della ricerca medica.

32 Conseguenze per i privati

È indiscutibile che per il fatto dell'applicazione della presente legge, le persone private che trattano dati dovranno sopportare certe spese. Queste saranno dovute in massima parte alla registrazione delle comunicazioni all'estero e alla comunicazione di dati alle persone interessate. Le aziende bene organizzate non avranno però difficoltà per far fronte a tali esigenze. Le spese, soprattutto quelle relative al diritto d'accesso non vanno tuttavia sopravvalutate. Come dimostrano le esperienze fatte all'estero, le spese dovute all'esercizio del diritto d'accesso non sono per nulla sproporzionate: non soltanto il diritto d'accesso è istituzione relativamente poco usata, ma poi il rilascio di informazioni è molto facilitato dalle tecniche informatiche.

4 Linee direttive della politica di governo

Il presente rapporto è preannunciato nel rapporto sul programma di legislatura 1987-1991 (FF *1988* I 377 n. 2.17).

5 Costituzionalità

Il fondamento costituzionale della presente legge è oggetto dei numeri 12 e 22.41 ai quali rinviamo.

6 Delega di competenze

Gli articoli 6 capoverso 5, 7 capoverso 4, 8 capoverso 2, 13 capoverso 2, 21 capoverso 1 e 30 capoversi 2-6 sono deleghe di competenza legislativa a favore del Consiglio federale che esulano dal potere abituale regolamentare dello stesso. Il rapido sviluppo dell'informatica può in effetti richiedere, per certi tipi di trattamento, l'introduzione di altre regolamentazioni, che eseguono disposizioni della legge o che vi derogano. La maggior parte delle nuove norme saranno tuttavia regole d'ordine tecnico o amministrativo. Troverete spiegazioni più dettagliate a tale proposito nel commento dei rispettivi articoli.

7 Relazioni con il diritto europeo

Il presente progetto tiene già conto, sia per il settore privato, sia per il settore pubblico, delle esigenze poste dalla Convenzione n. 108 del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone per rapporto al trattamento automatizzato dei dati personali. Per aderire a tale convenzione, occorre tuttavia che anche i Cantoni sottopongano il loro settore pubblico a una legge sulla protezione dei dati. Fintanto che i Cantoni non soddisferanno le esigenze minime poste dalla convenzione, è esclusa qualsiasi possibilità d'adesione della Svizzera[68)].

1654

[1] Cfr. Sentenza del Tribunale costituzionale della Repubblica federale di Germania del 15 dicembre 1983 (Zensus-Urteil), BVerGE 65, 43.

[2] Cfr. DTF *44* II 319 segg., come pure DTF *107* Ia 148 segg., *109* Ia 273 segg.

[3] Cfr. DTF *106* Ia 33 segg.

[4] DTF *107* Ia 52 segg.: cfr. anche DTF *108* IV 158 segg.

[5] Cfr. p. es. Giurisprudenza delle autorità federali (GAAC) 48/1984, n. 21, pag. 143 segg.; n. 26, pag. 157 segg.

[6] Cfr. BVerGE 65, 43.

[7] Cfr. DTF *97* II 97 segg.

[8] Messaggio del Consiglio federale del 5 maggio 1982 concernente la revisione del Codice civile svizzero, FF *1982* II 628 segg. (650).

[9] DTF *97* II 97 segg.; cfr. inoltre DTF *109* II 353 segg., 62 II 101, *44* II 319.

[10] Cfr. DTF *107* II 6, *111* II 209 segg.; cfr. anche *84* II 573.

[11] DTF *109* Ia 279 con altri rinvii; cfr. anche DTF *106* Ia 280.

[12] Cfr. GAAC 48/1984, n. 25, pag. 155 segg.; DTF *98* Ib 297.

[13] Cfr. DTF *113* Ia 10, *101* Ia 18, *109* Ia 296 segg.

[14] FF *1981* I 1229, *1983* II 1155, *1986* III 838.

[15] Cfr. Ordinanza del 28 novembre 1985 su rilevazioni a mezzo sondaggi presso la popolazione (microcensimento; RS *431.116*), Ordinanza dell'8 luglio 1981 su rilevamenti sperimentati di dati in vista di una statistica penitenziaria (RS *431.341*), Ordinanza del DFI del 1° marzo 1984 sulle statistiche dell'assicurazione contro gli infortuni (RS *431.835*), Ordinanza del 18 aprile 1984 sulla tenuta di un registro delle imprese e degli stabilimenti (RS *431.903*).

[16] Cfr. ad es., Jörg Müller/Stefan Müller, Grundrechte, Parte speciale, Berna 1985, pag. 25; Charles-Albert Morand, Problèmes constitutionnels relatifs à la protection de la personnalité à l'égard des banques de données électroniques, in: Informatique et protection de la personnalité, Friburgo, 1981, pag. 15 segg.

[17] Cfr. tuttavia DTF *110* Ia 83 segg., *95* I 103 segg.

[18] Cfr. Jürg Boll, Die Entbindung vom Arzt- und Anwaltsgeheimnis, tesi Zurigo 1983, pag. 3; René Russek, Das ärztliche Berufsgeheimnis, tesi Zurigo 1954, pag. 42.

[19] Cfr. Peter Schäfer, Aerztliche Schweigepflicht und Elektronische Datenverarbeitung, tesi Zurigo 1987, pag. 29.

[20] Per quello che segue, cfr. in particolare: Consiglio d'Europa Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasburgo 1981; Organisation de Coopération et de Développement Economiques (OCDE), Lignes Directrices Régissant la Protection de la Vie Privée et les Flux Transfrontalières de Données de Caractère Personnel, Exposé de motifs, Parigi 1980.

[21] Cfr. Hans Huber, Berner Kommentar, numeri 105 e segg. relativi all'art. 6 CC, pag. 512 segg.; Raymond Didisheim, La notion du droit civil fédéral, contribution à l'étude de l'art. 64 de la Constitution fédérale, tesi Losanna 1973, pag. 200 segg.

[22] BU CN *1972* II pag. 2127 segg.

[23] BU CN *1972* II pag. 2131.

[24] Cfr. p. es., le leggi sulla protezione dei dati degli Stati Uniti d'America, del Canada, d'Israele, di Norvegia, della Repubblica federale di Germania e (in certa misura) della Francia.

[25] Per la protezione della sfera privata cfr. DTF *97* II 100; Jean Nicolas Druey, Geheimsphäre des Unternehmens, Basilea e Stoccarda 1977, pag. 153 seg.; Pierre Tercier, Le

nouveau droit de la personnalité, Zurigo 1984, pag. 75 segg. Si rinvia anche alla protezione penale, in particolare quella dell'articolo 162 (violazione del segreto di fabbrica e commerciale) e dell'*art. 273* (spionaggio economico). CP (RS *311.0*), come pure alla protezione contro la concorrenza sleale commessa con la violazione di segreti degli art. 4 lett. c e 6 LCS del 19 dicembre 1986 (FF *1987* I 26).

[26] Jörg Paul Müller/Stefan Müller (FN 16), pag. 14; Ulrich Häfelin/Walter Haller, Schweizerisches Bundesstaatsrecht, Zurigo 1984, pag. 350.

[27] Cfr., fra gli altri, Christian Dominicé, La personnalité juridique internationale du CICR, in: Etudes en l'honneur de Jean Pictet, Ginevra/L'Aia 1984, pag, 666; Paul Reuter, La personnalité juridique internationale du Comité International de la Croix Rouge, ibidem, pag. 728; cfr. anche FF *1987* I 297 segg., 309.

[28] Cfr. art. 22 della Legge federale del 7 dicembre 1922 concernente il diritto d'autore sulle opere letterarie ed artistiche (RS *231.1*).

[29] Cfr. ad es., art. 42 della Legge federale del 23 marzo 1962 concernente la procedura dell'Assemblea federale e la forma, la pubblicazione, l'entrata in vigore dei suoi atti (L sui rapporti tra i Consigli; RS *171.11*); art. 2 segg. del Regolamento del Consiglio nazionale (RS *171.13*) e gli art. 17 e 20 segg. del Regolamento del Consiglio degli Stati (RS *171.14*).

[30] Cfr. Simitis/Damman/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden 1978, NN. 19 segg. ad § 2.

[31] DTF *100* Ib 114.

[32] Cfr. Schnyder/Murer, Berner Kommentar zum Schweizerischen Privatrecht, vol. II, sez. 3, parte sistematica, n. 54.

[33] Art. 7 Legge sul diritto penale amministrativo (RS *313.0*).

[34] DTF *44* II 319 segg.; cfr. anche art. 179bis CP (RS *311.0*).

[35] ZR 43/1944, N. 217.

[36] DTF *112* Ia 100, *110* Ia 85, *103* Ia 492, *100* Ia 10.

[37] Anche il Messaggio (nota 8), pag. 683.

[38] Cfr. art. 934 segg. CO (RS *220*) e l'Ordinanza del 7 giugno 1937 sul registro di commercio (RS *221.411*).

[39] Tercier (nota 25), n. 682.

[40] Messaggio (nota 8), pag. 680/681; Tercier (nota 25), n. 840 segg.

[41] Cfr. Tercier (nota 25) n. 799 segg.

[42] DTF *103* II 294, *85* II 18 segg., *73* II 65.

[43] Erich Richner, Umfang und Grenzen der Freiheitsrechte der Beamten nach schweizerischem Recht, Aarau 1954, pag. 129; Paul Reichlin, Die Schweigepflicht des Verwaltungsbeamten, Zurigo 1953, pag. 21.

[44] Cfr. però art. 30 della Legge federale del 22 marzo 1974 sul diritto penale amministrativo (RS *313.0*).

[45] Cfr. DTF *108* Ib 231, *96* IV 183, *87* IV 141, *86* IV 136.

[46] Cfr. ad es., art. 50 LAVS (RS *831.10*); art. 102 LAINF (RS *832.20*), art. 97 della Legge sull'assicurazione contro la disoccupazione (RS *837.0*), come pure l'art. 125 dell'Ordinanza sull'assicurazione contro gli infortuni (RS *832.202*) e l'art. 125 dell'ordinanza sull'assicurazione contro la disoccupazione (RS *837.02*).

[47] Cfr. a tale proposito l'Ordinanza sul registro centrale degli stranieri (RS *142.215*).

[48] Cfr. ad es., l'art. 90 del Decreto del Consiglio federale del 9 dicembre 1940 concernente la riscossione d'una imposta federale diretta (RS *642.11*), l'art. 32 della Legge federale del 27 giugno 1973 sulle tasse di bollo (RS *641.10*), l'art. 36 della Legge federale del 13 ottobre 1965 su l'imposta preventiva (RS *642.21*), l'art. 4 cpv. 2 lett. c e art. 7 cpv. 2 del Decreto del Consiglio federale del 29 luglio 1941 che istituisce un'imposta sulla cifra d'affari (RS *641.20*).

[49] Decreto del Consiglio federale del 29 aprile 1958 concernente il servizio di polizia del Ministero pubblico della Confederazione (RS *172.213.52*) e le prescrizioni del DFGP del 19 aprile 1958 (FF *1958* II 794 seg.).

[50] DTF *104* Ib 384, *101* Ib 110; Fritz Gygi, Bundesverwaltungsrechtspflege, 2ª edizione riveduta, Berna 1983.

[51] FF *1985* II 709 segg., 854 seg.

[52] Cfr. art. 20 del Codice penale (RS *311.0*): DTF *107* IV 193 segg., 207 cons. 3.

[53] Urs Chr. Nef, Aktuelle Probleme des Personaldatenschutzes im arbeitsrechtlichen Rechtsverhältnis, Zeitschrift für schweizerisches Recht, 92 (I) 1973, pag. 357 segg.; Bernhard Frei, Der Persönlichkeitsschutz des Arbeitnehmers nach CO art. 328 cpv. 1. Unter besonderer Berücksichtigung des Personaldatenschutzes, Berna 1982, pag. 48 segg.; GAAC 48/1984, n. 33, pag. 198 segg.

[54] FF *1988* I 5.

[55] FF *1972* I 410.

[56] Cfr. anche il disegno di legge federale sulla protezione della gravidanza e il carattere punibile della sua interruzione, FF *1977* III 92 segg.

[57] Cfr. Günther Stratenwerth, Schweizerisches Strafrecht, Parte speciale I, 3ª edizione, riveduta, Berna 1983, pag. 150; Peter Schäfer, Aerztliche Schweigepflicht und Elektronische Datenverarbeitung, tesi Zurigo, 1978, pag. 30 segg.

[58] Sul diritto di agire dei genitori cfr. DTF *87* IV 105.

[59] Cfr. DTF *94* IV 7 cons. 1.

[60] DTF *109* Ia 244 segg.

[61] DTF *74* IV 213.

[62] Cfr. art. 1 dell'Ordinanza concernente il servizio d'identificazione del Ministero pubblico della Confederazione, RS *172.213.57*.

[63] Cfr. anche DTF *109* Ia 156.

[64] Cfr. art. 9 e 17 dell'Ordinanza concernente il servizio d'identificazione del Ministero pubblico della Confederazione (cfr. nota 59).

[65] Markus Peter, Ermittlungen nach Bundesstrafprozess, Kriminalistik 1973, pag. 565; Robert Hauser, Zeitschrift für Schweiz. Strafrecht 1972, pag. 137 segg.

[66] Cfr. DTF *96* IV 141; *95* IV 47.

[67] Cfr. DTF *109* IV 63.

[68] Cfr. art. 4 della Convenzione n. 108 e n. 117 del Messaggio.