Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.059

Messaggio concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati

del 15 settembre 2017

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di legge federale relativo alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi relativi alla protezione dei dati nonché il disegno di decreto federale che approva lo scambio di note tra la Svizzera e l'Unione europea sul recepimento della direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Nel contempo vi proponiamo di togliere dal ruolo i seguenti interventi parlamentari:

- Postulato Hodgers 10.3383 «Adeguare la legge sulla protezione dei dati alle nuove tecnologie»;
- Postulato Graber 10.3651 «Attacchi alla sfera privata e minacce indirette alle libertà individuali»;
- Postulato Schwaab 12.3152 «Diritto all'oblio in Internet»;
- Postulato Recordon 13.3989 «Violazioni della personalità riconducibili al progresso delle tecnologie dell'informazione e della comunicazione»;
- Mozione Comte 14.3288 «Rendere l'usurpazione dell'identità un reato a sé stante»;
- Postulato Derder 14.3655 «Definire la nostra identità digitale e identificare le soluzioni per proteggerla»;
- Postulato Schwaab 14.3739 «Control by design. Potenziare i diritti di proprietà per impedire le connessioni indesiderate»;
- Postulato Gruppo liberale-radicale 14.4137 «Registrazioni video di privati. Migliorare la tutela della sfera privata»;
- Postulato Comte 14.4284 «Registrazioni video di privati. Migliorare la tutela della sfera privata»;

– Postulato Béglé 16.3383 «Dati digitali: informare le persone lese in caso di pirateria»;
– Postulato Béglé 16.3384 «Dati medici digitali. Garantire una raccolta protetta, trasparente e mirata nella revisione della legge federale sulla protezione dei dati».

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

15 settembre 2017

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Doris Leuthard
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

Il presente disegno di legge si prefigge di rafforzare la protezione dei dati aumentando la trasparenza del trattamento di dati e le possibilità delle persone interessate di controllare i dati che le riguardano. Nel contempo intende aumentare il senso di responsabilità dei titolari del trattamento, obbligandoli ad esempio a rispettare le disposizioni sulla protezione dei dati sin dalla progettazione di nuovi trattamenti. Il disegno mira inoltre a migliorare l'applicazione e il rispetto delle norme federali sulla protezione dei dati. Infine, intende consolidare e migliorare la competitività della Svizzera, agevolando in particolare la comunicazione di dati all'estero e promuovendo lo sviluppo di nuovi settori economici nell'ambito della digitalizzazione della società, sulla base di un livello di protezione riconosciuto su scala internazionale.

Situazione iniziale e obiettivi del progetto

Il presente progetto intende realizzare due obiettivi principali. Da una parte è teso a rafforzare le disposizioni sulla protezione dei dati per far fronte alla rapidissima evoluzione tecnologica. Dall'altra, tiene conto degli sviluppi nel Consiglio d'Europa e nell'Unione europea. L'avamprogetto è stato posto in consultazione dal 21 dicembre 2016 al 4 aprile 2017.

Il 27 aprile 2016 l'Unione europea ha riveduto la propria legislazione sulla protezione dei dati, che comprende due atti normativi: il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nel settore del diritto penale. Soltanto la direttiva fa parte dell'acquis di Schengen. Per quanto riguarda il Consiglio d'Europa, un protocollo d'emendamento della Convenzione STE 108 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale deve ancora essere adottato dal Comitato dei Ministri.

Il presente disegno intende garantire che la legislazione federale sia compatibile con la Convenzione STE 108 riveduta. È infatti nell'interesse della Svizzera approvare il Protocollo d'emendamento di tale Convenzione non appena sarà aperto alla firma. Inoltre, il progetto intende attuare i requisiti della direttiva (UE) 2016/680 e permettere pertanto alla Svizzera di adempiere agli obblighi risultanti dall'Accordo di associazione a Schengen. Il progetto mette altresì in atto le raccomandazioni dell'Unione europea elaborate in occasione della valutazione della Svizzera nell'ambito dell'Accordo di associazione a Schengen, tra cui in particolare quella di estendere le competenze dell'Incaricato federale della protezione dei dati e della trasparenza (Incaricato). Infine, il presente progetto ha lo scopo di adeguare in generale la legislazione svizzera sulla protezione dei dati ai requisiti del regolamento (UE) 2016/679. Secondo il Consiglio federale, insieme alla ratifica della revisione della Convenzione STE 108, tale adeguamento costituisce il presupposto decisivo per la futura decisione di adeguatezza. Con tale decisione la Commissione europea confermerebbe che la legislazione svizzera garantisce una protezione ade-

guata dei dati. La decisione di adeguatezza è di fondamentale importanza soprattutto per l'economia svizzera.

L'adozione del messaggio concernente il presente disegno figura tra gli obiettivi del Consiglio federale del 2017 e nel programma di legislatura 2015–2019. Negli ultimi anni la revisione della protezione dei dati è stata inoltre oggetto di numerosi interventi parlamentari, a testimonianza della volontà politica di perfezionare la legislazione federale in tale settore.

Contenuto del progetto

Il disegno di legge prevede innanzitutto una revisione totale della legge federale sulla protezione dei dati.

Conformemente alle norme europee e alla maggior parte degli ordinamenti giuridici esteri, il disegno di legge sulla protezione dei dati abolisce la protezione dei dati delle persone giuridiche e adegua di conseguenza il campo d'applicazione della legge stessa. Ciò agevola in particolare la comunicazione di dati all'estero.

In generale, il progetto migliora la trasparenza del trattamento di dati. L'obbligo di informare la persona interessata in occasione della raccolta di dati si applica a tutti i trattamenti da parte di titolari privati, ma sono previste singole eccezioni. L'informazione può essere fornita in forma semplice e standardizzata. Inoltre, la persona interessata deve essere informata sulle decisioni basate su un trattamento puramente automatico dei dati. Se sono soddisfatte determinate condizioni, deve altresì avere la possibilità di esporre il suo punto di vista e di chiedere che la decisione sia riesaminata da una persona fisica. Sono infine estese le informazioni da fornire alla persona interessata quando questa fa valere il suo diritto d'accesso.

La revisione mira a promuovere l'autoregolazione presso i titolari del trattamento, soprattutto attraverso codici di condotta tesi ad agevolare le loro attività, e a migliorare il rispetto della legge. Tali codici sono elaborati dai rami interessati e possono essere sottoposti all'Incaricato.

L'indipendenza e la posizione dell'Incaricato sono rafforzate. La revisione prevede che, alla stregua dei suoi omologhi europei, l'Incaricato possa aprire, d'ufficio o su querela, un'inchiesta nei confronti dei titolari o dei responsabili del trattamento ed emanare una decisione dopo la conclusione dell'inchiesta.

Infine, la revisione inasprisce sotto vari punti di vista le disposizioni penali della legge sulla protezione dei dati, soprattutto poiché, diversamente dai suoi omologhi europei, l'Incaricato non può infliggere sanzioni amministrative.

Oltre alla revisione totale della legge sulla protezione dei dati, il disegno prevede anche la revisione parziale di altre leggi federali, in particolare per attuare i requisiti della direttiva (UE) 2016/680. Si tratta soprattutto del Codice penale, del Codice di procedura penale, della legge federale sull'assistenza giudiziaria in materia penale e della legge sullo scambio di informazioni con gli Stati Schengen.

Indice

Messaggio

1 Punti essenziali del progetto

1.1 Situazione iniziale a livello nazionale

1.1.1 Diritto vigente

A livello federale la protezione dei dati è attualmente retta principalmente dalla legge federale del 19 giugno 1992[1] sulla protezione dei dati (LPD), entrata in vigore il 1° luglio 1993.

La LPD disciplina il trattamento dei dati riguardanti persone fisiche e giuridiche effettuato da privati o da organi federali (art. 2 cpv. 1). Non si applica tuttavia ai dati personali trattati da una persona fisica per uso esclusivamente personale e che non vengono comunicati a estranei (cpv. 2 lett. a), ai dibattiti delle Camere federali e delle commissioni parlamentari (cpv. 2 lett. b), ai procedimenti civili, penali e di assistenza giudiziaria internazionale pendenti, come pure a quelli di diritto pubblico e di diritto amministrativo, eccettuate le procedure amministrative di prima istanza (cpv. 2 lett. c), ai registri pubblici relativi ai rapporti di diritto privato (cpv. 2 lett. d) e ai dati personali trattati dal Comitato internazionale della Croce Rossa (CICR; cpv. 2 lett. e).

La LPD sancisce i principi da rispettare in occasione del trattamento dei dati. Prevede in particolare che i dati personali possono essere trattati soltanto in modo lecito (art. 4 cpv. 1), che il trattamento deve essere conforme al principio della buona fede e della proporzionalità (art. 4 cpv. 2) e che può essere effettuato soltanto per lo scopo indicato all'atto della raccolta dei dati, risultante dalle circostanze o previsto da una legge (art. 4 cpv. 3). La raccolta di dati personali e in particolare le finalità del trattamento devono inoltre essere riconoscibili da parte della persona interessata (art. 4 cpv. 4). L'articolo 4 capoverso 5 definisce le condizioni applicabili al consenso della persona interessata. Infine, la persona privata o l'organo federale che tratta i dati personali deve accertarsi della loro esattezza (art. 5).

La LPD disciplina inoltre la comunicazione di dati all'estero (art. 6) e il diritto d'accesso (art. 8–10). L'articolo 10*a* regola il trattamento di dati da parte di terzi, mentre l'articolo 11*a* prevede l'obbligo dell'Incaricato federale della protezione dei dati e della trasparenza (Incaricato) di tenere un registro delle collezioni di dati accessibile al pubblico via Internet e l'obbligo dei detentori di notificare le loro collezioni di dati, fatte salve alcune deroghe.

La terza sezione della LPD contiene norme specifiche per il trattamento di dati da parte di privati. I privati che trattano dati personali non possono ledere illecitamente la personalità delle persone interessate (art. 12 cpv. 1). In particolare non possono trattare, senza giustificazione, dati personali contro l'esplicita volontà della persona interessata (art. 12 cpv. 2 lett. b e art. 13). L'articolo 14 prevede l'obbligo dei privati di informare la persona interessata di qualsiasi raccolta di dati personali degni di

[1] RS **235.1**

particolare protezione o profili della personalità che la riguardano, fatte salve alcune deroghe. Infine, la terza sezione disciplina le pretese di diritto civile che possono far valere le persone lese e la relativa procedura (art. 15).

Gli articoli 16–25 LPD disciplinano il trattamento di dati personali da parte di organi federali. Questi hanno il diritto di trattare dati personali soltanto se esiste una base legale (art. 17 cpv. 1). Per il trattamento di dati degni di particolare protezione e per i profili della personalità è necessaria una base legale in una legge formale (art. 17 cpv. 2). Secondo l'articolo 18*a* gli organi federali che raccolgono dati personali hanno l'obbligo di informare la persona interessata, fatte salve alcune deroghe (art. 18*b*). Inoltre, possono in linea di massima comunicare dati a terzi soltanto se sussiste una base legale (art. 19 cpv. 1) e permettere l'accesso a dati personali mediante una procedura di richiamo soltanto se lo prevede esplicitamente la legge (art. 19 cpv. 3). Le condizioni sono ancora più severe nel caso di dati degni di particolare protezione o profili della personalità; questi possono essere resi accessibili mediante una procedura di richiamo soltanto qualora lo preveda esplicitamente una legge in senso formale (art. 19 cpv. 3). L'articolo 25, infine, disciplina le pretese che le persone interessate possono far valere nei confronti dell'organo federale responsabile del trattamento di dati che le riguardano.

Gli articoli 26 e 26*a* LPD disciplinano la nomina, lo statuto, il rinnovo e la cessazione del mandato dell'Incaricato, mentre gli articoli 27–33 ne definiscono i compiti e le competenze. L'Incaricato sorveglia il rispetto della LPD da parte degli organi federali e consiglia i privati. Può accertare i fatti ed emanare raccomandazioni. Se un privato non si attiene a una raccomandazione, l'Incaricato può deferire la pratica al Tribunale amministrativo federale ed è legittimato a ricorrere contro la decisione di quest'ultimo (art. 29 cpv. 4). Se un organo federale non dà seguito a una raccomandazione, l'Incaricato può deferire la pratica al dipartimento competente o alla Cancelleria federale (art. 27 cpv. 5). È legittimato a ricorrere contro la decisione dell'autorità superiore e contro quella dell'autorità di ricorso (art. 27 cpv. 6).

Infine, gli articoli 34 e 35 LPD prevedono disposizioni penali in caso di violazione degli obblighi d'informazione, di notifica, di collaborazione e di discrezione.

Su riserva dell'articolo 37 e delle disposizioni di leggi federali speciali, il trattamento di dati da parte degli organi cantonali (e comunali) è retto dal diritto cantonale, anche quando tali organi eseguono il diritto federale o hanno ottenuto i dati mediante un accesso in linea a una banca dati federale.

In molti settori, oltre alla LPD, si applicano leggi speciali che contengono anch'esse disposizioni sulla protezione dei dati (norme sulla protezione dei dati specifiche a un settore).

1.1.2 Lavori preliminari e piano

Tra il 2010 e il 2011 la LPD è stata oggetto di una valutazione[2] da cui è risultato che l'evoluzione tecnologica e sociale intervenuta dopo la sua entrata in vigore comporta nuove minacce per la protezione dei dati e che la sua efficacia va migliorata. La LPD non garantisce più una protezione sufficiente. Fondandosi sulle conclusioni del rapporto del 9 dicembre 2011[3], il nostro Consiglio ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di esaminare misure legislative che permettano di migliorare la protezione dei dati tenendo conto delle nuove minacce che incombono sulla sfera privata.

Per dare seguito al mandato del nostro Consiglio del 9 dicembre 2011, l'Ufficio federale di giustizia (UFG) ha istituito un gruppo di lavoro incaricandolo di avviare i lavori di revisione della LPD. Il gruppo era composto da rappresentanti dell'Amministrazione federale[4], dei Cantoni[5], dell'economia[6] e delle associazioni di protezione dei consumatori[7], come pure da esperti. Ha presentato le proprie riflessioni in un rapporto del 29 ottobre 2014[8] dal titolo «Esquisse d'acte normatif relative à la révision de la loi sur la protection des données [Bozza di atto normativo relativo alla revisione della legge sulla protezione dei dati]».

Il 1° aprile 2015 il nostro Consiglio ha preso atto del rapporto del gruppo di lavoro, incaricando il DFGP di elaborare, in collaborazione con l'Incaricato, il Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) e il Dipartimento federale dell'interno (DFI), un avamprogetto di legge che tenga conto delle conclusioni del rapporto e delle riforme del Consiglio d'Europa e dell'Unione europea.

L'avamprogetto è stato posto in consultazione il 21 dicembre 2016 e verteva su tre oggetti. In primo luogo un avamprogetto di legge, ossia un atto modificatore unico intitolato «Avamprogetto di legge federale relativo alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati». Esso riuniva sotto un unico titolo la revisione totale della LPD (AP-LPD) e la revisione parziale di altre leggi federali dello stesso livello. L'avamprogetto conteneva, in secondo luogo, l'avamprogetto di decreto federale che approva lo

2 Büro Vatter / Institut für Europarecht, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Berna 11 mar. 2011, www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf (disponibile soltanto in tedesco).

3 Rapporto del Consiglio federale del 9 dic. 2011 concernente la valutazione della legge federale sulla protezione dei dati, FF **2012** 227.

4 Nel gruppo di lavoro erano rappresentate le autorità federali seguenti: l'Ufficio federale di giustizia (UFG, direzione), l'Incaricato, l'Ufficio federale delle comunicazioni (UFCOM), l'Archivio federale svizzero (AFS), l'Ufficio federale del consumo (UFDC) e la Segreteria generale del Dipartimento federale di giustizia e polizia (SG-DFGP).

5 I Cantoni erano rappresentati dall'Associazione degli incaricati svizzeri della protezione dei dati (PRIVATIM).

6 L'economia era rappresentata da economisuisse e dall'Unione svizzera delle arti e mestieri (USAM).

7 Le associazioni di protezione dei consumatori erano rappresentate dalla Fédération romande des consommateurs.

8 www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf.
Il rapporto è disponibile in francese e in tedesco, il link è alla versione francese.

scambio di note tra la Svizzera e l'Unione europea sul recepimento della direttiva (UE) 2016/680 e, in terzo luogo, il progetto di modernizzazione della Convenzione del Consiglio d'Europa STE 108 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (P-STE 108).

L'avamprogetto aveva in particolare i seguenti obiettivi:

- trasporre i requisiti della direttiva (UE) 2016/680[9] (cfr. n. 2);
- attuare le raccomandazioni ricevute nel quadro della valutazione Schengen del 2014 (cfr. n. 1.2.2.3);
- adeguare la LPD ai requisiti del regolamento (UE) 2016/679[10] (cfr. n. 4);
- recepire i requisiti del P-STE 108 (cfr. n. 3).

La procedura di consultazione si è conclusa il 4 aprile 2017.

Sulla base dei risultati della consultazione il nostro Consiglio ha elaborato un disegno di legge. La forma è la stessa dell'avamprogetto, ossia un atto mantello sottoposto a referendum facoltativo (disegno di legge federale relativo alla revisione totale della legge federale sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, qui appresso «disegno di legge»). L'atto mantello contiene, da una parte, una cifra I che comprende la revisione totale della LPD (D-LPD) e, nell'allegato, gli adeguamenti di altre leggi federali resisi necessari in seguito alla revisione della LPD; dall'altra, una cifra II con le modifiche di leggi federali legate alla trasposizione della direttiva (UE) 2016/680 nell'ambito dell'Accordo del 26 ottobre 2004[11] tra la Confederazione Svizzera, l'Unione europea e la Comunità europea, riguardante l'associazione della Svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (Accordo di associazione a Schengen). Nel presente messaggio gli atti normativi da modificare sono indicati con «D», seguito dall'abbreviazione della legge in questione.

1.1.3 Strategia «Svizzera digitale»

Il 20 aprile 2016 il nostro Consiglio ha adottato la strategia «Svizzera digitale»[12], in sostituzione della strategia del 9 marzo 2012 per una società dell'informazione in Svizzera.

9 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 apr. 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 119 del 4.5.2016 pag. 89.

10 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 apr. 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L 119 del 4.5.2016 pag. 1.

11 RS **0.362.31**

12 La «Strategia Svizzera digitale» è consultabile sul sito www.bakom.admin.ch > Svizzera digitale e Internet > Strategia «Svizzera digitale».

La nuova strategia è tesa a permettere alla Svizzera di trarre maggior profitto dalla crescente digitalizzazione e di svilupparsi in modo ancora più dinamico come economia innovatrice. Intende in particolare sviluppare una politica in materia di dati coerente e rivolta al futuro, che offra alla Svizzera la possibilità di sfruttare appieno il potenziale di crescita inerente alla raccolta e al trattamento di dati, senza tuttavia perdere il controllo su questi ultimi. La nuova strategia «Svizzera digitale» è una strategia globale che coordina numerose attività e i gruppi di esperti. Il coordinamento è garantito dal Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC). Per realizzare la Strategia è stato ideato un piano d'azione[13] che comprende le misure che l'Amministrazione federale deve mettere in atto. Il disegno di legge fa parte di tali misure (n. 1.2 e 1.7 del piano d'azione).

Nell'ambito della politica in materia di dati che intende sviluppare, il nostro Consiglio ha conferito al DFGP l'incarico di esaminare varie questioni giuridiche riguardanti la riutilizzazione dei dati digitali. Il DFGP esaminerà, tra le altre cose, l'opportunità di introdurre nell'ordinamento giuridico svizzero un diritto alla portabilità dei dati personali. Analizzerà inoltre le possibilità per la Confederazione, secondo le leggi in vigore e i progetti di legge in corso, di riutilizzare dati personali per uno scopo di interesse pubblico (p. es. a fini statistici). Il DFGP dovrà sottoporre i risultati del suo lavoro al nostro Consiglio entro la fine del 2017.

Nel quadro dell'elaborazione della strategia «Svizzera digitale», l'Ufficio federale delle comunicazioni (UFCOM) ha conferito alla Scuola universitaria di Berna l'incarico di redigere uno studio sulla problematica dei Big Data (numero molto elevato di dati)[14]. Tale studio giunge in parte alle stesse conclusioni della valutazione della LPD: è necessario un intervento legislativo. Secondo lo studio occorre inoltre migliorare il funzionamento del mercato, conferendo maggiori poteri agli utenti e rafforzando la regolamentazione e il controllo degli attori privati da parte dello Stato. Le misure previste dal disegno di legge vanno in questa direzione.

1.1.4 Altri progetti dell'Amministrazione federale legati alla protezione dei dati

Numerosi progetti dell'Amministrazione federale tangono la protezione dei dati. Tra quelli attualmente in corso si possono citare i più importanti:

Strategia nazionale per la protezione della Svizzera contro i cyber-rischi del 27 giugno 2012 (SNPC)[15]: la strategia riguarda la protezione dai cyber-rischi delle infrastrutture che utilizzano le tecnologie dell'informazione e della comunicazione e mira a individuare precocemente le minacce nel cyber-spazio, migliorare la capacità di resistenza delle infrastrutture d'importanza vitale e ridurre i cyber-rischi legati in

13 www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/strategia-svizzera-digitale/attuazione.html.

14 «Big data: opportunità, rischi e necessità d'intervento della Confederazione», disponibile (solo in tedesco) all'indirizzo: www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/big-data.html

15 www.isb.admin.ch/isb/it/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html.

particolare alla criminalità, allo spionaggio e al sabotaggio informatici. L'attuazione della strategia compete al Dipartimento federale delle finanze (DFF). L'attuazione della strategia sarà portata a termine quest'anno conformemente alle scadenze previste. Secondo il rapporto annuale 2016 sullo stato dell'attuazione della SNPC, adottato dal nostro Consiglio il 26 aprile 2017[16], 15 delle 16 misure previste sono già realizzate. Visto l'aumento dei cyber-rischi, il nostro Consiglio ha deciso di fare elaborare una seconda strategia per il periodo 2018–2023, che risponda alle minacce attuali e tenga conto dei risultati della valutazione dell'efficacia della SNPC.

Strategia Open Government Data Svizzera del 16 aprile 2014[17]: la strategia intende promuovere la pubblicazione di dati raccolti dall'Amministrazione sotto forma di Open Government Data (OGD), ossia dati pubblici dell'Amministrazione liberamente riutilizzabili. Pur trattandosi in generale della pubblicazione di dati aggregati e precedentemente anonimizzati in vista dell'utilizzazione, i principi della protezione dei dati restano applicabili.

Programma nazionale di ricerca 75 «Big Data» (PNR 75)[18]: nel 2015 il nostro Consiglio ha avviato questo programma di ricerca, dotato di un budget di 25 milioni di franchi. Lo scopo è fornire le basi scientifiche per l'utilizzazione efficace e adeguata di megadati. Il programma si articola intorno a tre moduli: un modulo sulle tecnologie dell'informazione e i servizi di gestione dei dati nonché sulle questioni d'accesso, di sorveglianza e di confidenzialità, uno sulle sfide che Big Data pone alla società e uno sullo sviluppo di applicazioni dei megadati in diversi ambiti della società. Dall'inizio del 2017 sono stati lanciati 35 progetti di ricerca, ciascuno di una durata da 24 a 48 mesi. I primi risultati saranno disponibili a partire dal 2019. Fino al 2022 il programma prevede numerose attività tese al trasferimento del sapere.

Gruppo di esperti «Futuro del trattamento e della sicurezza dei dati»: il gruppo di esperti è stato costituito dal DFF in seguito all'adozione della mozione Rechsteiner 13.3841 «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati». Non è improbabile che i lavori del gruppo portino a ulteriori riforme nel settore della protezione dei dati, anche se, visto che occorre tenere conto del contesto europeo, il margine di manovra del legislatore svizzero è limitato. Se dovessero rivelarsi necessarie, queste ulteriori riforme potrebbero essere prese in considerazione in una prossima tappa. Non è d'altronde escluso che la necessità di riforme riguardi settori diversi dalla protezione dei dati (p. es. il Codice delle obbligazioni[19] [CO], il diritto sulla proprietà intellettuale, la sicurezza degli oggetti, il diritto in materia di concorrenza). I lavori della commissione saranno probabilmente conclusi non prima della metà del 2018.

Giovani e media – protezione dell'infanzia e della gioventù dai rischi dei media digitali: il 13 maggio 2015, adottando il rapporto «Giovani e media. Futura impostazione della protezione dell'infanzia e della gioventù dai rischi dei media in Svizzera», il nostro Consiglio ha deciso di proseguire le attività avviate nel contesto del

16 www.newsd.admin.ch/newsd/message/attachments/48043.pdf
17 www.isb.admin.ch/isb/it/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html.
18 www.nfp75.ch/fr.
19 RS **210**

programma nazionale «Giovani e media»[20], realizzato dal 2011 al 2015. Il DFI (Ufficio federale delle assicurazioni sociali, UFAS) è pertanto incaricato di attuare e coordinare le attività educative e di regolamentazione. La protezione dei dati fa parte dei temi affrontati nel contesto delle attività educative.

Rapporto del Consiglio federale dell'11 gennaio 2017[21] *sulle condizioni generali per un'economia digitale*: il rapporto affronta diversi ambiti di fondamentale importanza per l'economia digitale. Sono stati esaminati cinque ambiti: mercato del lavoro, ricerca e sviluppo, sharing economy, finanza digitale e politica in materia di concorrenza. Il nostro Consiglio ha incaricato la Segreteria di Stato dell'economia (SECO) di analizzare l'adeguatezza al mondo digitale delle leggi esistenti ed economicamente importanti e di valutare la necessità di una loro revisione, fondandosi su un sondaggio presso le associazioni interessate, le parti sociali e varie imprese selezionate («test digitale»). Si tratta soprattutto di individuare le regolamentazioni che a seguito dell'evoluzione tecnologia hanno in gran parte perso la loro utilità.

Programmi nazionali di ricerca (PNR) sul tema «Evoluzione digitale dell'economia e della società»[22]: il 5 luglio 2017 il nostro Consiglio ha incaricato il DEFR, ovvero la Segreteria di Stato per la formazione, la ricerca e l'innovazione, di valutare se avviare una serie di PNF sul tema «Evoluzione digitale dell'economia e della società». Si tratta di esaminare, d'intesa con i Cantoni, gli effetti della digitalizzazione sul settore della formazione e di analizzare se occorra colmare eventuali lacune nella ricerca delle scuole universitarie, al fine di superare le sfide della trasformazione digitale. Un'attenzione particolare va rivolta all'ampiezza che le capacità di ricerca in Svizzera devono raggiungere per garantire il trasferimento delle conoscenze e delle tecnologie all'economia e la gestione sicura delle infrastrutture critiche.

1.1.5 Iniziative e interventi parlamentari

Negli ultimi anni, la protezione dei dati è stata oggetto di numerose iniziative e interventi parlamentari. Qui appresso si menzionano soltanto quelli più importanti.

– Iniziativa parlamentare Vischer 14.413 «Per il diritto fondamentale all'autodeterminazione informativa». Secondo l'autore, l'articolo 13 capoverso 2 della Costituzione federale[23] (Cost.) protegge solo «da un uso abusivo dei dati personali». Ne risulterebbe che l'onere di provare l'uso abusivo incombe al cittadino e non allo Stato o al fornitore di accesso a Internet. L'iniziativa chiede pertanto di modificare l'articolo 13 capoverso 2 Cost. affinché la protezione dei dati personali si trasformi da protezione da un uso abusivo dei dati a diritto fondamentale all'autodeterminazione informativa. La Commissione delle istituzioni politiche del Consiglio nazionale ha approvato l'iniziativa il 29 agosto 2014, quella del Consiglio degli Stati il 20 agosto 2015.

20 www.giovaniemedia.ch/it/home.html
21 www.seco.admin.ch/seco/it/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html
22 Cfr. www.sbfi.admin.ch/sbfi/de/home/themen/forschung-und-innovation-in-der-schweiz/foerderinstrumente/nationale-forschungsprogramme-nfp.html.
23 RS **101**

– Iniziativa parlamentare Derder 14.434 «Proteggere l'identità digitale dei cittadini». L'iniziativa prevede di modificare l'articolo 13 Cost. come segue: «Ognuno ha diritto al rispetto della sua vita privata e familiare, della sua abitazione, della sua corrispondenza epistolare, delle sue relazioni via posta e telecomunicazioni e dei dati che lo concernono» (cpv. 1) e «Tali dati sono di proprietà della persona in questione, la quale ha diritto d'essere protetta da un loro impiego abusivo» (cpv. 2). La Commissione delle istituzioni politiche del Consiglio nazionale ha approvato l'iniziativa il 16 gennaio 2015, quella del Consiglio degli Stati il 20 agosto 2015.

– Postulato Hodgers 10.3383 «Adeguare la legge sulla protezione dei dati alle nuove tecnologie». L'intervento parlamentare, adottato dal Consiglio nazionale il 1° ottobre 2010, chiede di verificare la possibilità di rafforzare la protezione dei dati e il diritto alla protezione della vita privata modificando la LPD per adeguarla alle nuove tecnologie. Il nostro Consiglio ha parzialmente adempito il postulato con il rapporto del 9 dicembre 2011[24] concernente la valutazione della legge federale sulla protezione dei dati.

– Postulato Graber 10.3651 «Attacchi alla sfera privata e minacce indirette alle libertà individuali». Il 17 dicembre 2010, il Consiglio nazionale ha adottato l'intervento. L'autore chiede al nostro Consiglio di elaborare un rapporto sui rischi che presentano le tecnologie di sorveglianza e di raccolta di informazioni per la sfera privata, sui limiti che intende imporre per tutelare la sfera privata, definendo, se del caso, un nocciolo duro e inviolabile della sfera privata, e sull'opportunità di rafforzare la legislazione a tutela della sfera privata e dei dati personali. Il nostro Consiglio ha parzialmente adempito il postulato con il rapporto del 9 dicembre 2011 concernente la valutazione della legge federale sulla protezione dei dati.

– Postulato Schwaab 12.3152 «Diritto all'oblio in Internet». Il 15 giugno 2012, il Consiglio nazionale ha adottato l'intervento che incarica il nostro Consiglio di valutare la possibilità di sancire o precisare nella legislazione un diritto all'«oblio in Internet» e di esaminare come facilitarne l'uso da parte dei consumatori.

– Mozione Rechsteiner 13.3841 «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati». La mozione chiede di istituire una commissione interdisciplinare di esperti per garantire al meglio il futuro del trattamento e della sicurezza dei dati. Il Consiglio degli Stati e il Consiglio nazionale hanno adottato l'intervento rispettivamente il 3 dicembre 2013 e il 13 marzo 2014. I relativi lavori, affidati al DFF, oltrepassano il contesto del presente disegno (cfr. n. 1.1.4), che ciononostante prevede determinate misure tese ad adempire la mozione.

– Postulato Recordon 13.3989 «Violazioni della personalità riconducibili al progresso delle tecnologie dell'informazione e della comunicazione». L'11 dicembre 2013 il Consiglio degli Stati ha adottato il postulato, che incarica il nostro Consiglio di stilare un rapporto sui rischi per i diritti della personalità

24 FF **2012** 227, in particolare pag. 231.

insiti nel progresso delle tecnologie dell'informazione e della comunicazione e sulle soluzioni ipotizzabili.

– Mozione Comte 14.3288 «Rendere l'usurpazione d'identità un reato penale a sé stante». L'intervento è stato adottato dalle Camere federali il 12 giugno e il 24 novembre 2014 e incarica il nostro Consiglio di presentare una modifica del diritto penale che renda l'usurpazione d'identità un reato a sé stante.

– Postulato Derder 14.3655 «Definire la nostra identità digitale e identificare le soluzioni per proteggerla». Il 26 settembre 2014 il Consiglio nazionale ha adottato l'intervento. L'autore incarica il nostro Consiglio di redigere un rapporto che permetta di definire l'identità digitale dei cittadini integrandola nella loro personalità giuridica attuale, tratti le tracce digitali dei dati personali potenzialmente pubblici e indichi le minacce alla nostra sfera privata e le modalità di proteggerla dalle imprese o dai servizi d'informazione svizzeri o esteri.

– Postulato Schwaab 14.3739 «Control by design. Potenziare i diritti di proprietà per impedire le connessioni indesiderate». Il 12 dicembre 2014, il Consiglio nazionale ha adottato l'intervento che incarica il nostro Consiglio di valutare l'introduzione nella legislazione di un «controllo fin dalla progettazione» (control by design), affinché il proprietario o il possessore di un oggetto abbia il diritto di opporsi alla connessione del suddetto oggetto a qualsivoglia rete. L'intervento invita in particolare il nostro Consiglio a valutare se occorra adeguare la legislazione relativa al trasferimento della proprietà e alla protezione dei dati.

– Postulato Schwaab 14.3782 «Regole per la ‹morte digitale›». L'intervento, accolto dal Consiglio nazionale il 12 dicembre 2014, incarica il nostro Consiglio di valutare l'opportunità di integrare il diritto successorio al fine di disciplinare i diritti degli eredi ai dati personali e agli accessi digitali del defunto nonché le conseguenze del suo decesso sulla sua esistenza virtuale.

– Postulato del Gruppo liberale radicale 14.4137 «Registrazioni video di privati. Migliorare la tutela della sfera privata». Il postulato chiede al nostro Consiglio di redigere un rapporto incentrato sui rischi dell'utilizzo di videocamere private installate nei droni e negli occhiali connessi. È stato adottato dal Consiglio nazionale il 20 marzo 2015.

– Postulato Comte 14.4284 «Registrazioni video di privati. Migliorare la tutela della sfera privata». L'intervento, adottato dal Consiglio degli Stati il 19 marzo 2015, ha lo stesso tenore del postulato del Gruppo liberale radicale 14.4137.

– Postulato Derder 15.4045 «Diritto all'utilizzo dei dati personali. Diritto alla copia». Il postulato incarica il nostro Consiglio di esaminare in che misura i privati e l'economia potrebbero approfittare dell'ulteriore utilizzo dei loro dati personali e disporre di un diritto di ottenere una copia di tali dati. Il Consiglio nazionale ha adottato l'intervento il 18 dicembre 2015.

- Postulato Béglé 16.3383 «Dati digitali. Informare le persone lese in caso di pirateria». Il postulato incarica il nostro Consiglio di valutare l'opportunità di obbligare gli organismi vittima di pirateria informatica riguardante dati digitali sotto la loro responsabilità di avvertire le persone lese affinché possano agire per limitare i danni. Il 30 settembre 2016 il Consiglio nazionale ha approvato l'intervento.
- Postulato Béglé 16.3384 «Dati medici digitali. Garantire una raccolta protetta, trasparente e mirata nella revisione della legge federale sulla protezione dei dati». Il postulato incarica il nostro Consiglio di valutare l'opportunità di integrare nella revisione della LPD i seguenti elementi al fine di offrire la massima garanzia per i dati medici: disposizioni severe e uniformi per tutti sulla sicurezza dello stoccaggio, della trasmissione e dell'accesso ai dati; introduzione del principio del «consenso vero e proprio» del paziente e dei principi «privacy by default» e «privacy by design»; sensibilizzazione delle persone interessate in merito ai rischi della trasmissione di determinati dati personali. Il 30 settembre 2016 il Consiglio nazionale ha accolto il postulato.
- Postulato Béglé 16.3386 «Riappropriazione dei dati personali. Favorire l'autodeterminazione informatica». Il postulato incarica il nostro Consiglio di vagliare il miglior mezzo per favorire la riappropriazione dei dati personali da parte delle persone interessate. Il Consiglio nazionale ha adottato l'intervento il 30 settembre 2016.
- Postulato Schwaab 16.3682 «Inquadrare le prassi delle società che forniscono dati sulla solvibilità». Il postulato chiede al nostro Consiglio di esaminare la necessità di migliorare l'inquadramento delle società che forniscono dati sulla solvibilità, in particolare introducendo limiti chiari quanto ai metodi utilizzabili per ottenere informazioni sulla solvibilità dei privati e delle imprese. Seguendo la proposta del nostro Collegio, il 16 dicembre 2016 il Consiglio nazionale ha adottato il postulato.
- Iniziativa parlamentare 16.409 Leutenegger Oberholzer «Procedura di nomina dell'Incaricato della protezione dei dati e della trasparenza». L'iniziativa chiede che l'Incaricato sia eletto dall'Assemblea federale. Il 20 gennaio 2017, la Commissione delle istituzioni politiche del Consiglio nazionale ha deciso di dare seguito all'iniziativa. Il 31 marzo 2017, quella del Consiglio degli Stati ha deciso di aderire a tale decisione.

1.2 Situazione internazionale

1.2.1 Osservazioni generali sulla protezione della sfera privata su scala internazionale

Il 16 luglio 2014 l'allora Alto commissario delle Nazioni unite per i diritti umani, Navi Pillay, ha presentato il suo rapporto sulla tutela della sfera privata nell'era digitale (A/HRC/27/37; cfr. n. 1.2.4). Il rapporto fornisce una panoramica concisa che mette in relazione la protezione dei dati nell'era digitale con i diritti dell'uomo e stila un bilancio sconfortante sull'attuale situazione giuridica.

A livello internazionale è vieppiù riconosciuto che qualsiasi trattamento di dati personali può in linea di massima tangere la sfera privata e altri diritti dell'uomo. Per proteggere efficacemente la sfera privata vanno create norme che giustifichino le ingerenze. I diritti applicabili al di fuori di Internet devono valere anche in rete. Oltre al diritto alla sfera privata, che è garantito dall'articolo 13 della Costituzione federale, ma anche da diversi trattati internazionali vincolanti (Convenzione del 28 gennaio 1981[25] per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale [Convenzione STE 108], art. 8 della Convenzione del 4 novembre 1950[26] per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali [CEDU], art. 17 del Patto internazionale del 16 dicembre 1966[27] relativo ai diritti civili e politici [Patto II dell'ONU]), il trattamento di dati può toccare anche altri diritti fondamentali e umani, in particolare la libertà d'opinione e d'informazione (art. 16 Cost., art. 10 CEDU, art. 19 Patto II dell'ONU), la libertà di riunione (art. 22 Cost., art. 11 CEDU, art. 21 Patto II dell'ONU) e d'associazione (art. 23 e 28 Cost., art. 11 CEDU, art. 22 Patto II dell'ONU).

La limitazione della protezione della sfera privata deve in particolare rispettare i requisiti posti dall'articolo 8 capoverso 2 CEDU a un'ingerenza lecita (base legale, ingerenza giustificata da uno dei motivi esplicitamente menzionati nell'art. 8 cpv. 2 e principio della proporzionalità). Pur concedendo regolarmente agli Stati parte un ampio margine di manovra in riferimento alla legittimità delle finalità perseguite[28], la Corte europea dei diritti dell'uomo (Corte EDU) pone requisiti molto elevati alla forma della base legale: la legge che permette l'ingerenza deve essere sufficientemente precisa, contenere misure preventive contro l'uso abusivo dei dati e concedere alle persone interessate la possibilità di ricevere informazioni sui dati che le riguardano. La legge deve inoltre disciplinare chi può trattare i dati e a quale scopo, la durata di conservazione dei dati e le modalità di controllo del rispetto delle disposizioni. Nel caso di dati degni di particolare protezione i requisiti sono più elevati.

1.2.2 Unione europea

1.2.2.1 Normativa pertinente

Negli ultimi decenni l'Unione europea ha adottato vari atti normativi tesi a proteggere i dati personali. L'atto più importante è la direttiva 95/46/CE del 24 ottobre 1995[29] relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (direttiva 95/46/CE). Tale direttiva è stata completata dalla decisione quadro 2008/977/GAI del 27 novembre 2008[30] sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (decisione quadro 2008/977/GAI).

25 RS **0.235.1**
26 RS **0.101**
27 RS **0.103.2**
28 Cfr. ad esempio Corte EDU 59842/00 (Vetter conto Francia) del 31 ago. 2005; Corte EDU 44647/98 (Peck contro Regno Unito) del 28 gen. 2003; Corte EDU 27798/95 (Amann contro Svizzera) del 16 feb. 2000.
29 GU L 281 del 23.11.1995, pag. 31.
30 GU L 350 del 30.12.2008, pag. 60.

Nell'ambito del programma di Stoccolma[31], l'Unione europea ha dichiarato di voler disporre di una nuova legislazione uniforme sulla protezione dei dati, in particolare al fine di garantire il diritto fondamentale alla protezione dei dati personali, permettere lo sviluppo dell'economia digitale e migliorare la lotta alla criminalità e al terrorismo. Il Consiglio d'Europa ha quindi invitato la Commissione europea a verificare l'efficacia della direttiva 95/46/CE e della decisione quadro 2008/977/GAI e di presentargli, se necessario, nuove proposte sulla protezione dei dati. Nella comunicazione del 4 novembre 2010[32] intitolata «Un approccio globale alla protezione dei dati personali nell'Unione europea», la Commissione europea ha concluso che l'Unione europeo aveva bisogno di una politica più globale e più coerente riguardo al diritto fondamentale alla protezione dei dati personali.

Il 27 aprile 2016 il Parlamento europeo e il Consiglio dell'Unione europea hanno adottato una riforma della legislazione sulla protezione dei dati comprendente due atti normativi. Si tratta, da una parte, del regolamento (UE) 2016/679, che abroga la direttiva 95/46/CE (cfr. n. 4), e, dall'altra, della direttiva (UE) 2016/680/CE, che abroga la decisione quadro 2008/977/GAI del Consiglio (cfr. n. 2).

Per la Svizzera, la direttiva (UE) 2016/680 fa parte dell'acquis di Schengen. In virtù dell'Accordo di associazione a Schengen, il nostro Paese deve pertanto attuare la direttiva. Non è invece tenuto a recepire il regolamento (UE) 2016/679, poiché secondo l'Unione europea non si tratta di uno sviluppo dell'acquis di Schengen.

Nell'ambito della strategia relativa al mercato interno digitale in Europa, il 10 gennaio 2017 la Commissione europea ha proposto un progetto di regolamento sulla vita privata e la comunicazione elettronica che dovrà sostituire la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002[33], relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni. Il regolamento costituirebbe una legge speciale rispetto al regolamento (UE) 2016/679, poiché completa e precisa quest'ultimo in riferimento alla comunicazione elettronica[34]. Non si tratta di uno sviluppo dell'acquis di Schengen.

1.2.2.2 Decisione di adeguatezza

Nei settori che non riguardano la cooperazione istituita da Schengen, la Svizzera è considerata uno Stato terzo. Lo scambio di dati tra uno Stato terzo e gli Stati membri dell'Unione europea può essere effettuato soltanto se lo Stato terzo garantisce un livello di protezione adeguato ai sensi della direttiva 95/46/CE. Tale livello di protezione è verificato periodicamente dalla Commissione europea e constatato in una decisione di adeguatezza. Tale decisione può essere revocata in qualsiasi momento.

31 GU C 115, del 4.5.2010, pag. 1.
32 COM (2010) 609 final.
33 ABl. L 201, 31.7.2002 S. 37 -47
34 N. 1.2 dell'«Explanatory memorandum» relativo al progetto.

Nella decisione di adeguatezza del 26 luglio 2000 la Commissione europea ha confermato che la Svizzera dispone di una protezione adeguata dei dati[35]. Tale decisione si fonda tuttavia sul livello di protezione definito dalla direttiva 95/46/CE.

Con missiva del 25 gennaio 2017, la Commissione europea ha informato la Missione della Svizzera presso l'Unione europea che, in seguito a una decisione della Corte di giustizia dell'Unione europea del 6 ottobre 2015 (causa «Schrems»), essa è tenuta a verificare periodicamente il livello di protezione dei dati garantito dagli Stati terzi che beneficiano di una decisione di adeguatezza. La Commissione europea ha pertanto chiesto alla Svizzera di presentarle un rapporto che illustri la situazione legale relativa alla protezione dei dati e le principali modifiche legislative dopo il 2000. Tale rapporto sarà trasmesso alla Commissione europea entro la fine del 2017.

In futuro, l'esame della legislazione svizzera sarà effettuato alla luce dei requisiti del regolamento (UE) 2016/679. Affinché la decisione di adeguatezza della protezione dei dati rimanga valida anche in futuro o, in caso di revoca, possa essere emanata nuovamente, è di fondamentale importanza, in particolare per l'economia, che la Svizzera disponga di una legislazione che garantisce una protezione conforme ai requisiti del suddetto regolamento.

1.2.2.3 Raccomandazioni in relazione con gli accordi di Schengen

Con l'associazione a Schengen e a Dublino, la Svizzera si è impegnata a trattare i dati personali, nel quadro della cooperazione instaurata dall'accordo, in modo conforme alla normativa comunitaria applicabile alla protezione dei dati, in particolare la direttiva 95/46/CE e la decisione quadro 2008/977/GAI.

Nell'ambito della valutazione Schengen, l'Unione europea verifica periodicamente se gli Stati associati, e quindi anche la Svizzera, rispettino tale impegno. L'ultima valutazione Schengen della Svizzera si è svolta nel primo semestre del 2014.

L'11 settembre 2014 il Consiglio dell'Unione europea ha adottato il rapporto del comitato di valutazione sulla protezione dei dati in Svizzera nell'ambito della cooperazione di Schengen. Secondo tale rapporto, la legislazione svizzera sulla protezione dei dati è conforme ai requisiti dell'acquis di Schengen. Il rapporto di valutazione esorta tuttavia la Svizzera a rafforzare le competenze dell'Incaricato, attribuendogli poteri decisionali. Sarebbe inoltre opportuno potenziare le sue competenze sanzionatorie. In occasione della prossima valutazione, prevista nel 2018, la Svizzera dovrà rendere conto del modo in cui ha messo in atto le raccomandazioni degli esperti.

Il D-LPD tiene conto delle raccomandazioni del Consiglio dell'Unione europea in quanto conferisce all'Incaricato la competenza di emanare decisioni (cfr. art. 44 e 45 D-LPD). Per contro, riteniamo che non sia opportuno conferire all'Incaricato la competenza di pronunciare sanzioni amministrative nei confronti degli organi federali, poiché tale possibilità, prevista in altri Paesi, non è conforme alla tradizione

35 Decisione della Commissione, del 26 lug. 2000, riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE, GU L 215 del 25.8.2000, pag. 1.

giuridica svizzera. Siamo inoltre del parere che la possibilità dell'Incaricato di bloccare o sospendere il trattamento da parte di un organo federale e l'inasprimento delle disposizioni penali della LPD siano misure sufficientemente efficaci.

1.2.3 Consiglio d'Europa (Convenzione STE 108)

Il 28 gennaio 1981 il Consiglio d'Europa ha adottato il primo trattato internazionale sulla protezione dei dati: la Convenzione STE 108, ratificata dalla Svizzera il 2 ottobre 1997. La Convenzione è stata completata dal Protocollo aggiuntivo dell'8 novembre 2001[36] alla Convenzione STE 108 concernente le autorità di controllo e i flussi internazionali di dati (STE 181, qui appresso «Protocollo aggiuntivo»), che la Svizzera ha ratificato il 20 dicembre 2007. Nel frattempo, la Convenzione è stata ratificata anche da Stati che non sono membri del Consiglio d'Europa (cfr. n. 3.1).

Nel 2011 il Consiglio d'Europa ha avviato un processo di modernizzazione della Convenzione STE 108 e del suo Protocollo aggiuntivo teso a consentire di affrontare meglio le sfide che la globalizzazione, l'evoluzione tecnologica e l'aumento del flusso internazionale di dati rappresentano per la protezione della sfera privata e dei diritti fondamentali delle persone interessate. Il Comitato consultivo della Convenzione STE 108, presieduto dalla Svizzera, ha elaborato un progetto di modernizzazione della Convenzione. I lavori del comitato ad hoc (CAHDATA) istituito dal Comitato dei Ministri si sono conclusi nel giugno 2016. Il protocollo di emendamento della Convenzione STE 108 deve essere adottato dal Comitato dei Ministri (cfr. n. 3.2). Il presente messaggio si basa sul progetto di modernizzazione nella versione di settembre 2016[37]), che non dovrebbe più subire modifiche sostanziali.

Il contenuto del P-STE 108 è molto simile a quello della direttiva (UE) 2016/680 e del regolamento (UE) 2016/679, ma è meno dettagliato e meno denso. La Commissione europea, che durante i negoziati ha rappresentato gli Stati membri dell'Unione europea, ha provveduto affinché il testo del P-STE 108 sia conforme al nuovo diritto dell'Unione europea.

1.2.4 Nazioni Unite

In seguito al caso Snowden, il diritto alla sfera privata è diventato un tema prioritario per varie istituzioni dell'ONU. Nel dicembre 2013 l'Assemblea generale ha adottato una risoluzione[38] che invita ogni Stato a rivedere la propria legislazione al fine di tutelare il diritto alla vita privata e che chiede all'Alto commissariato delle Nazioni unite per i diritti umani (OHCHR) di redigere un rapporto relativo alla promozione del diritto alla vita privata nel contesto della sorveglianza e dell'intercettazione di comunicazioni digitali nonché della raccolta, anche su grande scala, di dati sul

36 RS **0.235.11**
37 Il testo francese è reperibile all'indirizzo seguente: https://rm.coe.int/16806b6f7b
38 Risoluzione 68/167 del 18 dic. 2013 disponibile in francese al seguente indirizzo: www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167

territorio nazionale e all'estero. Il rapporto è stato presentato in luglio 2014[39]. Inoltre, in marzo 2015 il Consiglio dei diritti umani dell'ONU ha istituito, per la durata di tre anni, un relatore speciale sul diritto alla vita privata. Il relatore ha il compito di analizzare le sfide che la rapidissima evoluzione tecnologica e le risultanti nuove possibilità di sorveglianza della comunicazione privata comportano per la tutela del diritto alla sfera privata. La Svizzera ha sostenuto queste due iniziative partecipandovi attivamente.

Finora il relatore speciale ha presentato due rapporti, il primo l'8 marzo 2016[40] e il secondo il 27 febbraio 2017[41].

Nel primo rapporto il relatore speciale presenta una panoramica della situazione relativa alla protezione della vita privata all'inizio del 2016 e un piano d'azione per i primi tre anni del suo mandato. Sottolinea in particolare che l'assenza di una definizione universale vincolante della nozione di sfera privata costituisce uno degli ostacoli principali alla protezione esaustiva di quest'ultima. Constata inoltre che mentre originariamente vi era il timore di un uso abusivo di dati personali da parte degli Stati, ora tale timore vige nei confronti delle imprese ed è quindi necessario instaurare un dialogo su scala internazionale sul modo in cui le imprese raccolgono e trattano i dati personali e li trasmettono a servizi statali[42]. Inoltre, il relatore speciale constata che i consumatori sono sempre più consapevoli dei rischi per il diritto alla sfera privata, come testimonia la rapida crescita del mercato di prodotti e servizi tesi a tutelare la sfera privata[43]. Infine, riconosce l'importanza del rapido sviluppo di prodotti protetti sotto il profilo biometrico e sottolinea l'intenzione di collaborare con la ricerca, le autorità di perseguimento penale, i servizi d'informazione e la società civile per individuare adeguati meccanismi di protezione materiali e giuridici[44].

Il secondo rapporto si concentra sulle misure di sorveglianza statale su scala nazionale e internazionale. Descrive gli sviluppi e le tendenze più recenti e illustra alcune possibilità per assicurare il controllo della sorveglianza. Propone in particolare di elaborare uno strumento internazionale per la protezione della sfera privata nel ciberspazio. Secondo il relatore speciale le sue raccomandazioni completano gli strumenti in vigore (p. es. la Convenzione del Consiglio d'Europa del 13 novembre 2001[45] sulla cibercriminalità) e le diverse iniziative su scala internazionale[46].

La Svizzera segue questi sviluppi con attenzione.

39 OHCHR «Le droit à la vie privée à l'ère du numérique», 2014.
40 A/HRC/31/64
41 A/HRC/34/60
42 A/HRC/31/64, n. 9 e 46 seg.
43 A/HRC/31/64, n. 50.
44 A/HRC/31/64, n. 15 e 46(e).
45 RS **0.311.43**, ratificata dalla Svizzera il 21. set. 2011.
46 Cfr. p. es. il «Mapping-project»; www.mappingtheinternet.eu/

1.2.5 Linee guida OCSE sulla protezione dei dati e il flusso internazionale di dati personali

Conformemente all'impostazione economica dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), le sue linee guida del 1980 sulla protezione dei dati[47], sottoposte a revisione nel 2013, mirano ad armonizzare i diversi livelli nazionali della protezione dei dati. Salvaguardando i diritti dell'uomo, le direttive intendono istituire una base per il disciplinamento dello scambio internazionale di dati, al fine di evitare ostacoli al commercio e garantire a livello globale uno scambio di dati e un flusso di informazioni liberi. Pur avendo solo carattere di raccomandazione e pur non essendo vincolanti, le direttive hanno avuto un influsso durevole sull'evoluzione del diritto in materia di protezione di dati a livello internazionale e nazionale.

Le linee guida relative alla protezione dei dati si applicano a tutti i dati del settore pubblico e privato che in base al tipo di trattamento, alla loro natura e alle circostanze in cui sono usati rappresentano un rischio per la sfera privata e altre libertà individuali. Con otto principi giuridici fondamentali della protezione dei dati (ossia limitazione della raccolta dei dati, qualità dei dati, finalità, limitazione dell'uso, sicurezza dei dati, trasparenza, diritto di partecipazione delle persone i cui dati sono trattati e responsabilità)[48], intesi come standard minimi, s'intende creare un equilibrio tra i due concetti contrapposti della sfera privata e del libero flusso di informazioni. Le linee guida riviste sono entrate in vigore nel luglio 2013 e, pur mantenendo i suddetti otto principi fondamentali, contengono diverse precisazioni ed estensioni: tra le altre cose sono definiti in modo più preciso i criteri per la comunicazione di dati all'estero ed è intensificata la cooperazione internazionale[49]. Le linee guida riviste prevedono esplicitamente che, a prescindere dal luogo in cui si trovano i dati, il titolare del trattamento è sempre responsabile dei dati sotto il suo controllo[50] (OCSE; Linee guida 2013, principio 16). Infine, il trasferimento internazionale di dati tra uno Stato membro e un altro Stato non va limitato se quest'ultimo rispetta le linee direttive o se sussistono garanzie sufficienti che assicurino il livello di protezione richiesto dalle linee direttive.

1.3 Obiettivi del disegno

Il presente disegno dà seguito al mandato conferito dal nostro Consiglio al DFGP di preparare un avamprogetto di legge che tenga conto delle conclusioni del rapporto del 29 ottobre 2014 «Esquisse d'acte normatif relative à la révision de la sur

47 Linee guida OCSE relative alla protezione dei dati e al flusso internazionale di dati personali, 1980, consultabili all'indirizzo: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm;
Linee guida OCSE relative alla protezione dei dati e al flusso internazionale di dati personali, 2013, consultabili all'indirizzo: www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

48 OCSE, Linee guida sulla protezione dei dati 1980, principi 6–14; OCSE, Privacy Framework 2013, pag. 22 e pag. 47 seg.

49 OCSE, Linee guida sulla protezione dei dati 2013, principi 16–18, 19 lett. g e 20–23.

50 OCSE; Linee guida 2013, principio 16.

loi la protection des données [Bozza di atto normativo relativo alla revisione della legge sulla protezione dei dati]» come pure delle riforme del Consiglio d'Europa e dell'Unione europea. L'adozione del messaggio figura anche tra gli obiettivi del nostro Consiglio del 2017 e nel programma di legislatura 2015–2019 (n. 12.1). Attua numerosi interventi parlamentari elencati al n. 1.1.4.

Il disegno di legge persegue diversi obiettivi che si completano a vicenda.

Innanzitutto il disegno intende adeguare il diritto svizzero alla rapida evoluzione tecnologica, che si ripercuote fortemente sulla protezione dei dati. Da una parte si tratta di permettere alle persone interessate di riottenere il controllo dei loro dati che, con l'evoluzione della società digitale, sono oggetto di raccolte massicce («Big Data») e il cui trattamento è sempre meno trasparente (p. es. profilazioni basate su algoritmi). Dall'altra, occorre anche responsabilizzare i titolari dei trattamenti, che devono tenere conto delle disposizioni sulla protezione dei dati già al momento della pianificazione di nuovi trattamenti, prevedendo, per impostazione predefinita, la soluzione standard più favorevole alla protezione dei dati. Infine, si tratta di preservare e rafforzare la competitività della Svizzera, creando condizioni che facilitino il flusso internazionale di dati e consolidino l'attrattività del nostro Paese per nuove attività legate alla società digitale. A tal fine è necessario un livello di protezione elevato, riconosciuto su scala internazionale.

Ulteriori obiettivi della presente revisione si evincono dall'evoluzione del diritto dell'Unione europea, di fondamentale importanza nel settore della protezione dei dati, poiché lo scambio transfrontaliero di dati avviene quotidianamente. La direttiva (UE) 2016/680 costituisce uno sviluppo dell'acquis di Schengen e la Svizzera ha l'obbligo di adeguarvi la sua legislazione. Il presente disegno deve altresì attuare le raccomandazioni che l'Unione europea ha emanato nel 2014 in seguito alla valutazione della Svizzera nel quadro dell'accordo di associazione a Schengen. Gli esperti europei hanno infatti raccomandato alla Svizzera di conferire competenze decisionali all'Incaricato (cfr. n. 1.2.2.3). Inoltre è indispensabile che la Svizzera usufruisca anche in futuro di una decisione di adeguatezza della Commissione europea con cui questa riconosce una protezione adeguata dei dati (cfr. n. 1.2.2.2). A tal fine la legislazione svizzera va adeguata al regolamento (UE) 2016/679, senza tuttavia attuarlo completamente.

Infine, il disegno intende rendere compatibile la legislazione svizzera con il P-STE 108, poiché è nell'interesse del nostro Paese ratificare la Convenzione riveduta non appena sarà aperta alla firma degli Stati parte. Ciò vale anche in relazione alla decisione di adeguatezza della Commissione europea, poiché la firma della Convenzione rivista è di fondamentale importanza per tale decisione. Visto che il testo della Convenzione è in linea di massima definitivo e che il suo contenuto, seppur meno dettagliato, corrisponde in gran parte a quelli della direttiva (UE) 2016/680 e del regolamento (UE) 2016/679, il nostro Consiglio ha deciso di anticipare le relative spiegazioni integrandole nel presente messaggio.

Riassumendo, con la realizzazione dei suddetti obiettivi s'intende da una parte adeguare la legislazione svizzera all'attuale evoluzione tecnologica e, dall'altra, garantire che la Svizzera rispetti gli impegni risultanti dall'Accordo di associazione a Schengen e possa ratificare la Convenzione STE 108 rivista. Infine occorre assicura-

re che la Commissione europea attesti in una decisione di adeguatezza che il nostro Paese fa parte degli Stati terzi con una protezione adeguata dei dati. Tale decisione è di notevole importanza in particolare per l'economia svizzera.

Il presente disegno implica pertanto la revisione totale della LPD (compresa la revisione di altre norme inerenti alla protezione dei dati) e la revisione parziale delle leggi settoriali applicabili alla cooperazione giudiziaria e di polizia instaurata da Schengen.

1.4 Presentazione del D-LPD

1.4.1 Punti essenziali della revisione

La revisione totale si basa su sette principi che fungono da elementi fondamentali per le singole modifiche.

Un primo elemento fondamentale della revisione è l'approccio basato sui rischi. Il disegno di revisione si basa in modo coerente sui rischi potenziali per le persone i cui dati sono trattati, poiché i rischi per la sfera privata di queste ultime dipendono in gran parte dalle attività dei vari titolari e responsabili del trattamento. Pertanto i titolari le cui attività presentano un rischio maggiore (p. es. le imprese la cui attività principale è il trattamento di dati) sottostanno a obblighi più severi rispetto a quelli le cui attività presentano rischi minori (p. es. trattamento di dati che si limita a un catalogo di clienti senza dati degni di particolare protezione).

Un secondo elemento è il carattere tecnologicamente neutro della revisione. Alla stregua della legge vigente, anche il D-LPD deve trattare, nei limiti del possibile, allo stesso modo tutte le tecnologie. In tal modo la legge non si preclude allo sviluppo tecnologico e non impedisce innovazioni.

Il terzo elemento fondamentale è la modernizzazione della terminologia, soprattutto per migliorare la compatibilità con il diritto dell'Unione europea. Determinati termini vengono pertanto ripresi dal diritto europeo: «detentore della raccolta di dati» è sostituito da «titolare del trattamento» e «profilo della personalità», che è un termine prettamente svizzero, è sostituito da «profilazione». La nozione di «dati personali degni di particolare protezione» comprende ora anche i dati genetici» e i dati biometrici.

Il quarto elemento fondamentale è il miglioramento della trasmissione transfrontaliera di dati. La normativa applicabile alla comunicazione internazionale di dati viene parzialmente estesa. A causa dell'incertezza giuridica che ne consegue, è abolito il principio secondo cui nessun dato può essere trasmesso all'estero in assenza di una protezione adeguata dei dati. Dati potranno essere trasmessi all'estero se il nostro Consiglio ha constatato, per mezzo di un'ordinanza, che il Paese destinatario o l'organismo internazionale offre un livello di protezione adeguato. In assenza di una tale constatazione, il D-LPD prevede diversi mezzi per garantire una protezione sufficiente dei dati, di modo che resta possibile la comunicazione di dati all'estero.

Un quinto elemento fondamentale della revisione è l'estensione dei diritti delle persone interessate per mezzo di diversi strumenti che permettono loro di controllare meglio i loro dati e decidere in merito all'uso di questi ultimi. Sono in particolare precisate le condizioni per la validità del consenso della persona interessata.

Il sesto elemento fondamentale, teso a precisare gli obblighi dei titolari del trattamento basandoli maggiormente sulla protezione della persona interessata, è strettamente connesso al quinto. Il D-LPD amplia l'obbligo di informare e i titolari sono tenuti a effettuare una valutazione d'impatto sulla protezione dei dati. Accorgimenti tecnici devono garantire l'allestimento di sistemi favorevoli alla protezione dei dati. I nuovi obblighi sono tuttavia compensati da certe agevolazioni. È ad esempio previsto di sopprimere l'obbligo del settore privato di notificare all'Incaricato le collezioni di dati, il che riduce l'onere dei titolari.

Il settimo elemento fondamentale è il potenziamento del controllo. Lo statuto e l'indipendenza dell'Incaricato sono rafforzati. Le sue competenze saranno così paragonabili a quelle delle autorità di controllo all'estero. A differenza della maggior parte dei suoi omologhi europei, non avrà tuttavia il diritto di infliggere sanzioni amministrative; in compenso il D-LPD prevede un inasprimento delle disposizioni penali della legge.

1.4.2 Principali novità

1.4.2.1 Modifica del campo d'applicazione della nuova LPD

Il D-LPD propone di rinunciare alla protezione dei dati delle persone giuridiche; gli atti normativi sulla protezione dei dati dell'Unione europea e del Consiglio d'Europa, come pure la maggior parte degli ordinamenti giuridici stranieri, non prevedono tale protezione. Poiché la portata di quest'ultima è limitata, l'abolizione non dovrebbe avere conseguenze negative, vista in particolare la protezione garantita da altre leggi in settori specifici (protezione della personalità, concorrenza sleale, diritto d'autore). Questa modifica intende facilitare la comunicazione di dati a Stati la cui legislazione non prevede la protezione dei dati delle persone giuridiche.

Per il settore pubblico, l'abrogazione della protezione dei dati delle persone giuridiche avrebbe come conseguenza che le basi legali del diritto federale che autorizzano gli organi federali a trattare dati personali non si applicherebbero al trattamento di dati riguardanti persone giuridiche. L'articolo 5 Cost. esige tuttavia che l'attività dello Stato si fondi sul diritto. Inoltre, anche le persone giuridiche beneficiano della tutela della sfera privata, anche se non sono toccate da tutti gli aspetti tutelati dall'articolo 13 Cost.[51]. Proponiamo pertanto di creare una serie di basi legali nella legge del 21 marzo 1997[52] sull'organizzazione del Governo e dell'Amministrazione (LOGA) che disciplinino il trattamento di dati di persone giuridiche (cfr. n. 9.2.8). Inoltre, una disposizione transitoria di cinque anni intende evitare eventuali lacune giuridiche (cfr. art. 66 D-LPD e il relativo commento nel n. 9.1.11).

51 DTF **137** II 371 consid. 6
52 RS **172.010**

1.4.2.2 Maggiore trasparenza del trattamento di dati e maggiore controllo da parte della persona interessata

Il D-LPD intende migliorare la trasparenza del trattamento dei dati. L'obbligo d'informare in occasione della raccolta di dati è esteso a tutti i trattamenti da parte di titolari privati. Tale obbligo può essere espletato in modo standardizzato e sono inoltre previste eccezioni. Il disegno introduce altresì l'obbligo d'informare in occasione di decisioni automatizzate e il diritto della persona interessata, a determinate condizioni, di far valere il suo punto di vista e di esigere che una persona fisica verifichi la decisione. Il D-LPD amplia inoltre le informazioni che devono essere fornite alla persona interessata che esercita il suo diritto d'accesso.

I diritti della persona interessata sono definiti in modo più chiaro in diversi punti. Tra le altre cose, il D-LPD menziona esplicitamente il diritto alla cancellazione dei dati, cosa che la LPD in vigore fa solo implicitamente. Inoltre, l'accesso alle vie legali è agevolato grazie all'abolizione delle spese processuali nelle procedure contro i titolari del trattamento privati.

Per tenere conto dei risultati della consultazione, i diversi obblighi dei titolari del trattamento e i diritti delle persone interessate sono stati riveduti in modo da non porre requisiti più severi rispetto al diritto europeo.

1.4.2.3 Incoraggiamento all'autoregolazione

La revisione intende incoraggiare l'autoregolazione e un comportamento responsabile dei titolari del trattamento. Visti i risultati della consultazione, il meccanismo è stato riveduto. È ora previsto che le associazioni professionali ed economiche che elaborano codici di condotta possano sottoporle all'Incaricato, che esprime un parere in merito e lo pubblica.

I codici di condotta elaborati dalle cerchie interessate permettono di precisare determinati termini e le modalità di determinati diritti o obblighi.

I codici di condotta non hanno carattere vincolante.

1.4.2.4 Rafforzamento dello statuto dell'Incaricato nonché estensione delle sue competenze e dei suoi obblighi

Lo statuto e l'indipendenza dell'Incaricato sono rafforzati. Il suo mandato può essere rinnovato due volte e l'esercizio di un'attività accessoria è consentito solo a determinate condizioni. Il D-LPD prevede inoltre che, al termine di un'inchiesta aperta d'ufficio o a querela di parte, l'Incaricato può, alla stregua dei suoi omologhi europei, prendere decisioni vincolanti nei confronti dei titolari e dei responsabili del trattamento. Soltanto l'organo federale o la persona privata contro cui è stata aperta l'inchiesta è parte della procedura d'inchiesta.

1.4.2.5 Inasprimento delle sanzioni penali

Le disposizioni penali della LPD sono inasprite sotto vari punti di vista, in particolare per compensare il fatto che l'Incaricato, contrariamente a quasi tutte le autorità europee di sorveglianza della protezione dei dati, non può infliggere sanzioni amministrative. L'importo massimo della multa è aumentato a 250 000 franchi; l'elenco degli atti punibili è adeguato ai nuovi obblighi dei titolari del trattamento; è introdotta una contravvenzione in caso di inosservanza di una decisione dell'Incaricato o di un'autorità di ricorso; è introdotta la possibilità dell'Incaricato di avvalersi, nel procedimento penale, dei diritti dell'accusatore privato; il termine di prescrizione dell'azione penale è prolungato. In caso di contravvenzione commessa nell'azienda, le autorità di perseguimento penale possono rinunciare, a determinate condizioni, a perseguire la persona responsabile e condannare in sua vece l'azienda al pagamento della multa.

Il Codice penale[53] (CP) è completato dall'articolo 179^{decies}, che punisce l'usurpazione d'identità con una pena detentiva fino a un anno o con una pena pecuniaria.

In sede di consultazione, il sistema di sanzioni penali previsto dall'avamprogetto (art. 50 segg.), è stato oggetto di numerose osservazioni. La critica principale riguarda il fatto che le sanzioni contemplano innanzitutto le persone fisiche, mentre, secondo i partecipanti, dovrebbero essere punibili esclusivamente le imprese, per mezzo di sanzioni amministrative pronunciate dall'Incaricato (o da una commissione istituita a tale scopo). I partecipanti temono che siano puniti semplici impiegati senza poteri decisionali. Sono stati inoltre oggetto di numerose critiche anche l'inasprimento delle sanzioni – in particolare l'importo delle multe, la mancanza di precisione di determinate fattispecie e l'elenco dei comportamenti punibili come pure il fatto che sia punita la negligenza.

Il disegno tiene conto di queste critiche riducendo, rispetto all'avamprogetto, l'elenco dei comportamenti punibili e l'importo delle multe, nonché sopprimendo il reato per negligenza.

Abbiamo invece rinunciato alla punibilità diretta delle imprese per mezzo di sanzioni amministrative, poiché non riteniamo opportuno introdurre questo tipo di sanzioni nella LPD. Tali sanzioni, che hanno carattere penale, devono essere limitate a casi eccezionali e a settori in cui la cerchia dei destinatari è limitata (in particolare cartelli, giochi in denaro). In assenza di regole procedurali applicabili specificamente alle suddette sanzioni, si corre il rischio di violare le garanzie procedurali di cui dovrebbero beneficiare coloro che contravvengono alla legge.

Non vi è ragione di temere che possa essere punito qualsiasi collaboratore di un'impresa che tratta dati personali. La maggior parte dei comportamenti punibili riguarda il titolare del trattamento. Se si tratta di una persona giuridica, secondo l'articolo 29 CP, il reato è imputato ai rappresentanti degli organi dell'impresa. Inoltre, nel caso di inosservanza di una decisione dell'Incaricato si rende punibile la persona fisica che in seno all'impresa avrebbe dovuto provvedere affinché sia dato seguito alla decisione dell'Incaricato. Il disegno rafforza inoltra la responsabilità degli organi dirigenti, in quanto dichiara applicabile l'articolo 6 della legge federale del 22 marzo

53 RS **311.0**

1974[54] sul diritto penale amministrativo (DPA; infrazioni commesse nell'azienda). Infine, il D-LPD prevede che l'impresa può essere condannata al pagamento della multa, se quest'ultima non supera i 50 000 franchi e se la determinazione delle persone punibili esige provvedimenti d'inchiesta sproporzionati all'entità della pena.

1.5 Revisione di altre leggi federali

Nelle leggi specifiche applicabili alla cooperazione giudiziaria e di polizia istituita da Schengen, il presente disegno di legge introduce, tra le altre cose, l'obbligo dell'autorità competente di distinguere, per quanto possibile, le diverse categorie di persone interessate nonché i dati fondati sui fatti da quelli fondati su giudizi personali. Anche i diritti delle persone interessate vengono rafforzati. A determinate condizioni, esse possono ad esempio esigere dall'Incaricato la verifica della liceità del trattamento di dati che le riguardano. In caso di trattamento illecito, possono chiedergli di aprire un'inchiesta che può portare a una decisione impugnabile. Infine, il disegno di legge disciplina la protezione dei dati nel caso della comunicazione di dati tra Stati membri di Schengen o tra un'autorità svizzera e uno Stato terzo nel quadro della cooperazione giudiziaria e di polizia instaurate da Schengen.

1.6 Valutazione della soluzione proposta

1.6.1 Valutazione dei risultati della consultazione

Nell'ambito della procedura di consultazione sono pervenuti 222 pareri[55]. Tra i partecipanti invitati hanno espresso un parere tre tribunali della Confederazione, tutti i Cantoni, sette partiti, l'Unione delle città svizzere e undici organizzazioni. Infine, hanno presentato un parere 178 partecipanti facenti parte delle cerchie interessate.

In linea di principio, nessun partecipante si oppone a un nuovo disciplinamento della protezione dei dati e la maggioranza degli interpellati lo approva esplicitamente. Il recepimento della direttiva (UE) 2016/680 e dei requisiti del P-STE 108 non è contestato.

Praticamente tutti i partecipanti hanno formulato osservazioni. Queste riguardano quasi esclusivamente l'AP-LPD e si possono individuare due tendenze fondamentali. Per la maggioranza degli interpellati, l'avamprogetto crea oneri amministrativi troppo elevati e oltrepassa, in alcuni punti, le esigenze europee, soprattutto per quanto riguarda gli obblighi del titolare del trattamento. Alcuni partecipanti ritengono invece che l'avamprogetto non sia sufficientemente severo e dovrebbe contenere provvedimenti supplementari per migliorare la protezione delle persone interessate.

Le principali osservazioni sono illustrate qui di seguito.

54 RS **313.0**

55 Il rapporto sui risultati della consultazione è consultabile sul sito dell'UFG: www.bj.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html.

– Terminologia: l'AP-LPD aggiorna la terminologia legale riprendendo determinati termini del diritto europeo. La soppressione della nozione di profilo della personalità e l'introduzione del termine «profilazione» sono in particolare state bene accolte dalla maggioranza dei partecipanti. La maggior parte ritiene tuttavia che la definizione di «profilazione» sia troppo estesa (art. 3 lett. f AP-LPD) e che occorrerebbe basarsi su quella del diritto europeo.

– Obblighi dei titolari del trattamento e diritti delle persone interessate: i vari obblighi dei titolari del trattamento, in particolare determinati obblighi di notifica all'Incaricato, sono ritenuti troppo burocratici da un gran numero di partecipanti appartenenti al settore dell'economia. Secondo loro, soprattutto le piccole e medie imprese avrebbero difficoltà a rispettare i loro obblighi in materia poiché non dispongono di un servizio giuridico e degli strumenti adeguati. Ciò riguarda soprattutto le comunicazioni all'estero (art. 5 e 6 AP-LPD), gli obblighi d'informazione (art. 13–15 AP-LPD) e l'analisi d'impatto sulla protezione dei dati (art. 16 AP-LPD). In certi punti l'AP-LPD andrebbe per altro, senza motivo, oltre quanto previsto dal diritto europeo.

– Autoregolazione: anche se la volontà del nostro Consiglio d'incoraggiare l'autoregolazione è accolta con favore, il sistema delle raccomandazioni di buona prassi previsto dagli articoli 8 e 9 AP-LPD non convince. Le cerchie dell'economia si oppongono in larga misura al fatto che l'Incaricato possa emanare le raccomandazioni di sua iniziativa, poiché ritengono che tale competenza debba spettare esclusivamente ai rami interessati, che sono maggiormente in grado di considerare le specificità del loro settore. Poiché le sue raccomandazioni sarebbero di fatto rispettate dalle autorità, l'Incaricato avrebbe d'altronde quasi una funzione legislativa, tuttavia senza alcuna legittimazione democratica. È altresì criticata l'approvazione delle raccomandazioni dei rami economici da parte dell'Incaricato, soprattutto per l'assenza di rimedi giuridici. Secondo alcuni partecipanti, se non è obbligatorio, lo strumento delle raccomandazioni di buona prassi non servirà a niente. Altri, infine, ritengono che nella prassi l'Incaricato non avrà le risorse necessarie per elaborare raccomandazioni efficaci e pertanto gli articoli 8 e 9 AP-LPD resteranno lettera morta.

– Un certo numero di partecipanti deplora che l'AP-LPD non menzioni più la facoltà di nominare un consulente per la protezione dei dati. A tale proposito le cerchie economiche chiedono che i titolari del trattamento che ne hanno nominato uno beneficino di determinate agevolazioni amministrative.

– Statuto e nomina dell'Incaricato: alcuni partecipanti contestano la procedura di nomina e chiedono che l'Incaricato sia eletto direttamente e esclusivamente dal Parlamento. Inoltre, alcuni Cantoni chiedono l'indipendenza budgettaria dell'Incaricato. Sono altresì criticati, soprattutto da singoli Cantoni, la limitazione del numero di mandati dell'Incaricato e il divieto di esercitare un'attività accessoria in un Cantone o in un Comune. Infine, numerosi partecipanti appartenenti al settore dell'economia si oppongono alla rielezione tacita dell'Incaricato, per altro già prevista dal diritto in vigore.

– Regime delle sanzioni: le disposizioni penali previste dall'AP-LPD (art. 50 segg.) sono state oggetto di numerose critiche. Molti partecipanti chiedono la rielaborazione totale del sistema previsto. La critica principale riguarda il fatto che le sanzioni penali contemplano innanzitutto le persone fisiche, mentre, secondo i partecipanti, dovrebbero essere di carattere amministrativo e l'Incaricato (o una commissione istituita a tale scopo) dovrebbe poterle infliggere direttamente alle imprese. Si teme che siano puniti semplici impiegati senza potere decisionale.

La maggioranza dei Cantoni sono contrati al mantenimento della competenza cantonale di perseguire e giudicare i reati. Ritengono che il numero notevole di comportamenti incriminati e l'inasprimento delle sanzioni provocheranno un aumento del numero dei procedimenti e renderebbero necessaria l'assunzione di collaboratori specializzati.

Anche l'inasprimento delle sanzioni, in particolare l'importo delle multe, la mancanza di precisione di certe fattispecie e l'elenco dei comportamenti punibili, è stato oggetto di numerose critiche.

Vari partecipanti appartenenti al settore dell'economia propongono delle modifiche basate in sostanza su un sistema di sanzioni amministrative per le imprese pronunciate da una «Commissione per la protezione dei dati» che potrebbe essere aggregata al DFI o al DFGP. L'elenco dei reati dovrebbe adeguarsi il più possibile a quello del regolamento (UE) 2016/679 e non essere più ampio di quest'ultimo. Tuttavia, al contrario del regolamento, che prevede multe di più milioni di euro, nel disegno di legge l'importo massimo delle multe non dovrebbe superare i 500 000 franchi.

1.6.2 Principali modifiche rispetto all'avamprogetto

1.6.2.1 Principali modifiche del D-LPD

Rispetto all'AP-LPD sono stati modificati soprattutto i punti illustrati qui appresso.

– In seguito ai risultati della consultazione sono stati rivisti diversi aspetti della sistematica della legge.

– Sono state modificate alcune deroghe al campo d'applicazione della legge. Sono state altresì rielaborate le deroghe concernenti i trattamenti nei procedimenti dinanzi ai tribunali o ad altre autorità federali giurisdizionali. Il D-LPD enumera inoltre le autorità federali che non sottostanno alla sorveglianza dell'Incaricato. Infine, è stata reintrodotta, in una certa misura, la deroga concernente i registri pubblici relativi ai rapporti di diritto privato: il D-LPD prevede che tali registri, in particolare l'accesso e i diritti delle persone interessate, siano retti dalle disposizioni speciali delle leggi federali applicabili.

– Il D-LPD adegua al diritto europeo la definizione di profilazione. È inoltre introdotta una definizione di violazione della sicurezza dei dati, dato che in sede di consultazione il termine è risultato poco chiaro.

- La disposizione sulla sicurezza dei dati è precisata poiché il suo campo d'applicazione risultava poco chiaro. È adeguata anche la norma concernente la comunicazione di violazioni della sicurezza dei dati. Sono ora previste varie eccezioni ed è garantito che la norma non violi il divieto di dover deporre a carico di sé stessi.
- In seguito ai risultati della consultazione il D-LPD introduce una disposizione sul consulente per la protezione dei dati e, a determinate condizioni, un'agevolazione relativa all'obbligo di informare l'Incaricato in merito alla valutazione d'impatto sulla protezione dei dati.
- Per tenere conto delle critiche della consultazione esterna, le raccomandazioni di buona prassi sono state sostituite da codici di condotta la cui elaborazione compete esclusivamente alle associazioni professionali ed economiche nonché agli organi federali. Possono sottoporli all'Incaricato, che esprime il suo parere e lo pubblica. Nell'ambito della sua attività di consulenza, l'Incaricato potrà anche in futuro elaborare guide e altri strumenti ausiliari e di lavoro.
- L'obbligo generale di documentazione, che in sede di consultazione è apparso poco preciso, è sostituito da una disposizione su un elenco delle attività di trattamento.
- Le regole relative alla comunicazione di dati personali sono state in parte rielaborate per tenere conto dei risultati della consultazione. Il principio secondo cui dati personali non possono essere trasmessi all'estero se la personalità della persona interessata ne potrebbe risultare gravemente minacciata è abolito poiché crea incertezza giuridica in relazione alla sistematica della regolamentazione. La terminologia relativa alle comunicazioni di dati personali all'estero per mezzo di garanzie appropriate è adeguata a quella del regolamento (UE) 2016/279. Le eccezioni relative alla comunicazione di dati personali a uno Stato la cui legislazione non garantisce un livello di protezione adeguato sono inoltre leggermente allentate. Infine sono mantenuti soltanto gli obblighi d'informare l'Incaricato o di ottenere la sua approvazione richiesti dal P-STE 108.
- In seguito ai risultati della consultazione, la disposizione relativa ai dati di una persona deceduta è radicalmente riformulata. È ora possibile un'ampia ponderazione degli interessi e va tenuto conto di un eventuale segreto d'ufficio o professionale. È stato inoltre inserito l'esecutore testamentario.
- Le disposizioni sull'obbligo d'informazione e le eccezioni sono precisate. Anche l'obbligo specifico d'informazione in caso di decisioni individuali automatizzate è riformulato in modo più preciso e sono aggiunte tre deroghe.
- La soglia per l'analisi d'impatto sulla protezione dei dati è alzata e sono previste eccezioni. In seguito ai risultati della consultazione il termine dell'Incaricato per reagire è abbreviato.
- Visti i risultati della consultazione, le disposizioni sul diritto d'accesso sono leggermente adeguate. Le eccezioni sono ora esplicitamente elencate, senza modifiche sostanziali.

– Sono stati adeguati i casi in cui i trattamenti di dati personali da parte degli organi federali devono poggiare su una base legale prevista da una legge in senso formale. Contrariamente all'avamprogetto, il D-LPD prevede la necessità di una base legale in senso formale quando lo scopo o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali della persona interessata. Nel primo caso (scopo del trattamento) la condizione di una base legale in senso formale è necessaria a causa dell'abrogazione della nozione di «profilo della personalità» e quindi anche della necessità di una base legale in senso formale per questo tipo di trattamento. Una grave ingerenza nei diritti fondamentali della persona interessata può anche risultare dal tipo di trattamento, ad esempio da determinate decisioni individuali automatizzate. Il D-LPD prevede pertanto la condizione di base legale in una legge formale anche per questi casi. Rispetto all'avamprogetto, le condizioni del livello normativo rimangono invece immutate per il trattamento di dati personali degni di particolare protezione e per la profilazione.
– È abolito il diritto della persona interessata di chiedere che un organo federale limiti il trattamento di dati personali che la riguardano. Il D-LPD prevede che la limitazione del trattamento costituisce per l'organo federale un'alternativa alla cancellazione o alla distruzione dei dati, se sono soddisfatte determinate condizioni.
– Contrariamente all'AP-LPD, che conferiva all'Incaricato la facoltà di decidere se aprire o meno un'inchiesta, il D-LPD ne prevede l'obbligo. L'Incaricato può rinunciarvi soltanto se la violazione delle disposizioni sulla protezione dei dati sono di lieve entità.
– È completato l'elenco dei provvedimenti amministrativi che l'Incaricato è autorizzato a pronunciare. La modifica non estende i poteri decisionali dell'Incaricato, ma si limita a precisare che egli può anche ordinare a un titolare del trattamento di rispettare determinati obblighi, quali quelli d'informazione o di comunicazione. Infine, il D-LPD conferisce all'Incaricato la competenza di pronunciare un ammonimento se sono soddisfatte determinate condizioni. Tale competenza non era prevista dall'AP-LPD.
– Contrariamente all'AP-LPD, il D-LPD non prevede più che i ricorsi contro i provvedimenti cautelari pronunciati dall'Incaricato non abbiano effetto sospensivo. Saranno in futuro applicabili le disposizioni generali della legge federale del 20 dicembre 1968[56] sulla procedura amministrativa (PA).
– Il disciplinamento dell'assistenza amministrativa tra l'Incaricato e le autorità estere incaricate della protezione dei dati è ampliato.
– Il D-LPD introduce l'obbligo per l'Incaricato di riscuotere emolumenti dai privati per determinati compiti legali.
– Il sistema delle sanzioni penali è stato rielaborato in seguito alle osservazioni in sede di consultazione. Il limite massimo della multa è abbassato a 250 000 franchi. L'elenco dei comportamenti punibili è stato sfoltito al fine di concentrarsi sulle violazioni degli obblighi fondamentali del titolare del

56 RS **172.021**

trattamento. La violazione dell'obbligo di discrezione è di nuovo una contravvenzione e non contempla più la comunicazione di dati trattati a fini commerciali. Per controbilanciare la mancanza di punibilità diretta dell'impresa, prevediamo di inasprire la responsabilità penale degli organi dirigenti applicando l'articolo 6 DPA in aggiunta all'articolo 29 CP. È inoltre introdotto il reato di inosservanza di una decisione dell'Incaricato, che permetterà di individuare e condannare più facilmente il dirigente responsabile dell'osservanza della decisione. Insieme alla possibilità, già prevista dall'AP-LPD, di rinunciare al perseguimento delle persone fisiche responsabili e di punire direttamente l'azienda se la multa non è superiore a 50 000 franchi e se la determinazione delle persone punibili esige provvedimenti d'inchiesta sproporzionati, questa misura offre maggiori possibilità di punire, anche se non l'azienda stessa, almeno i suoi dirigenti.

– Le disposizioni transitorie concernenti gli obblighi dei titolari privati del trattamento sono estese ad altri compiti.

1.6.2.2 Principali modifiche delle altre leggi federali

Le principali modifiche delle leggi federali che figurano nell'allegato del D-LPD riguardano i punti elencati qui appresso.

– Sono state abrogate o modificate le basi legali che autorizzano gli organi federali a trattare profili della personalità.

– Contrariamente all'avamprogetto, il disegno di legge adegua le disposizioni speciali relative alla comunicazione di dati personali all'estero agli articoli 13 e 14 D-LPD, al fine di garantire un disciplinamento uniforme nel diritto federale.

– Nella LOGA il disegno di legge introduce un certo numero di disposizioni che disciplinano per gli organi federali il trattamento di dati relativi a persone giuridiche. Infatti, in seguito all'abrogazione, nel D-LPD, della protezione dei dati delle persone giuridiche, le basi legali previste dal diritto federale che autorizzano gli organi federali a trattare dati personali non si applicano quando questi trattano dati riguardanti persone giuridiche. Con le disposizioni introdotte sono rispettati gli articoli 5, 13 capoverso 2 e 36 Cost.

1.6.2.3 Principali modifiche delle leggi federali che attuano i requisiti della direttiva (UE) 2016/680

Il nuovo capitolo relativo alla protezione dei dati personali introdotto nella legge federale del 20 marzo 1981[57] sull'assistenza internazionale in materia penale (AIMP) è parzialmente modificato. Rispetto all'avamprogetto l'obbligo d'informare è abolito, poiché la trasparenza dei trattamenti di dati personali è garantita dalla legge.

57 RS **351.1**

Per contro, i diritti delle persone interessate sono oggetto di un nuovo disciplinamento, da una parte per attuare i requisiti della direttiva (UE) 2016/ 680 e, dall'altra, per tenere conto della deroga di cui all'articolo 2 capoverso 3 D-LPD.

1.6.3 Altre osservazioni importanti in sede di consultazione

Alcuni partecipanti chiedono che la protezione dei dati in Svizzera sia retta dal principio secondo cui dati personali possono essere trattati soltanto se la persona interessata vi acconsente espressamente.

Vari partecipanti deplorano che l'AP-LPD non prevede un diritto alla portabilità dei dati sul modello del regolamento (UE) 2016/679. Tale diritto, che permette di ricevere i dati trattati che li riguardano in un formato standard e trasmetterli a un altro fornitore, garantirebbe un migliore controllo dei dati e favorirebbe la loro riutilizzazione e lo sviluppo di nuovi servizi. Altri partecipanti approvano invece esplicitamente la soluzione proposta dal nostro Consiglio, poiché ritengono che il diritto alla portabilità dei dati non è tesa direttamente a proteggere e genererebbe costi notevoli.

Alcuni partecipanti chiedono di introdurre l'inversione dell'onere della prova a favore della persona interessata, affinché, in caso di procedimento giudiziario, spetti al titolare del trattamento dimostrare che ha trattato lecitamente i dati. Singoli partecipanti approvano invece esplicitamente la rinuncia all'inversione.

Vari partecipanti deplorano che l'AP-LPD non preveda per le persone interessate strumenti per far valere i loro diritti in modo collettivo. Tale mancanza è invece esplicitamente approvata da altri partecipanti.

Singoli partecipanti chiedono di vietare gli archivi sulla solvibilità. Ritengono che questi archivi contenenti informazioni sulla solvibilità di persone private possano costituire una grave ingerenza nella vita privata. In effetti, le informazioni contenute in questi archivi sono spesso errate e inoltre la procedura per chiedere la cancellazione o la soppressione dei dati è spesso poco chiara, se non inesistente. Altri partecipanti chiedono almeno di verificare se non sia opportuno rendere la legge più severa nei confronti delle imprese che trattano archivi sulla solvibilità (cfr. in merito il postulato Schwaab 16.3682 «Inquadrare le prassi delle società che forniscono dati sulla solvibilità», nel cui ambito il nostro Consiglio intende esaminare l'opportunità di un disciplinamento specifico per le imprese che forniscono informazioni commerciali e le soluzioni giuridiche ipotizzabili).

Alcuni partecipanti ritengono che la LPD dovrebbe applicarsi anche a imprese che non hanno sede in Svizzera ma che procedono a trattamenti che esplicano effetti in Svizzera. Queste imprese dovrebbero in particolare avere un rappresentante in Svizzera.

Vari partecipanti ritengono che dovrebbe essere previsto un diritto all'oblio, poiché si tratta di un aspetto importante del diritto europeo che manca nell'AP-LPD. Altri partecipanti ne approvano invece esplicitamente la mancanza nell'AP-LPD poiché può essere dedotto dalle regole in vigore.

1.6.4 Valutazione del disegno di legge

Il disegno di legge sostituisce la LPD del 1992, al fine di rispondere meglio alle sfide legate alle nuove tecnologie e tenere conto dei requisiti del diritto europeo. Riprende, nei limiti del possibile, le regole e i principi consolidati. Non crea nuove competenze per la Confederazione e non intacca la sovranità dei Cantoni nel trattamento di dati da parte degli organi cantonali, su riserva dei requisiti europei e delle disposizioni sulla protezione dei dati delle leggi federali speciali. Il disegno di legge aggiorna la terminologia, incoraggia l'autoregolazione, rafforza gli obblighi dei titolari del trattamento e i diritti delle persone interessate, conferisce nuove competenze all'Incaricato e inasprisce le disposizioni penali. Le modifiche creano un quadro giuridico più chiaro, compatibile con le esigenze dell'innovazione e che permette alla Svizzera di restare competitiva su scala internazionale.

Il disegno di legge prevede anche la revisione parziale delle leggi specifiche del settore della cooperazione Schengen, in cui la Svizzera deve adempiere gli impegni presi nei confronti dell'Unione europea.

La scelta di un ampio progetto comprendente la revisione totale della LPD e modifiche di numerose altre leggi si è imposta perché sarebbe stato molto complicato attuare determinati requisiti della direttiva (UE) 2016/680 soltanto per certi trattamenti (ad esempio il potere decisionale dell'Incaricato). L'opzione scelta permette inoltre di istituire una legislazione coerente che realizza un quadro legale della protezione dei dati chiaro e applicabile nel modo più ampio possibile.

1.7 Altre misure esaminate

Nel contesto dei suoi lavori, il Consiglio federale ha esaminato altre misure, decidendo alla fine di non integrarle nel disegno di legge. Alcune delle misure sono state proposte anche in sede di consultazione (cfr. n. 1.6.1). Si tratta in particolare delle misure illustrate qui appresso.

1.7.1 Emanazione, da parte dell'Incaricato, di regole vincolanti sulla protezione dei dati

L'opzione di autorizzare l'Incaricato a emanare regole vincolanti è stata scartata in sede di avamprogetto. Pur avendo il vantaggio che l'Incaricato avrebbe potuto obbligare direttamente i destinatari delle regole, tale soluzione avrebbe creato un certo numero di problemi connessi al principio della legalità (delega di competenze all'Incaricato, densità normativa). Inoltre, rispetto alla soluzione delle raccomandazioni di buona prassi, proposta dall'avamprogetto, la procedura di emanazione di tali regole sarebbe stata più lenta, poiché sarebbe stato necessario seguire ogni volta la procedura per l'emanazione delle ordinanze dell'Amministrazione federale. Infine, questa opzione avrebbe lasciato poco margine di manovra alle cerchie interessate, inducendole a non rispettare le regole.

1.7.2 Inversione dell'onere della prova

Il nostro Consiglio ha rinunciato all'inversione dell'onere della prova secondo l'articolo 13*a* della legge federale del 19 dicembre 1986[58] sulla concorrenza sleale (LCSl), secondo cui il giudice potrebbe esigere dal titolare o responsabile del trattamento di dati la prova del trattamento conforme alla protezione dei dati se, tenuto conto degli interessi legittimi delle parti al procedimento, tale esigenza sembra appropriata nel singolo caso. Già oggi, nell'ambito della libera valutazione delle prove e dell'obbligo di partecipare delle parti, i giudici civili sono in grado di affrontare i problemi probatori. Inoltre, la consultazione relativa alla legge federale sui servizi finanziari (LSF)[59] ha evidenziato che le proposte di invertire l'onere della prova incontrano una forte opposizione. L'Incaricato avrebbe tuttavia auspicato l'inversione.

1.7.3 Applicazione collettiva del diritto

In adempimento della mozione 13.3931 Birrer-Heimo, il nostro Consiglio sta elaborando un avamprogetto di legge teso a facilitare l'applicazione collettiva del diritto. Esso contemplerà il settore privato in generale e quindi anche la protezione dei dati. Riteniamo che non sia opportuno prevedere un regime speciale introducendo nella LPD una normativa specifica sull'applicazione collettiva dei diritti (ad esempio, l'estensione del diritto delle azioni collettive e introduzione di un'azione o di un concordato collettivi[60]).

1.7.4 Diritto alla portabilità dei dati

Il nostro Consiglio ha valutato se introdurre un diritto della persona interessata alla portabilità dei dati, come quello previsto all'articolo 20 del regolamento (UE) 2016/679. Il diritto alla portabilità permette alla persona interessata di trasmettere i suoi dati da un sistema di trattamento automatizzato a un altro e implica che essa riceva in un formato strutturato, usuale e leggibile elettronicamente i dati che ha messo a disposizione del titolare del trattamento. Riteniamo tuttavia che tale diritto, piuttosto che proteggere la personalità delle persone interessate, consenta loro di riutilizzare i loro dati al fine di far giocare la concorrenza. Appare pertanto problematico emanare le pertinenti norme legali. Tanto più che l'attuazione del diritto di portabilità potrebbe rivelarsi difficile, in quanto presuppone un'intesa tra i titolari del trattamento e un accordo, perlomeno implicito, sui supporti e gli standard informatici utilizzati. L'analisi dell'impatto di un'eventuale regolamentazione ha inoltre mostrato che l'introduzione del diritto di portabilità dei dati potrebbe rivelarsi molto costosa, in particolare per le imprese con più di 50 collaboratori, poiché queste dovrebbero assumere il personale supplementare necessario per applicare tale diritto.

58 RS **241**
59 Cfr. il messaggio del Consiglio federale del 4 nov. 2015 concernente la legge sui servizi finanziari (LSF) e la legge sugli istituti finanziari (LIFin), FF **2015** 7293.
60 Cfr. art. 101 segg. dell'avamprogetto di legge sui servizi finanziari (LSF).

Prima di prendere in considerazione l'introduzione del diritto alla portabilità dei dati, il nostro Consiglio preferisce attendere le esperienze raccolte in seno all'Unione europea. Proseguirà tuttavia il suo esame nel quadro della «Strategia Svizzera digitale». L'Incaricato avrebbe preferito introdurre nella legge il diritto alla portabilità dei dati.

1.7.5 Commissione extraparlamentare per l'elaborazione e l'approvazione delle raccomandazioni di buona prassi

Il nostro Consiglio ha valutato se conferire a una commissione extraparlamentare il compito di elaborare e approvare raccomandazioni di buona prassi. La soluzione è stata scartata in fase di avamprogetto in quanto comporterebbe oneri amministrativi e finanziari supplementari e sarebbe più burocratica.

1.7.6 Modifica dell'organizzazione dell'autorità di controllo

Il nostro Consiglio ha valutato l'opportunità di trasformare l'Incaricato in un'autorità collegiale, decidendo tuttavia alla fine di mantenere la struttura attuale, poco burocratica, semplice e che garantisce decisioni rapide come pure un buon flusso delle informazioni. Si tratta inoltre di una soluzione adottata con successo nei Cantoni e in numerosi Paesi europei (Germania, Polonia, Spagna).

1.7.7 Introduzione di meccanismi speciali per gestire i conflitti

Il nostro Consiglio ha esaminato l'opportunità di istituire un organo incaricato di risolvere in sede extragiudiziaria i conflitti in materia di protezione dei dati. Vi ha tuttavia rinunciato poiché, visto che esiste già in numerosi settori (organo di conciliazione delle telecomunicazioni [ombudscom], ombudsman delle banche, ombudsman delle assicurazioni private e della SUVA, ecc.), un ulteriore organo di conciliazione genererebbe conflitti di competenza. Inoltre, l'introduzione di un organo aggregato all'Incaricato causerebbe costi notevoli.

1.8 Analisi d'impatto della regolamentazione

L'analisi d'impatto della regolamentazione (AIR) è uno strumento che permette di esaminare e illustrare le ripercussioni economiche dei progetti legislativi della Confederazione. Si tratta di uno strumento vincolante, importante in particolare nel caso di messaggi, rapporti esplicativi e proposte del nostro Consiglio. Le basi legali

dell'AIR si trovano agli articoli 170 Cost. e 141 capoverso 2 della legge federale del 13 dicembre 2002[61] sul Parlamento (LParl).

L'UFG e la Segreteria di Stato dell'economia (SECO) hanno incaricato l'impresa PwC di procedere a un'AIR[62] relativa all'avamprogetto. L'analisi doveva servire da base per la valutazione di quest'ultimo. Poiché il disegno riprende la maggior parte delle misure analizzate, le conclusioni relative all'avamprogetto sono valide anche per il disegno. L'analisi si fonda soprattutto sui risultati di un sondaggio condotto in rete presso le imprese e su colloqui effettuati con specialisti della protezione dei dati. Nel sondaggio l'avamprogetto è stato in generale valutato in modo positivo.

L'AIR esamina cinque punti: la necessità e la possibilità di un intervento dello Stato; le ripercussioni del progetto per i vari gruppi della società; le ripercussioni per l'economia nel suo insieme; le regolamentazioni alternative da prendere in considerazione e gli aspetti pratici dell'esecuzione.

1.8.1 Necessità e possibilità di un intervento dello Stato

La necessità di emanare norme legali è dovuta alle importanti evoluzioni tecnologiche e sociali degli ultimi anni, che creano timori nella popolazione e nuove minacce per la protezione dei dati. L'avamprogetto intendeva soprattutto migliorare la sorveglianza e la disponibilità dei dati come pure la trasparenza dei trattamenti e ciò vale anche per il disegno. La necessità della Confederazione di intervenire risulta inoltre dagli sviluppi del diritto internazionale. Ciò riguarda in particolare il P-STE 108 e, in virtù della cooperazione nell'ambito di Schengen, la direttiva (UE) 2016/680; va tuttavia tenuto conto anche del regolamento (UE) 2016/679.

1.8.2 Ripercussioni del progetto per i diversi gruppi della società

Le modifiche previste dall'avamprogetto riguardavano tutte le imprese che operano in Svizzera. PwC le ha classificate secondo la loro «esposizione al diritto in materia di protezione dei dati», riconducibile al ramo in cui operano e alla loro dimensione. Sono stati formati i seguenti segmenti:

- segmento A: imprese debolmente esposte al diritto in materia di protezione dei dati,
- segmento B: imprese da mediamente a fortemente esposte al diritto in materia di protezione dei dati,
- segmento C: imprese fortemente esposte, e in maniera per loro essenziale, al diritto in materia di protezione dei dati.

61 RS **171.10**
62 L'AIR è disponibile in tedesco sul sito dell'UFG: www.bj.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html

Se si applica questa suddivisione ai rami economici svizzeri, circa 335 000 imprese (55,1 %) rientrano nel segmento A, circa 265 000 nel segmento B (43,5 %) e quasi 8000 nel segmento c (1,4 %).

Secondo i risultati dell'analisi, le imprese del segmento A erano in generale poco toccate dalle misure previste dall'AP. Alcuni esperti hanno tuttavia osservato che le imprese del segmento A sarebbero più toccate dalle misure dell'AP rispetto alle grandi imprese, poiché spesso non dispongono di un servizio apposito per conformarsi alle nuove disposizioni, il che comporterebbe costi supplementari. Per contro, a causa delle loro attività, delle dimensioni e delle relazioni con l'estero, le imprese dei segmenti B e C sono maggiormente toccate dal D-LPD[63].

1.8.3 Ripercussioni per l'economia in generale

Occorre distinguere gli effetti sull'economia da quelli sulla società in generale. Per l'economia, la discussione sui presunti effetti era incentrata sul problema della concorrenza. Se l'Unione europea non dovesse più giudicare la Svizzera un Paese dotato di un livello di protezione dei dati adeguato o se la Svizzera adottasse una normativa valida soltanto a livello nazionale o più restrittiva rispetto al diritto dell'Unione europea, sarebbero prevedibili gravi svantaggi competitivi nei confronti degli Stati membri dell'Unione europea.

In Svizzera, le modifiche previste sono in gran parte considerate neutre dal punto di vista della concorrenza poiché le imprese di un determinato segmento sono tutte toccate in misura uguale. Per contro, secondo l'AIR resta controverso in che misura una maggiore protezione dei dati comporti un vantaggio competitivo su scala internazionale.

Quanto alle ripercussioni sulla società, va constatato che non risultano in linea di massima obblighi specifici per le persone interessate. Gli esperti interrogati ritengono che le misure analizzate nell'ambito dell'AIR siano atte ad agevolare, almeno sotto il profilo formale, l'esercizio dei diritti delle persone interessate. Gli esperti si riferiscono soprattutto all'estensione del diritto d'accesso, alla maggiore trasparenza del trattamento, ai miglioramenti in generale dei diritti delle persone interessate nonché all'introduzione di un diritto di portabilità alla quale il nostro Consiglio ha in seguito rinunciato (cfr. n. 1.7.4). Le persone interessate trarranno concretamente profitto dalle misure analizzate soprattutto nella misura in cui accorderanno importanza alla protezione dei loro dati personali. In tale contesto l'impostazione predefinita (privacy by default) favorevole alla protezione dei dati può rivelarsi uno strumento importante.

63 Per una visione dettagliata dell'impatto di ciascuna misura, si veda la tabella riassuntiva alle pagg. 54–58 dell'AIR.

1.8.4 Regolamentazioni alternative

Nei colloqui con gli esperti, oltre alle misure previste, sono state discusse anche altre proposte, ad esempio quella di applicare ai dati le regole dei diritti reali. Le proposte sono state tuttavia spesso giudicate inattuabili perché troppo distanti dagli sviluppi internazionali (nessun altro Paese europeo prevede ad esempio diritti di proprietà sui dati). Per motivi di competitività si propone di rinunciare a misure più vincolanti rispetto a quelle previste negli Stati dell'Unione europea, evitando così una regolamentazione troppo severa. La possibilità di istituire una commissione di esperti incaricata di formulare raccomandazioni di «buona prassi», alla quale il nostro Consiglio ha rinunciato, è stata accolta con favore poiché permetterebbe un rapido adeguamento alle novità tecnologiche (cfr. n. 1.7.5).

1.8.5 Aspetti pratici dell'esecuzione

Per limitare i costi risultanti dall'attuazione delle misure, la maggioranza degli esperti interrogati raccomanda di concedere alle imprese la possibilità di conformarsi in modo standardizzato agli obblighi d'informazione. Ciò potrebbe essere realizzato mediante spiegazioni relative al diritto in materia di protezione dei dati oppure per mezzo di pittogrammi sul sito Internet delle imprese o nelle condizioni generali. Secondo gli esperti, l'introduzione di obblighi d'informazione «individualizzati» causerebbe invece costi notevoli.

Per motivi inerenti alla certezza del diritto e alla trasparenza, il disegno di legge dovrebbe usare concetti chiaramente definiti (definizioni legali) e designare chiaramente i fatti che comportano degli obblighi. Occorrerebbe indicare, ad esempio, i casi in cui è necessario procedere a un'analisi d'impatto sulla protezione dei dati. Per migliorare la consapevolezza dei problemi posti dalla protezione dei dati e facilitare l'attuazione della legge, gli esperti segnalano la necessità di una comunicazione mirata (p. es. mediante note, opuscoli) e l'elaborazione di guide. Queste misure potrebbero giovare in particolare alle imprese meno esposte al diritto in materia di protezione dei dati. In questo contesto, l'idea di istituire una commissione di esperti è stata accolta con favore dalla maggior parte degli esperti.

2 Direttiva (UE) 2016/680

2.1 Presentazione della direttiva (UE) 2016/680

2.1.1 Negoziati

Le deliberazioni degli Stati membri dell'Unione europea e dei quattro Stati associati allo spazio Schengen (Norvegia, Islanda, Svizzera e Principato del Liechtenstein nel quadro dei loro diritti di partecipazione) si sono svolte tra il 2012 e il 2015 nei gruppi di lavoro del Consiglio europeo (comitati misti), sotto la direzione dello Stato membro dell'UE cui spettava la presidenza. All'elaborazione della direttiva in seno ai comitati misti hanno partecipato rappresentanti della Confederazione e dei

Cantoni. Il 27 aprile 2016 il Parlamento europeo e il Consiglio dell'Unione europea hanno formalmente adottato la direttiva (UE) 2016/680.

2.1.2 Breve panoramica

La direttiva (UE) 2016/680 intende proteggere i dati personali trattati a fini di prevenzione, indagine, accertamento e perseguimento di reati o d'esecuzione di sanzioni penali, compresa la protezione e la prevenzione contro le minacce alla sicurezza pubblica. La normativa mira a garantire un livello elevato di protezione dei dati delle persone fisiche, agevolando nel contempo lo scambio di tali dati tra le autorità competenti negli Stati membri di Schengen. A differenza della decisione quadro 2008/977/GAI, la direttiva si applica sia ai trattamenti internazionali di dati sia a quelli effettuati dalle autorità giudiziarie e di polizia a livello strettamente nazionale. Il testo della direttiva (UE) 2016/680 si basa su quello del regolamento (UE) 2016/679 (cfr. n. 4), al fine di applicare, per grandi linee, gli stessi principi generali. Prevede tuttavia determinati adeguamenti per trovare il giusto equilibrio tra il diritto della persona interessata alla protezione della sua sfera privata e le necessità delle autorità penali. Qui appresso sono presentate le novità più importanti.

La direttiva (UE) 2016/680 introduce l'obbligo di distinguere tra le diverse categorie di persone interessate (art. 6) e prevede regole per tale distinzione e per la verifica della qualità dei dati. L'articolo 8 disciplina la liceità del trattamento. Il trattamento deve in linea di massima poggiare su una base legale. Altri motivi giustificativi, ad esempio il consenso della persona interessata, non sono applicabili ai trattamenti che rientrano nel campo d'applicazione della direttiva. L'articolo 11 sancisce il principio secondo cui una decisione basata unicamente su un trattamento automatizzato è vietata, salvo se autorizzata dal diritto nazionale e se è garantito il diritto della persona interessata di ottenere l'intervento umano da parte del titolare del trattamento.

Il capo III disciplina il diritto della persona interessata. L'articolo 16 paragrafo 3 stabilisce che, anziché cancellare i dati, il titolare del trattamento deve limitarne il trattamento quando l'esattezza dei dati personali è contestata dalla persona interessata e l'esattezza o l'inesattezza non può essere accertata. L'articolo 17 dispone che in caso di limitazione del trattamento la persona interessata deve poter esercitare i suoi diritti anche tramite l'autorità di controllo. Secondo l'articolo 18 gli Stati membri di Schengen possono disporre che i diritti di cui agli articoli 13, 14 e 16 siano esercitati conformemente al diritto dello Stato membro qualora i dati personali figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale.

Il capo IV disciplina gli obblighi del titolare e del responsabile del trattamento. Introduce il principio della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 19 e 20). L'articolo 24 prevede l'obbligo del titolare e del responsabile del trattamento di tenere un registro di tutte le categorie di attività di trattamento sotto la loro responsabilità. Prima di procedere a determinati trattamenti, il titolare del trattamento è inoltre tenuto a effettuare una valutazione d'impatto sulla protezione dei dati (art. 27) e consultare, se necessario, l'autorità di controllo (art. 28). Gli articoli 30 e 31 obbligano il titolare del trattamento a notificare deter-

minati casi di violazione dei dati personali all'autorità di controllo e, se necessario, alla persona interessata.

Il capo V disciplina il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali. La Commissione europea è incaricata di valutare il livello di protezione garantito da uno Stato terzo, da un territorio o da uno o più settori specifici dello Stato terzo (art. 36). Se la Commissione europea non ha constatato l'adeguatezza del livello di protezione nel Paese terzo, i dati possono ciononostante essere trasferiti se sono fornite garanzie appropriate per la loro protezione (art. 37) oppure in virtù di deroghe in situazioni particolari (art. 38). L'articolo 39 disciplina il trasferimento di dati personali a destinatari stabiliti in Paesi terzi qualora i dati non possano essere trasmessi alle autorità competenti mediante i canali usuali della cooperazione giudiziaria e di polizia.

Il capo VI obbliga gli Stati membri di Schengen a istituire un'autorità di controllo della protezione dei dati. Gli articoli 45–47 disciplinano le competenze, i compiti e i poteri di tale autorità. Secondo l'articolo 45 paragrafo 2 gli Stati membri di Schengen dispongono che l'autorità di controllo non sia preposta a controllare i trattamenti effettuati dai tribunali nell'ambito della loro attività giurisdizionale. Sempre secondo tale disposizione gli Stati membri di Schengen possono prevedere una deroga anche per i trattamenti di dati effettuati da altre autorità giudiziarie indipendenti nell'ambito della loro attività giurisdizionale. L'articolo 47 paragrafo 1 obbliga gli Stati membri a disporre che l'autorità di controllo abbia poteri d'indagine effettivi, ossia perlomeno il potere di ottenere, dal titolare o dal responsabile del trattamento, l'accesso a tutti i dati personali oggetto del trattamento e a tutte le informazioni necessarie per l'adempimento dei suoi compiti. Secondo l'articolo 47 paragrafo 2 l'autorità di controllo deve avere poteri correttivi effettivi, quali ad esempio il potere di rivolgere avvertimenti al titolare o al responsabile del trattamento, di ingiungere loro di conformare i trattamenti, ordinando in particolare la rettifica o la cancellazione dei dati, come pure di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. I poteri dell'autorità di controllo non devono tuttavia intaccare le regole specifiche della procedura penale, incluse le inchieste e il perseguimento di reati, e l'indipendenza del potere giudiziario.

Il capo VIII tratta i rimedi giuridici, la responsabilità e le sanzioni. Secondo l'articolo 52 la persona interessata deve avere il diritto di proporre reclamo all'autorità di controllo e secondo l'articolo 53 essa deve avere anche il diritto a un ricorso giurisdizionale effettivo contro una decisione dell'autorità di controllo che la riguarda. Infine, l'articolo 55 sancisce il diritto della persona interessata di incaricare, a determinate condizioni, un rappresentante di proporre il reclamo per suo conto.

2.2 Recepimento della direttiva (UE) 2016/680 in quanto sviluppo dell'acquis di Schengen

In virtù dell'articolo 2 paragrafo 3 dell'Accordo di associazione a Schengen la Svizzera s'impegna in linea di massima ad accettare, attuare e applicare gli sviluppi dell'acquis di Schengen. La direttiva (UE) 2016/680 costituisce uno sviluppo dell'acquis di Schengen. Come si vedrà al numero 2.4, il recepimento della direttiva

(UE) 2016/680 implica l'adozione di un certo numero di misure legislative a livello nazionale, poiché il diritto in vigore non soddisfa tutti i requisiti dell'atto normativo dell'Unione europea.

Conformemente all'Accordo di associazione, una volta ricevuta la notifica dell'Unione europea dell'avvenuta adozione di atti normativi che costituiscono uno sviluppo dell'acquis di Schengen, la Svizzera deve pronunciarsi in merito all'accettazione del loro contenuto e al recepimento nel proprio ordinamento giuridico nei trenta giorni successivi alla loro adozione (art. 7 par. 2 lett. a dell'Accordo di associazione a Schengen).

Se l'atto normativo in questione è giuridicamente vincolante, la notifica dell'Unione europea e la risposta della Svizzera sono trasmesse in forma di uno scambio di note. Per la Svizzera tale scambio costituisce un trattato internazionale. Secondo la Costituzione federale la conclusione di un trattato compete direttamente al Consiglio federale oppure è sottoposta all'approvazione del Parlamento e, in caso di referendum, del Popolo.

Il Parlamento europeo e il Consiglio dell'Unione europea hanno adottato la direttiva (UE) 2016/680 il 27 aprile 2016. L'atto è stato tuttavia notificato alla Svizzera soltanto il 1° agosto 2016, rendendo impossibile al nostro Paese indirizzare la sua notifica al Segretariato generale del Consiglio entro il termine previsto dall'Accordo di associazione. La Svizzera ha potuto trasmettere la sua notifica soltanto il 1° settembre 2016.

Nel presente caso l'Assemblea federale deve approvare lo scambio di note concernente il recepimento della direttiva (UE) 2016/680. Poiché la direttiva sarà vincolante per la Svizzera soltanto una volta soddisfatti i requisiti costituzionali, il nostro Consiglio ne ha informato l'Unione europea nella sua risposta del 1° settembre 2016 (art. 7 par. 2 lett. b dell'Accordo di associazione a Schengen).

Entro due anni dalla notifica (anche in caso di un eventuale referendum) la Svizzera deve recepire e attuare l'atto normativo in questione nel proprio ordinamento giuridico. Una volta conclusa la procedura nazionale, la Svizzera informa immediatamente per scritto gli organi competenti dell'Unione europea che i requisiti costituzionali sono soddisfatti, il che corrisponde alla ratifica dello scambio di note tra la Svizzera e l'Unione europea. Lo scambio di note concernente la direttiva (UE) 2016/680 entra in vigore al momento della comunicazione della Svizzera. Poiché la direttiva (UE) 2016/680 è stata notificata alla Svizzera il 1° agosto 2016, il termine per il recepimento e l'attuazione dell'atto normativo è il 1° agosto 2018.

2.3 Scelta legistica

La direttiva (UE) 2016/680 non è direttamente applicabile né per gli Stati membri dell'UE né per la Svizzera e deve quindi essere trasposta nel diritto nazionale. Per attuare la normativa, la Svizzera deve adeguare varie leggi federali, poiché esse non sono del tutto conformi ai requisiti della direttiva (UE) 2016/680.

In quanto Stato associato a Schengen, il nostro Paese è tenuto in linea di massima ad applicare la direttiva soltanto nella misura in cui i trattamenti si svolgono nel quadro della cooperazione prevista da Schengen nel settore penale. Sarebbe pertanto sufficiente una trasposizione limitata a questo settore. Tuttavia, visto che, pur essendo più dettagliato, il contenuto della direttiva (UE) 2016/680 corrisponde in gran parte a quello del P-STE 108, il nostro Consiglio propone una trasposizione più estesa della direttiva secondo i criteri illustrati qui di seguito.

– Le disposizioni della direttiva (UE) 2016/680 che corrispondono ai requisiti del P-STE 108 sono trasposti nel D-LPD e si applicano a tutti i trattamenti di dati da parte di privati e di organi federali.
– I requisiti della direttiva (UE) 2016/680 che corrispondono ai principi generali della protezione dei dati senza tuttavia essere previsti dal P-STE 108 sono trasposti nel D-LPD e si applicano a tutti i trattamenti di dati da parte degli organi federali, al fine di evitare livelli di protezione dei dati divergenti nel settore pubblico.
– Le disposizioni della direttiva (UE) 2016/680 relative all'autorità di controllo della protezione dei dati sono attuate nel D-LPD. Una parte di tali requisiti è prevista anche dal P-STE 108. Su scala federale, l'autorità nazionale competente per il controllo di tutte le regole federali sulla protezione dei dati è l'Incaricato. La normativa applicabile all'Incaricato deve essere uniforme, a prescindere dal settore di sorveglianza.
– I requisiti della direttiva (UE) 2016/680 che costituiscono regole specifiche della cooperazione prevista da Schengen nel settore penale sono trasposte unicamente negli atti normativi applicabili a tale settore (cfr. n. 9.3).

2.4 Principali modifiche legislative necessarie

Oltre alle modifiche della LPD, il recepimento della direttiva (UE) 2016/680 implica anche quelle di altri atti normativi federali: il CP, il Codice di procedura penale (CPP)[64], l'AIMP, la legge federale del 22 giugno 2001[65] sulla cooperazione con la Corte penale internazionale, la legge federale del 3 ottobre 1975[66] relativa al trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale, la legge federale del 7 ottobre 1994[67] sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati, la legge federale del 13 giugno 2008[68] sui sistemi d'informazione di polizia della Confederazione (LSIP), la legge federale del 12 giugno 2009[69] sullo scambio di informazioni con gli Stati Schengen (LSIS). Le disposizioni della direttiva (UE) 2016/680 che devono essere trasposte nel D-LPD e nelle summenzionate leggi settoriali sono indicate nei commenti ai singoli articoli.

64 RS **312.0**
65 RS **351.6**
66 RS **351.93**
67 RS **360**
68 RS **361**
69 RS **362.2**

Dato che molte leggi federali che riguardano il settore della polizia contengono disposizioni sulla protezione dei dati, ci si può chiedere se tale dispersione normativa non ostacoli l'applicazione del diritto e se non vada valutata l'introduzione di una legge federale che disciplini complessivamente le attività nel settore della polizia; molti Cantoni hanno infatti scelto questa soluzione.

3 P-STE 108

3.1 Breve panoramica

Gli Stati parte sono tenuti ad applicare il P-STE 108 a tutti i trattamenti di dati di competenza della loro giurisdizione nel settore pubblico e privato. Soltanto il trattamento di dati da parte di una persona nell'ambito delle sue attività personali è escluso dal campo d'applicazione del progetto di modernizzazione (art. 3).

Il P-STE 108 estende gli obblighi del titolare del trattamento. Questi è tenuto a notificare all'autorità di controllo competente determinati casi di violazione della protezione dei dati (art. 7 par. 2). Il suo obbligo di informare la persona interessata va anche esteso, in particolare in relazione alle informazioni da fornire e in caso di decisione individuale automatizzata. Gli Stati parte devono altresì prevedere l'obbligo del titolare del trattamento di effettuare una valutazione d'impatto prima di determinati trattamenti e di applicare i principi della protezione dei dati sin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default) (art. 8bis par. 2 e 3).

Gli Stati parte devono concedere alla persona interessata il diritto di non essere oggetto di una decisione presa unicamente sulla base di un trattamento automatizzato dei suoi dati, senza avere la possibilità di far valere il suo punto di vista (art. 8 lett. a). Anche il diritto d'accesso della persona interessata (art. 8 lett. b) deve essere esteso e lo stesso vale per le condizioni applicabili al suo consenso.

Gli Stati parte sono tenuti a stabilire un regime di sanzioni e un sistema di ricorso (art. 10).

Il principio fondamentale secondo cui i dati possono essere trasferiti verso uno Stato terzo soltanto se è garantito un livello adeguato di protezione rimane uguale a quello della Convenzione STE 108 attuale. Secondo il P-STE 108 (art. 12), un livello adeguato di protezione può essere garantito dal diritto dello Stato terzo o dell'organizzazione internazionale destinatari o mediante determinate garanzie comunicate all'autorità di controllo prima della trasmissione dei dati. In assenza di un livello di protezione adeguato, i dati possono essere trasmessi verso uno Stato terzo soltanto se la persona interessata vi acconsente e in altri casi eccezionali. Infine, il P-STE 108 obbliga gli Stati parte a disporre che l'autorità di controllo possa esigere dalla persona che trasferisce i dati di dimostrare l'efficacia delle garanzie fatte e ad autorizzare l'autorità a bloccare o sospendere il trasferimento dei dati.

Gli Stati parte sono tenuti a istituire un'autorità di controllo, analogamente a quanto previsto dall'attuale Convenzione STE 108. Secondo il P-STE 108 (art. 12bis), le autorità di controllo devono essere autorizzate a prendere decisioni vincolanti impugnabili e a pronunciare sanzioni amministrative. Soltanto i trattamenti effettuati da

parte di organi nell'esercizio delle loro funzioni giurisdizionali non sono soggetti alla vigilanza dell'autorità di controllo. Quest'ultima ha inoltre il compito di sensibilizzare il pubblico e coloro che trattano dati.

3.2 Ratifica del Protocollo di emendamento alla Convenzione STE 108

Il P-STE 108 intende trasformare la Convenzione STE 108 in uno strumento universale. Anche la Convenzione in vigore può essere ratificata da Stati che non sono membri del Consiglio d'Europa. Tra i circa 50 Stati che l'hanno ratificata, quattro non sono membri del Consiglio d'Europa (Maurizio, Senegal, Tunisia e Uruguay). Inoltre, vari altri Stati non membri stanno per ratificarla (Argentina, Capo Verde, Burkina Faso e Marocco). L'interesse da parte degli Stati extraeuropei alla ratifica della Convenzione potrebbe crescere visto che l'Unione europea considera tale ratifica un criterio determinante per l'ottenimento della decisione di adeguatezza.

Il P-STE 108 consente di armonizzare e migliorare il livello di protezione dei dati su scala internazionale, il che migliora anche la protezione di cui beneficiano i cittadini svizzeri i cui dati sono oggetto di trattamento all'estero. Il P-STE 108 contribuisce inoltre ad agevolare la comunicazione di dati tra gli Stati parte e dunque l'accesso delle imprese svizzere ai mercati degli altri Stati. La ratifica del Protocollo di emendamento alla Convenzione STE 108 da parte della Svizzera è d'altronde probabilmente un presupposto fondamentale affinché l'Unione europea confermi nuovamente che la Svizzera dispone di una protezione adeguata dei dati. Solo tale conferma garantisce l'accesso illimitato del nostro Paese al mercato europeo.

Per la Svizzera è opportuno accettare rapidamente il Protocollo d'emendamento alla Convenzione STE 108, sia per ragioni inerenti alla tutela dei diritti dell'uomo sia per ragioni economiche (agevolazione della comunicazione transfrontaliera di dati). In varie risposte a interventi parlamentari, il Consiglio federale ha annunciato il suo sostegno al P-STE 108. Il Collegio governativo si è d'altronde impegnato per una migliore protezione dei dati nel quadro dei suoi sforzi a favore dei diritti dell'uomo[70]. Infine occorre osservare che le misure previste dal P-STE 108 coincidono con gli obiettivi del Consiglio federale fissati nella decisione del 9 dicembre 2011[71] fondata sulla valutazione della legge sulla protezione dei dati.

L'articolo 4 P-STE 108 obbliga gli Stati parte a disporre nel proprio diritto interno le misure necessarie per dare effetto alle disposizioni della Convenzione. Tali misure devono inoltre entrare in vigore al momento della ratifica della nuova Convenzione STE 108. Infine, gli Stati parte non possono formulare riserve (art. 25).

70 Il nostro Consiglio ha in particolare dichiarato di sostenere i lavori in corso presso il Consiglio d'Europa negli interventi parlamentari seguenti: Ip. Eichenberger 13.4209 («US-Swiss Safe Harbor Framework. Ripristino della fiducia nell'ambito dello scambio di dati con gli Stati Uniti»); Int. Gross 13.1072 («Patto dell'ONU relativo ai diritti civili e politici. Integrazione della protezione dei dati»).

71 FF **2012** 227

Il contenuto del D-LPD coincide in gran parte con i requisiti del P-STE 108 e pertanto a tempo debito sarà possibile una ratifica senza bisogno di modificare la legislazione svizzera.

3.3 Principali modifiche legislative necessarie

Le disposizione del P-STE 108 non sono direttamente applicabili. Per poter ratificare il Protocollo d'emendamento della Convenzione STE 108 la Svizzera deve adeguare determinate disposizioni del diritto federale. Le disposizioni del P-STE 108 che devono essere trasposte nel D-LPD sono illustrate nel commento ai singoli articoli di quest'ultimo.

4 Regolamento (UE) 2016/679 sulla protezione dei dati personali

4.1 Breve panoramica

Il regolamento (UE) 2016/679 è l'atto normativo sulla protezione dei dati fondamentale dell'Unione europea; non fa parte dell'acquis di Schengen. Il contenuto della direttiva (UE) 2016/680 si basa sul regolamento e quindi i due atti contengono in gran parte norme concordanti. Tuttavia il regolamento è più dettagliato, mentre alcune disposizioni della direttiva sono adeguate alle esigenze delle autorità penali.

Il regolamento (UE) 2016/679 disciplina soprattutto la protezione dei dati trattati nell'ambito del mercato interno ma si applica anche al settore pubblico. Stabilisce le regole relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (art. 1).

Il capo III disciplina i diritti delle persone interessate. Rispetto alla direttiva 95/46/CE tali diritti sono rafforzati. Il regolamento (UE) 2016/679 garantisce ad esempio alle persone interessate un migliore accesso ai dati che le riguardano (art. 12–15). Esse hanno inoltre il diritto alla rettifica (art. 16) e alla cancellazione (art. 17, cosiddetto «diritto all'oblio») dei dati, come pure alla limitazione del trattamento (art. 18). Dispongono altresì di un diritto alla portabilità dei dati da un fornitore di servizi a un altro (portabilità dei dati, art. 20). Infine, hanno il diritto di opporsi al trattamento di dati personali in particolare ai fini di una profilazione (art. 21) e di non essere oggetto di una decisione basata unicamente sul trattamento automatizzato (art. 22).

Il capo IV disciplina gli obblighi del titolare e del responsabile del trattamento. Sancisce il principio della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25) e definisce le condizioni applicabili al conferimento del trattamento a un responsabile (art. 28 e 29). I titolari del trattamento hanno l'obbligo, in determinati casi, di notificare le violazioni dei dati personali all'autorità di controllo e alla persona interessata (art. 33 e 34). Prima di determinati trattamenti, i titolari del trattamento sono inoltre tenuti a effettuare una valutazione d'impatto sulla protezione dei dati (art. 35) e a consultare, se necessario, l'autorità di controllo (art. 36). Inoltre, gli organi pubblici e le imprese che trattano dati che presentano dei

rischi devono designare un incaricato della protezione dei dati (art. 37–39). Infine, gli Stati membri dell'Unione europea devono incoraggiare l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del regolamento (UE) 2016/679 (art. 40 e 41) e l'istituzione di meccanismi di certificazione della protezione dei dati (art. 42 e 43).

Il capo V disciplina il trasferimento di dati verso Stati terzi od organizzazioni internazionali. La Commissione è incaricata di valutare il livello di protezione garantito da un territorio o da uno o più settori specifici all'interno del Paese terzo (art. 45). Se la Commissione non constata mediante una decisione il carattere adeguato del livello di protezione su un territorio o in un settore, i dati possono ciononostante essere trasferiti in presenza di garanzie adeguate (art. 46), sulla base di norme vincolanti d'impresa (art. 47) o di deroghe in situazioni specifiche (art. 49).

Il capo VI riguarda le autorità di controllo indipendenti. Gli Stati membri possono istituire una o più autorità di controllo incaricate di sorvegliare l'applicazione del regolamento (UE) 679/2016 e, se del caso, anche della direttiva (UE) 2016/680. Nei due atti normativi i requisiti applicabili all'indipendenza dell'autorità di controllo sono identici. L'autorità di controllo deve disporre di determinati poteri d'indagine (art. 58 par. 1) ed è autorizzata ad adottare i provvedimenti correttivi previsti dal regolamento (UE) 2016/679 (art. 58 par. 2).

Il capo VII stabilisce meccanismi tesi a garantire l'applicazione coerente della legislazione sulla protezione dei dati all'interno dell'Unione europea. Prevede in particolare che in casi transfrontalieri in cui intervengono più autorità di controllo sia presa un'unica decisione. Tale principio, noto con il nome di «sportello unico», permette a un'impresa con filiali in diversi Stati membri di avere a che fare soltanto con l'autorità di controllo dello Stato membro in cui ha la sua sede principale. Tale autorità è designata come «autorità di controllo capofila» (art. 56). La cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate è retta dall'articolo 60. Tali autorità s'impegnano a trovare un consenso sul progetto di decisione preparato dall'autorità di controllo capofila. Il capo VII prevede inoltre l'assistenza reciproca tra le autorità di controllo (art. 61) e operazioni congiunte (art. 62).

Il capo VIII tratta i mezzi di ricorso, la responsabilità e le sanzioni. Secondo l'articolo 77, la persona interessata ha il diritto di proporre reclamo all'autorità di controllo. In virtù dell'articolo 78, la persona interessata ha altresì il diritto di proporre un ricorso giurisdizionale effettivo contro una decisione dell'autorità di controllo che la riguarda. L'articolo 80 prevede infine il diritto della persona interessata di farsi rappresentare a determinate condizioni e l'articolo 83 stabilisce le condizioni alle quali l'autorità di controllo è autorizzata a pronunciare multe.

Il capo IX contiene varie disposizioni che disciplinano situazioni particolari del trattamento di dati, in particolare in relazione alla libertà d'espressione e d'informazione (art. 85), all'accesso del pubblico ai documenti ufficiali (art. 86) nonché in riferimento al trattamento ai fini dell'archiviazione d'interesse pubblico, della ricerca e della statistica (art. 89).

4.2 Adeguamento della legislazione svizzera

In seno all'Unione europea il regolamento (UE) 2016/679 sostituirà la direttiva 95/46/CE. Le sue disposizioni non sono vincolanti per la Svizzera, poiché non si tratta di uno sviluppo dell'acquis di Schengen. Tuttavia ciò non significa che nel nostro Paese non esplichino effetto nei settori in cui esso è considerato un Paese terzo (settori al di fuori della cooperazione Schengen). Il regolamento è importante soprattutto per il settore privato. Infatti, come osservato al n. 1.2.2.2, la Commissione europea ha constatato mediante decisione[72] che la Svizzera garantisce un livello di protezione dei dati adeguato. Tale decisione può tuttavia essere revocata in qualsiasi momento. Inoltre, in seguito alla decisione Schrems, l'Unione europea ha deciso di seguire un approccio più dinamico e di esaminare permanentemente l'evoluzione della legislazione sulla protezione dei dati personali negli Stati terzi che beneficiano di una decisione di adeguatezza. Se intende beneficiare anche in futuro di una decisione di adeguatezza dell'Unione europea, la Svizzera, in quanto Stato terzo, ha pertanto l'interesse ad avvicinare la propria legislazione ai requisiti europei. I criteri definiti all'articolo 45 del regolamento (UE) 2016/679 saranno in futuro determinanti per giudicare l'adeguatezza della protezione dei dati prevista dalla legislazione svizzera. Il D-LPD è teso a permettere di garantire un livello di protezione adeguato ai sensi del regolamento.

5 Swiss-US Privacy Shield

Gli Stati Uniti non garantiscono un livello di protezione dei dati sufficiente. Per la comunicazione di dati personali dalla Svizzera a questo Stato si è pertanto resa necessaria l'adozione di un disciplinamento specifico, lo «Swiss-US Safe Harbor»[73], che corrisponde ampiamente a quello in vigore tra l'Unione europea e gli Stati Uniti, ossia l'«US-EU Safe Harbor», approvato dalla Commissione europea nel 2000[74]. Con questo disciplinamento specifico, gli Stati Uniti s'impegnano ad applicare i principi che garantiscono una protezione dei dati personali simile a quella della Svizzera e dell'Unione europea.

Il 6 ottobre 2015, la Corte di giustizia dell'Unione europea ha annullato la decisione dell'Unione europea che approvava il regime dell'US-EU Safe Harbor[75]. Ha constatato che la Commissione europea non aveva verificato se gli Stati Uniti rispettavano effettivamente, mediante la propria legislazione, i loro impegni internazionali che alcuna regola impediva allo Stato americano di usufruire di un accesso illimitato ai dati personali dei cittadini dell'Unione europea e che non esistevano strumenti giuridici efficaci contro tali ingerenze. A febbraio 2016, gli Stati Uniti e l'Unione europea hanno presentato una nuova regolamentazione, l'«EU-US Privacy Shield»,

72 GU L 215 del 25.8.2000, pag. 1.
73 In una missiva del 9 dic. 2008 al Dipartimento del commercio degli Stati Uniti, la Svizzera ha riconosciuto che lo «Swiss-US Safe Harbor» garantiva un livello adeguato di protezione conformemente all'art. 6 cpv. 1 LPD.
74 Decisione 2000/520/CE del 26 lug. 2000.
75 Sentenza CGUE del 6 ott. 2015 causa C-362/14 ECLI:EU:C:2015:650 (Schrems).

adottato dalla Commissione europea il 12 luglio 2016 e applicato dagli Stati Uniti il 1° agosto 2016.

In seguito alla summenzionata decisione della Corte di giustizia dell'Unione europea e al nuovo EU-US Privacy Shield, la Confederazione (Seco) ha rinegoziato le regole per la comunicazione di dati personali dalla Svizzera agli Stati Uniti. L'11 gennaio 2017, il nostro Consiglio ha preso atto di questa nuova regolamentazione, lo «Swiss-US Privacy Shield» (Privacy Shield), che corrisponde ampiamente alla soluzione in vigore tra gli Stati Uniti, da una parte, e l'Unione europea e lo Spazio economico europeo (SEE), dall'altra.

Mediante una serie di misure, il Privacy Shield migliora il meccanismo di applicazione delle regole da parte delle imprese americane. Le misure prevedono nuovi obblighi per le imprese americane (obbligo d'informare le persone interessate, obbligo di pubblicare le decisioni della Federal Trade Commission [FTC] o di un tribunale, obbligo di cooperare con il Dipartimento del commercio statunitense [DOC] o con l'Incaricato).

Il Privacy Shield rafforza altresì le competenze di gestione e di sorveglianza del DOC. Ad esempio, prima di iscrivere un'impresa nell'elenco del Privacy Shield, il DOC verifica che abbia descritto bene le attività per le quali ha chiesto informazioni dalla Svizzera, che abbia precisato quali informazioni sono contemplate dalla certificazione, nonché il modo di pubblicare la certificazione (sito Internet con link al sito del DOC o altro modo). Il DOC s'impegna anche a identificare false dichiarazioni di partecipazione al Privacy Shield e, in caso di mancata cancellazione delle informazioni errate da parte dell'impresa, a intraprendere passi giuridici e trasmettere il dossier alla FTC, al Dipartimento dei trasporti o a altri organi esecutivi.

È stato inoltre istituito un organo arbitrale che tratta i casi di violazione del Privacy Shield da parte di imprese con sede negli Stati Uniti, ai quali non si è rimediato con altri mezzi di ricorso e contro cui non sono state, parzialmente o del tutto, prese misure. Una persona il cui caso è già stato oggetto di un arbitrato o di un giudizio o il cui reclamo è già stato trattato precedentemente non ha accesso all'organo arbitrale. I cittadini svizzeri potranno sporgere reclamo dinanzi a questo organo e non dovranno assumersi le spese della procedura. L'organo arbitrale sarà finanziato da contributi delle imprese statunitensi.

Per rispondere alla preoccupazione europea riguardo all'uso abusivo di dati personali da parte dei servizi d'informazione degli Stati Uniti, il Dipartimento di Stato ha creato un Ombudsman, indipendente dai servizi d'informazione, incaricato di contattare questi ultimi su richiesta. L'Ombudsman fa rapporto direttamente al Segretario di Stato, il quale vigila affinché il primo eserciti la sua funzione in modo oggettivo.

Per l'Incaricato, lo Swiss-US Privacy Shield implica determinati obblighi di cooperazione. Trasmette i reclami al DOC e all'Ombudsman del Dipartimento di Stato. Visti il notevole aumento dell'outsourcing dei trattamenti di dati negli Stati Uniti e l'uso oggi molto diffuso in Svizzera di servizi di imprese americane quali Facebook, Google o Apple, è prevedibile una moltiplicazione dei reclami che dovrà trattare l'Incaricato. Se le imprese certificate si sono dichiarate disposte a collaborare con l'Incaricato, quest'ultimo deve inoltre sostenerle nella soluzione di problemi inerenti alla protezione dei dati. L'incaricato trasmette altresì le domande d'informazioni

all'Ombudsman del Dipartimento di Stato. Infine, deve verificare ogni anno, in collaborazione con gli uffici federali competenti (p. es. la Seco), la qualità delle misure previste dal Swiss-US Privacy Shield per tutelare i diritti della personalità delle persone interessate e stilare un rapporto.

6 Confronto con legislazioni di Stati non europei che non hanno ratificato la Convenzione STE 108

Per conoscere la situazione legislativa in alcuni Stato non membri dell'Unione europea e che non hanno ratificato la Convenzione STE 108, l'UFG ha conferito un pertinente mandato all'Istituto svizzero di diritto comparato. Lo studio[76] si è soprattutto soffermato sui punti seguenti: le competenze e l'indipendenza dell'autorità di controllo, l'esistenza di buone prassi, i diritti delle persone interessate (p. es. rimedi giuridici, mediazione), gli obblighi dei titolari del trattamento (p. es. obbligo di documentazione, analisi d'impatto sulla protezione dei dati), i Big Data, la profilazione, l'Internet degli oggetti, la portabilità dei dati e l'attuazione del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita.

Va osservato che l'adozione di una legislazione sulla protezione dei dati non è più un'esclusiva degli Stati europei.

6.1 Argentina

L'autorità di controllo dell'Argentina è la Direzione nazionale di protezione dei dati personali (Dirección Nacional de Protección de Datos Personales – DNPDP). I suoi compiti sono retti dall'articolo 29 della legge 25.326[77]. L'autorità di controllo svolge un ruolo di sostegno, consulenza e sorveglianza. L'articolo 29 del decreto 1558/2001[78] le permette di emanare regole amministrative e procedurali in relazione al registro delle banche di dati personali (registro), il quale permette di identificare e controllare tali banche dati. Secondo lo stesso articolo 29 la DNPDP può trattare i ricorsi e i reclami presentati conformemente alla legge 25.326. La DNDPD deve inoltre approvare i codici di condotta delle organizzazioni di rappresentanza degli utenti o dei titolari delle banche dati (art. 30 della legge 25.326).

L'articolo 14 della legge 25.326 sancisce un diritto d'accesso che conferisce alle persone interessate il diritto di ottenere informazioni sui loro dati personali contenuti in banche dati private o pubbliche. Una volta presentata la domanda, il titolare della banca dati ha dieci giorni di tempo per rispondere. Decorso tale termine, la persona interessata può adire la via del ricorso. L'articolo 16 consente alle persone fisiche di

76 Le informazioni si basano su una perizia dell'ISDC del 3 ago. 2016.

77 Ley 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: Octubre 4 de 2000, disponibile all'indirizzo www.jus.gob.ar/media/33481/ley_25326.pdf.

78 Decreto 1558/2001, Protección de los datos personales, disponibile all'indirizzo www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

chiedere la rettifica, l'aggiornamento e la cancellazione dei dati che le riguardano. I titolari delle banche dati hanno un termine di cinque giorni per rispondere alla richiesta e possono rifiutarla soltanto se necessario per la protezione dello Stato, dell'ordine o della sicurezza pubblici oppure degli interessi di terzi. Una volta decorso il termine di cinque giorni o in caso di risposta negativa, la persona interessata può interporre ricorso.

I titolari del trattamento hanno in particolare il compito di iscrivere la banca dati nel registro, vigilare sulla sicurezza dei dati raccolti, garantire la confidenzialità dei dati e fornire i documenti e le informazioni richiesti dalla DNPDP.

La legislazione sulla protezione dei dati si applica anche alla raccolta di megadati nel caso in cui l'insieme dei dati permette di identificare una persona specifica. Quanto alla profilazione, l'articolo 27 del decreto 1558/2001 contiene una regola per il settore della pubblicità. Secondo tale articolo si possono raccogliere, trattare e trasmettere dati senza il consenso della persona interessata, se l'obiettivo è creare profili per categorizzare preferenze e comportamenti. Tale possibilità è tuttavia soggetta a due condizioni: le persone interessate devono essere identificabili soltanto per la loro appartenenza a un gruppo generico e il numero di dati individuali raccolti deve essere limitato allo stretto necessario. Inoltre, in qualsiasi comunicazione a scopi pubblicitari deve essere menzionata la possibilità per la persona interessata di chiedere il ritiro o il blocco dei dati che la riguardano.

Infine, per quanto riguarda l'attuazione del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita, la DNPDP ha approvato una guida di buona prassi nello sviluppo di applicazioni informatiche destinata a chi sviluppa applicazioni. La guida ha soprattutto il compito di rammentare agli sviluppatori l'obbligo di rispettare la vita privata delle persone fin dalla progettazione dell'applicazione.

6.2 Nuova Zelanda

In Nuova Zelanda la protezione dei dati è retta principalmente dal «Privacy Act 1993»[79]. Attualmente è in corso una revisione di tale atto e il progetto dovrebbe essere presentato al Parlamento nel 2017.

La revisione riguarda soprattutto il ruolo dell'autorità pubblica incaricata di sorvegliare la protezione dei dati, il «Privacy Commissioner» (PC). Il ruolo del PC, già ora incaricato di approvare le regole di buona prassi, sarà rafforzato. Sarà infatti introdotto un sistema di dichiarazione obbligatoria delle violazioni dei dati, accompagnato da due miglioramenti per il PC. Esso potrà in futuro presentare richieste urgenti per ottenere informazioni che giudica necessarie e stendere un rapporto sulle violazioni del «Privacy Act».

79 Le «Privacy Act 1993» è disponibile al seguente indirizzo: www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

La revisione non si prefigge di rafforzare i diritti dei privati, considerati già sufficienti nel «Privacy Act 1993». La sua seconda parte, gli «Information Privacy Principles» (IPP), conferisce infatti dei diritti alle persone interessate. In particolare, l'IPP 6 permette alle persone interessate di chiedere se sono conservati dati che le riguardano e di avervi accesso. L'IPP 7 prevede che le persone interessate possano chiedere di correggere i dati che le riguardano e, se la domanda è respinta, di allegare ai dati una dichiarazione indicante che è stata presentata una richiesta di modificare i dati.

Attualmente tutti gli enti (Agency)[80] devono garantire che al loro interno vi sia almeno un «Privacy Officer» (PO) i cui obblighi statutari sono: promuovere la conformità con i vari IPP, occuparsi delle domande presentate all'organismo e collaborare con il PC nelle indagini riguardanti l'ente. La revisione prevede due importanti modifiche per gli obblighi degli enti: l'obbligo di comunicare al PC determinate violazioni della protezione dei dati e di adottare i provvedimenti adeguati per disporre di una protezione dei dati adeguata in occasione degli scambi con altri Stati.

Il PC svolge un ruolo importante per l'attuazione del principio della protezione fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default). Infatti, la sezione 13(1)(n) del «Privacy Act 1993» gli conferisce la possibilità di fare ricerche e seguire l'evoluzione del trattamento dei dati e delle nuove tecnologie informatiche e soprattutto di provvedere affinché gli effetti negativi di tale evoluzione sulla tutela della vita privata siano ridotti al minimo. Ciò gli permette di promuovere la protezione dei dati fin dalla progettazione. La revisione non prevede altre regole per la protezione fin dalla progettazione e per impostazione predefinita.

6.3 Corea del Sud

Dal 2011 la Corea del Sud dispone di una legislazione nel settore della protezione dei dati, il «Personal Information Protection Act» (PIPA).

A causa della sua storia e delle sue numerose leggi, la Corea del Sud ha un sistema assai complesso che prevede varie autorità che si occupano della protezione dei dati. Per le questioni regolamentari la responsabilità compete alla «Personal Information Protection Commission». Il «Personal Information Dispute Mediation Committee» è invece incaricato della mediazione in caso di azioni individuali o collettive. In occasione di divergenze tra le persone interessate e l'istituzione che tratta i dati, tale comitato può presentare una proposta di conciliazione (art. 47 PIPA). Le azioni legate alle tecnologie dell'informazione sono trattate dalla «Korea Internet & Security Agency», che ha una hotline e ha inoltre elaborato una serie di guide e raccomandazioni per il settore privato. Il Ministero dell'interno svolge un ruolo importante nell'attuazione della legislazione sulla protezione dei dati. Gli spetta infatti l'elaborazione di un piano di base per la protezione dei dati («Data Protection Basic Plan»), valido per tre anni (art. 9 PIPA), e di direttive (art. 12 PIPA).

80 È considerata «Agency» praticamente qualsiasi persona od organizzazione che detiene dati personali.

Secondo l'articolo 4 PIPA, i privati hanno il diritto di informarsi sul trattamento dei dati che li riguardano. Hanno anche il diritto di chiedere la cancellazione o la rettifica di determinati dati. La legge prevede altresì il diritto al rimborso dei danni.

Per trattare i dati, il titolare del trattamento deve ottenere il consenso della persona interessata (art. 22 PIPA). Il titolare ha inoltre l'obbligo di informare la persona interessata quando tratta dati ricevuti da terzi (art. 20 PIPA). Infine, deve distruggere i dati alla scadenza del termine convenuto o dopo aver adempito il suo compito (art. 21 PIPA). Il capitolo IV PIPA fissa le garanzie che il titolare del trattamento deve rispettare. In particolare, l'articolo 29 obbliga i responsabili ad adottare tutte le misure fisiche, tecniche e amministrative per prevenire la perdita, il furto, la diffusione, la falsificazione o la distruzione dei dati. I dati devono essere trattati in modo da ridurre al minimo i rischi di violazione della vita privata (art. 3 par. 6 PIPA) e anonimizzandoli (art. 3 par. 7 PIPA).

Il titolare del trattamento in un'impresa deve inoltre adottare e pubblicare una strategia di protezione dei dati (privacy policy; art. 30 PIPA). È inoltre richiesta la nomina di un consulente per la protezione dei dati (privacy officer; art. 31 PIPA). Le istituzioni pubbliche devono, da parte loro, registrare le proprie raccolte di dati (art. 32 PIPA) e procedere a un'analisi d'impatto del trattamento (art. 35 PIPA), anch'esso da registrare.

6.4 Giappone

Dal 2016 il Giappone dispone di un'autorità di controllo della protezione dei dati (Personal Information Protection Commission) che esercita funzioni di sorveglianza, regolamentazione e mediazione. Altre due istituzioni meritano di essere menzionate. Nel settore privato, la legge sulla protezione dei dati (Act on the Protection of Personal Information [APPI])[81], adottata nel 2003, permette a organizzazioni private di protezione dei dati accreditate dal Governo di trattare i ricorsi contro le imprese e di fornire informazioni che contribuiscono a migliorare l'applicazione della protezione dei dati; esse hanno inoltre la possibilità di adottare i provvedimenti necessari all'attuazione dei principi della protezione dei dati (art. 37 APPI). Nel settore pubblico l'«Information Disclosure and Personal Information Protection Review Board» è l'autorità cui compete garantire la protezione dei dati nelle indagini in materia di trasparenza.

L'APPI conferisce ai privati il diritto di ottenere informazioni sull'esistenza e lo scopo di un trattamento di dati (art. 24 cpv. 2 e 25 APPI). Per il trattamento della richiesta può essere riscosso un emolumento (art. 30 APPI). Inoltre, le persone interessate possono chiedere la rettifica, l'integrazione o la soppressione di dati errati. In tale contesto il titolare del trattamento dei dati ha il compito di esaminare i reclami presentati e d'informare la persona interessata in caso di rifiuto della richiesta (art. 30 APPI). I privati possono anche ottenere la sospensione o il blocco del trattamento, se esso è contrario al suo scopo o se i dati sono stati ottenuti illecitamente.

81 L'APPI è disponibile in inglese al seguente indirizzo: www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

Una tale domanda non è tuttavia ammissibile quando potrebbe creare costi elevati o quando si rivela troppo complicata e il titolare del trattamento ha adottato altre misure per proteggere i dati e gli interessi della persona interessata (art. 27 APPI). Gli stessi principi si applicano al trasferimento di dati a terzi (art. 27 cpv. 2 APPI).

Il titolare del trattamento deve specificare lo scopo del trattamento nel modo più preciso possibile (art. 15 lett. f APPI). Inoltre, le informazioni relative allo scopo del trattamento e ai diritti delle persone interessate devono essere a disposizione del pubblico (art. 24 APPI). Il titolare del trattamento deve altresì ottenere il consenso, anche solo implicito, della persona interessata. Il titolare non può procurarsi dati con mezzi fraudolenti o illeciti (art. 17 APPI) e deve sforzarsi a garantire la correttezza dei dati. Il trasferimento di dati a terzi è consentito soltanto in determinati casi specifici (per esempio per proteggere la vita e l'integrità fisica di una persona o la salute pubblica o nell'ambito della cooperazione con le autorità; art. 23 APPI). In generale, devono essere adottate misure di sicurezza per evitare la perdita o il danneggiamento dei dati (art. 20 APPI) e le persone incaricate del trattamento di dati devono sottostare a una sorveglianza (art. 21 lett. f APPI). Per contro, la legge non prevede alcun obbligo d'informazione in caso di perdita dei dati.

A parte l'articolo 20 APPI già menzionato, non sembrano esserci misure specifiche tese a promuovere il principio della protezione dei dati fin dalla progettazione e per impostazione predefinita. È tuttavia probabile che l'autorità di sorveglianza adotti prossimamente provvedimenti in tal senso.

6.5 Singapore

L'autorità di controllo è la «Personal data protection commission» (PDPC). È stata istituita nel 2013 in attuazione del «Personal Data Protection Act[82]» (PDPA), entrato in vigore nel 2012. La PDPC esercita, tra le altre cose, una funzione di sorveglianza e di regolamentazione del trattamento di dati da parte di organi privati (il PDPA non si applica al settore pubblico). Può emanare direttive o decisioni per garantire il rispetto del PDPA e in caso di violazione della legge può pronunciare multe fino a un milione di dollari (art. 28 e 29 PDPA). La PDPC dispone di importanti strumenti d'indagine, dal diritto di penetrare in proprietà private a quello di esigere informazioni e documenti che possono essere sequestrati (allegato 9 PDPA). Può anche cercare di risolvere le controversie mediante una mediazione (art. 27 PDPA). Inoltre, ha il compito di elaborare e attuare politiche ufficiali (p. es. tramite l'adozione di direttive) tese a sensibilizzare le varie organizzazioni e i privati al rispetto della protezione dei dati. Infine, la PDPC rappresenta il governo di Singapore su scala internazionale in tutte le questioni inerenti alla protezione dei dati (art. 6 PDPA).

Le persone interessate possono chiedere accesso ai loro dati personali raccolti o controllati da un organismo. Hanno anche il diritto di ottenere informazioni sul modo in cui i loro dati personali sono stati utilizzati o diffusi nell'anno precedente la loro

82 Il PDPA è disponibile in inglese al seguente indirizzo: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0.

domanda, a condizione che non vi si opponga un interesse pubblico o privato preponderante (art. 21 PDPA). Le persone interessate possono infine esigere la correzione di un errore o di un'omissione nei loro dati personali (art. 22 PDPA).

I titolari del trattamento sono in linea di massima tenuti a ottenere il consenso esplicito o tacito delle persone interessate dal momento in cui raccolgono, utilizzano o diffondono dati personali. La condizione del consenso della persona interessata è tuttavia meno severa che negli altri ordinamenti giuridici analizzati. Infatti, il diritto di Singapore prevede numerose eccezioni in cui il consenso non è necessario o può essere presupposto (art. 13–15 PDPA). Il trattamento dei dati deve essere effettuato per uno scopo noto alla persona interessata o che appaia ragionevole a qualsiasi persona che si trovi nelle stesse circostanze (art. 18 PDPA). Il titolare del trattamento deve provvedere a garantire la correttezza dei dati (art. 23 PDPA) e ad adottare i provvedimenti cautelari per evitare la fuga, la copia o l'accesso non autorizzato ai dati personali in suo possesso (art. 24 PDPA). Deve inoltre distruggere o rendere anonimi i dati personali non appena la loro conservazione non corrisponde più allo scopo per cui sono stati raccolti e alcun motivo giuridico o economico permette di giustificarne la conservazione (art. 25 PDPA). Infine, la comunicazione di dati personali all'estero è autorizzata soltanto se lo Stato destinatario garantisce un livello di protezione equivalente a quello di Singapore (art. 26 PDPA).

Non sembrano essere state adottate misure specifiche per promuovere il principio della protezione dei dati fin dalla progettazione e per impostazione predefinita. Tuttavia, la competenza di effettuare campagne di sensibilizzazione alla protezione dei dati, che la legge conferisce alla PDPC (art. 6 PDPA), potrebbe permetterle di promuovere tali misure.

7 Attuazione

Nel quadro AIR è stato suggerito di evitare, per quanto possibile, termini giuridici indefiniti. La LPD è tuttavia una legge quadro che prescinde dalle tecnologie utilizzate, deve essere applicabile a una moltitudine di casi diversi e potersi sviluppare in modo dinamico. I codici di condotta permettono di precisare determinate nozioni come pure le modalità di determinati diritti e obblighi, tenendo conto delle caratteristiche dei diversi settori. Inoltre, anche in futuro l'Incaricato potrà elaborare guide e altri strumenti di lavoro per sostenere i titolari e i responsabili del trattamento nell'adempimento dei loro compiti e le persone interessate nell'esercizio dei loro diritti.

Inoltre, per non sovraccaricare la legge, è previsto di adeguare l'ordinanza del 14 giugno 1993[83] relativa alla legge sulla protezione dei dati (OLPD).

Anche se il disegno di legge non prevede esplicitamente la valutazione della sua attuazione, l'efficacia delle sue misure sarà esaminata conformemente all'articolo 170 Cost. Inoltre, come sinora, l'Incaricato dovrà presentare periodicamente un rapporto d'attività all'Assemblea federale. Le informazioni contenute in tale rapporto permetteranno di usufruire di una panoramica dell'attuazione della nuova LPD.

83 RS **235.11**

Infine, nella misura in cui il recepimento della direttiva (UE) 2016/680 e la ratifica del Protocollo d'emendamento alla Convenzione STE 108 da parte svizzera vincolano anche i Cantoni, questi devono adeguare le norme che non adempiono le condizioni di questi strumenti.

8 Stralcio di interventi parlamentari

I seguenti interventi parlamentari possono essere tolti dal ruolo:

- Postulato Hodgers 10.3383 «Adeguare la legge sulla protezione dei dati alle nuove tecnologie». Rivedendo la LPD per adeguarla alle nuove tecnologie, il nostro Consiglio adempie il postulato.
- Postulato Graber 10.3651 «Attacchi alla sfera privata e minacce indirette alle libertà individuali». Questo postulato è stato in parte adempito dal rapporto di valutazione della LPD. Con il presente progetto di revisione il nostro Consiglio dà seguito alle questioni restanti, riguardanti i limiti che intende porre alle tecnologie di sorveglianza e di raccolta dei dati nonché l'opportunità di proporre un consolidamento della legislazione a tutela della sfera privata e dei dati personali.
- Postulato Schwaab 12.3152 «Diritto all'oblio in Internet». Il nostro Consiglio ha esaminato l'opportunità di disciplinare o precisare nella legislazione il diritto all'«oblio in Internet» e le modalità per agevolarne l'uso da parte dei consumatori. Il diritto all'oblio, in Internet o in generale, è già previsto dalla LPD. Menzionando esplicitamente il «diritto alla cancellazione» nel D-LPD, intendiamo facilitare la comprensione della legge alle persone interessate. Disposizioni più dettagliate di questioni relative a Internet sarebbero contrarie al carattere tecnologicamente neutro della legge. Per questo ambito, secondo il nostro Consiglio è preferibile ricorrere ai codici di condotta delle cerchie interessate e alle guide dell'Incaricato.
- Postulato Recordon 13.3989 «Violazioni della personalità riconducibili al progresso delle tecnologie dell'informazione e della comunicazione». Nel contesto dei lavori di revisione il nostro Consiglio ha esaminato le nuove minacce per i diritti della personalità. Il D-LPD prevede misure per migliorare la tutela di tali diritti.
- Mozione Comte 14.3288 «Rendere l'usurpazione d'identità un reato penale a sé stante». La mozione è stata adempita con l'introduzione nel CP dell'articolo 179^{decies}.
- Postulato Derder 14.3655 «Definire la nostra identità digitale e identificare le soluzioni per proteggerla». Il nostro Consiglio ha valutato l'opportunità di definire l'identità digitale nell'ambito della revisione, rinunciandovi a causa del carattere tecnologicamente neutro della legge. Le misure proposte permettono tuttavia di migliorare la protezione dell'identità digitale dei cittadini. Inoltre, la questione dell'identità digitale sarà approfondita nell'ambito dei lavori del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati che si concluderanno nel 2018.

- Postulato Schwaab 14.3739 «Control by design. Potenziare i diritti di proprietà per impedire le connessioni indesiderate». Il D-LPD adempie parzialmente il postulato in quanto migliora la protezione delle persone interessate. Le altre questioni sollevate dal postulato, ossia la sicurezza dei prodotti e di Internet, saranno approfondite nell'ambito dei lavori del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati.
- Postulati Gruppo liberale radicale 14.4137 e Comte 14.4284 «Registrazioni video di privati. Migliorare la tutela della sfera privata». Il D-LPD prevede di inasprire le disposizioni penali della legge. In futuro, la raccolta di dati in violazione dell'obbligo d'informare – obbligo che nel settore privato è esteso a tutti i tipi di dati – potrà essere sanzionato in modo più efficace. La modifica, in combinazione con le disposizioni vigenti sulla violazione del segreto e della sfera privata, offre una protezione più estesa. Il D-LPD stabilisce che sussiste un rischio elevato per la personalità o i diritti fondamentali della persona interessata, che obbliga il titolare del trattamento a effettuare una valutazione d'impatto sulla protezione dei dati, in particolare quando sono sorvegliati sistematicamente luoghi pubblici (art. 20 cpv. 2 lett. c D-LPD).
- Postulato Béglé 16.3383 «Dati digitali. Informare le persone lese in caso di pirateria». Secondo l'articolo 22 D-LPD la violazione della sicurezza dei dati deve essere comunicata all'Incaricato e, in determinate circostanze, deve essere informata anche la persona interessata. Il contenuto della comunicazione o dell'informazione sarà precisato nell'ordinanza.
- Postulato Béglé 16.3384 «Dati medici digitali. Garantire una raccolta protetta, trasparente e mirata nella revisione della legge federale sulla protezione dei dati». La legge sulla protezione dei dati si applica ai dati medici, salvo disposizioni contrarie in una legge speciale. Il D-LPD prevede diversi obblighi del titolare e del responsabile del trattamento che si applicano, se del caso, anche ai dati medici. Questi obblighi tengono conto delle richieste del postulato. Ulteriori misure, quali ad esempio il rafforzamento delle competenze dell'Incaricato e delle sanzioni penali come l'elaborazione di codici di condotta e di guide, dovrebbero portare a una maggiore protezione anche per i dati medici.

I seguenti interventi parlamentari possono essere tolti parzialmente dal ruolo:

- Postulato Schwaab 14.3782 «Regole per la ‹morte digitale›». L'articolo 16 D-LPD prevede il diritto di accedere ai dati di una persona deceduta e permette inoltre agli eredi o all'eventuale esecutore testamentario di chiedere la cancellazione dei suoi dati. Pertanto il D-LPD attua alcune richieste fondamentali del postulato. Altre richieste saranno esaminate nell'ambito della revisione del diritto successorio.
- Postulato Derder 15.4045 «Diritto all'utilizzo dei dati personali. Diritto alla copia». Il nostro Consiglio ritiene che nell'ambito della revisione della LPD non sia opportuno introdurre un diritto di portabilità dei dati (cfr. n. 1.7.4). La questione sarà esaminata nel quadro della «Strategia Svizzera digitale» (cfr. n. 1.1.3).

– Postulato Béglé 16.3386 «Riappropriazione dei dati personali. Favorire l'‹autodeterminazione informatica›». Per gli stessi motivi addotti per il diritto di portabilità dei dati (cfr. n. 1.7.4), il D-LPD non prevede alcuna precisazione in merito alla riappropriazione dei dati personali. La questione sarà esaminata nell'ambito della «Strategia Svizzera digitale» (cfr. n. 1.1.3).
– Postulato Schwaab 16.3682 «Inquadrare le prassi delle società che forniscono dati sulla solvibilità». Poiché si tratta di una normativa generale, il D-LPD non prevede disposizioni tese a regolare specificamente le attività delle società che forniscono dati sulla solvibilità. Ciononostante la protezione delle persone interessate è rafforzata, poiché il D-LPD amplia i loro diritti, la trasparenza dei trattamenti, gli obblighi dei titolari del trattamento e la sorveglianza dell'Incaricato. Inoltre, il D-LPD prevede condizioni più severe per i motivi giustificativi che permettono al titolare del trattamento di trattare dati personali allo scopo di valutare la solvibilità della persona interessata (art. 27 cpv. 2 lett. c D-LPD). Nel rapporto in adempimento al presente postulato, il nostro Consiglio intende esaminare l'opportunità di una legislazione specifica sulle attività delle società che forniscono dati sulla solvibilità e le soluzioni ipotizzabili.

9 Commento ai singoli articoli

9.1 Commento agli articoli del D-LPD

9.1.1 Ingresso

Riteniamo opportuno introdurre nell'ingresso l'articolo 97 capoverso 1 Cost., che conferisce alla Confederazione la competenza di legiferare sulla protezione dei consumatori. Infatti, il D-LPD contiene infatti un certo numero di disposizioni che rafforzano in particolare la trasparenza dei trattamenti di dati personali, il controllo da parte delle persone interessate e il sistema di sorveglianza da parte dell'Incaricato. Tali disposizioni migliorano la protezione dei consumatori.

9.1.2 Scopo e campo d'applicazione nonché autorità di vigilanza della Confederazione

Art. 1 Scopo

Lo scopo della nuova LPD è identico a quello della legge in vigore (art. 1 LPD). La LPD concretizza, in relazione ai dati personali, il diritto all'autodeterminazione informativa di cui all'articolo 13 capoverso 2 Cost., ossia il diritto della persona interessata di poter decidere in linea di massima autonomamente se e a quale scopo possono essere trattati i dati che la riguardano[84].

[84] DTF **140** I 2, consid. 9.1

La disposizione è modificata soltanto sotto il profilo redazionale con l'esplicita menzione che la protezione è limitata alle persone fisiche. L'adeguamento è una conseguenza della modifica del campo d'applicazione (cfr. il commento all'art. 2 D-LPD).

Art. 2 Campo d'applicazione

Il presente disegno estende parzialmente il campo d'applicazione della LPD, in particolare per soddisfare i requisiti del P-STE 108. Prevede di adeguare le deroghe per i procedimenti civili, penali e di assistenza giudiziaria internazionale pendenti, come pure per quelli di diritto pubblico e di diritto amministrativo (art. 2 cpv. 2 lett. c LPD), nonché quelle per i registri pubblici relativi ai rapporti di diritto privato (art. 2 cpv. 2 lett. d LPD).

Va inoltre osservato che, alla stregua del diritto vigente, il D-LPD disciplina la protezione dei dati in generale. Se il trattamento di dati rientra nel campo d'applicazione di altre leggi federali, in virtù della regola della lex specialis (secondo cui le norme speciali prevalgono sulle norme generali) si applicano in linea di massima le norme sulla protezione dei dati specifiche a un determinato settore[85].

Cpv. 1 Applicazione alle persone private

Secondo il disegno, la LPD si applica al trattamento di dati di persone fisiche da parte di privati e organi federali.

Rinuncia alla protezione dei dati di persone giuridiche

Il D-LPD prevede di rinunciare alla protezione dei dati delle persone giuridiche poiché gli atti normativi dell'Unione europea e del Consiglio d'Europa sulla protezione dei dati, come pure la maggior parte dei legislatori esteri, non contemplano tale protezione. La sua importanza pratica è limitata e l'Incaricato non ha mai emanato una raccomandazione in materia. D'altronde resta immutata l'ampia protezione garantita dagli articoli 28 e seguenti (lesioni della personalità, ad esempio della reputazione) del Codice civile (CC)[86], dalla LCSl, dalla legge federale del 9 ottobre 1992[87] sul diritto d'autore o dalle regole sul segreto professionale, d'affari o di fabbricazione, nonché dall'articolo 13 Cost. La rinuncia permette di migliorare la protezione nei settori in cui vi sono lacune nell'attuazione, garantendo nel contempo maggiore credibilità alla legge[88]. Questa soluzione ha anche il vantaggio che la comunicazione all'estero di dati riguardanti persone giuridiche non è più soggetta alla condizione che lo Stato destinatario garantisca un livello di protezione adeguato (art. 13 D-LPD), il che dovrebbe favorire il flusso internazionale di dati. È infine importante osservare che la maggior parte degli esperti consultati nell'ambito dell'AIR relativa alla revisione della LPD e la maggior parte dei partecipanti alla consultazione si sono dette favorevoli a rinunciare alla protezione dei dati delle

85 Cfr. DTF **128** II 311 consid. 8, FF **1988** II 353, in particolare pag. 384 e Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 286 segg.
86 RS **210**
87 RS **231.1**
88 In merito alla questione cfr. DECHSLER CHRISTIAN, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, AJP 2016, pag. 80 segg., pag. 85–86.

persone giuridiche[89]. Lo stesso vale per il Parlamento, che ha rifiutato di dare seguito a una mozione che proponeva di mantenere la protezione dei dati delle persone giuridiche[90].

Quanto al trattamento di dati da parte di organi federali, l'abrogazione della protezione dei dati personali delle persone giuridiche implica che le basi legali previste dal diritto federale autorizzanti gli organi federali a trattare dati personali non si applicano quando detti organi trattano informazioni riguardanti persone giuridiche. Dato che l'articolo 5 Cost. esige che l'attività dello Stato sia retta dalla legge, il presente disegno di legge introduce nella LOGA una serie di disposizioni che disciplinano il trattamento di dati di persone giuridiche (cfr. n. 9.2.8). Inoltre, una disposizione transitoria è tesa ad evitare eventuali lacune nella legge durante un periodo di cinque anni. (cfr. n. 9.1.11).

La legge del 17 dicembre 2004[91] sulla trasparenza (LTras) conferisce a ogni persona il diritto di consultare i documenti ufficiali delle autorità federali soggette al principio della trasparenza. Dal nuovo campo d'applicazione del D-LPD consegue che l'accesso a documenti ufficiali che contengono dati su persone giuridiche non può più essere limitato per motivi inerenti alla protezione dei dati. Una limitazione è possibile soltanto se l'informazione può comportare la rivelazione di segreti professionali, di fabbricazione o d'affari (art. 7 cpv. 1 lett. g LTras) o se sussiste il rischio di una lesione della sfera privata della persona giuridica, ad esempio della buona reputazione. Per tutelare i diritti delle persone giuridiche nel caso in cui una domanda si riferisca a documenti ove la concessione dell'accesso potrebbe pregiudicare la loro sfera privata, il D-LPD adegua alcune disposizioni della LTras (cfr. n. 9.2.7).

In seguito all'abrogazione della protezione dei dati delle persone giuridiche, queste non possono più far valere il diritto d'accesso in virtù del D-LPD. Possono tuttavia far valere i loro diritti procedurali ed eventualmente chiedere l'accesso ai documenti pubblici in virtù della LTras, se tali documenti contengono informazioni che le riguardano.

Cpv. 2 Deroghe al campo d'applicazione

Come sinora, la LPD non si applica al trattamento di dati da parte di persone fisiche per uso esclusivamente personale (lett. a); l'adeguamento redazionale non implica modifiche materiali.

Continua a essere escluso dal campo d'applicazione anche il trattamento di dati personali effettuato dalle Camere federali e dalle commissioni parlamentari nell'ambito dei loro dibattiti (lett. b), per i motivi già illustrati nel messaggio del 23 marzo 1988[92].

Secondo la lettera c, i beneficiari istituzionali di cui all'articolo 2 capoverso 1 della legge del 22 giugno 2007[93] sullo Stato ospite (LSO) che godono dell'immunità in Svizzera non sottostanno al D-LPD. In tal modo si mantiene la situazione vigente

89 Cfr. pag. 46 AIR.
90 Mozione Béglé 16.3379 «Promuovere la Svizzera quale cassaforte digitale universale».
91 RS **152.3**
92 FF **1988** II 353, in particolare pag. 381.
93 RS **192.12**

concernente il Comitato internazionale della Croce Rossa (CICR) e si menzionano esplicitamente anche gli altri beneficiari istituzionali. In virtù del diritto internazionale e della LSO, questi beneficiari istituzionali godono dell'indipendenza e della libertà d'agire necessarie affinché possano assolvere la loro funzione. Da uno Stato non si può pretendere che, in riferimento al trattamento di dati da parte delle sue rappresentanze diplomatiche e consolari, si sottoponga alle norme del diritto svizzero. Da parte sua, la Svizzera non è tenuta a rispettare le norme estere sulla protezione dei dati nella sua rete di rappresentanze all'estero. Anche da un'organizzazione internazionale, che per definizione opera in numerosi Stati, non si può pretendere che rispetti le condizioni del diritto nazionale di ciascuno Stato in cui opera, poiché ciò le impedirebbe di assolvere le funzioni attribuitele in virtù del proprio statuto.

Cpv. 3 Trattamento di dati personali nei procedimenti

Secondo l'articolo 2 capoverso 3 D-LPD il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali sono retti dal diritto procedurale applicabile. La norma disciplina il rapporto tra la LPD e il diritto procedurale e stabilisce come principio generale che le modalità del trattamento di dati personali e i diritti delle persone interessate nell'ambito di procedimenti sono rette esclusivamente dal diritto procedurale applicabile. Il diritto procedurale garantisce anch'esso la tutela della personalità e dei diritti fondamentali di tutte le persone coinvolte assicurando così una protezione equivalente a quella della LPD. Se in questo settore si applicasse la LPD, si correrebbe il rischio di un conflitto normativo e di contraddizioni, che potrebbero intaccare il ponderato sistema del diritto procedurale applicabile. Per questi motivi anche l'articolo 9 numero 1 lettera a P-STE 108 prevede un'eccezione analoga. Sotto il profilo materiale il disciplinamento del D-LPD corrisponde al diritto vigente.

La deroga del capoverso 3 si applica ai «procedimenti giudiziari». Di questi fanno parte tutti i procedimenti dinanzi a tribunali penali, civili e amministrativi cantonali o federali, ma anche dinanzi a tribunali arbitrali con sede in Svizzera. Inoltre, la deroga riguarda tutti i procedimenti secondo gli ordinamenti procedurali federali, a prescindere dall'autorità che li conduce. Fanno parte degli ordinamenti procedurali federali segnatamente la legge del 17 giugno 2005[94] sul Tribunale federale (LTF), la legge del 17 giugno 2005[95] sul Tribunale amministrativo federale (LTAF), la legge del 20 marzo 2009[96] sul Tribunale federale dei brevetti (LTFB), la PA, nella misura in cui non si tratti della procedura amministrativa di prima istanza, il Codice di procedura civile[97] (CPC), la legge federale dell'11 aprile 1889[98] sulla esecuzione e sul fallimento (LEF), il CPP, la DPA, la Procedura penale militare del 23 marzo 1979[99] (PPM) e l'AIMP.

94 RS **173.110**
95 RS **173.32**
96 RS **173.41**
97 RS **272**
98 RS **281.1**
99 RS **322.1**

A differenza del diritto vigente, il D-LPD rinuncia al termine «procedimento pendente». Poiché si parla di litispendenza soltanto nel diritto di procedura civile, il termine ha a volte creato problemi di delimitazione. Come criterio determinante è ora previsto il fatto che un procedimento si svolga dinanzi a un giudice o sia disciplinato da un ordinamento procedurale federale. Un procedimento si svolge dinanzi a un giudice se quest'ultimo si occupa per la prima volta di un caso per il quale il procedimento è stato avviato conformemente all'ordinamento procedurale determinante. Un procedimento è disciplinato dagli ordinamenti procedurali federali non appena un'autorità tratta una determinata fattispecie conformemente alle disposizioni di una delle suddette leggi. L'ordinamento procedurale determinante resta applicabile anche dopo la conclusione del procedimento. Affinché la situazione degli atti non venga modificata posteriormente da elementi estranei al procedimento, il diritto procedurale prevede procedure specifiche per la cura, la consultazione e la conservazione degli atti. Riassumendo, il criterio determinante per l'applicabilità o meno della LPD, è l'assenza o la presenza, sotto il profilo funzionale, di un rapporto diretto con un procedimento (giudiziario). Un tale rapporto sussiste se il trattamento di dati personali in questione può avere ripercussioni concrete sul procedimento o sul suo esito oppure sui diritti procedurali delle parti.

Nei casi in cui si applica la disposizione di cui al capoverso 3, il trattamento di dati personali e i diritti delle persone interessate sono retti esclusivamente dal diritto procedurale. Sia i trattamenti di dati effettuati dai tribunali nei confronti delle parti sia quelli effettuati da una parte nei confronti delle altre parti sono retti dal diritto procedurale applicabile. Ciò vale in particolare per i diritti delle parti di conoscere i dati che confluiscono nel procedimento, come pure il trattamento di dati nell'ambito dei procedimenti giudiziari in generale. Questo significa che i vari rimedi giuridici previsti dalla LPD non sono applicabili né al trattamento di dati da parte dei tribunali nell'ambito di un procedimento né al trattamento di dati da parte di altre parti coinvolte. Le parti del procedimento non possono ad esempio far valere il diritto di accedere ai dati secondo la LPD per ottenere dal giudice la consultazione degli atti o per acquisire prove presso le altre parti del procedimento (cfr. n. 9.1.5). In altre parole, nei confronti del giudice o di altre parti coinvolte non si può procedere, appellandosi alla LPD, ad atti rilevanti per il procedimento che sono esclusi dal diritto procedurale applicabile o che sono consentiti solo a determinate condizioni e secondo determinate regole o principi. Poiché devono coincidere con il risultato del procedimento, anche gli atti di un procedimento chiuso possono essere modificati (rettifica, spiegazione, revisione) soltanto conformemente al diritto procedurale. Non è tuttavia escluso che dopo la conclusione del procedimento, il diritto procedurale preveda l'applicabilità della LPD (cfr. art. 99 CPP). Se il pertinente diritto procedurale non disciplina il diritto d'accesso di terzi dopo la conclusione del procedimento, andrebbero applicate le disposizioni della legge sulla protezione dei dati.

A differenza dell'avamprogetto posto in consultazione, in seguito alle critiche espresse in tale sede, il capoverso 3 non esclude più soltanto il trattamento di dati di determinate istituzioni dal campo d'applicazione della LPD, ma anche il trattamento da parte delle parti. Inoltre il conflitto di norme è risolto in altro modo, in quando è determinante la norma del diritto applicabile. In particolare per i tribunali della Confederazione, questo significa tuttora che, per quanto riguarda il trattamento di

dati nell'ambito della loro attività giurisdizionale, non rientrano nel campo d'applicazione della LPD. In tal modo si rispetta la separazione dei poteri.

Dall'articolo 2 capoverso 3 risulta, a contrario, che la LPD è applicabile al trattamento di dati da parte dei servizi amministrativi dei tribunali e delle autorità, ad esempio al trattamento dei dati sul personale[100]. Inoltre, quando archiviano mezzi di prova e decisioni i tribunali devono rispettare le pertinenti disposizioni sulla sicurezza dei dati. Sono tuttavia previste delle eccezioni alla sorveglianza dell'Incaricato (cfr. art. 3 cpv. 2 D-LPD e il relativo commento).

In virtù del secondo periodo, la disposizione dell'articolo 2 capoverso 3 D-LPD non si applica alle procedure amministrative di prima istanza. Tale regola è ripresa senza modifiche dal diritto vigente.

Cpv. 4 Registri pubblici relativi ai rapporti di diritto privato

La deroga riguardante i registri pubblici relativi ai rapporti di diritto privato prevista dall'articolo 2 capoverso 2 lettera d LPD non è compatibile con l'articolo 3 del P-STE 108. Infatti, la futura Convenzione non prevede deroghe per questo tipo di registri e lo stesso vale per il regolamento (UE) 2016/679.

Le persone interessate hanno il diritto di pretendere che i registri pubblici relativi ai rapporti di diritto privato rispettino i principi della protezione dei dati personali. Tuttavia, sussiste anche un interesse pubblico alla tenuta di questi registri e alla loro consultazione (cfr. consid. 73 del regolamento (UE) 2016/679). In una decisione del 9 marzo 2017[101], la Corte di giustizia dell'Unione europea (CGUE) si è pronunciata sul rapporto tra la protezione dei dati e la pubblicità di un registro delle imprese tenuto dalle autorità italiane. Nella causa in questione un ex amministratore e liquidatore di un'impresa dichiarata fallita chiedeva la cancellazione dal registro di determinati dati personali che lo riguardavano. Per risolvere la controversia la Corte di cassazione italiana ha chiesto alla Corte di giustizia di esaminare se il principio della conservazione dei dati previsto dall'articolo 6 paragrafo 1 lettera e della direttiva 95/46/CE, secondo cui i dati a carattere personale sono conservati in una forma che permette l'identificazione della persona interessata per una durata non superiore a quella necessaria per raggiungere le finalità per le quali tali dati sono stati trattati, prevalga sul principio della pubblicità del registro delle imprese previsto dalla prima direttiva 68/181/CE[102].

Secondo la Corte di giustizia, la pubblicità del registro delle imprese mira a garantire la certezza del diritto nelle relazioni tra le società e i terzi e a permettere a questi ultimi di accedere agli atti essenziali della società in questione e a determinati dati riguardanti le persone che hanno il potere di rappresentarla. La pubblicità di tali informazioni è giustificata anche dopo lo scioglimento di una società. In vista di un'eventuale azione penale può infatti rivelarsi necessario verificare ad esempio la legalità di un atto compiuto da una società durante la sua attività. Secondo la Corte

100 Cfr. FF **1988** II 353, in particolare pag. 383.
101 Sentenza CGUE del 9 mar. 2017, causa ECLI:EU:C:2017:197 (Manni).
102 Prima direttiva 68/181/CE del Consiglio, del 9 mar, 1968, intesa a coordinare, per renderle equivalenti, le garanzie che sono richieste, negli Stati Membri, alle società di cui all'articolo 58, secondo comma, del Trattato, per tutelare gli interessi dei soci e dei terzi, GU L 65 del 14.3.1968, pag. 8.

di giustizia, vista l'eterogeneità dei termini di prescrizione previsti dai diversi diritti nazionali, risulta impossibile identificare un termine univoco, allo spirare del quale non è più necessario lasciare nel registro i dati menzionati. Alla luce di questa situazione, la Corte di giustizia ritiene che gli Stati membri non siano tenuti a garantire, in virtù dell'articolo 6 paragrafo 1 lettera e della direttiva 95/46/CE, alle persone fisiche i cui dati sono iscritti nel registro delle imprese, il diritto di ottenere, decorso un certo periodo di tempo dallo scioglimento della società, la cancellazione dei dati personali che le riguardano. Nondimeno, pur prevalendo la certezza del diritto e gli interessi dei terzi, la Corte non esclude che, in situazioni particolari e in via eccezionale, una persona possa far valere interessi legittimi e preponderanti affinché l'accesso ai dati personali che la riguardano sia limitato. La Corte di giustizia conclude pertanto che spetta agli Stati membri decidere se le persone interessate possano chiedere all'autorità incaricata di tenere il registro di valutare, caso per caso, se sia eccezionalmente giustificato, per motivi legittimi preponderanti, limitare, decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società in questione, l'accesso ai dati che la riguardano. Anche se la decisione della Corte di giustizia si basa sulla direttiva 95/46/CE, che non è più applicabile dopo l'entrata in vigore del regolamento (UE) 2016/679, le sue considerazioni restano valide anche con la nuova legislazione.

Come risulta dal principio generale sancito all'articolo 9 del Codice civile, i registri pubblici fanno piena prova dei fatti che attestano, finché non sia dimostrata l'inesattezza del loro contenuto. Viste le finalità dei registi relativi ai rapporti di diritto privato, riteniamo che motivi inerenti alla protezione dei dati non debbano ostacolare la loro pubblicità. Lo stesso vale per i registri nell'ambito del diritto immateriale: il legislatore ha già ponderato i vari interessi e garantisce la pubblicità di questi registri. Secondo il nostro Consiglio non spetta alla LPD disciplinare i diritti delle persone interessate in tale settore. È pertanto opportuno prevedere nel capoverso 4 una riserva a favore delle disposizioni speciali del diritto federale applicabile. Tale modifica riguarda soltanto i registri pubblici di diritto privato tenuti dalle autorità federali, ossia il registro informatizzato della Stato civile, Zefix, il registro aeronautico dell'Ufficio federale dell'aviazione civile e i registri dell'Istituto federale della proprietà intellettuale (in particolare quelli dei marchi, dei brevetti e del design).

I registri pubblici di diritto privato di competenza dei Cantoni sono retti dal diritto cantonale sulla protezione dei dati, anche nel caso in cui i dati siano trattati in esecuzione del diritto federale. Tuttavia il diritto cantonale non può impedire l'applicazione corretta e uniforme del diritto privato federale e in particolare il principio della pubblicità dei registri. L'abrogazione dell'articolo 2 capoverso 2 lettera c LPD non ha pertanto conseguenze per i registri cantonali seguenti: il registro fondiario, il registro del naviglio, i registri cantonali di commercio, i registri sulle esecuzioni e sul fallimento e il registro pubblico sulle riserve di proprietà. Il capoverso 4 non esplica effetti neppure sui registri di diritto pubblico, ad esempio il registro delle professioni mediche, ai quali si applica la pertinente legge speciale e sussidiariamente la LPD.

Campo d'applicazione territoriale

Al contrario di quanto previsto dal regolamento (UE) 2016/679 (art. 3), il D-LPD non contiene disposizioni specifiche relative al campo d'applicazione territoriale della legge. Riteniamo che il diritto attuale permetta già in larga misura di applicare la LPD a situazioni che presentano aspetti internazionali. In virtù della teoria degli effetti, ciò vale anche per il diritto pubblico[103].

Piuttosto che in riferimento al campo d'applicazione territoriale, le difficoltà si pongono in relazione all'attuazione ed esecuzione delle decisioni, in particolare nel settore di Internet. Il nostro Consiglio ha valutato di obbligare i titolari e i responsabili del trattamento a indicare un recapito in Svizzera, al fine di agevolare l'esecuzione di decisioni che li riguardano. Vi ha tuttavia rinunciato per i motivi già indicati nel rapporto dell'11 dicembre 2015 sulla responsabilità civile dei provider[104]. Sarebbe invece preferibile una soluzione per mezzo di accordi di assistenza giudiziaria bilaterali o multilaterali che permettano l'invio postale di atti che devono essere notificati all'estero. Simili accordi nel settore del diritto civile esistono già con alcuni Stati, quali l'Irlanda o gli Stati Uniti, in cui hanno sede note imprese di Internet. Nel settore penale, il nostro Consiglio ha confermato questa opzione nella risposta alla mozione Levrat 16.4082 «Facilitare l'accesso delle autorità di perseguimento penale ai dati delle reti sociali». Infine, il nostro Consiglio osserva che l'obbligo di designare un recapito è previsto nella PA e nella LTAF.

L'Incaricato avrebbe auspicato che il disegno di legge contenesse una disposizione analoga all'articolo 3 del regolamento (UE) 2016/69 e che i titolari del trattamento di dati fossero tenuti ad avere una sede in Svizzera.

Art. 3 Incaricato federale della protezione dei dati e della trasparenza

Cpv. 1 Sorveglianza da parte dell'incaricato

Il capoverso 1 menziona l'autorità di sorveglianza competente nell'ambito della protezione dei dati. Stabilisce il principio secondo cui l'Incaricato è l'autorità cui compete la sorveglianza del rispetto delle disposizioni federali sulla protezione dei dati (art. 39 segg. D-LPD).

Nel testo tedesco si usa esclusivamente il termine maschile, quando ci si riferisce all'Incaricato in quanto istituzione. Ciò riguarda la maggior parte delle disposizioni della legge. Nella prima sezione del capitolo 7 si parla invece della persona dell'incaricato (ad eccezione dell'art. 42 D-LPD). In queste disposizioni nel testo tedesco si usano la forma maschile e quella femminile.

103 Il Tribunale federale ha applicato questo principio in riferimento alla protezione dei dati. Secondo tale principio le immagini riprese in Svizzera e pubblicate in modo tale da essere consultabili in Svizzera hanno una connessione con la Svizzera anche se sono trattate all'estero e non sono messe su Internet direttamente in Svizzera (DTF **138** II 346 consid. 3.3 «Google Street View»).

104 www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-f.pdf. Il rapporto è disponibile in tedesco e francese (link alla versione francese).

Cpv. 2 Deroghe alla sorveglianza

Il capoverso 2 prevede che determinate autorità non sono soggette alla sorveglianza dell'Incaricato. Tali eccezioni sono dovute essenzialmente al fatto che assoggettando queste autorità alla sorveglianza dell'Incaricato si pregiudicherebbe la separazione dei poteri e l'indipendenza della giustizia.

L'Assemblea federale (lett. a) e il Consiglio federale (lett. b) non sono sottoposti alla sorveglianza dell'Incaricato.

Nella misura in cui il trattamento di dati personali da parte dei tribunali federali rientra nella LPD, questi ultimi non sono sottoposti alla sorveglianza dell'Incaricato (lett. c). Questa eccezione va vista in considerazione del fatto che il D-LPD conferisce all'Incaricato la competenza di emanare decisioni nei confronti di organi federali. Per i tribunali della Confederazione vi sarebbe quindi il pericolo che ciò pregiudichi la loro indipendenza e la separazione dei poteri. Inoltre, il Tribunale amministrativo federale e il Tribunale federale sono le autorità di ricorso per le decisioni dell'Incaricato e potrebbero quindi essere chiamate a pronunciarsi in merito a un proprio ricorso. Per soddisfare i requisiti della direttiva (UE) 2016/680 e del P-STE 108, ciascun tribunale della Confederazione dovrà provvedere a una forma propria e indipendente di sorveglianza sulla protezione dei dati. Nella misura del possibile, tale sorveglianza sarà simile a quella esercitata dall'Incaricato e istituita mediante l'adeguamento delle pertinenti ordinanze dei tribunali della Confederazione non appena sarà entrata in vigore la nuova LPD.

Secondo la lettera d, anche il Ministero pubblico della Confederazione non è sottoposto alla sorveglianza dell'Incaricato, nella misura in cui tratta dati personali nell'ambito di un procedimento penale[105]. Resteranno invece sottoposti alla sorveglianza dell'Incaricato le autorità federali di polizia, anche nel caso in cui agiscano su incarico del Ministero pubblico della Confederazione. Per la sorveglianza l'Incaricato applica le disposizioni sulla protezione dei dati del diritto procedurale applicabile (cfr. art. 2 cpv. 3 D-LPD).

Infine, secondo la lettera e non sottostanno alla sorveglianza dell'Incaricato le autorità federali, nella misura in cui trattano dati personali nell'ambito di attività giurisdizionali o di procedure di assistenza giudiziaria internazionale in materia penale. Questa eccezione riguarda soprattutto il Ministero pubblico della Confederazione e l'Ufficio federale di giustizia. Secondo la dichiarazione della Svizzera relativa all'articolo 1 della Convenzione europea del 20 aprile 1959[106] di assistenza giudiziaria in materia penale, l'Ufficio federale di giustizia deve essere considerato un'autorità giudiziaria svizzera ai fini della Convenzione. La portata di questa eccezione è tuttavia limitata, poiché l'Incaricato può verificare la liceità di un trattamento di dati se la persona interessata fa valere i suoi diritti secondo l'articolo 11*c* D-AIMP.

105 Cfr. consid. 80 della direttiva (UE) 2016/680 e il relativo art. 18.
106 RS **0.351.1**

9.1.3 9.1.3 Disposizioni generali sulla protezione dei dati

9.1.3.1 Definizioni e principi generali

Art. 4 Definizioni

Lett. a Dati personali

Occorre precisare che il D-LPD utilizza in linea di massima il termine «dati personali». All'interno dello stesso capoverso si usa a volte come sinonimo il termine «dati», se dal contesto risulta chiaro che si tratta di dati personali.

La nozione di «dati personali» rimane invariata rispetto al diritto vigente e comprende tutte le informazioni relative a una persona identificata o identificabile. Una persona fisica è identificabile se può esser identificata direttamente o indirettamente, ad esempio grazie alle informazioni risultanti dalle circostanze o dal contesto (numero d'identificazione, dati relativi alla sua ubicazione, elementi specifici riguardanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali). L'identificazione può avvenire in base a un solo elemento (numero di telefono, numero dell'immobile, numero AVS, impronte digitali) o correlando varie informazioni (indirizzo, data di nascita e stato civile). Come nel diritto attuale, la mera possibilità teorica che qualcuno possa essere identificato non è sufficiente per supporre che sia identificabile. Come osservato dal nostro Consiglio nel messaggio concernente la LPD del 1988: «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 […] non si può parlare di possibilità d'identificazione»[107]. Occorre invece tenere conto, in ogni singolo caso, di tutti i mezzi che possono essere ragionevolmente impiegati per identificare una persona. La ragionevolezza dei mezzi a disposizione deve essere valutata in relazione a tutte le circostanze, quali il dispendio di tempo e l'onere finanziario necessari per applicarli, tenendo conto delle tecnologie disponibili al momento del trattamento e della loro evoluzione.

La legge non si applica ai dati che sono stati resi anonimi e la cui identificazione da parte di un terzo è impossibile (i dati sono stati anonimizzati in modo completo e definitivo) o sarebbe possibile soltanto con uno sforzo che nessun interessato è disposto a fare. Tale regola vale anche per i dati pseudonimizzati.

Lett. b Persona interessata

La persona interessata è la persona fisica i cui dati sono oggetto di trattamento. La limitazione alle persone fisiche risulta dall'abolizione della protezione dei dati delle persone giuridiche (cfr. il commento all'art. 2 cpv. 1 P-LPD al n. 9.1.2).

Lett. c Dati personali degni di particolare protezione

Il numero 1 resta immutato.

Il numero 2 è completato: in conformità con la direttiva (UE) 2016/680 (art. 10) e il regolamento (UE) 2016/679, la nozione di «dati personali degni di particolare prote-

107 FF **1988** II 353, in particolare pag. 385.

zione» è estesa ai dati sull'appartenenza etnica. Il D-LPD mantiene il riferimento all'appartenenza a una razza. Come l'Unione europea, teniamo a precisare che l'uso di questa espressione non significa che il nostro Consiglio aderisce a teorie che tendono a dimostrare l'esistenza di razze umane distinte. Il D-LPD mantiene anche il riferimento ai dati sulla sfera privata e su quella intima. Sono considerati dati sulla sfera intima in particolare i dati sulla vita e l'orientamento sessuali della persona interessata (cfr. anche P-STE 108 [art. 6 par. 1], direttiva [UE] 2016/680 [art. 10] e regolamento [UE] 2016/679 [art. 9]). A seconda delle circostanze anche l'identità sessuale di una persona può rientrare nella sfera intima (o nei dati sulla salute).

La nozione di «dati personali degni di particolare protezione» è inoltre estesa ai dati genetici (n. 3) e ai dati biometrici che identificano una persona in modo univoco (n. 4). Questa modifica traspone nel diritto svizzero i requisiti del P-STE 108 (art. 6 par. 1) e della direttiva (UE) 2016/680 (art. 10). Il regolamento (UE) 2016/679 (art. 9) prevede un disciplinamento analogo (art. 9).

I dati genetici sono informazioni sul patrimonio genetico di una persona ottenute attraverso un esame genetico; ne fa parte anche il profilo del DNA (art. 3 lett. l della legge federale dell'8 ottobre 2004[108] sugli esami genetici sull'essere umano [LEGU]).

I dati biometrici qui in oggetto sono i dati relativi a caratteristiche fisiche, fisiologiche o comportamentali ottenuti grazie a un processo tecnico specifico e che permettono di identificare univocamente una persona o di confermarne l'identificazione. Si tratta ad esempio di un'impronta digitale, un'immagine del viso, un'immagine dell'iride o una registrazione della voce. Questi dati devono obbligatoriamente basarsi su un processo tecnico che permetta l'identificazione o l'autenticazione univoca della persona. Nel caso di normali fotografie, ad esempio, questa premessa non è data.

Lett. d Trattamento

Il termine «trattamento» resta invariato sotto il profilo del contenuto. L'elenco è tuttavia stato completato con i termini «registrazione» e «cancellazione», al fine di adeguare la definizione a quella del diritto europeo (art. 2 lett. b P-STE 108, art. 4 par. 1 del regolamento [UE] 2016/679 e art. 3 n. 2 della direttiva [UE] 2016/680). Come nel diritto vigente, l'elenco delle attività di trattamento non è esaustivo e quindi vi possono rientrare numerose operazioni (organizzazione, classificazione, modifica, analisi, ecc.). Il termine «distruzione» va più in là rispetto a «cancellazione» e implica che i dati siano eliminati in modo irreversibile. Se i dati sono su carta, questa dovrà essere bruciata o sminuzzata. Se si trovano su un supporto informatico, la distruzione richiede sforzi maggiori. Se i dati sono stati trasmessi su un CD o una chiave USB, occorre rendere inutilizzabili tali supporti. Inoltre, tutte le copie devono essere trattate in maniera tale che i dati non siano più leggibili. Se i dati personali sono allegati a un messaggio di posta elettronica, devono essere distrutti anche gli eventuali salvataggi intermedi del messaggio. Gli ordini usuali di soppressione o una mera riformattazione non costituiscono una distruzione, bensì una cancellazione[109].

108 RS **810.12**
109 Cfr. la sentenza del Tribunale amministrativo federale 2015/13, consid. 3.3.4 e riferimenti.

A differenza del diritto svizzero («bearbeiten»), l'Unione europea utilizza il termine tedesco «verarbeiten». Per ragioni pratiche il D-LPD rinuncia ad adeguare la terminologia tedesca del diritto svizzero, tanto più che sotto il profilo materiale i due termini sono identici.

Lett. f Profilazione

Proponiamo di abrogare l'espressione «profilo della personalità», definita nell'articolo 3 lettera d LPD, poiché si tratta di una particolarità della nostra legislazione. Né il diritto europeo né altre legislazioni estere la utilizzano. Dall'entrata in vigore della LPD nel 1993, questa espressione non ha avuto molta importanza[110] e, vista l'evoluzione tecnologica, appare oggi obsoleta. Nel D-LPD è pertanto sostituita con il termine «profilazione», che si trova nell'articolo 3 numero 4 della direttiva (UE) 2016/680 e nell'articolo 4 numero 4 del regolamento (UE) 2016/679. Anche se sono simili, le due nozioni non coincidono. Il profilo della personalità è il risultato di un processo di trattamento ed è quindi un dato statistico. La profilazione invece indica una determinata forma di trattamento e quindi un processo dinamico. Inoltre, la profilazione mira a un determinato scopo.

In base ai pareri espressi in sede di consultazione, il contenuto del termine «profilazione» è adeguato alla terminologia europea e comprende in particolare soltanto il trattamento automatizzato di dati personali. Per profilazione s'intende pertanto la valutazione di determinate caratteristiche di una persona sulla base di dati trattati automaticamente, in particolare per analizzare o predire il rendimento professionale, la situazione economica, la salute, il comportamento, gli interessi, il luogo di soggiorno o gli spostamenti di una persona. La valutazione può ad esempio essere effettuata per accertare se una persona sia idonea a svolgere una determinata attività. In altre parole, una profilazione valuta in modo automatico i dati personali per analizzare, sempre in modo automatico, le caratteristiche di una persona. Sussiste quindi una profilazione soltanto se il processo di valutazione è interamente automatico. Per valutazione automatica s'intende qualsiasi valutazione per mezzo di tecniche di analisi informatiche. A tal fine possono essere usati anche algoritmi, ma il loro impiego non è un elemento costitutivo di una profilazione. Il criterio determinante è la presenza di un processo di valutazione automatico; una semplice raccolta di dati non analizzati non costituisce una profilazione. La valutazione automatica è effettuata in particolare per analizzare o predire determinati comportamenti di una persona. Il D-LPD menziona a titolo esemplificativo caratteristiche di una persona, quali il rendimento professionale, la situazione economica o la salute. Sono tuttavia ipotizzabili anche altre caratteristiche quali gli interessi, il credito o il luogo di soggiorno di una persona. Non ha importanza se il titolare che effettua la profilazione lo fa per scopi propri o per terzi.

Poiché il termine «profilo della personalità» è abolito, devono essere adeguate anche le basi legali che permettono agli organi federali di trattare profili della personalità (cfr. n. 9.2.2).

110 Cfr. tuttavia la sentenza del Tribunale amministrativo federale A-4232/2015 del 18 par. 2017 nella causa Moneyhouse AG (v. n. 9.1.6).

I dati ottenuti per mezzo di una profilazione sono in linea di massima dati personali ai sensi dell'articolo 4 lettera a D-LPD. A seconda del loro contenuto può trattarsi anche di dati degni di particolare protezione.

Lett. g Violazione della sicurezza dei dati

A differenza dell'avamprogetto, il D-LPD contiene una definizione della violazione della sicurezza dei dati, poiché in sede di consultazione si è constatato che il concetto non era sufficientemente chiaro. Sussiste una violazione della sicurezza dei dati se i dati vanno persi, sono cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate; questo a prescindere dal fatto che ciò si verifichi intenzionalmente oppure illecitamente o meno. Il termine si riallaccia all'articolo 7 D-LPD, secondo cui il titolare e il responsabile del trattamento devono garantire la sicurezza dei dati mediante provvedimenti tecnici e organizzativi appropriati. Sotto il profilo del contenuto l'espressione corrisponde agli articoli 7 paragrafo 2 P-STE 108, 3 numero 11 della direttiva (UE) 2016/680 e 4 numero 12 del regolamento (UE) 2016/679.

È determinante unicamente che i processi summenzionati si verifichino. Affinché sussista una violazione della sicurezza dei dati, è irrilevante che vi sia stata la mera possibilità che i dati siano divulgati o resi accessibili a persone non autorizzate o che tale divulgazione si sia effettivamente verificata. Se per esempio va perso un supporto di dati, è spesso impossibile provare che i dati ivi registrati sono stati effettivamente consultati o usati da terzi. Pertanto la perdita costituisce di per sé una violazione della sicurezza dei dati. La portata e l'importanza di una violazione della sicurezza dei dati sono invece rilevanti per i provvedimenti da adottare; a tal fine ci si deve basare in particolare sulla valutazione del rischio secondo l'articolo 22 capoverso 1.

Lett. i Titolare del trattamento

Il D-LPD sostituisce la nozione di «detentore di una collezione di dati» con «titolare del trattamento» al fine di usare la stessa terminologia del P-STE 108 (art. 2 lett. b), della direttiva (UE) 2016/680 (art. 3 n. 8) e del regolamento (UE) 2016/679 (art. 4 n. 7). Salvo l'abolizione del riferimento alla collezione di dati, questa modifica non comporta cambiamenti materiali. Il titolare del trattamento, come il detentore della collezione dei dati, è colui che determina gli obiettivi e i mezzi (trattamento materiale o automatico, software) del trattamento di dati[111].

Nel testo tedesco è usata esclusivamente la forma maschile poiché nella maggior parte dei casi, anche se non sempre, i titolari del trattamento sono persone giuridiche.

Lett. j Responsabile del trattamento

Si tratta della persona privata o dell'organo federale che tratta dati per conto del titolare del trattamento. L'espressione riprende quella del P-STE 108 (art. 2 lett. f), della direttiva (UE) 2016/680 (art. 3 n. 9) e del regolamento (UE) 2016/679 (art. 4 n. 8).

111 FF **1988** II 353, in particolare pag. 388 seg.

Il contratto che vincola il titolare e il responsabile del trattamento può essere di varia natura: a seconda degli obblighi del responsabile del trattamento, può trattarsi di un mandato (art. 394 segg. CO), di un contratto di appalto (art. 363 segg. CO) o di un contratto misto. Il responsabile del trattamento cessa di essere considerato un terzo dal momento in cui inizia la sua attività contrattuale per conto del titolare del trattamento.

Nel testo tedesco è usata esclusivamente la forma maschile poiché nella maggior parte dei casi, anche se non sempre, i titolari del trattamento sono persone giuridiche.

Definizioni immutate

Le seguenti definizioni restano immutate o subiscono soltanto adeguamenti redazionali rispetto al diritto vigente: comunicazione (lett. e) e organi federali (lett. h).

Definizioni abrogate

Oltre a quelle di «profilo della personalità» e «detentore di una collezione di dati» il D-LPD abroga le definizioni seguenti:

– Collezione di dati: il D-LPD rinuncia a questo termine in conformità alla soluzione prevista dal P-STE 108, che in sua vece ricorre all'espressione «trattamento di dati». In effetti, grazie alle nuove tecnologie, i dati possono oggi essere gestiti come una collezione anche quando sono disseminati. Un esempio lampante è la profilazione, mediante la quale si cercano dati in diverse fonti, che non costituiscono una raccolta di dati, per analizzare determinate caratteristiche di una persona. Queste attività non sono contemplate dalle disposizioni della legge vigente che implicano la presenza di una collezione di dati, come ad esempio il diritto d'accesso (art. 8 LPD) o l'obbligo d'informare (art. 14 LPD). Ma è proprio per questo tipo di attività che è necessaria maggiore trasparenza. Sottolineiamo inoltre che una parte della dottrina tende a interpretare in senso molto lato la nozione di collezione di dati: il criterio determinante è che l'attribuzione di un dato a una persona non deve implicare sforzi sproporzionati[112].
– Legge in senso formale: il D-LPD sopprime questa definizione poiché è superflua.

Art. 5 Principi

Cpv. 2 Buona fede e proporzionalità

La versione francese del capoverso 2 è oggetto di una modifica redazionale.

In base al principio di proporzionalità possono essere trattati soltanto i dati adeguati e necessari per raggiungere le finalità del trattamento. Inoltre, deve esserci un rapporto ragionevole tra le finalità e i mezzi utilizzati, poiché i diritti della persona interessata devono essere tutelati nella misura del possibile (principio di proporzionalità

112 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 563; Belser Urs, in: Maurer-Lambrou/Vogt (a c. di), Basler Kommentar, Datenschutzgesetz, 2ª ed., Basilea 2006, art. 3 LPD N 32; GAAC 62.57.

in senso stretto)[113]. Il principio secondo cui vanno evitati trattamenti non necessari e quello secondo cui il trattamento deve essere circoscritto al minimo necessario costituiscono due elementi del principio di proporzionalità[114]. Il primo implica che, se possibile, lo scopo del trattamento deve essere raggiunto senza raccogliere nuovi dati. Il secondo impone che siano trattati soltanto i dati assolutamente necessari per raggiungere lo scopo perseguito. Questi due principi devono essere rispettati sin dalla progettazione di nuovi sistemi e collimano pertanto in parte con i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (cfr. il commento all'art. 6 D-LPD).

Cpv. 3 Finalità e riconoscibilità

Il capoverso 3 riunisce i principi della finalità vincolante e della riconoscibilità, attualmente contenuti nei capoversi 3 e 4 della legge vigente. Per adeguare il diritto federale al tenore del P-STE 108 (art. 5 par. 4 lett. b), il D-LPD sancisce che i dati devono essere raccolti per determinate finalità riconoscibili da parte della persona interessata. Questa nuova formulazione non implica modifiche materiali rispetto al diritto in vigore: sia la raccolta di dati che le finalità del trattamento devono essere riconoscibili. Ciò è in linea di principio il caso quando s'informa la persona interessata, quando il trattamento è previsto da una legge o quando lo si evince chiaramente dalle circostanze. Il carattere determinato delle finalità implica che non è sufficiente indicare scopi vaghi, non definiti o imprecisi. La determinatezza va giudicata secondo le circostanze, fermo restando l'obiettivo di garantire un equilibrio tra gli interessi delle persone interessate, del titolare o del responsabile del trattamento e della società in generale.

Il capoverso 3 stabilisce che i dati devono essere trattati in modo compatibile con le finalità iniziali. Questa nuova formulazione permette di adeguare il tenore della legge a quello del P-STE 108 (art. 5 par. 4 lett. b). Non implica tuttavia cambiamenti notevoli: come nel diritto vigente, un ulteriore trattamento non è ammissibile se la persona interessata può legittimamente considerarlo inatteso, inappropriato o contestabile (cfr. anche il par. 47 del rapporto esplicativo relativo al P-STE 108 del CAHDATA[115]). Si possono ipotizzare i casi seguenti:

- l'utilizzazione a fini pubblicitari di indirizzi ottenuti in occasione della raccolta di firme per un'iniziativa popolare;
- la raccolta e l'analisi di abitudini di consumo grazie ai pagamenti effettuati con la carta di credito o la carta clienti (per una finalità che non sia la scoperta di una frode), senza il consenso della persona interessata;
- la raccolta e l'utilizzazione, per l'invio di spam, di indirizzi di posta elettronica trasmessi da una persona interessata per una determinata finalità[116];
- la raccolta da parte di un'impresa privata di indirizzi IP di titolari di collegamenti che offrono illecitamente copie illegali da scaricare[117].

113 FF **1988** II 353, in particolare pag. 390.
114 Baeriswyl Bruno, Commento all'art. 4, in: Baeriswyl/Pärli (a c. di), Datenschutz – Stämpfli Handkommentar, Berna 2015, n. 23.
115 rm.coe.int/16806af190.
116 GAAC 69.106 consid. 5.6.

Per contro, se la persona interessata trasmette il suo indirizzo a un'impresa per ottenere una carta cliente o per ordinare qualcosa (in linea o no), l'ulteriore utilizzazione dell'indirizzo a fini commerciali da parte dell'impresa stessa va considerata una finalità inizialmente riconoscibile e quindi compatibile con le finalità iniziali[118]. Il trattamento ulteriore è ritenuto compatibile con le finalità iniziali anche nel caso in cui la modifica di tali finalità è prevista dalla legge, richiesta da una modifica legislativa o legittimata da un altro motivo giustificativo (p. es. il consenso della persona interessata).

Cpv. 4 Durata di conservazione dei dati personali

Secondo il capoverso 4 i dati devono essere distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento. Ciò corrisponde ai requisiti del P-STE 108 (art. 5 par. 4 lett. e, cfr. anche il n. 51 del rapporto esplicativo concernente il P-STE 108 del CAHDATA), della direttiva (UE) 2016/680 (art. 4 par. 1 lett. e) e del regolamento (UE) 2016/679 (art. 5 par. 1 lett. e). Implicitamente, l'obbligo si evince anche dal principio generale di proporzionalità, sancito nel capoverso 2 della presente disposizione. Riteniamo tuttavia importante sancire esplicitamente questo obbligo, vista l'evoluzione tecnologica e le possibilità quasi illimitate di registrare dati. Il rispetto di questo obbligo implica che il titolare del trattamento stabilisca dei termini di conservazione. Sono fatte salve disposizioni speciali che prevedono termini di conservazione particolari.

Cpv. 5 Esattezza

L'articolo 5 capoverso 5 del D-LPD riprende il principio dell'esattezza dei dati, che nel diritto vigente figura all'articolo 5 LPD. Questa modifica permette di riunire i principi fondamentali della protezione dei dati in un solo articolo, analogamente a quanto previsto dall'articolo 5 del P-STE 108, dall'articolo 4 della direttiva [UE] 2016/680 e dall'articolo 5 del regolamento [UE] 2016/679. Nel testo francese il termine «correctes» è sostituito da «exactes»; le versioni tedesca e italiana usano già questa terminologia.

La disposizione prevede che chi tratta dati personali deve accertarsi che siano esatti. Deve prendere tutte le misure necessarie per rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto alle finalità per le quali sono stati raccolti o trattati. I dati che non possono essere rettificati o completati devono essere cancellati o distrutti. La portata dell'obbligo di accertamento va definita di caso in caso e dipende in particolare dalla finalità del trattamento, dalla sua estensione e dal tipo di dati trattati. Se del caso, l'obbligo di accertamento può implicare l'aggiornamento costante dei dati.

Determinati obblighi legali possono opporsi alla rettifica, alla cancellazione o all'aggiornamento dei dati[119]. In riferimento all'attività di archivi, musei, biblioteche e altre istituzioni della memoria collettiva, il principio di esattezza e gli obblighi

117 DTF **136** II 508 consid. 4.
118 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 731.
119 Ad esempio l'obbligo di conservare i dati inalterati, come ad esempio previsto dall'art. 7 della legge federale del 10 ott. 1997 sul riciclaggio di denaro (LRD; RS **955.0**).

connessi devono essere giudicati in modo differenziato. Il compito di queste istituzioni è in particolare di inventariare, conservare, rendere accessibili e far conoscere documenti (anche digitali; cfr. art. 2 cpv. 1 della legge del 18 dicembre 1992[120] sulla Biblioteca nazionale). Tali documenti non possono essere modificati, poiché sarebbe contrario allo scopo dell'archiviazione. Gli archivi hanno infatti il compito di rappresentare, per mezzo di documenti, un'immagine momentanea del passato la cui «esattezza» va giudicata unicamente in riferimento alla rappresentazione fedele dei documenti stessi. In altre parole, gli archivi raccolgono i dati così come si presentavano nel passato, a prescindere dal fatto che, da un punto di vista odierno, siano ritenuti esatti o meno. Questa attività specifica è di notevole interesse pubblico (su tali questioni si vedano gli art. 28 cpv. 1 lett. b e 37 cpv. 5 D-LPD e i relativi commenti nei n. 9.1.6 e 9.1.7).

Cpv. 6 Consenso

Il capoverso 6 stabilisce che, quando il trattamento di dati personali è subordinato al consenso della persona interessata, il consenso è valido soltanto se, dopo debita informazione, è espresso liberamente e in modo inequivocabile in riferimento a uno o più trattamenti specifici. In tal modo la persona interessata dà il suo consenso a una violazione della personalità in seguito a un trattamento di dati.

Il tenore leggermente modificato permette un adeguamento terminologico al P-STE 108 (art. 5 par. 2) al fine di rispettarne i requisiti. Non ne consegue tuttavia una modifica sostanziale della normativa attuale. Come secondo il diritto vigente, affinché il consenso sia valido il trattamento, in particolare la sua portata e lo scopo, deve essere sufficientemente definito. Il consenso può essere espresso anche per più trattamenti simili o differenti. È inoltre ipotizzabile che lo scopo perseguito esiga diversi trattamenti. La cura presso un medico può ad esempio rendere necessario lo scambio di dati con gli specialisti e i servizi che hanno curato il paziente prima o che lo cureranno dopo. Lo stesso dicasi per la fatturazione e gli accertamenti con le assicurazioni. Il consenso deve riguardare lo scopo del trattamento, per il quale funge da motivo giustificativo. Se i dati sono trattati per altri scopi, per i quali la persona interessata non ha dato il suo consenso, tale trattamento deve essere giustificato da altri motivi. Inoltre, il consenso deve essere dato in modo inequivocabile, per cui dalla dichiarazione della persona si deve evincere chiaramente, a seconda delle circostanze di ogni singolo caso, la sua volontà. Quanto più sensibili sono i dati personali in questione, tanto più inequivocabile deve essere il suo consenso[121]. Anche secondo il D-LPD il consenso non sottostà a particolari regole formali e non è pertanto necessaria una dichiarazione scritta[122]. Il consenso inequivocabile ai sensi del capoverso 6 può essere dato anche per mezzo di una manifestazione tacita della volontà (cfr. art. 1 CO). Si è in presenza di una tale manifestazione quando la volontà non si evince da una dichiarazione, bensì da un comportamento che, in base al contesto, può essere interpretato come espressione inequivocabile[123]. Ciò si verifica

120 RS **432.21**
121 Cfr. FF **2003** 1885, in particolare pag. 1909.
122 Cfr. FF **2003** 1885, in particolare pag. 1910.
123 Kren Kostkiewicz Jolanta, Art. 1 CO N 17, in: Kren Kostkiewicz Jolanta et al. (a c. di), OR, Schweizerisches Obligationenrecht, Kommentar, 3ª ed., Zurigo, e i relativi riferimenti.

nel caso di un cosiddetto comportamento concludente, in cui la persona interessata esprime la sua volontà attraverso un determinato atto, ad esempio adempiendo gli obblighi contrattuali. Deve comunque essere espressa una volontà, per cui il silenzio o l'inattività non possono essere considerati un consenso valido per una violazione della personalità[124]. È fatto salvo l'articolo 6 CO, se le parti hanno concordato l'accettazione tacita.

In virtù del secondo periodo del capoverso 6, nel caso di dati personali degni di particolare protezione o di profilazione è necessario l'espresso consenso. Anche il consenso per la profilazione è soggetto ai requisiti più severi già previsti dal diritto vigente per il trattamento di profili della personalità. L'«espresso» consenso è un requisito più severo rispetto al consenso inequivocabile secondo il primo periodo di questa disposizione. La sua portata è controversa già nel diritto vigente[125]. Riteniamo tuttavia che non vi sia motivo di modificare la situazione giuridica attuale. Nelle versioni francese e italiana del testo, i termini «explicite» ed «esplicito» sono sostituiti da «exprès» ed «espresso», in modo da adeguare la terminologia all'articolo 1 CO. Il testo tedesco non subisce invece alcuna modifica La manifestazione di volontà è espressa se risulta direttamente da una dichiarazione scritta o orale oppure da appositi segni[126]. Il modo in cui avviene tale manifestazione deve rendere di per sé chiara la volontà della persona in questione[127]. Questo è possibile in particolare apponendo una croce in un'apposita casella, optando per determinati parametri tecnici nel caso di servizi di imprese che trattano informazioni oppure ricorrendo a un altro tipo di dichiarazione. Lo stesso vale per una manifestazione non verbale per mezzo di un segno o un movimento chiaramente interpretabile nel contesto concreto, il che si verifica in particolare nell'ambito di un rapporto di cura medica. A titolo di esempio si possono menzionare il fatto di annuire o di aprire la bocca per il prelievo di uno striscio della mucosa orale, dopo debita informazione. Laddove è richiesto l'espresso consenso, quest'ultimo non può essere manifestato tacitamente.

Art. 6 Protezione dei dati fin dalla progettazione e per impostazione predefinita

L'articolo 6 D-LPD introduce l'obbligo della protezione dei dati fin dalla progettazione e per impostazione predefinita. Dato che sono strettamente connessi ai principi della protezione dei dati, questi obblighi sono stati trasferiti nelle disposizioni generali sulla protezione dei dati. La disposizione attua i requisiti dell'articolo 8bis numero 3 P-STE 108 e dell'articolo 20 paragrafo 1 della direttiva (UE) 2016/680. L'articolo 25 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

124 Haas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Diss. Luzern, Zürich 2007, N 393 mit zahlreichen Hinweisen.

125 Cfr. VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16 nov. 2015.

126 DTF **121** III 31, consid. 2c pag. 34; Kren Kostkiewicz Jolanta, art. 1 CO N 17, in: Kren Kostkiewicz Jolanta et al. (a c. di), OR, Schweizerisches Obligationenrecht, Kommentar, 3ª ed., Zurigo 2016; Gauch Peter/Schluep Walter/Schmid Jörg/Emmenegger Susan, Schweizerisches Obligationenrecht Allgemeiner Teil, Volume 1, 10ª ed., Zurigo 2014 N 188.

127 Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16 nov. 2015, N 26 seg.

Cpv. 1 Protezione dei dati fin dalla progettazione

Secondo il capoverso 1, il titolare del trattamento è tenuto ad adottare, fin dalla progettazione del trattamento, le misure appropriate per attuare le disposizioni sulla protezione dei dati. Il D-LPD introduce pertanto il principio della protezione dei dati fin dalla progettazione (privacy by design). L'idea alla base della protezione fin dalla progettazione è che la tecnica e il diritto si completino a vicenda. Una tecnica favorevole alla protezione dei dati permette di ridurre la necessità di regole giuridiche (o di codici di condotta), in quanto gli accorgimenti tecnici rendono impossibile una violazione della protezione dei dati o perlomeno ne riducono notevolmente il rischio. Nel contempo le tecnologie che favoriscono la protezione dei dati sono imprescindibili per l'applicazione delle disposizioni sulla protezione dei dati. Infatti, il trattamento di dati è un fenomeno onnipresente e tenderà ancora ad aumentare (ubiquitous computing). Ne consegue un'innumerevole quantità di dati che devono essere trattati conformemente alle regole sulla protezione dei dati. A tal fine gli accorgimenti tecnici sono d'importanza fondamentale. In generale, la protezione dei dati fin dalla progettazione non è legata a una determinata tecnologia. Si tratta piuttosto di progettare, sotto il profilo tecnico e organizzativo, i sistemi per il trattamento dei dati in modo tale da conformarli in particolare ai principi di cui all'articolo 5 D-LPD. In altre parole, il sistema deve attuare i requisiti per un trattamento dei dati conforme alla legge in modo tale da ridurre o escludere il rischio di violazioni delle disposizioni sulla protezione dei dati. È ad esempio possibile impostare un sistema di modo che i dati siano cancellati a intervalli regolari o anonimizzati in maniera standardizzata. Per la protezione fin dalla progettazione è d'importanza particolare che i dati raccolti siano ridotti al minimo indispensabile, affinché sia rispettato uno dei principi generali di cui all'articolo 5 D-LPD. Sin dall'inizio, il trattamento deve essere pertanto progettato in modo tale da raccogliere e trattare il minor numero possibile di dati o perlomeno in modo tale da doverli conservare meno tempo possibile.

Anche il diritto vigente prevede che gli organi federali annuncino senza indugio al responsabile della protezione dei dati da loro designato o, in sua assenza, all'Incaricato tutti i progetti di trattamento automatizzato di dati personali, al fine di garantire che i requisiti della protezione dei dati siano rispettati fin dalla progettazione (art. 20 OLPD).

Cpv. 2 Adeguatezza dei provvedimenti

Il capoverso 2 precisa i requisiti posti ai provvedimenti di cui al capoverso 1: devono essere adeguati in particolare allo stato della tecnica, alla natura e all'estensione del trattamento dei dati come pure al grado di probabilità e di gravità del rischio che il trattamento implica per la personalità e i diritti fondamentali della persona interessata. La disposizione si riferisce al trattamento di dati da parte di privati e da parte di organi federali e quindi si parla di rischi per la personalità e per i diritti fondamentali.

La disposizione si basa su un approccio basato sui rischi. Il rischio che consegue da un trattamento deve essere messo in relazione con le possibilità tecniche di ridurlo. Quanto più alto è il rischio e la probabilità che si verifichi e quanto più ampio è il trattamento di dati, tanto più elevati dovranno essere i requisiti posti ai provvedimenti tecnici, affinché siano da ritenersi adeguati ai sensi della presente disposizione.

Cpv. 3 Protezione dei dati per impostazione predefinita

Secondo il capoverso 3, il titolare del trattamento è tenuto a garantire, mediante appropriate impostazioni predefinite, che il trattamento di dati personali sia in linea di massima circoscritto al minimo indispensabile per le finalità perseguite, sempreché la persona interessata non disponga altrimenti. La disposizione introduce l'obbligo della protezione dei dati per impostazione predefinita (privacy by default). Le impostazioni predefinite sono impostazioni standard, in particolare di software, che sono applicate se l'utente non le modifica. Possono essere previste dal prodotto oppure programmate, ad esempio quando una determinata stampante è definita come stampante standard. Nel contesto del trattamento di dati questo significa che il pertinente sistema è impostato in modo da favorire la protezione dei dati, a meno che la persona interessata modifichi le impostazioni. È ad esempio ipotizzabile che una pagina web permetta acquisti chiedendo ai clienti di fornire soltanto indicazioni basilari, quali nome e indirizzo, senza che sia necessario allestire un profilo di utente. Se invece desiderano usufruire di ulteriori servizi della pagina web, ad esempio accedere a tutti i loro acquisti del passato o allestire elenchi di beni da acquistare, i clienti devono allestire un profilo di utente, il che comporta anche un ampio trattamento dei loro dati personali. Anche nel caso delle impostazioni predefinite è evidente lo stretto nesso con le tecnologie che favoriscono la protezione dei dati. Le impostazioni predefinite fanno parte della struttura favorevole alla protezione dei dati di un intero sistema informatico. Una particolarità delle impostazioni predefinite favorevoli alla protezione dei dati è costituita dalla possibilità della persona interessata di intervenire. Anche se non può modificare il sistema in sé, essa ha la possibilità di modificarne le impostazioni. Queste ultime sono pertanto strettamente connesse al consenso della persona interessata (cfr. art. 5 cpv. 6 D-LPD). Le impostazioni predefinite che favoriscono la protezione dei dati permettono pertanto alla persona interessata di acconsentire a un determinato trattamento di dati.

Nel settore pubblico, il principio della protezione dei dati per impostazione predefinita svolge un ruolo secondario, poiché in tale settore il trattamento di dati si fonda su obblighi legali piuttosto che sul consenso della persona interessata.

Il titolare del trattamento può dimostrare, in particolare attraverso la certificazione o la valutazione d'impatto sulla protezione dei dati, di rispettare gli obblighi della presente disposizione.

Art. 7 Sicurezza dei dati personali

L'articolo 7 D-LPD riprende l'articolo 7 LPD, con alcune modifiche redazionali. L'obbligo di garantire la sicurezza dei dati è una condizione del P-STE 108 (art. 7) e della direttiva (UE) 2016/680 (art. 29). Il regolamento (UE) 2016/679 (art. 32) prevede un disciplinamento analogo.

Secondo il capoverso 1, il titolare e il responsabile del trattamento devono garantire, mediante provvedimenti tecnici e organizzativi appropriati, che la sicurezza dei dati personali sia adeguata al rischio. Quanto più alto è il rischio di una violazione tanto più elevati dovranno essere i requisiti posti ai provvedimenti da adottare.

Il capoverso 2 elenca gli obiettivi dei suddetti provvedimenti. Questi devono permettere di evitare violazioni della sicurezza dei dati, ossia qualsiasi violazione in seguito alla quale, in modo accidentale o illecito, dati personali vanno persi, sono cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate (art. lett. g D-LPD). Sono ipotizzabili i seguenti provvedimenti: pseudonimizzazione dei dati, adozione di misure che garantiscono la confidenzialità e la disponibilità del sistema e dei suoi servizi, sviluppo di procedure che permettano di esaminare, verificare e valutare regolarmente l'efficienza delle misure tecniche e organizzative volte a garantire la sicurezza dei dati.

Anche se vi è un rapporto reciproco tra la protezione dei dati e la sicurezza dei dati, le due nozioni vanno distinte. La protezione dei dati riguarda la protezione della personalità del singolo individuo. La sicurezza dei dati concerne invece in generale i dati presso un titolare o un responsabile del trattamento e riguarda il quadro tecnico e organizzativo del trattamento. La protezione dei dati della singola persona è pertanto possibile soltanto se vengono adottati i provvedimenti tecnici necessari per garantire la sicurezza dei dati. Da ciò si evince la delimitazione tra l'obbligo della sicurezza dei dati dell'articolo 7 D-LPD e la protezione dei dati fin dalla progettazione dell'articolo 6 capoverso 1 D-LPD. L'articolo 7 obbliga sia il titolare che il responsabile del trattamento a prevedere per i loro sistemi un'adeguata architettura di sicurezza, proteggendoli ad esempio da software dannosi o dalla perdita di dati. L'articolo 6 capoverso 1 mira invece a garantire, mediante mezzi tecnici appropriati, il rispetto delle disposizioni sulla protezione dei dati, ad esempio la proporzionalità del trattamento rispetto allo scopo perseguito. Ciò non toglie che singoli provvedimenti, quali ad esempio rendere anonimi i dati, possono essere importanti per l'adempimento di entrambi gli obblighi.

Il capoverso 3 obbliga il nostro Consiglio a definire i requisiti minimi in materia di sicurezza dei dati.

Art. 8 Trattamento dei dati da parte di un responsabile

L'articolo 8 riprende sostanzialmente il vigente articolo 10*a* LPD (trattamento dei dati da parte di terzi). I capoversi 1, 2 e 4 contengono modifiche terminologiche resesi necessarie a causa delle nuove espressioni introdotte nel D-LPD (responsabile del trattamento, titolare del trattamento). Come secondo il diritto vigente, si può affermare che il trattamento da parte di un responsabile di dati personali tutelati dall'articolo 321 CP (p. es. dati contemplati dal segreto medico) non è vietato dalla disposizione dell'articolo 8 capoverso 1 lettera b D-LPD, se il responsabile è da considerarsi un ausiliare ai sensi dell'articolo 321 numero 1 comma 1 CP[128]. Se sono soddisfatte le altre condizioni del trattamento da parte di un responsabile, tale trattamento è lecito anche senza il consenso ulteriore della persona interessata[129].

128 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, n. 1227 con altri rinvii.

129 Di parere diverso ad esempio Wohlers Wolfgang, Outsourcing durch Berufsgeheimnisträger, Patienten- und Mandantengeheimnisse als Schranke bei der Auslagerung von Datenverarbeitungen, digma 2016, pag. 114 segg.

Il capoverso 1 sancisce l'obbligo del titolare del trattamento di garantire che, nel caso di affidamento del trattamento a un responsabile, i diritti della persona interessata siano salvaguardati. Il titolare del trattamento deve garantire che il responsabile del trattamento rispetti la legge in misura uguale a lui. Ciò riguarda in particolare il rispetto dei principi generali, delle regole relative alla sicurezza dei dati, espressamente menzionate nel capoverso 2, e delle regole relative alla comunicazione all'estero. Analogamente a quanto previsto dall'articolo 55 CO, il titolare del trattamento deve impedire le violazioni della LPD. Deve pertanto scegliere con cura il responsabile del trattamento, istruirlo in modo adeguato e sorvegliarlo nella misura del necessario[130].

Secondo il nuovo capoverso 3, il responsabile del trattamento può conferire il trattamento a un terzo soltanto previa autorizzazione del titolare del trattamento. Nel settore privato, l'autorizzazione non sottostà a regole formali. Spetta tuttavia al responsabile del trattamento provarne l'esistenza e quindi questi ha tutto l'interesse a documentarla. Nel settore pubblico l'autorizzazione deve invece essere scritta. Si tratta di una condizione della direttiva (UE) 2016/680 (art. 22 par. 2). Il nostro Consiglio lo stabilirà in un'ordinanza. Sia nel settore privato che in quello pubblico, l'autorizzazione può essere specifica o generale. Nel secondo caso il responsabile del trattamento informa il titolare di qualsiasi modifica (aggiunta o sostituzione di mandatari), in modo da permettergli di presentare obiezioni.

I trattamenti in seno a una stessa persona giuridica (succursale, unità amministrativa, collaboratore) non costituiscono in linea di principio un caso di conferimento del trattamento a un responsabile[131].

Se i dati sono conservati in una cosiddetta cloud, si tratta fondamentalmente di un caso di trattamento da parte di un responsabile e devono quindi essere soddisfatte le pertinenti condizioni. Se a tal fine sono comunicati dati all'estero, devono inoltre essere soddisfatte le condizioni di cui agli articoli 13 e 14 D-LPD.

Art. 9 Consulente per la protezione dei dati

L'articolo 9 disciplina il ruolo del consulente interno per la protezione dei dati. Il diritto vigente impiega il termine «Datenschutzverantwortlicher» in tedesco, «responsabile della protezione dei dati» in italiano e «conseiller à la protection des données» in francese (art. 11*a* cpv. 5 lett. e LPD). Per evitare confusione con il «Verantwortlicher» di cui all'articolo 4 lettera i D-LPD e il «responsabile» di cui all'articolo 4 lettera j nelle versioni rispettivamente tedesca e italiana, il D-LPD introduce i termini «Datenschutzberater» e «consulente per la protezione dei dati». In questo modo la terminologia è uniforme in tutte e tre le lingue.

Il consulente per la protezione dei dati sorveglia il rispetto delle disposizioni sulla protezione dei dati in seno a un'impresa e fornisce consulenza ai titolari del trattamento nelle questioni inerenti alla protezione dei dati. Spetta tuttavia unicamente ai

130 FF **1988** 353, in particolare pag. 403.
131 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, n. 1201. Sulla questione del collaboratore si veda anche la considerazione 23 del progetto di rapporto esplicativo del P-STE 108.

titolari del trattamento assumersi la responsabilità per il trattamento dei dati personali conforme alle disposizioni sulla protezione dei dati.

Questa disposizione è introdotta nel D-LPD, poiché in sede di consultazione è stata auspicata la menzione esplicita del consulente per la protezione dei dati nella legge. Il D-LPD è tuttavia meno severo del diritto dell'Unione europea, che in certi casi prevede l'obbligo di nominare un consulente, un obbligo che avrebbe auspicato anche l'Incaricato. Secondo il D-LPD le imprese sono libere di nominare o meno un consulente, mentre gli organi federali sono tenuti a farlo.

Cpv. 1 e 2 Nomina

I titolari privati del trattamento sono in linea di massima liberi di nominare un consulente per la protezione dei dati in qualsiasi momento (cpv. 1). In riferimento alla valutazione d'impatto sulla protezione dei dati la legge prevede agevolazioni per i titolari del trattamento che hanno nominato un consulente.

Il capoverso 2 definisce le condizioni che devono essere soddisfatte affinché si applichino tali agevolazioni (lett. a), riprendendo in larga misura il diritto vigente (cfr. art. 12*a* seg. OLPD).

Il titolare del trattamento può nominare consulente per la protezione dei dati un collaboratore o un terzo. Secondo la lettera a, il consulente deve tuttavia esercitare la sua funzione in modo indipendente e senza essere vincolato alle istruzioni del titolare del trattamento. Se la funzione è svolta da un collaboratore, l'ordine gerarchico in seno all'impresa deve garantire che il consulente resti indipendente. In linea di principio dovrebbe essere sottoposto direttamente alla direzione del titolare del trattamento.

La lettera b precisa ulteriormente l'indipendenza del consulente per la protezione dei dati: egli non può svolgere attività inconciliabili con i suoi compiti. Ciò potrebbe essere il caso se il consulente è membro della direzione, esercita funzioni nel settori della conduzione del personale o della gestione dei sistemi informatici oppure se fa parte di un'unità che tratta dati personali degni di particolare protezione. È invece ipotizzabile affidare alla stessa persona le funzioni di consulente per la protezione dei dati e incaricato della sicurezza delle informazioni.

Secondo la lettera c, il consulente per la protezione dei dati deve disporre delle conoscenze tecniche necessarie per assolvere la sua funzione. Sono necessarie conoscenze sia del settore della legislazione sulla protezione dei dati sia degli standard della sicurezza dei dati.

In riferimento ai trattamenti di dati effettuati dall'impresa per cui svolge la sua funzione, il consulente per la protezione dei dati è un'importante persona di contatto sia per la persona interessata sia per l'Incaricato. Secondo la lettera d il titolare del trattamento deve pubblicare e comunicare all'Incaricato le coordinate di contatto del consulente. L'ordinanza dovrà prevedere un obbligo analogo anche per gli organi federali.

Cpv. 3 Consulente per la protezione dei dati degli organi federali

Il capoverso 3 obbliga il nostro Consiglio ad emanare le regole per la nomina del consulente per la protezione dei dati da parte degli organi federali. Anche nel diritto vigente la maggior parte di tali regole si trova nell'ordinanza.

In virtù dell'articolo 32 della direttiva (UE) 2016/680, nell'ambito di Schengen gli organi federali sono tenuti a nominare un consulente per la protezione dei dati.

Art. 10 Codice di condotta

Il nostro Consiglio intende incoraggiare l'elaborazione di codici di condotta Questi corrispondono a un bisogno identificato dall'analisi d'impatto della regolamentazione (cfr. n. 1.8) in considerazione del carattere generale della legislazione e del suo ampio campo d'applicazione personale e materiale. I codici di condotta permetterebbero di precisare certi concetti, quali il rischio elevato (art. 20 D-LPD), o le modalità di determinati obblighi, quali l'obbligo di informare (art. 17–19 D-LPD) o quello di effettuare un'analisi d'impatto sulla protezione dei dati (art. 20 P-LPD). L'idea è anche di trovare soluzioni più precise in ambiti specifici che oggi sollevano numerose questioni, quali la videosorveglianza, il cloud-computing o le reti sociali[132].

Permettendo alle cerchie interessate di partecipare attivamente alla regolamentazione del settore, intendiamo favorire soluzioni specifiche, concordate e largamente accettate dai singoli settori. Per incoraggiare l'autoregolamentazione, proponiamo inoltre che i titolari del trattamento che adottano codici di condotta possano, a certe condizioni, rinunciare all'analisi d'impatto sulla protezione dei dati (art. 20 cpv. 5 D-LPD).

Anche secondo il regolamento (UE) 2016/679 (art. 40 e 57 par. 1 lett. m) l'autorità di controllo deve incoraggiare gli Stati membri ad adottare codici di condotta.

Nel settore privato i codici di condotta devono essere elaborati dalle associazioni professionali ed economiche autorizzate dai loro statuti a difendere gli interessi economici dei loro membri[133]. Singoli titolari o responsabili del trattamento non possono sottoporre codici di condotta all'Incaricato, poiché questi ultimi hanno come obiettivo una certa uniformazione all'interno di un determinato ramo. Nel settore pubblico i codici di condotta possono invece essere elaborati da un singolo organo federale, il che si giustifica in particolare con le numerose basi legali e la molteplicità dei compiti dei vari organi.

132 Va osservato che nel settore di Internet e delle telecomunicazioni, le cerchie interessate hanno adottato documenti che, benché non riguardino direttamente la protezione dei dati, in determinati casi tutelano anche i diritti delle persone interessate. Si tratta, da una parte, della recente iniziativa dell'Associazione svizzera delle telecomunicazioni per una migliore protezione della gioventù nei nuovi mezzi di comunicazione e per la promozione delle competenza in materia nella società, che, per i firmatari, prevede certi obblighi riguardanti il blocco di determinati siti Internet e l'adozione di misure per migliorare la protezione della gioventù nei nuovi mezzi di comunicazione. Dall'altra, si tratta del Codice di condotta hosting, (CCH) adottato dalla Swiss Internet Industry Association (Simsa) il 1° feb. 2013 e destinato ai fornitori di servizi di hosting.

133 Si tratta della formulazione usata anche nell'art. 10 cap. 2 LCSl

Il capoverso 1 prevede che i codici di condotta possono essere sottoposti all'Incaricato, il quale si esprime in merito (cpv. 2). Il termine entro cui deve esprimere un parere dipende dalle circostanze del singolo caso.

Il parere dell'Incaricato non costituisce una decisione e quindi le cerchie interessate non possono dedurre diritti da un parere positivo o dall'assenza di un parere. Ciononostante, se l'Incaricato fornisce un parere favorevole si può supporre che un comportamento conforme al codice di condotta non sarà oggetto di provvedimenti amministrativi. L'Incaricato pubblica il suo parere a prescindere dal fatto che sia positivo o negativo.

L'Incaricato avrebbe auspicato un obbligo delle associazioni professionali ed economiche di sottoporgli i codici di condotta per approvazione. Vi abbiamo tuttavia rinunciato in seguito ai risultati della consultazione, ma anche perché l'Incaricato avrebbe dovuto emanare una decisione amministrativa, il che avrebbe causato spese ulteriori.

Art. 11 Registro delle attività di trattamento

In sostituzione dell'obbligo di documentazione dell'avamprogetto, il D-LPD prevede l'obbligo di tenere un registro delle attività di trattamento, poiché in sede di consultazione l'obbligo di documentazione è stato giudicato troppo poco chiaro. Inoltre, il registro delle attività di trattamento è ora inserito nelle disposizioni generali sulla protezione dei dati, al fine di evidenziare lo stretto nesso con i principi della protezione dei dati. L'obbligo di tenere un registro delle attività di trattamento sostituisce l'obbligo di notificazione delle collezioni di dati previsto dal diritto vigente. Anche l'articolo 24 della direttiva (UE) 2016/680 prevede un tale registro e l'articolo 30 del regolamento (UE) 2016/679 contiene una disposizione analoga.

Secondo il capoverso 1, l'obbligo di tenere un registro delle attività di trattamento incombe al titolare e al responsabile del trattamento.

Il capoverso 2 enumera le indicazioni minime che il registro deve contenere. Ne fanno parte innanzitutto l'identità (il nome) del titolare del trattamento (lett. a) e lo scopo del trattamento (lett. b). Va inoltre indicata una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati (lett. c). Per categorie di persone interessate s'intendono gruppi tipici che hanno determinate caratteristiche comuni, ad esempio i «consumatori», i «membri dell'esercito» o i «lavoratori». La categoria di dati personali designa il tipo di dati trattati, ad esempio dati personali degni di particolare protezione. Vanno inoltre elencate le categorie di destinatari (lett. d) cui sono resi noti i dati personali. Anche in questo caso s'intendono gruppi tipici con caratteristiche comuni, ad esempio le «autorità di sorveglianza». Secondo la lettera e l'elenco deve contenere la durata di conservazione dei dati personali. Dato che la durata di conservazione secondo l'articolo 5 capoverso 4 si basa sullo scopo del trattamento, a volte non è possibile fissare la durata di conservazione per cui è stata aggiunta l'espressione «se possibile». Se non sono possibili indicazioni precise il registro deve contenere almeno i criteri che determinano la durata di conservazione. Secondo la lettera f il registro deve infine contenere, se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati secondo l'articolo 7. Tale descrizione mira a permettere di illustrare le lacune nei provvedi-

menti per garantire la sicurezza. L'espressione «se possibile» chiarisce che la descrizione è richiesta soltanto se i provvedimenti possono essere illustrati in modo sufficientemente chiaro. Se i destinatari dei dati personali si trovano all'estero, dal registro si deve poter evincere se sono adempite le condizioni per la comunicazione all'estero. Pertanto, secondo la lettera g, devono essere indicati lo Stato terzo e le garanzie di cui all'articolo 13 capoverso 2.

L'elenco del capoverso 2 chiarisce che il registro contiene una descrizione generale delle attività di trattamento da cui si evince il tipo e la portata del trattamento. Il registro non è invece un diario di tutti i trattamenti del titolare o del responsabile del trattamento in cui, alla stregua di un verbale, è elencata ogni singola attività. Contiene piuttosto una descrizione delle informazioni più importanti relative a tutti i trattamenti di un titolare o responsabile. Permette quindi di ricavare informazioni importanti sulla conformità di un trattamento con i principi della protezione dei dati. Inoltre, le indicazioni minime di cui al capoverso 2 corrispondono in gran parte alle indicazioni che la persona interessata deve ricevere in virtù dell'obbligo di informarla e del diritto d'accesso.

Il capoverso 3 contiene un elenco più breve delle indicazioni che deve contenere il registro del responsabile del trattamento. Si tratta in particolare delle categorie di trattamenti eseguiti su incarico di ciascun titolare e pertanto il registro del responsabile contiene anche l'identità dei titolari su incarico dei quali tratta dati.

Secondo il capoverso 4 gli organi federali notificano i loro registri all'Incaricato. Conformemente all'articolo 50 D-LPD, quest'ultimo tiene un registro della attività di trattamento degli organi federali. Tale registro è pubblico. Per gli organi federali non risultano pertanto in linea di massima modifiche rispetto al diritto vigente. Già oggi devono infatti elaborare un regolamento per il trattamento e annunciare il trattamento all'Incaricato.

Il capoverso 5 conferisce al nostro Consiglio la possibilità di prevedere eccezioni dall'obbligo di tenere un registro per le imprese con meno di 50 collaboratori. Questa disposizione intende in particolare sgravare le piccole e medie imprese. Oltre che della grandezza dell'impresa, il nostro Consiglio dovrà tenere conto anche dei rischi che comportano i loro trattamenti di dati.

Art. 12 Certificazione

L'articolo 12 D-LPD disciplina la certificazione facoltativa che figura attualmente all'articolo 11 LPD. Oltre ai sistemi di trattamento dei dati (procedura e organizzazione) e ai prodotti (programmi, sistemi), sarà in futuro possibile certificare anche determinati servizi.

I titolari del trattamento oggetto di una certificazione sono liberati dall'obbligo di procedere a un'analisi d'impatto sulla protezione dei dati (art. 20 cpv. 5 D-LPD).

La procedura di accreditamento per i servizi di certificazione indipendenti svolta dal Servizio di accreditamento svizzero, a cui è associato anche l'Incaricato, resta invariata[134].

L'Incaricato avrebbe auspicato introdurre un obbligo di certificazione per i trattamenti ad alto rischio. Vi abbiamo rinunciato poiché non si tratta di un requisito del diritto dell'Unione europea.

9.1.3.2 Comunicazione di dati personali all'estero

Art. 13 Principi

La disposizione soddisfa i requisiti dell'articolo 12 del P-STE 108, che sancisce il principio secondo cui i dati possono essere trasmessi all'estero soltanto se è garantita una protezione adeguata (par. 2). Il paragrafo 3 di tale articolo definisce i casi in cui tale condizione è soddisfatta. Il disciplinamento previsto dall'articolo 13 D-LPD costituisce anche un adeguamento al diritto dell'Unione europea (art. 45 segg. del regolamento (UE) 2016/679).

Le regole relative alla comunicazione di dati personali sono in parte state rivedute per tenere conto dei risultati della procedura di consultazione. Il principio secondo cui non può essere trasmesso all'estero alcun dato personale se ne risulta un grave rischio per la personalità della persona interessata è stato soppresso poiché crea un'incertezza giuridica in relazione alla sistematica della normativa. La terminologia relativa alla comunicazione di dati personali all'estero per mezzo di garanzie appropriate è adeguata a quella del regolamento (UE) 2016/679. Le eccezioni relative alla comunicazione di dati personali a uno Stato la cui legislazione non garantisce una protezione dei dati adeguata sono inoltre leggermente meno severe. Infine sono mantenuti soltanto gli obblighi d'informare l'Incaricato o di ottenere la sua autorizzazione previsti dal P-STE 108.

Cpv. 1 Constatazione del Consiglio federale mediante decisione

Secondo il capoverso 1 possono essere comunicati dati all'estero se il Consiglio federale ha constatato che la legislazione dello Stato estero o l'organismo internazionale garantisce una protezione adeguata dei dati. La disposizione conferisce esplicitamente al nostro Consiglio la competenza di verificare l'adeguatezza della legislazione estera in materia di protezione dei dati.

La situazione attuale è insoddisfacente, poiché secondo il diritto vigente spetta al detentore della collezione di dati che intende comunicare dati all'estero verificare che lo Stato destinatario garantisca una protezione dei dati adeguata[135], ricorrendo,

134 Cfr. l'ordinanza del 17 giu. 1996 sull'accreditamento e sulla designazione (RS **946.512**) e l'art. 2 dell'ordinanza del 28 sett. 2007 sulle certificazioni in materia di protezione dei dati (RS **235.13**).

135 FF **2003** 1885, in particolare pag. 1910 seg.

se del caso, all'elenco degli Stati che soddisfano tale condizione pubblicato dall'Incaricato (art. 7 OLPD)[136].

Per garantire l'applicazione uniforme dell'articolo 13, l'adeguatezza della legislazione di uno Stato estero sarà in futuro verificata dal nostro Consiglio. Oltre a verificare che lo Stato estero disponga di una legislazione che sotto il profilo materiale adempie i requisiti del P-STE 108, nel suo esame il nostro Consiglio dovrà anche valutare il modo in cui tale Stato applica la legislazione. La verifica può anche riguardare l'adeguatezza della protezione garantita da un organismo internazionale. La nozione di «organismo internazionale» comprende qualsiasi istituzione internazionale, a prescindere che si tratti di un'organizzazione o di un'autorità giurisdizionale.

Il risultato della verifica sarà pubblicato in un'ordinanza del nostro Consiglio inserita nella Raccolta sistematica del diritto federale. In tale ordinanza occorrerà precisare che il nostro Consiglio dovrà regolarmente verificare la situazione e che l'Incaricato pubblicherà anche sul suo sito un elenco degli Stati o organismi internazionali per i quali il nostro Consiglio ha constatato una protezione adeguata dei dati.

L'ordinanza è strutturata come elenco positivo ed enumera gli Stati che dispongono di una legislazione che garantisce una protezione adeguata. Se uno Stato estero non figura nell'elenco, ciò significa che la sua legislazione non è ancora stata esaminata oppure che il nostro Consiglio è giunto alla conclusione che essa non soddisfa i requisiti per garantire una protezione adeguata. Con la revisione, l'elenco del nostro Consiglio diventa un criterio legale vincolante per i titolari del trattamento, mentre l'elenco dell'Incaricato previsto dal diritto vigente è inteso come mero strumento ausiliario messo a disposizione dei titolari. La nuova soluzione favorisce la certezza del diritto.

Per la sua verifica, il nostro Consiglio potrà fondarsi sulle fonti disponibili, in particolare le valutazioni effettuate nell'ambito della Convenzione STE 108 o dell'Unione europea. Sarebbe anche pensabile che collabori con autorità estere e si associ ai loro processi di verifica.

Se il nostro Consiglio constata che la legislazione di uno Stato o un organismo internazionale garantisce una protezione adeguata, la libera comunicazione di dati personali a tale Stato o a tali organismi è consentita sia nel settore privato che in quello pubblico.

Cpv. 2 Assenza di una decisione del Consiglio federale

In assenza di una decisione del nostro Consiglio ai sensi del capoverso 1, il capoverso 2 prevede che i dati personali possono essere comunicati all'estero se è garantita una protezione appropriata dei dati.

Secondo la lettera a, una protezione appropriata può essere garantita da un trattato internazionale. Per «trattato internazionale» non s'intende soltanto una convenzione internazionale sulla protezione dei dati di cui lo Stato destinatario sia parte, come ad esempio la Convenzione STE 108 e il suo Protocollo aggiuntivo, e i cui requisiti sono stati trasposti nel diritto nazionale, bensì anche qualsiasi altro trattato interna-

136 L'elenco dell'Incaricato è consultabile al seguente indirizzo: www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=it.

zionale che preveda lo scambio di dati tra gli Stati contraenti e che rispetti sostanzialmente le condizioni della Convenzione STE 108. Può anche trattarsi di un trattato internazionale che il nostro Consiglio ha concluso in virtù dell'articolo 62 lettera b D-LPD.

Il capoverso 2 lettere b–d corrisponde alle condizioni dell'articolo 12 paragrafo 3 lettera b del P-STE 108, secondo cui una protezione dei dati appropriata può essere assicurata mediante garanzie contrattuali specifiche o standardizzate, fissate da strumenti giuridici vincolanti e opponibili, concluse e attuate dalle persone coinvolte nel trasferimento e nel successivo trattamento dei dati. L'articolo 46 del regolamento (UE) 2016/679 prevede una regolamentazione analoga. Lo stesso vale per la direttiva (UE) 2016/680 (art. 37).

Lett. b Clausole contrattuali di protezione dei dati

Secondo il capoverso 2 lettera b i dati possono essere trasferiti all'estero se il titolare o il responsabile del trattamento e la controparte hanno concordato clausole contrattuali di protezione dei dati. La nozione di «clausole contrattuali di protezione dei dati» corrisponde alla terminologia dell'articolo 46 paragrafo 3 lettera a del regolamento (UE) 2016/679. Le clausole devono essere previamente comunicate all'Incaricato. Non appena tale obbligo di comunicazione è stato rispettato, i dati personali possono essere trasmessi all'estero. Se del caso, l'Incaricato può aprire un'inchiesta per stabilire se le clausole sono sufficienti. Come nel diritto vigente, spetta al titolare del trattamento dimostrare che ha preso tutti i provvedimenti necessari affinché sia garantita una protezione appropriata e che il destinatario rispetta le clausole contrattuali sulla protezione dei dati. Contrariamente alle clausole standardizzate sulla protezione dei dati (lett. d), le clausole di un contratto valgono solo per le comunicazioni previste da tale contratto.

Lett. c Garanzie specifiche

Nel settore pubblico, l'organo federale può, quando acconsente alla cooperazione con uno Stato estero, fissare garanzie specifiche da rispettare in materia di protezione dei dati. Può ad esempio trattarsi di una convenzione con lo Stato estero in questione. L'organo federale deve previamente comunicare le garanzie all'Incaricato. Non appena ha adempito tale obbligo, può comunicare i dati personali all'estero.

Lett. d Clausole tipo di protezione dei dati

Secondo il capoverso 2 lettera d, i dati personali possono essere comunicati all'estero per mezzo di clausole tipo di protezione dei dati. La disposizione riprende la terminologia dell'articolo 46 paragrafo 2 lettera c del regolamento (UE) 2016/679. Le clausole possono essere elaborate dai privati, dalle cerchie interessate o dagli organi federali oppure stabilite o riconosciute dall'Incaricato. Per «clausole tipo» s'intendono ad esempio clausole contrattuali standardizzate inserite nel contratto tra il titolare del trattamento e il destinatario o anche un codice di condotta elaborato dal settore privato al quale le persone private possono aderire volontariamente.

Nel primo caso, le clausole devono essere previamente approvate dall'Incaricato. Questa condizione è più rigida rispetto al diritto in vigore, il quale prevede soltanto l'obbligo di informare l'Incaricato (art. 6 cpv. 3 LPD). Corrisponde a quella prevista

dall'articolo 12bis paragrafo 2 lettera b P-STE 108. Il titolare del trattamento non può comunicare dati all'estero prima di aver ricevuto una pertinente decisione impugnabile dell'Incaricato (art. 5 PA). Durante tale procedura può tuttavia avvalersi dell'articolo 13 capoverso 2 lettere b o c. Il termine entro cui l'Incaricato deve rendere la sua decisione è retto dall'ordinanza del 25 maggio 2011[137] sui termini ordinatori: secondo il suo articolo 4 il termine fissato all'autorità per prendere la decisione dipende dalla complessità della domanda; il termine massimo è di tre mesi.

Nel secondo caso, il titolare del trattamento può anche ricorrere alle clausole tipo stabilite o riconosciute dall'Incaricato, ad esempio contratti modello. Se il titolare del trattamento comunica dati all'estero ricorrendo alle clausole tipo ai sensi del capoverso 2 lettera d, si può presumere che egli abbia preso tutti i provvedimenti necessari per garantire una protezione dei dati appropriata. Tuttavia, questa presunzione non lo libera da qualsiasi responsabilità per eventuali pregiudizi risultanti dalla violazione di tali clausole, in particolare da parte del destinatario dei dati. Sarà pertanto opportuno prevedere nell'ordinanza l'obbligo dell'Incaricato di pubblicare un elenco di clausole tipo di protezione dei dati standardizzate consolidate o riconosciute, come d'altronde previsto dal diritto in vigore (art. 6 cpv. 3 OLPD).

Lett. e Norme vincolanti d'impresa

Secondo il capoverso 2 lettera e, dati personali possono essere comunicati all'estero se la loro protezione è garantita da norme vincolanti d'impresa previamente approvate dall'Incaricato o da un'autorità incaricata della protezione dei dati all'estero. Questa disposizione sostituisce l'articolo 6 capoverso 2 lettera g LPD e si adegua al diritto dell'Unione europea, che prevede che i membri di un gruppo imprenditoriale possono comunicarsi dati se la loro protezione è garantita da norme vincolanti d'impresa previamente approvate dall'autorità di controllo della protezione dei dati (art. 47 del regolamento (UE) 2016/679). L'approvazione delle norme vincolanti d'impresa è disciplinata dall'articolo 57 paragrafo 1 lettera s del regolamento (UE) 2016/679. Il capoverso 2 lettera e costituisce un inasprimento del diritto in vigore poiché le norme vincolanti d'impresa devono essere approvate. Il titolare del trattamento non può ricorrere alle norme vincolanti d'impresa prima di aver ottenuto una decisione impugnabile dell'Incaricato (art. 5 PA). Durante tale procedura può tuttavia avvalersi dell'articolo 13 capoverso 2 lettere b o c.

Per tenere conto delle esigenze dei gruppi imprenditoriali con sedi in vari Stati, il capoverso 2 lettera e prevede che un'impresa con sede in Svizzera appartenente a un tale gruppo può anche ricorrere alle norme vincolanti d'impresa approvate da un'autorità incaricata della protezione dei dati appartenente a uno Stato che garantisce una protezione adeguata.

Le norme di cui al capoverso 2 lettera e devono essere «vincolanti», vale a dire che tutte le società che fanno parte di uno stesso gruppo imprenditoriale sono tenute a rispettarle e applicarle. Le norme devono precisare almeno la comunicazione di dati, le categorie dei dati comunicati, le finalità, le categorie di persone interessate e i Paesi destinatari. Inoltre, devono disciplinare i diritti delle persone interessate e precisare i meccanismi del gruppo imprenditoriale volti a garantire il controllo delle

137 RS **172.010.14**

regole normative. Se necessario, nell'ordinanza d'esecuzione il nostro Consiglio definirà i criteri che devono soddisfare le norme vincolanti d'impresa.

Cpv. 3 Delega legislativa

La disposizione autorizza il nostro Consiglio a prevedere altre garanzie appropriate ai sensi del capoverso 2. Non è infatti escluso che si sviluppino altri strumenti, quali un regime di autocertificazione analogo a quello previsto dallo Swiss-US Privacy Shield (cfr. art. 46 par. 2 lett. f del regolamento [UE] 2016/679).

Art. 14 Deroghe

Cpv. 1

Analogamente al diritto in vigore (art. 6 cpv. 2 LPD), l'articolo 14 capoverso 1 D-LPD disciplina i casi in cui i dati possono essere comunicati all'estero nonostante l'assenza di una protezione appropriata. L'articolo corrisponde sostanzialmente all'articolo 12 paragrafo 4 del P-STE 108 e all'articolo 49 del regolamento (UE) 2016/679. L'articolo 38 della direttiva (UE) 2016/680 prevede un disciplinamento analogo.

La lettera a corrisponde all'articolo 6 capoverso 2 lettera b LPD, salvo che il consenso della persona interessata deve essere dato espressamente e la precisazione «nel caso specifico» è stata soppressa. Il consenso espresso è un requisito del P-STE 108 (art. 12 par. 4 lett. a). Su questo punto rinviamo al commento all'articolo 5 capoverso 6 D-LPD. La persona interessata deve in particolare sapere il nome dello Stato terzo (art. 17 cpv. 4 D-LPD) ed essere informata sui rischi della comunicazione dei dati in seguito al livello della protezione dei dati dello Stato estero. Quanto all'espressione «nel caso specifico», riteniamo che possa essere soppressa. Come si evince dall'articolo 5 capoverso 6 D-LPD, la persona interessata dà il suo consenso per uno o più trattamenti determinati. La precisazione «nel caso specifico» è pertanto superflua.

La lettera b corrisponde all'articolo 6 capoverso 2 lettera c LPD, salvo che i dati personali possono essere comunicati all'estero se la comunicazione è in relazione diretta con la conclusione o l'esecuzione diretta di un contratto non solo tra il titolare del trattamento e la persona interessata, ma anche tra il titolare e un altro contraente, nell'interesse della persona interessata. L'articolo 49 paragrafo 1 del regolamento (UE) 2016/679 prevede una disposizione analoga.

La lettera c numero 1 corrisponde al primo caso contemplato dall'articolo 6 capoverso 2 lettera d LPD. Nella frase introduttiva, il termine «indispensabile» è sostituito da «necessario» in adeguamento ai testi europei. L'interesse pubblico preponderante deve essere dimostrato con le circostanze del caso specifico e non è sufficiente un interesse meramente ipotetico. Per «interesse pubblico preponderante» s'intende ad esempio la sicurezza interna della Svizzera o di uno Stato terzo. In virtù di questa disposizione possono essere comunicati dati all'estero anche nell'ambito di operazioni umanitarie, ad esempio se il titolare del trattamento li comunica per aiutare a cercare persone disperse in una regione di conflitto o in una regione ove si è verificata una catastrofe naturale.

La lettera c numero 2 corrisponde al secondo caso contemplato dall'articolo 6 capoverso 2 lettera d LPD, salvo che l'espressione «in giustizia», ritenuta troppo limitativa, è sostituita con «dinanzi a un'autorità giudiziaria o amministrativa».

La lettera d precisa che la comunicazione è lecita se è necessaria non solo per proteggere la vita o l'integrità fisica della persona interessata ma anche quella di un terzo, e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole, ad esempio perché non è fisicamente in grado di farlo o perché non è raggiungibile con i mezzi di comunicazione usuali.

La lettera e corrisponde all'articolo 6 capoverso 2 lettera f LPD.

La lettera f è una nuova disposizione. Precisa che la condizione dell'appropriatezza della protezione dei dati non si applica se si tratta di comunicare all'estero dati provenienti da un registro pubblico previsto dalla legge, a condizione che siano soddisfatte determinate condizioni legali. L'articolo 49 paragrafo 1 lettera g del regolamento (UE) 2016/679 va nella stessa direzione, in quanto dispone che in assenza di una protezione appropriata la comunicazione di dati a partire da un registro è lecita se, a norma del diritto dell'Unione europea o degli Stati membri, mira a fornire informazioni al pubblico e se sono soddisfatte determinate condizioni legali.

Cpv. 2

Secondo questa disposizione l'Incaricato può chiedere al titolare o al responsabile del trattamento di informarlo sulla comunicazione di dati personali di cui al capoverso 1 lettere b numero 2, c e d. La norma corrisponde ai requisiti dell'articolo 12 paragrafo 5 P-108. Il penultimo periodo dell'articolo 49 paragrafo 1 del regolamento (UE) 2016/679 va oltre, poiché prevede l'obbligo del titolare del trattamento di informare spontaneamente l'autorità di controllo sulla comunicazione di dati personali effettuata in virtù dell'articolo 47.

Art. 15 Pubblicazione di dati personali in forma elettronica

Questa disposizione riprende il contenuto dell'articolo 5 OLPD e disciplina la comunicazione di dati personali mediante Internet o altri servizi d'informazione o di comunicazione al fine di informare il pubblico. 'È quindi possibile consultare all'estero su Internet informazioni contenenti dati personali, anche in uno Stato che non garantisce una protezione adeguata dei dati. La pubblicazione di dati personali su Internet al fine di informare il pubblico, come ad esempio nel caso dei mezzi d'informazione, non è pertanto assimilata alla comunicazione di dati all'estero.

9.1.3.3 Dati di persone decedute

Art. 16

La disposizione disciplina vari aspetti riguardanti la gestione di dati di persone decedute, che sollevano regolarmente questioni pratiche. Alcune sono di tipo fondamentale, ad esempio in che misura sia protetta la personalità di una persona deceduta e sia necessario proteggere gli interessi di eventuali congiunti. Sotto il profilo

costituzionale la protezione della personalità (art. 10 e 13 Cost.) si applica anche oltre la morte, ad esempio per quanto riguarda il desiderio di una persona deceduta in riferimento alla sua sepoltura[138]. Per contro, in Svizzera non sussiste un diritto della personalità posteriore alla morte che protegga il defunto che in vita non ha espresso un relativo desiderio o che non ha congiunti che ne tutelino i diritti[139]. Dal punto di vista del diritto civile la personalità si estingue con la morte (cfr. art. 31 cpv. 1 CC)[140]. Ciononostante il Tribunale federale è del parere che in determinati ambiti il diritto della personalità, e quindi pure la sua tutela, sussista anche dopo la morte[141]. Poiché la protezione dei dati serve alla tutela della personalità, tale principio va parimenti applicato ai dati delle persone decedute. Sotto il profilo del diritto penale la personalità è tutelata anche dopo la morte, ad esempio nell'ambito della tutela del segreto[142].

Nel diritto vigente, il trattamento dei dati di persone defunte è disciplinato unicamente dall'articolo 1 capoverso 7 OLPD. La consultazione dei dati di una persona deceduta è parte del diritto d'accesso. Si tratta tuttavia di un diritto che la persona interessata può far valere soltanto in relazione al trattamento di dati che la riguardano personalmente. Con la disposizione dell'ordinanza il diritto d'accesso è stato esteso a terzi che possono chiedere informazioni sui dati di un altro terzo, senza che la legge preveda una pertinente base legale. La trasposizione nella legge permette dunque di risolvere questo problema. Sotto il profilo sistematico la norma è inserita nelle disposizioni generali sulla protezione dei dati, staccandola così da quelle sul diritto d'accesso, poiché quest'ultimo deve rimanere circoscritto alla persona interessata. Di fatto, il D-LPD riprende il diritto in vigore apportando le modifiche formali e materiali necessarie ed eliminando le incertezze attuali. Garantisce inoltre che la volontà della persona deceduta sia rispettata nel miglior modo possibile.

Oltre a garantire l'accesso ai dati di una persona deceduta, la disposizione proposta risponde a parte del postulato 14.3782 Schwaab «Regole per la ‹morte digitale›», in quanto il capoverso 2 prevede il diritto degli eredi di cancellare o distruggere i dati della persona deceduta. Ciò permette in linea di principio agli eredi di provocare la «morte digitale», a condizione che non vi si oppongano interessi preponderanti del defunto, del titolare del trattamento o di terzi oppure che, in vita, il defunto l'abbia esplicitamente vietato. Altre questioni sollevate dal postulato, ad esempio quelle relative alla portabilità dei dati, sono esaminate nell'ambito della revisione in corso del diritto successorio[143]. Parallelamente al diritto d'accesso secondo l'articolo 16 D-LPD, la revisione in corso del diritto successorio prevede un diritto di consultazione che vale soltanto per le persone che possono far valere diritti ereditari e che è teso a permettere loro di far valere i propri diritti patrimoniali nell'ambito della devoluzione dell'eredità (art. 601*a* AP-CC).

138 DTF **129** I 173 consid. 4; **127** I 115 consid. 4a; SGK-Schweizer, art. 10 Cost. N 10; BSK-Tschentscher, art. 10 Cost. N 47 segg. Non è chiaro se ciò si applichi anche all'autodeterminazione delle informazioni di cui all'art. 13 cpv. 2 Cost.
139 Cfr. BSK-Tschentscher, art. 10 Cost. N 47 segg.
140 Cfr. DTF **109** II 353; **127** I 145; **129** I 173; **129** I 302
141 DTF **129** I 302 consid. 1.2.
142 Cfr. DTF **135** III 597; **125** IV 298; **118** IV 319; **118** IV 153.
143 Cfr. www.bj.admin.ch/bj/it/home/gesellschaft/gesetzgebung/erbrecht.html.

Rispetto all'avamprogetto, la disposizione è più stringata e precisa, senza tuttavia modificare sostanzialmente il contenuto. In particolare non è stato ripreso l'articolo 12 capoverso 3 AP-LPD e le disposizioni sul segreto d'ufficio e professionale restano pertanto applicabili (cfr. sotto), poiché occorre evitare lacune sotto il profilo del diritto penale.

Cpv. 1 Consultazione

Secondo il capoverso 1, il titolare del trattamento deve concedere gratuitamente l'accesso ai dati di una persona deceduta se sussistono le tre condizioni di cui alle lettere a–c.

Secondo la lettera a l'accesso è concesso se sussiste un interesse alla consultazione degno di protezione o se la persona che chiede l'accesso è un parente in linea retta della persona deceduta o al momento del decesso era coniugata, viveva in unione domestica registrata o conviveva di fatto con la persona deceduta, oppure se è l'esecutore testamentario del defunto. Sussiste ad esempio un interesse alla consultazione degno di protezione se per la persona che chiede l'accesso i dati in questione sono o potrebbero essere rilevanti in un procedimento o in riferimento ai suoi diritti, quali ad esempio la tutela della sua personalità. Anche il chiarimento di conflitti familiari o personali oppure un progetto di ricerca scientifica può costituire un interesse degno di protezione. La mera curiosità non è invece considerata un interesse degno di protezione. Contrariamente a tutte le altre persone, quelle elencate alla lettera a non devono provare un interesse degno di protezione, poiché lo stretto legame di parentela o la loro relazione con il defunto motiva di per sé l'interesse alla consultazione dei dati[144]. Lo stesso vale per l'esecutore testamentario che può così assolvere pienamente il suo compito di difendere gli interessi del defunto, eseguire la sua volontà e in particolare gestirne l'eredità. Queste persone devono provare unicamente che avevano con il defunto uno dei rapporti menzionati.

Secondo la lettera b, l'accesso è concesso se non vi si oppone una dichiarazione esplicita o un interesse degno di protezione della persona deceduta. La volontà espressa del defunto è sempre prioritaria, il che permette che ciascuno decida autonomamente in merito all'accesso ai propri dati personali e alle persone autorizzate, anche dopo la sua morte. Una persona può vietare la consultazione in generale o limitarla a determinate persone o a determinati dati, ma deve farlo espressamente, come nel caso dell'articolo 26 capoverso 2 lettera b D-LPD, al cui commento si può rinviare in questa sede. In prospettiva della morte del dichiarante, per essere facilmente dimostrabile, la dichiarazione deve essere fatta, per quanto possibile, in forma di testo, ad esempio in forma di istruzione anticipata o messaggio esplicito (su carta o elettronico) indirizzati direttamente al titolare del trattamento. È ipotizzabile anche una dichiarazione sotto forma di testamento. Può tuttavia sussistere un interesse degno di protezione della persona defunta anche senza una sua dichiarazione esplicita. Ciò può essere ad esempio il caso se un incarto medico o la corrispondenza con un avvocato contiene dati (medici) specifici che non fanno parte delle informazioni usuali perché riguardano la vita sessuale, determinate malattie, il modo di vivere

144 Per la nozione di convivenza di fatto si rinvia in particolare alla dottrina e alla giurisprudenza in merito all'art. 165 cpv. 1 lett. a CPC o all'art. 10 cpv. 1 n. 2 LEF.

(dissoluto) o determinati negozi giuridici, per i quali occorre supporre che la persona deceduta non volesse concedere l'accesso in generale o a una determinata persona.

Secondo la lettera c l'accesso è negato se vi si oppongono interessi preponderanti del titolare del trattamento o di terzi. I congiunti di cui al vigente articolo 1 capoverso 7 OLPD rientrano nel concetto di «terzi». La disposizione richiede una ponderazione tra l'interesse del richiedente che chiede di consultare i dati in questione e l'interesse del titolare del trattamento o di terzi di mantenere segrete o di non fornire al richiedente le informazioni in questione. Occorre decidere nel singolo caso quali siano gli interessi preponderanti, tenendo conto, tra le altre cose, del significato che i dati rivestono per le persone coinvolte e dello scopo della consultazione. Si può essere in presenza di interessi preponderanti del titolare del trattamento nel caso in cui vi sia un suo interesse o addirittura un obbligo a mantenere il segreto. Nella prassi, i casi più importanti sono probabilmente quelli in cui all'accesso si oppongono interessi di terzi, ad esempio se dalla consultazione dei dati risulta che la persona deceduta era già stata sposata una volta o aveva un figlio nato fuori dal matrimonio. Va osservato che le persone hanno il diritto di non essere informate (cfr. art. 6 LEGU).

L'articolo 16 D-LPD si applica anche se la domanda di consultazione riguarda i dati protetti dall'obbligo penale del segreto d'ufficio o professionale (art. 320 seg. CP) del titolare del trattamento oppure dalle disposizioni penali dell'articolo 56 D-LPD. Si pensi ad esempio al figlio che chiede al medico di casa del padre defunto di consultare i dati medici di quest'ultimo. L'obbligo di diritto penale del segreto d'ufficio o professionale si applica anche dopo la morte del detentore del segreto[145], per cui in linea di principio i titolari del segreto non possono essere obbligati a rivelarlo. Se tuttavia sono adempite le condizioni di cui all'articolo 16 capoverso 1 D-LPD, il titolare del segreto è autorizzato a concedere l'accesso ai dati di una persona deceduta. In questo caso la rivelazione dei dati è un atto lecito ai sensi dell'articolo 14 CP e il titolare del segreto non può essere punito per violazione del segreto d'ufficio o professionale. L'articolo 16 D-LPD introduce pertanto un nuovo motivo giustificativo per il titolare del segreto, dato che attualmente l'unico motivo giustificativo è il consenso, anche tacito, del detentore del segreto.

L'articolo 16 D-LPD esige una ponderazione degli interessi da parte del titolare del segreto, che nella maggior parte dei casi non dovrebbe porre problemi. Se il titolare del segreto si sbaglia in merito all'importanza o all'adempimento delle condizioni di cui all'articolo 16 capoverso 1 D-LPD, occorre esaminare se vi è errore sui fatti ai sensi dell'articolo 13 CP o errore sull'illiceità ai sensi dell'articolo 21 CP. Se il titolare del segreto lo rivela nonostante abbia dubbi sulla correttezza della sua valutazione e non siano soddisfatte le condizioni di cui all'articolo 16, può esservi violazione per duolo eventuale dell'obbligo di mantenere il segreto.

Il titolare del segreto d'ufficio o professionale che dubita della ponderazione degli interessi ha comunque la possibilità di farsi formalmente liberare dall'obbligo del segreto da un'autorità competente ai sensi dell'articolo 320 n. 2 o 321 n. 2 CP. In tal caso è l'autorità che procede alla ponderazione degli interessi richiesta dall'articolo 16 capoverso 1 D-LPD e il titolare del segreto d'ufficio o professionale non rischia più di essere punito.

145 DTF **87** IV 105, 107.

Se un segreto professionale (art. 321 CP) è rivelato dopo la morte del detentore del segreto, possono sporgere querela terzi, purché una legge lo preveda; tale diritto può risultare anche da una norma al di fuori del Codice penale. Se un'informazione riguarda più persone (p. es. informazioni su una paternità segreta) hanno diritto di sporgere querela i terzi che sono detentori del segreto[146].

Il titolare del segreto d'ufficio o professionale che ha un interesse personale di mantenerlo può farlo valere conformemente al capoverso 1 lettera c.

Le azioni nei confronti di titolari privati del trattamento per far valere il diritto d'accesso secondo l'articolo 12 capoverso 1 D-LPD possono essere promosse con procedura semplificata, conformemente all'articolo 243 capoverso 2 lettera d D-CPC. Tale procedura si distingue in particolare per il fatto che è poco complicata e accessibile anche a chi non è giurista («sozialer Zivilprozess»)[147]. Il giudice accerta i fatti d'ufficio nei casi di cui all'articolo 243 capoverso 2 CPC (massima inquisitoria limitata, art. 247 cpv. 2 lett. b CPC) e interviene in maniera più attiva nel procedimento. Ciò intende permettere ai privati di accedere a un tribunale senza bisogno di un avvocato. In virtù dell'articolo 113 capoverso 2 lettera g e 114 lett. f D-CPC la procedura è gratuita.

Cpv. 2 Richiesta all'autorità di vigilanza

Il capoverso 2 contempla il caso in cui un titolare del trattamento che sottostà a un segreto d'ufficio o professionale nega l'accesso rinviando a tale segreto. La disposizione prevede che allora anche le persone autorizzate secondo il capoverso 1 lettera a possono rivolgersi all'autorità competente secondo gli articoli 320 e 321 CP per liberare il titolare del trattamento dall'obbligo del segreto.

In linea di principio soltanto il titolare del segreto, nel nostro caso il titolare del trattamento, può rivolgersi all'autorità di vigilanza o all'autorità superiore per farsi liberare dall'obbligo del segreto d'ufficio o professionale, poiché è nel suo interesse disporre di un motivo giustificativo per il suo comportamento, dato che costituisce una fattispecie punibile[148]. Secondo il capoverso 2, in futuro anche un terzo potrà rivolgersi direttamente all'autorità competente per chiedere la liberazione dal segreto. Questa possibilità è prevista per la costellazione particolare del diritto di accedere ai dati di un defunto, tanto più che in questo caso il detentore del segreto (deceduto) non può liberare il titolare del trattamento dal segreto, salvo che lo abbia fatto ancora in vita. In tal modo si tiene conto in modo equo dei diversi interessi. Il titolare del trattamento può sgravarsi indirizzando all'autorità di sorveglianza la persona che chiede l'accesso ai dati, soprattutto se ha dubbi che possa o meno concedere l'accesso ai dati. Viceversa, la persona che chiede l'accesso non è bloccata semplicemente per il fatto che il titolare del trattamento non intende rivolgersi all'autorità di vigilanza.

146 Cfr. DTF **87** IV 105, 110; Oberholzer Niklaus, Basler Kommentar Strafrecht II, Basilea 2013, art. 321 N 34; Riedo Christof, Der Strafantrag, Basilea 2004, 302 segg.

147 Cfr. MAZAN STEPHAN, Vorbemerkungen zu Art. 243–247 ZPO, in: Spühler Karl/Tenchio Luca/Infanger Dominik, Commento basilese del Codice di procedura civile, 3ª ed, Basilea 2017.

148 DTF **123** IV 75, 77 consid. 2b

L'autorità di sorveglianza decide esclusivamente in merito alla liberazione dal segreto d'ufficio o professionale, ma non obbliga il titolare del segreto a concedere l'accesso. Se nonostante la liberazione, quest'ultimo dovesse rifiutare l'accesso, ad esempio perché a suo parere il richiedente non ha di fatto convissuto con il defunto, si tratterebbe di una questione di diritto civile che, in caso di controversia e se il titolare del trattamento è un privato, dovrebbe essere risolta per vie procedurali.

Cpv. 3 Cancellazione

Secondo il capoverso 3, gli eredi o l'eventuale esecutore testamentario possono chiedere che il titolare del trattamento cancelli o distrugga i dati della persona defunta. Questo diritto sussiste a prescindere da una violazione della personalità o da un trattamento illecito dei dati. Si tratta di un caso particolare di applicazione del diritto all'oblio previsto dall'articolo 28 D-LPD per le persone in vita.

Il diritto di far cancellare o distruggere i dati è stato espressamente previsto soltanto per gli eredi e l'esecutore testamentario. Contrariamente a quanto previsto dall'avamprogetto posto in consultazione, gli eredi possono farlo valere soltanto congiuntamente. La modifica intende evitare qualsiasi conflitto tra gli eredi in merito all'esercizio del diritto di cancellazione; in caso di disaccordo tra gli eredi, la cancellazione o distruzione dei dati del defunto non può in linea di massima essere effettuata. Rispetto all'avamprogetto è stato aggiunto che anche un eventuale esecutore testamentario può far valere il diritto di cancellare o distruggere i dati.

Secondo la lettera a, la cancellazione o distruzione va rifiutata se in vita la persona deceduta lo ha espressamente vietato. In tal modo si tiene conto della volontà del defunto che, per esempio, ha deciso in merito al destino dell'archivio personale dopo la sua morte.

La cancellazione o la distruzione va inoltre negata se vi si oppongono interessi preponderanti della persona deceduta, del titolare del trattamento o di terzi (lett. b). A tale proposito rinviamo alle spiegazioni relative al capoverso 1 lettera b. Nonostante i timori di vari partecipanti alla consultazione, gli eredi non possono pertanto obbligare il titolare del trattamento a cancellare materiale incriminante per un processo. Gli interessi preponderanti del titolare del trattamento comprendono anche i suoi obblighi legali che si oppongono alla cancellazione.

Infine, la lettera c esclude la cancellazione o la distruzione dei dati se vi si oppone un interesse pubblico preponderante, che può essere fatto valere sia da titolari privati che da organi federali. Un interesse pubblico preponderante può ad esempio sussistere nel caso di documenti per i quali possono essere fatti valere diritti secondo la LTras. Sono tuttavia ipotizzabili anche obblighi di conservazione secondo il diritto federale o cantonale.

Le azioni nei confronti di titolari privati del trattamento per far valere il diritto alla cancellazione di cui all'articolo 16 capoverso 3 D-LPD possono essere promosse con procedura semplificata, conformemente all'articolo 243 capoverso 2 lettera d D-CPC.

9.1.4 Obblighi del titolare e del responsabile del trattamento

Il capitolo 3 disciplina gli obblighi del titolare e del responsabile del trattamento. Tali obblighi si applicano sia ai privati che agli organi federali.

Art. 17 Obbligo di informare in occasione della raccolta di dati personali

L'articolo 17 D-LPD riunisce gli articoli 14, 18 e 18*a* della LPD vigente. In tal modo si evitano sovrapposizioni e si applica un disciplinamento uniforme per il trattamento di dati da parte degli organi federali e dei titolari privati. L'articolo corrisponde alle disposizioni dell'articolo 7bis del P-STE 108 e dell'articolo 13 della direttiva (UE) 2016/680. Gli articoli 13 e seguente del regolamento (UE) 2016/679 prevedono un disciplinamento analogo.

L'obbligo di informare migliora la trasparenza del trattamento di dati personali, uno degli obiettivi fondamentali della revisione. Se non ne è informata, spesso la persona interessata non si rende conto che vengono trattati dati che la riguardano. Inoltre, può far valere i propri diritti conferitile dalla LPD soltanto se è a conoscenza di un trattamento di dati che la riguardano. Una migliore trasparenza nel trattamento di dati permette pertanto anche di rafforzare i diritti della persona interessata, anche questo uno degli obiettivi fondamentali della revisione. Infine, l'obbligo di informare serve a sensibilizzare i cittadini alla protezione dei dati; sensibilizzazione che è anch'essa un obiettivo della revisione.

Cpv. 1 Principio

Secondo il capoverso 1, il titolare del trattamento informa la persona interessata sulla raccolta di dati che la riguardano, anche nel caso in cui i dati sono raccolti presso terzi.

Il D-LPD non precisa la forma in cui deve essere fornita l'informazione. Il titolare del trattamento deve provvedere affinché la persona interessata possa effettivamente prendere atto dell'informazione in modo facilmente accessibile, ma non deve accertarsi che nel caso concreto si informi effettivamente. La possibilità di prendere atto dell'informazione varia notevolmente a seconda che i dati siano raccolti presso la persona interessata o presso terzi.

Un'informazione generale può essere sufficiente se i dati sono raccolti presso la persona interessata (riguardo alle condizioni generali di contratto, cfr. art. 18 cpv. 1). Si può ricorrere a una dichiarazione standardizzata su un sito Internet, ma anche a simboli o pittogrammi che contengono gli elementi necessari. Se si sceglie una forma generale, l'informazione deve tuttavia essere facilmente accessibile, completa e sufficientemente identificabile. Le informazioni possono essere rese accessibili anche attraverso vari livelli (p. es. dapprima una panoramica e poi informazioni più particolareggiate). La mera indicazione di una persona di contatto non è sufficiente, poiché la persona interessata deve ottenere le informazioni senza richiederle.

Se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento deve scegliere un modo che permetta a tale persona di venire effettivamente a conoscenza delle informazioni. In tal caso può non bastare mettere sempli-

cemente a disposizione le informazioni. Occorre informare attivamente la persona interessata in maniera generale o individuale. Una persona che non compra mai un libro, ad esempio, non visiterà probabilmente il sito di una libreria in linea per leggere la sua dichiarazione relativa alla protezione dei dati. Non verrà quindi mai a conoscenza del fatto che la libreria tratta dati che la riguardano, poiché non immagina nemmeno che ciò possa avvenire. L'obbligo d'informazione intende quindi anche evitare che dati personali siano trattati all'insaputa della persona interessata. Sono fatte salve le eccezioni di cui all'articolo 18.

Anche se non vi sono condizioni formali, per l'informazione va scelta una forma che rispetti il principio della trasparenza del trattamento dei dati. Per motivi probatori è altresì raccomandabile documentare l'informazione o fornirla per scritto. Inoltre, l'informazione deve essere redatta in modo sufficientemente chiaro per raggiungere il suo scopo, che è la trasparenza del trattamento dei dati.

Cpv. 2 Informazioni da comunicare

La frase introduttiva del capoverso 2 sancisce il principio su cui il titolare del trattamento si deve basare nel comunicare le informazioni. Deve comunicare alla persona interessata le informazioni necessarie affinché questa possa far valere i propri diritti e sia garantita la trasparenza del trattamento. Le lettere a–c precisano tale principio indicando le informazioni minime da comunicare in ogni caso alla persona interessata. Si tratta dell'identità, ossia del nome, e delle coordinate di contatto del titolare del trattamento (lett. a), dello scopo del trattamento (lett. b) e, se del caso, l'identità dei destinatari o le categorie di destinatari cui sono stati comunicati dati personali. Il titolare del trattamento è libero di decidere se intende indicare i destinatari o le categorie di destinatari. Come nell'Unione europea (cfr. art. 4 n. 9 del regolamento [UE] 2016/679), i responsabili del trattamento fanno parte dei destinatari ai sensi della disposizione. Se non intende rivelare l'identità dei destinatari, il titolare del trattamento può limitarsi a indicarne le categorie. L'Incaricato avrebbe auspicato anche l'obbligo di comunicare la base legale del trattamento.

La combinazione di una disposizione generale che contiene i requisiti fondamentali delle informazioni da comunicare con le indicazioni specifiche minime permette di strutturare in modo flessibile l'obbligo di informare. L'informazione dovrà essere più o meno dettagliata a seconda del tipo di dati trattati nonché della natura e della portata del trattamento. È quindi possibile che il titolare debba informare sulla durata del trattamento o sull'anonimizzazione dei dati. Questa flessibilità è necessaria poiché la LPD si applica a una grande varietà di trattamenti di dati. Garantisce inoltre che siano comunicate soltanto le informazioni necessarie e consente ai titolari del trattamento di concretizzare l'obbligo di informare nel loro settore specifico per mezzo di codici di condotta.

Cpv. 3 Categorie di dati personali

Secondo il capoverso 3, soltanto se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento deve comunicarle anche le categorie di dati personali trattati. Questa restrizione è dovuta al fatto che, se i dati sono raccolti presso la persona interessata, si può presumere che questa sia a conoscenza dei dati o perlomeno delle categorie di dati raccolti. Se invece sono raccolti presso terzi, la

persona interessata non ha alcuna possibilità di sapere quali categorie sono trattate e pertanto deve esserne informata.

Cpv. 4 Comunicazione di dati all'estero

Se sono comunicati dati personali all'estero, il titolare del trattamento deve comunicare alla persona interessata il nome dello Stato destinatario. Se tale Stato non garantisce una protezione adeguata e il titolare del trattamento ricorre alle garanzie ai sensi dell'articolo 13 capoverso 2, queste ultime devono essere comunicate alla persona interessata. Lo stesso vale se si applica una delle deroghe di cui all'articolo 14.

Cpv. 5 Momento della comunicazione

Secondo il capoverso 2, se i dati sono raccolti presso la persona interessata, questa deve esserne informata al momento della raccolta.

Il capoverso 5 stabilisce il momento dell'informazione qualora i dati non siano raccolti presso la persona interessata. La disposizione fissa un termine di un mese. Il secondo periodo prevede un termine più corto nel caso in cui il titolare del trattamento comunica i dati a terzi prima della scadenza del termine di un mese: in tal caso la persona interessata deve essere informata al momento della comunicazione a terzi.

Riassumendo, il termine è in linea di principio di un mese a partire dalla raccolta dei dati da parte del titolare del trattamento, a prescindere dallo scopo del trattamento. Il termine è più corto soltanto se il titolare comunica i dati a terzi.

Art. 18 Eccezioni all'obbligo di informare e limitazioni

L'articolo 18 D-LPD disciplina i casi in cui l'obbligo di informare non sussiste del tutto (cpv. 1 e 2) e quelli in cui l'informazione può essere limitata nonostante sussista in linea di massima il relativo obbligo (cpv. 3). Le due situazioni vanno nettamente separate. La disposizione riprende in parte le disposizioni del diritto vigente (art. 9, 14 cpv. 4 e 5 nonché 18*b* LPD), le quali, per motivi di chiarezza, vengono riunite in un solo articolo.

Cpv. 1 Eccezioni generali all'obbligo di informare

Il capoverso 1 definisce alcune situazioni in cui l'obbligo di informare decade del tutto per cui il titolare del trattamento non deve informare la persona interessata.

Secondo la lettera a, il titolare del trattamento è esentato dall'obbligo di informare se la persona interessata dispone già delle informazioni di cui all'articolo 17. Sono ipotizzabili diversi casi. Innanzitutto è possibile che la persona interessata sia stata informata precedentemente e in seguito le informazioni da comunicare non sono mutate. Inoltre si può presumere che la persona interessata abbia già ricevuto le informazioni se ha acconsentito a un trattamento di dati, dato che tale consenso è valido soltanto se la persona interessata è stata debitamente informata. Le informazioni necessarie a tale proposito corrispondono a quelle dell'articolo 17 e vanno anche oltre. Spesso il consenso è dato nelle condizioni generali di contratto (CGC). Queste possono quindi servire a informare la persona interessata, a condizione che contengano le informazioni necessarie. Quando essa stessa ha reso accessibili i

propri dati, senza l'intervento del titolare del trattamento (p. es. consegna della documentazione per una candidatura) la persona interessata è in linea di massima informata sulla raccolta di dati.

Secondo la lettera b, l'obbligo d'informare decade se il trattamento dei dati personali, sia da parte di un organo federale che di un privato, è previsto da una legge. In ogni caso gli organi federali possono trattare dati personali soltanto in presenza di una base legale da cui si evincono regolarmente le informazioni necessarie. Lo stesso vale per i privati che sono obbligati a trattare determinati dati dalla legge, ad esempio nell'ambito della lotta al riciclaggio di denaro.

Secondo la lettera c, il titolare privato del trattamento è esentato dall'obbligo di informare se è vincolato da un obbligo legale di mantenere il segreto. La disposizione evita un conflitto di norme sancendo la priorità dell'obbligo di confidenzialità nei confronti dell'obbligo di informare.

Secondo la lettera d, l'obbligo di informare decade se sono soddisfatte le condizioni di cui all'articolo 25, che disciplina le restrizioni del diritto d'accesso a favore dei mezzi di comunicazione a carattere periodico. Per gli stessi motivi è necessario un privilegio analogo anche per l'obbligo di informare dei mezzi di comunicazione, vista la funzione particolare che assolvono[149].

Cpv. 2 Limitazioni specifiche

Il capoverso 2 prevede una limitazione specifica dell'obbligo di informare se i dati personali non sono raccolti presso la persona interessata. In tal caso l'obbligo di informare non si applica se l'informazione non è possibile (lett. a) o esige mezzi sproporzionati (lett. b).

L'informazione è impossibile se la persona interessata non è identificabile, ad esempio perché si tratta della foto di uno sconosciuto. Non è comunque sufficiente supporre che l'identificazione sia impossibile e occorre invece procedere a un minimo di ricerche, entro limiti ragionevoli.

Gli sforzi per informare la persona interessata sono sproporzionati quando appaiono oggettivamente ingiustificati in relazione al beneficio che quest'ultima trarrebbe dall'informazione. Occorre in particolare tenere conto del numero di persone interessate. L'informazione necessita ad esempio di sforzi sproporzionati quando i dati sono trattati unicamente per scopi di archiviazione d'interesse pubblico. In tal caso l'informazione di tutte le persona interessate richiederebbe regolarmente sforzi notevoli ed è probabile che l'interesse di queste ultime all'informazione sia limitato, ad esempio perché i dati in questione sono vecchi.

Quest'ultima eccezione deve essere interpretata in maniera restrittiva: il titolare del trattamento non deve accontentarsi di una mera supposizione. Nel caso concreto, deve invece intraprendere tutti gli sforzi che si possono ragionevolmente esigere per assolvere al suo obbligo di informare. Soltanto se tali sforzi si rivelano vani, il titolare del trattamento può ritenere che sia impossibile informare la persona interessata.

149 Cfr. Weber Rolf H., Medien im Spannungsfeld von Informationsauftrag und Datenschutz, Jusletter 8, mag. 2017.

Cpv. 3 Limitazione dell'informazione

Il capoverso 3 disciplina le situazioni in cui il titolare del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi. Contrariamente ai capoversi 1 e 2, questo capoverso contempla anche situazioni in cui occorre ponderare gli interessi. Le modalità differiscono a seconda che il titolare del trattamento sia un organo federale o un privato. In base alla ponderazione degli interessi, il titolare del trattamento può rinunciare alla comunicazione delle informazioni, limitarla o differirla. L'elenco dei casi è completo e la disposizione va interpretata in modo restrittivo. L'informazione deve essere limitata soltanto per quanto assolutamente necessario e il suo motivo deve essere messo in relazione con la trasparenza del trattamento. In linea di massima va scelta la soluzione che sia più favorevole per la persona interessata e, in considerazione delle circostanze, garantisca per quanto possibile un trattamento trasparente dei dati.

Lett. a

Secondo la lettera a il titolare del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi se lo esigono gli interessi preponderanti di un terzo. La disposizione contempla soprattutto i casi in cui le informazioni sul trattamento dei dati personali della persona interessata contengono anche informazioni su terzi. In certi casi la comunicazione delle informazioni può ledere gli interessi di questi terzi.

Lett. b

Secondo la lettera b il titolare del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi se l'informazione compromette le finalità del trattamento. Questa deroga va interpretata in maniera restrittiva. Il titolare del trattamento può invocarla soltanto se l'informazione della persona interessata impedisce del tutto di raggiungere lo scopo del trattamento dei dati. Se un trattamento persegue più di uno scopo, è determinante quello principale. È necessario che lo scopo sia sufficientemente importante per giustificare la restrizione dell'obbligo di informare. Si pensi al caso di un giornalista che non rientra nella deroga di cui all'articolo 18 capoverso 1 lettera d D-LPD. L'obbligo di informare potrebbe impedire al giornalista che si occupa di uno scandalo politico per farne un documentario di indagare senza ostacoli sui fatti. Tale attività riveste anche un interesse pubblico considerevole che giustifica un'ampia restrizione dell'obbligo di informare. Si può anche pensare che nell'ambito di un procedimento conflittuale siano trattati dati utilizzati soltanto durante il processo. Anche in questo caso la comunicazione precoce delle informazioni pregiudicherebbe le finalità del trattamento. Tanto più che si tratta di un trattamento unico sia per il titolare del trattamento che per la persona interessata, poiché si suppone che né l'uno né l'altro siano implicati ogni giorno in procedimenti giudiziari di questo tipo. Nei due esempi esposti, il trattamento di dati è di grande interesse e il rischio che l'obbligo di informare ne comprometta le finalità è diretto e concreto. Inoltre, in entrambi casi la persona interessata verrà a conoscenza del trattamento al più tardi in occasione della pubblicazione dei dati o della loro utilizzazione nel processo.

La sistematica (inclusione della disposizione nel cpv. 3) indica che in linea di massima vige l'obbligo di informare. Il titolare del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi soltanto se questa compromette direttamente le finalità del trattamento. Il titolare deve adottare le misure che sono più favorevoli dal punto di vista della persona interessata e che restringono il diritto di quest'ultima alla trasparenza del trattamento dei dati soltanto nella misura in cui è strettamente necessario.

Occorre infine distinguere la deroga di cui alla lettera b da quella di cui alla lettera c. Per la lettera b è necessaria un'interpretazione restrittiva e la deroga si applica soltanto se l'informazione della persona interessata impedisce del tutto che si raggiunga lo scopo del trattamento di dati. Il titolare del trattamento non può invocarla soltanto perché gli sembra più gradevole o pratico rinunciare all'informazione. Non può neppure invocarla in modo sistematico per tutte le attività di trattamento. Infine, neppure gli interessi meramente economici (p. es. uso dei dati a fini pubblicitari) rientrano nel campo d'applicazione della lettera b. Questo genere di interessi del titolare del trattamento, meno importanti, possono eventualmente rientrare nel campo d'applicazione della lettera c.

Lett. c

Secondo la lettera c, il titolare privato del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi se lo esigono i suoi interessi preponderanti e non comunica i dati personali a terzi. Un interesse preponderante non va presunto senza una ponderazione accurata degli interessi. Quello della persona interessata di essere informata in merito a un determinato trattamento di dati affinché possa far valere i suoi diritti va attentamente ponderato con gli eventuali interessi del titolare del trattamento. In tale contesto possono rivelarsi parametri importanti il tipo di dati trattati e il modo del trattamento, il rischio di una lesione della personalità, lo scopo del trattamento, la misura in cui l'informazione della persona interessata ostacola tale scopo e l'importanza di quest'ultimo per l'attività del titolare del trattamento.

Lett. d

Secondo il capoverso 3 lettera d, un organo federale può limitare o differire la comunicazione delle informazioni oppure rinunciarvi se lo esige un interesse pubblico preponderante, in particolare la sicurezza interna o esterna della Svizzera (n. 1). Per sicurezza esterna s'intende, oltre al rispetto degli impegni internazionali della Svizzera, anche la cura di buone relazioni con l'estero. L'organo federale può inoltre limitare o differire la comunicazione delle informazioni oppure rinunciarvi se la comunicazione rischia di compromettere un'indagine, un'istruzione o un procedimento amministrativo o giudiziario (n. 2). Occorre evitare che la LPD permetta di eludere le disposizioni dei codici procedurali, quali il diritto di essere sentito e altri, di ostacolare procedimenti giudiziari o amministrativi.

Art. 19 Obbligo di informare la persona interessata in caso di decisione individuale automatizzata

L'articolo 19 D-LPD prevede un obbligo di informare la persona interessata in caso di decisione individuale automatizzata. La disposizione è conforme ai requisiti dell'articolo 8 lettera a del P-STE 108 e dell'articolo 11 della direttiva (UE) 2016/680. L'articolo 22 del regolamento (UE) 2016/679 contiene una disposizione analoga. L'introduzione della nozione di «decisione individuale automatizzata» è necessaria, poiché tali decisioni sono vieppiù frequenti in seguito allo sviluppo tecnologico.

Cpv. 1 Informazione

Secondo il capoverso 1 il titolare del trattamento deve informare la persona interessata nel caso di una decisione basata esclusivamente su un trattamento automatizzato, inclusa la profilazione, che abbia per lei effetti giuridici o ripercussioni notevoli.

Se necessario, il nostro Consiglio preciserà nell'ordinanza i casi in cui una decisione è presa esclusivamente in base a un trattamento automatico di dati personali. Tale tipo di decisione implica comunque che non vi è stata alcuna decisione sulla base di una valutazione da parte di una persona fisica. Si è in presenza di una decisione individuale automatizzata se si procede a un'analisi di dati senza intervento umano e tale analisi conduce a una decisione o a un giudizio nei confronti della persona interessata. Una decisione individuale automatizzata rimane tale anche nel caso in cui essa venga successivamente comunicata da una persona fisica che tuttavia non ha influito sul processo decisionale. Il criterio determinante è quindi la misura in cui una persona fisica possa procedere a un esame del contenuto e adottare su tale base una decisione definitiva. La decisione automatizzata deve tuttavia presentare un determinato grado di complessità. Non sono contemplate le decisioni semplici quali quelle in occasione di un prelievo a un bancomat (rilascio dell'importo richiesto a condizione che il saldo del conto sia sufficiente).

Occorre informare la persona interessata soltanto se la decisione individuale automatizzata ha per lei effetti giuridici o ripercussioni significative. Nel diritto privato gli effetti giuridici sono legati alla conclusione o alla risoluzione di un contratto. In tale contesto occorre procedere alle distinzioni necessarie. La conclusione di un contratto assicurativo, ad esempio, esplica effetti giuridici per la persona interessata. Ma se quest'ultima riceve successivamente a intervalli regolari gli avvisi di pagamento dei premi, questi non sono da considerarsi decisioni individuali con effetti giuridici, poiché il loro invio risulta dalla conclusione del contratto. Non vi sono inoltre effetti giuridici se la persona interessata non firma alcun contratto. Nel settore del diritto pubblico si è in presenza di effetti giuridici se decisioni amministrative si fondano su una decisione individuale automatizzata, ad esempio un'imposizione fiscale automatica.

Si possono presumere ripercussioni significative per la persona interessata se quest'ultima subisce durevolmente pregiudizi economici o personali. Una semplice molestia non è sufficiente. Tutto dipende dalle circostanze concrete del caso. Occorre in particolare tenere conto dell'importanza del bene in questione per la persona interessata, della durata degli effetti della decisione e delle eventuali alternative a disposizione. A seconda delle ripercussioni concrete la mancata conclusione di un contratto può avere ripercussioni significative o meno. Ripercussioni notevoli pos-

sono risultare anche in caso di prestazioni mediche effettuate sulla base di una decisione individuale automatizzata.

Il titolare del trattamento deve informare la persona interessata anche in caso di una profilazione che conduce a una decisione che abbia per la persona interessata effetti giuridici o ripercussioni significative. È ad esempio possibile che la persona interessata non ottenga una carta di credito soltanto a causa di una valutazione negativa della sua solvibilità. Questo esempio illustra bene il problema delle decisioni individuali automatizzate. Infatti, anche se può riflettere la situazione finanziaria reale di una persona, una valutazione negativa della sua solvibilità può anche fondarsi su dati falsi o vetusti che sono in contraddizione totale con la situazione reale. In tal caso la decisione automatizzata conduce a un pregiudizio ingiustificato nei confronti della persona interessata.

Cpv. 2 Esposizione del parere

Secondo il capoverso 2 il titolare del trattamento deve dare alla persona interessata, su richiesta, la possibilità di esporre il suo parere in merito al risultato della decisione e anche di chiedere come sia stata presa. S'intende così evitare in particolare che il trattamento di dati sia effettuato in base a dati incompleti, non aggiornati o non errati. Ciò è anche nell'interesse del titolare del trattamento, poiché decisioni individuali automatizzate non corrette possono avere conseguenze negative anche per quest'ultimo, ad esempio nel caso della mancata conclusione di un contratto perché una persona è stata erroneamente giudicata indegna di credito. La libertà contrattuale non ne risulta pregiudicata.

La legge non fissa il momento dell'informazione o quello in cui alla persona interessata deve essere data la possibilità di esprimere il proprio parere. Quest'ultima può quindi essere informata e invitata a esprimere il proprio parere prima o dopo la decisione, anche inviandole, ad esempio, la decisione individuale automatizzata contraddistinta come tale e dandole successivamente la possibilità di esprimersi nell'ambito del diritto di essere sentita o di una procedura di ricorso, a condizione che ciò non comporti costi supplementari troppo elevati (p. es. spese procedurali) che dissuadano la persona interessata.

Cpv. 3 Eccezioni

Secondo il capoverso 3, l'obbligo di informare e sentire la persona interessata non si applica se la decisione è in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare del trattamento e la persona interessata e la richiesta di quest'ultima è soddisfatta (lett. a). In tal caso si presume che l'informazione non interessi più la persona interessata. La richiesta di quest'ultima è soddisfatta se il contratto è concluso esattamente alle condizioni dell'offerta o a quelle richieste dalla persona interessata. Ciò è ad esempio il caso quando un contratto di leasing è concluso al tasso d'interesse previsto dall'offerta, ma non se il contratto di leasing è concluso a un tasso d'interesse meno favorevole rispetto all'offerta, poiché la solvibilità della persona interessata è stata giudicata insufficiente. Affinché questa disposizione sia applicabile, è necessario che la persona interessata abbia ottenuto la totalità delle prestazioni richieste. L'ottenimento di singole parti non è sufficiente.

L'obbligo di informare e di sentire la persona interessata non si applica neppure se quest'ultima ha espressamente acconsentito che la decisione sia presa in maniera automatizzata (lett. b). Si tratta di un'eccezione logica poiché affinché il suo consenso sia valido è necessario che la persona interessata sia stata precedentemente informata.

Cpv. 4 Decisioni individuali automatizzate emanate da un organo federale

Il capoverso 4 contempla le decisioni individuali automatizzate emanate da un organo federale. Di norma si tratta di decisioni amministrative. Secondo il capoverso 4 l'organo federale deve designare come tale la decisione individuale automatizzata, di modo che la persona interessata si renda conto che non è stata presa da una persona fisica. La persona interessata ha in linea di massima il diritto a un rimedio giuridico, in quanto può esporre il proprio punto di vista e far esaminare la decisione da una persona fisica. In altre parole, i diritti dell'articolo 19 capoverso 2 D-LPD sono già garantiti dal rimedio giuridico. Per questo motivo il secondo periodo della presente disposizione precisa che l'articolo 19 capoverso 2 non si applica se la persona interessata dispone di un rimedio giuridico contro la decisione.

Art. 20 Valutazione d'impatto sulla protezione dei dati

L'articolo 20 D-LPD introduce l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati. La disposizione concretizza le condizioni dell'articolo 8bis paragrafo 2 P-STE108 e degli articoli 27 e seguente della direttiva (UE) 2016/680. Gli articoli 35 e seguente del regolamento (UE) 2016/679 contengono disposizioni analoghe.

La definizione e la funzione della valutazione d'impatto sulla protezione dei dati si evincono dall'articolo 20 capoverso 3. Si tratta di uno strumento per riconoscere e valutare i rischi che un determinato trattamento di dati può comportare per la persona interessata. Sulla base di tale valutazione vanno, se del caso, presi i provvedimenti necessari per ridurre tali rischi. La valutazione è pertanto vantaggiosa anche per il titolare del trattamento, poiché gli permette di affrontare preventivamente eventuali problemi relativi alla protezione dei dati e di evitare costi successivi.

Gli organi federali sono già tenuti ad annunciare al consulente per la protezione dei dati o, in se tale funzione non è prevista, all'Incaricato ogni progetto di trattamento automatizzato di dati personali (art. 20 cpv. 2 OLPD). La procedura secondo il metodo di gestione dei progetti Hermes adempie probabilmente i requisiti di una valutazione d'impatto sulla protezione dei dati.

Cpv. 1 e 2 Motivi per effettuare la valutazione d'impatto sulla protezione dei dati

Secondo il capoverso 1 il titolare del trattamento deve effettuare una valutazione d'impatto sulla protezione dei dati quando il trattamento previsto può presentare un

rischio elevato per la personalità e i diritti fondamentali della persona interessata[150]. La regola vale sia per i titolari privati del trattamento sia per gli organi federali, ragion per cui la disposizione menziona un rischio elevato non solo per la personalità della persona interessata bensì anche per i suoi diritti fondamentali. Il titolare del trattamento è quindi tenuto a prevedere le conseguenze di un futuro trattamento per la persona interessata. Si tratta di valutare in particolare il modo e la misura in cui un trattamento si ripercuote sulla personalità e i diritti fondamentali della persona interessata.

Nell'individuazione dei rischi occorre tenere conto soprattutto del diritto all'autodeterminazione informativa e alla protezione della sfera privata. Questi diritti tutelano sia l'autonomia della persona interessata sia la sua dignità e identità[151]. In relazione alla protezione dei dati, l'autonomia significa soprattutto poter disporre autonomamente dei propri dati personali e non dover supporre che una quantità sconosciuta di dati personali si trovi in possesso di una moltitudine di terzi che ne dispongono liberamente. I dati personali sono infatti strettamente collegati all'identità di un individuo. Chi è in possesso di dati personali ed è in grado di connetterli può evincere un'immagine molto intima della persona in questione, che quest'ultima vorrebbe magari rivelare soltanto a persone che le sono molto vicine. Oltre a essere problematiche dal punto di vista della libertà di disporne, le informazioni su una persona possono influenzare l'ambiente che la circonda senza che essa ne conosca i motivi (p. es. stigmatizzazione a causa di una malattia, limitazione della libertà di contratto a causa della valutazione della solvibilità). La persona interessata può anche vedersi costretta a cambiare il suo comportamento perché sa di essere osservata. Infine le informazioni raccolte all'insaputa della persona interessata possono anche portare ad abusi che rischiano di ledere la sua dignità.

Per valutare il rischio, il titolare del trattamento deve mettere in relazione il trattamento di dati con il diritto all'autodeterminazione informativa e alla sfera privata della persona interessata. In altre parole, il trattamento deve essere valutato in relazione all'autodeterminazione, all'identità e alla dignità della persona interessata. Occorre in linea di massima presumere un rischio elevato quando le caratteristiche specifiche del trattamento previsto inducono a concludere che esso limiti o potrebbe limitare la libertà della persona interessata di disporre dei propri dati. Il rischio elevato può risultare ad esempio dal tipo di dati trattati o dal loro contenuto (p. es. dati degni di particolare protezione), dal tipo e dallo scopo del trattamento (p. es. profilazione), dalla quantità di dati trattati, dalla comunicazione a Stati terzi (p. es. in assenza di una legislazione estera che garantisca una protezione adeguata) oppure dal fatto che i dati sono resi accessibili a una quantità elevata o addirittura illimitata di persone.

Il capoverso 2 precisa che il rischio elevato risulta dal tipo, dalla portata, dalle circostanze e dallo scopo del trattamento. Se il trattamento è sistematico, i dati trattati

150 Cfr. le Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, Working Paper del Gruppo Article 29 Data Protection Working Party del 4 apr. 2017, in particolare pag. 7 segg.

151 Cfr. Diggelmann Oliver, in: Waldmann/Belser/Epiney (a c. di), Basler Kommentar, Bundesverfassung, Basilea 2015, Art. 13 Cost. N 7.

sono degni di particolare protezione e gli scopi del trattamento sono ampi, allora occorre concludere che il rischio sia elevato. Il capoverso 2 menziona due esempi in cui esiste tale rischio. Secondo la lettera a il rischio è elevato nel caso di un trattamento su grande scala di dati degni di particolare protezione, ad esempio nell'ambito di un progetto di ricerca in ambito medico. La lettera b presume un rischio elevato anche nel caso di profilazione. Lo stesso può valere in caso di decisioni basate esclusivamente sul trattamento automatico di dati che hanno effetti giuridici o ripercussioni significative per la persona interessata. Non bisogna infatti dimenticare che questo tipo di decisioni possono avere ripercussioni notevoli per la persona interessata. Anche in questi casi è pertanto necessaria una valutazione d'impatto sulla protezione dei dati. Secondo la lettera c, infine, sussiste un rischio elevato in caso di sorveglianza sistematica di luoghi pubblici (p. es. la sorveglianza di una stazione ferroviaria).

Il secondo periodo del capoverso 1 autorizza il titolare del trattamento a procedere a una valutazione d'impatto comune se prevede più operazioni di trattamento simili. Sono contemplati in particolare i trattamenti che perseguono uno scopo superiore comune. In tal caso non è necessario esaminare individualmente ciascuna tappa prevista sulla piattaforma di trattamento e la valutazione d'impatto può vertere sulla piattaforma nel suo insieme.

Cpv. 3 Contenuto della valutazione d'impatto sulla protezione dei dati personali

Secondo il capoverso 3 la valutazione d'impatto deve innanzitutto descrivere il trattamento previsto. Occorre ad esempio indicare i vari processi (p. es. la tecnologia usata), lo scopo del trattamento o la durata di conservazione dei dati. Inoltre vanno descritti i possibili rischi del trattamento per la personalità e per i diritti fondamentali della persona interessata. Si tratta di approfondire la valutazione dei rischi che va già effettuata per verificare la necessità di una valutazione d'impatto sulla protezione dei dati. Va indicato sotto quali aspetti il trattamento di dati può comportare un rischio elevato per la personalità e i diritti fondamentali della persona interessata e il modo in cui valutare tale rischio. Infine, la valutazione d'impatto deve illustrare le misure previste per ridurre i rischi indicati. A tale proposito sono determinanti soprattutto i principi di cui all'articolo 5 D-LPD, ma possono essere di rilievo anche gli obblighi della protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design/by default; art. 6 D-LPD). Nel decidere le misure si possono ponderare gli interessi della persona interessata e quelli del titolare del trattamento. Tale ponderazione va anch'essa illustrata e giustificata nella valutazione d'impatto

Cpv. 4 Eccezioni in caso di esecuzione di un obbligo legale

Il capoverso 4 esenta dall'obbligo di procedere a una valutazione d'impatto sulla protezione dei dati il titolare privato che è tenuto a effettuare il trattamento in virtù di un obbligo legale, ad esempio ai fini della lotta al terrorismo o al riciclaggio di denaro. Se il trattamento non ha finalità che non siano quelle previste dall'obbligo legale si può presumere che il legislatore abbia valutato gli eventuali rischi che il trattamento comporta per la persona interessata ed emanato, se necessario, le disposizioni per ridurli.

La disposizione non si applica invece ai trattamenti da parte di privati il cui scopo non è soltanto l'adempimento di un obbligo legale. In tal caso il titolare del trattamento deve imperativamente procedere alla valutazione d'impatto sulla protezione dei dati.

Cpv. 5 Eccezioni

Il titolare privato del trattamento può rinunciare alla valutazione d'impatto sulla protezione dei dati se è stato oggetto di una certificazione secondo l'articolo 12. La procedura di certificazione deve includere il trattamento per il quale sarebbe necessaria la valutazione d'impatto. L'Incaricato avrebbe preferito se l'eccezione si fosse limitata alla semplice certificazione.

L'analisi d'impatto non è neppure necessaria se il titolare privato del trattamento rispetta un codice di condotta secondo l'articolo 10 che soddisfa le condizioni del capoverso 5. Concretamente il codice di condotta deve basarsi su una valutazione d'impatto sulla protezione dei dati che ha permesso di analizzare i rischi che comporta il trattamento previsto (lett. a), prevedere misure a tutela della personalità o dei diritti fondamentali della persona interessata (lett. b). Deve inoltre essere sottoposto all'Incaricato (lett. c). Si può ad esempio pensare a un'organizzazione di avvocati che sviluppa una piattaforma per le gestione dei dati dei clienti. A tal fine procede a una valutazione d'impatto sulla protezione dei dati e sulla base dei risultati redige un codice di condotta. Il titolare privato del trattamento che rispetta tale codice di condotta quando usa la piattaforma dell'organizzazione professionale sarà pertanto esentato dall'obbligo di procedere a una valutazione d'impatto.

L'Incaricato avrebbe auspicato che l'eccezione sia limitata al caso della certificazione.

Art. 21 Consultazione dell'Incaricato

A differenza di quanto prevedeva l'avamprogetto, nel D-LPD la comunicazione dei risultati della valutazione d'impatto sulla protezione dei dati all'Incaricato è trattata in una disposizione a sé stante.

Cpv. 1 Obbligo di consultare l'Incaricato

Secondo il capoverso 1 il titolare del trattamento sente previamente il parere dell'Incaricato se dalla valutazione d'impatto sulla protezione dei dati emerge che il trattamento previsto presenterebbe un rischio elevato per la personalità o i diritti fondamentali della persona interessata qualora il titolare del trattamento non adottasse alcuna misura. Anche se il P-STE 108 non la prescrive, la consultazione è prevista dalle regole europee (art. 28 della direttiva [UE] 2016/680 e art. 36 del regolamento [UE] 2016/679[152]). È inserita nel D-LPD perché permette all'Incaricato di intervenire a titolo preventivo e di consulenza. Questa procedura è più efficiente anche per il titolare del trattamento, poiché permette di risolvere eventuali problemi legati alla protezione dei dati in una fase precoce del trattamento.

152 Cfr. consid. 94 del regolamento (UE) 2016/679

Cpv. 2 e 3 Obiezioni dell'Incaricato

Secondo il capoverso 2, l'Incaricato ha due mesi per comunicare al titolare del trattamento le sue obiezioni contro il trattamento previsto. In casi particolarmente complessi tale termine può essere prorogato di un mese. Se entro due mesi non riceve alcuna comunicazione, il titolare del trattamento può presumere che l'Incaricato non ha obiezioni contro il trattamento previsto.

Quando è informato del risultato della valutazione d'impatto sulla protezione dei dati, l'Incaricato verifica se le misure proposte sono sufficienti per tutelare la personalità e i diritti fondamentali della persona interessata. Se giunge alla conclusione che il trattamento, nella forma prevista, sarebbe contrario alle disposizioni sulla protezione dei dati, propone misure adeguate al titolare del trattamento.

L'Incaricato è tuttavia libero di avviare un'inchiesta in una fase successiva se sussistono le condizioni di cui all'articolo 43 D-LPD, ad esempio se nella valutazione d'impatto i rischi non sono stati valutati correttamente e di conseguenza le misure proposte si sono rivelate inadeguate allo scopo o insufficienti.

Cpv. 4 Consultazione del consulente per la protezione dei dati

Il titolare privato del trattamento non è tenuto a consultare l'Incaricato se ha nominato un consulente per la protezione dei dati ai sensi dell'articolo 9 D-LPD e l'ha consultato in merito alla valutazione d'impatto. Il consulente per la protezione dei dati deve essere effettivamente intervenuto nella valutazione d'impatto. La sola nomina non è sufficiente a esentare il titolare del trattamento dall'obbligo di consultare l'Incaricato. Il consulente deve in particolare controllare la valutazione dei rischi e le misure proposte per prevenire i rischi identificati. La disposizione intende sgravare le imprese offrendo loro nel contempo un incentivo per nominare un consulente per la protezione dei dati.

Benché discussa, l'idea di introdurre un'eccezione di questo tipo nel regolamento (UE) 2016/679 è infine stata abbandonata. Riteniamo tuttavia utile prevedere un'eccezione supplementare, in particolare per ridurre l'onere amministrativo. L'Incaricato avrebbe preferito rinunciare a quest'eccezione.

Art. 22 Comunicazione di violazioni della sicurezza dei dati personali

L'articolo 22 D-LPD introduce l'obbligo di comunicare qualsiasi violazione della sicurezza dei dati personali. La disposizione concretizza i requisiti previsti dagli articoli 2 paragrafo 2 del P-STE 108 e 30 e seguenti della direttiva (UE) 2016/680. Gli articoli 33 e seguente del regolamento (UE) 2016/679 contengono disposizioni analoghe.

Cpv. 1 Definizione e principio

Secondo il capoverso 1 il titolare del trattamento deve comunicare quanto prima all'Incaricato qualsiasi violazione della sicurezza dei dati personali che comporta verosimilmente un grave rischio per la personalità e i diritti fondamentali della persona interessata. La regola si applica sia ai titolari privati del trattamento sia agli organi federali, per cui la disposizione menziona non soltanto il rischio per la personalità della persona interessata, ma anche quello per i suoi diritti fondamentali.

La nozione di violazione della sicurezza dei dati è definita all'articolo 4 lettera g D-LPD. Si tratta di qualsiasi violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vanno persi, sono cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate. La violazione può essere causata da un terzo, ma anche da un collaboratore che oltrepassa le sue competenze o che agisce per negligenza. In seguito alla violazione della sicurezza dei dati, la persona interessata può perdere il controllo sui suoi dati o i suoi dati possono essere usati in modo abusivo. Inoltre, la violazione può portare anche a una lesione della personalità, ad esempio rendendo note informazioni che la persona interessata intende mantenere segrete. L'articolo 26 capoverso 2 lettera a D-LPD considera una lesione della personalità qualsiasi violazione della sicurezza dei dati.

Ai suddetti rischi la persona interessata può reagire soltanto se è a conoscenza della violazione della sicurezza dei dati, ragione per cui il titolare del trattamento deve in linea di principio comunicare un trattamento non autorizzato innanzitutto all'Incaricato e, se sono soddisfatte le condizioni di cui al capoverso 4, anche alla persona interessata. Il trattamento non autorizzato deve essere comunicato quanto prima. In linea di massima il titolare del trattamento deve agire rapidamente, ma la disposizione lascia un certo margine di apprezzamento. È determinante, tra le altre cose, la probabilità del rischio di ledere la persona interessata: quanto più elevati sono il rischio e il numero delle persone interessate, tanto più rapidamente dovrà reagire il titolare del trattamento.

La comunicazione all'Incaricato è tuttavia necessaria soltanto se la violazione della protezione dei dati rischia di ledere gravemente la personalità e i diritti fondamentali della persona interessata. Questa regola intende evitare la comunicazione di violazioni insignificanti. Il titolare del trattamento deve valutare comunque le possibili ripercussioni della violazione per la persona interessata.

Cpv. 2 Contenuto della comunicazione

Il capoverso 2 precisa le indicazioni minime che deve contenere la comunicazione all'Incaricato. Il titolare del trattamento deve indicare innanzitutto, per quanto possibile, il tipo di violazione. Si distinguono quattro tipi di violazioni: la cancellazione o la distruzione di dati, la loro perdita, la loro modifica o la loro divulgazione a terzi non autorizzati. La comunicazione deve anche illustrare, per quanto possibile, le conseguenze della violazione della sicurezza dei dati. Si tratta innanzitutto delle conseguenze per la persona interessata e non quelle per il titolare del trattamento. Infine, il titolare del trattamento deve illustrare le misure disposte o previste per rimediare alla violazione della sicurezza dei dati o per attenuare le sue conseguenze. La comunicazione deve in ogni caso permettere all'Incaricato di intervenire rapidamente e nel modo più efficace possibile.

Cpv. 3 Comunicazione del responsabile del trattamento

La violazione della sicurezza dei dati può anche verificarsi presso il responsabile del trattamento. In tal caso quest'ultimo deve informarne quanto prima il titolare del trattamento. Spetta poi al titolare del trattamento procedere a valutare i rischi e decidere se è necessaria la comunicazione all'Incaricato e l'informazione della persona interessata.

Cpv. 4 Informazione della persona interessata

Secondo il capoverso 4 la persona interessata deve essere informata qualora sia necessario per proteggerla o l'Incaricato lo esiga. Il titolare ha a disposizione un certo margine di apprezzamento per giudicare se sussista la prima condizione e deve valutare soprattutto se l'informazione permette di ridurre i rischi per la personalità e i diritti fondamentali della persona interessata, ad esempio consentendole di prendere provvedimenti per proteggersi (p. es. modificare i suoi dati d'accesso o le sue parole chiave).

Cpv. 5 Restrizioni dell'obbligo di informare la persona interessata

Secondo il capoverso 5 il titolare del trattamento può limitare o differire l'informazione della persona interessata oppure rinunciarvi se sussiste un motivo di cui all'articolo 24 capoversi 1 lettera b e 2 lettera b D-LPD o se vi si oppone un obbligo legale di mantenere il segreto (lett. a). Inoltre, la lettera b del presente capoverso consente una restrizione se l'informazione è impossibile o esige mezzi sproporzionati. L'informazione è impossibile se il titolare del trattamento non è in grado di identificare la persona la cui sicurezza dei dati è stata violata, ad esempio perché i file log che permetterebbero l'identificazione non sono più disponibili. Si presume invece che la comunicazione esigerebbe mezzi sproporzionati se occorresse informare individualmente un gran numero di persone interessate e ne risulterebbero costi eccessivi in proporzione all'utilità dell'informazione per le persone interessate. Il capoverso 5 lettera c si applica in particolare in questi casi; essa autorizza il titolare del trattamento a optare per una comunicazione pubblica se l'informazione della persona interessata è garantita in modo equivalente. Si presume che questa condizione sia soddisfatta quando una comunicazione individuale non permetterebbe di migliorare in modo significativo l'informazione della persona interessata.

Cpv. 6 Consenso della persona soggetta all'obbligo di comunicazione

L'obbligo di comunicare violazioni della sicurezza dei dati previsto dall'articolo 22 D-LPD può entrare in conflitto con il diritto di non contribuire alla propria incriminazione. Per questo caso, il capoverso 6 prevede che una comunicazione in virtù dell'articolo 22 D-LPD può essere usata nel quadro di un procedimento penale contro la persona soggetta all'obbligo di comunicazione soltanto con il suo consenso. La regola si applica sia ai titolari sia ai responsabili del trattamento che comunicano una violazione della sicurezza dei dati personali.

9.1.5 Diritti della persona interessata

Il capitolo 4 disciplina i diritti della persona interessata. I diritti nei confronti dei titolari privati sono disciplinati nel capitolo 5, quelli nei confronti degli organi federali nel capitolo 6.

Art. 23 Diritto d'accesso

Il diritto d'accesso funge da complemento all'obbligo d'informare del titolare del trattamento e costituisce la base fondamentale per permettere alle persone interessate

di far valere i loro diritti secondo la presente legge. Il diritto d'accesso è un diritto soggettivo prettamente personale, che può essere esercitato in modo autonomo, senza il consenso del rappresentante legale, anche da persone capaci di discernimento, ma incapaci di agire. Il carattere prettamente personale del diritto implica anche che nessuno può rinunciare preventivamente al diritto d'accesso (art. 23 cpv. 5 D-LPD).

Cpv. 1 Principio

Secondo il capoverso 1, chiunque può domandare gratuitamente al titolare del trattamento se dati che la concernono sono trattati. Salvo pochi adeguamenti redazionali, la disposizione resta invariata rispetto al diritto vigente.

Cpv. 2 Informazioni da comunicare

Secondo il capoverso 2, la persona interessata riceve, su richiesta, innanzitutto le informazioni che devono esserle comunicate in base all'obbligo di informare (cfr. art. 17 cpv. 2 D-LPD). Si tratta soprattutto delle informazioni necessarie affinché la persona interessata possa far valere i diritti previsti dalla legge e sia quindi garantito un trattamento trasparente dei dati. Questa disposizione sottolinea non solo lo stretto legame tra il diritto d'accesso e l'obbligo di informare, ma anche lo scopo fondamentale del diritto d'accesso. Come constatato dal Tribunale federale[153], il diritto d'accesso intende permettere alla persona interessata di far valere i propri diritti nell'ambito della protezione dei dati. Questa precisazione risponde ai numerosi pareri, espressi in sede di consultazione e dalla dottrina, che criticano il fatto che il diritto d'accesso sia spesso utilizzato per fini completamente estranei alla protezione dei dati[154]. Si tratta in particolare dei casi in cui il diritto d'accesso è usato esclusivamente per ottenere mezzi di prova per un processo civile che non hanno alcun legame con la protezione dei dati. Questo modo di procedere permette di procurarsi, in un modo che non è previsto dal diritto procedurale vigente, mezzi di prova che vanno considerati dati personali ai sensi della LPD, mentre i mezzi di prova che non sono considerati dati personali devono essere raccolti seguendo le vie ordinarie previste dal diritto procedurale. Ne risultano differenze nella raccolta di prove che non sono oggettivamente giustificabili.

Le lettere a–g contengono un elenco non esaustivo delle informazioni che devono essere in ogni caso comunicate alla persona interessata. Come detto sopra, si tratta in linea di massima delle informazioni che il titolare del trattamento è tenuto a comunicare alla persona interessata. La clausola generale della frase introduttiva permette sussidiariamente di chiedere altre informazioni necessarie affinché la persona interessata possa far valere i propri diritti in virtù della legge sulla protezione dei dati e affinché sia garantita la trasparenza del trattamento. Se tratta una quantità notevole di dati riguardanti la persona interessata, la persona tenuta a fornire le informazioni deve poter domandare a quest'ultima di precisare i dati o i trattamenti a cui si riferisce la sua domanda d'accesso[155].

153 DTF **138** III 425, consid. 5.3.
154 Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter 20 feb. 2017, N° 54 segg.
155 Cfr. le spiegazioni analoghe della considerazione 63 del regolamento (UE) 2016/679

La persona interessata deve in ogni caso ricevere informazioni sull'identità e i dati di contatto del titolare del trattamento (lett. a). A seconda dei casi, è possibile che disponga già di tali informazioni (p. es. in virtù dell'obbligo di informare) e quindi ne riceve solo conferma. Può tuttavia darsi che la persona interessata venga a conoscenza dell'identità del titolare del trattamento soltanto al momento dell'informazione di cui alla lettera a (p. es. in caso di una pluralità di titolari del trattamento). Inoltre, la persona interessata deve essere informata dei dati personali trattati (lett. b) e dello scopo del trattamento (lett. c), come pure della durata di conservazione dei dati oppure, qualora ciò non sia possibile, dei criteri per stabilirla (lett. d). Quest'ultima informazione permette in particolare alla persona interessata di verificare che il titolare del trattamento conservi i dati conformemente ai principi di cui all'articolo 5 D-LPD. Dato che la durata della conservazione dei dati non deve essere necessariamente comunicata nell'ambito dell'obbligo di informare, la persona interessata deve in ogni caso ottenere questa informazione nell'ambito del diritto d'accesso. Alla persona interessata sono altresì comunicate le informazioni disponibili sulla provenienza dei dati personali, ovviamente sempreché non sia stata lei stessa a fornirli (lett. e). È inoltre informata su un'eventuale decisione individuale automatizzata e sulla logica su cui si fonda tale decisione (lett. f). Non è necessario comunicarle gli algoritmi utilizzati, che spesso rivelano segreti d'affari, bensì piuttosto le ipotesi fondamentali che sottintendono alla logica algoritmica su cui si basa la decisione individuale automatizzata. Ciò significa ad esempio che la persona interessata deve essere informata che in base al risultato negativo dell'esame della sua solvibilità le condizioni proposte per la conclusione di un contratto sono meno favorevoli rispetto a quanto preannunciato. La quantità e la natura dei dati usati per tale esame e la loro ponderazione devono essere precisate. Infine, occorre indicare alla persona interessata gli eventuali destinatari o le categorie di destinatari cui sono comunicati i dati personali (lett. g). Se i destinatari si trovano all'estero, l'informazione deve specificare lo Stato interessato e, se del caso, le garanzie ai sensi dell'articolo 13 capoverso 2 D-LPD o l'applicazione di una deroga di cui all'articolo 14 D-LPD.

Cpv. 3 e 4

Secondo il capoverso 3 il titolare del trattamento può comunicare alla persona interessata, previo suo consenso, dati personali concernenti la salute per il tramite di un professionista della salute da essa designato. Tale professionista deve avere le qualifiche richieste. Ripresa dal diritto in vigore, la disposizione è stata adeguata in seguito ai pareri espressi in sede di consultazione. Uno degli adeguamenti riguarda la necessità di ottenere il consenso della persona interessata. Il termine «professionista della salute» amplia la cerchi dei terzi autorizzati e offre maggiori possibilità di scelta per la persona interessata.

Il primo periodo del capoverso 4 resta invariato. La disposizione stabilisce che il titolare del trattamento è in linea di massima tenuto a fornire le informazioni richieste anche se ha delegato il trattamento dei dati a un responsabile. Se la persona interessata presenta una domanda d'accesso direttamente al responsabile del trattamento, questi deve indicarle il nome del titolare del trattamento o trasmettere la domanda a quest'ultimo. Anche se egli stesso non è tenuto, in questo caso, a infor-

mare la persona interessata, il responsabile non deve tuttavia ostacolare l'esercizio del diritto d'accesso. Il secondo periodo del capoverso 4 è abrogato.

Cpv. 5

Questa disposizione corrisponde al vigente articolo 8 capoverso 6.

Cpv. 6

Il capoverso 6 consente al nostro Consiglio di prevedere, nell'ordinanza, deroghe alla gratuità. Questa possibilità, prevista anche dal diritto in vigore (cfr. art. 2 OLPD), era stata eliminata nell'avamprogetto posto in consultazione sollevando forti critiche soprattutto perché la deroga alla gratuità era un mezzo per prevenire le invocazioni abusive del diritto d'accesso. In seguito a tali critiche, abbiamo deciso di mantenere la possibilità di prevedere deroghe alla gratuità. In tal modo il nostro Consiglio potrà anche tenere conto del fatto che a volte determinate domande d'accesso cagionano al titolare del trattamento un onere di lavoro notevole.

Art. 24 Restrizioni del diritto d'accesso

L'articolo 24 disciplina le restrizioni del diritto d'accesso. Salvo qualche adeguamento redazionale, le restrizioni sono state riprese tali e quali dal diritto vigente.

Cpv. 1 lett. c

Si tratta dell'unica disposizione nuova ed è stata introdotta in seguito ai pareri espressi in sede di consultazione. Consente al titolare del trattamento di rifiutare, restringere o differire la comunicazione delle informazioni se la domanda d'accesso è manifestamente infondata o querulomane. Il suo contenuto si fonda sull'articolo 12 paragrafo 5 del regolamento (UE) 2016/679, ma riprende la terminologia usata nel diritto svizzero, ad esempio nell'articolo 108 LTF o negli articoli 132 e 253 CPC. Dato che si tratta di un'ingerenza grave nei diritti fondamentali, la disposizione è inserita nella legge e non nell'ordinanza.

La deroga della lettera c va interpretata in maniera restrittiva sotto due punti di vista. Da una parte, il titolare del trattamento non deve presumere con leggerezza che la domanda d'accesso sia manifestamente infondata o querulomane. Dall'altra, anche in presenza di una siffatta domanda, il titolare del trattamento deve scegliere l'opzione più favorevole per la persona interessata. Deve pertanto accontentarsi di limitare la comunicazione delle informazioni o, se necessario, differirla e può rifiutarla soltanto nei casi assolutamente chiari ed evidenti. In ogni caso deve informare la persona interessata della limitazione, del differimento o del rifiuto dell'accesso (cfr. cpv. 3).

Il diritto d'accesso può essere invocato senza giustificarlo con un interesse o un motivo particolare. È sufficiente la mera curiosità, come evidenziato dal riferimento alla trasparenza del trattamento nell'articolo 23 capoverso 2 D-LPD. Il titolare del trattamento non può quindi in linea di massima chiedere una motivazione. Il Tribunale federale ha tuttavia osservato che la persona tenuta a fornire le informazioni può chiedere una giustificazione se ritiene che il diritto d'accesso venga fatto valere

in modo abusivo[156]. Secondo la giurisprudenza federale, una domanda d'accesso è potenzialmente abusiva se persegue un obiettivo totalmente estraneo alla protezione dei dati, ad esempio quello di risparmiare le spese per la raccolta delle prove o di procurarsi informazioni su un'eventuale parte contraente[157]. Se in tal caso l'autore della domanda d'accesso fa valere un motivo che si dimostra senza dubbio infondato senza che sia necessario procedere a un esame approfondito, il titolare del trattamento può restringere il diritto d'accesso. Solo a queste condizioni si è in presenza di una domanda d'accesso manifestamente infondata. In altre parole, deve essere manifesto che il diritto d'accesso è stato invocato per uno scopo che non rientra nel campo d'applicazione della LPD o per una finalità del tutto diversa (p. intenzione fraudolenta). Se vi sono solo dubbi in merito all'infondatezza, non si può parlare di domanda manifestamente infondata.

Sono querulomani ad esempio le domande d'accesso spesso ripetute senza motivo plausibile o rivolte a un titolare di cui il richiedente sa che non tratta dati che lo riguardano. Ma anche in questi casi il titolare del trattamento non può presumere con leggerezza la natura querulomane della domanda.

In generale il titolare del trattamento non può avvalersi della restrizione di cui al capoverso 1 lettera c soltanto per preservare i propri interessi. Per potersene avvalere devono essere soddisfatte le condizioni di cui all'articolo 24 capoverso 2 lettera a. La disposizione del capoverso 1 lettera c intende invece permettere al titolare del trattamento di trattare in maniera ragionevole le domande d'accesso del tutto sconnesse dallo scopo perseguito con il diritto d'accesso.

L'Incaricato è del parere che le eccezioni previste dall'articolo 24 capoverso 1 lettera c D-LPD non siano compatibili con la Convenzione STE 108.

Cpv. 3

Secondo il capoverso 3, il titolare del trattamento che rifiuta, limita o differisce la comunicazione dell'informazione deve indicarne il motivo. Può in linea di massima invocare soltanto i motivi di cui ai capoversi 1 e 2. In tal caso gli organi federali devono rendere una decisione impugnabile. I titolari privati del trattamento non hanno obblighi quanto alla forma. Per motivi probatori dovrebbero tuttavia comunicare per scritto i motivi alla persona interessata.

In base ai motivi addotti, la persona interessata deve poter verificare se la comunicazione è stata rifiutata, limitata o differita lecitamente. I requisiti posti alla motivazione non possono tuttavia essere troppo elevati, per evitare che entrino in conflitto con i motivi della restrizione stessa dell'informazione.

Art. 25 Restrizioni del diritto d'accesso a favore dei mezzi di comunicazione di massa

L'articolo 25 D-LPD riprende l'attuale articolo 10 LPD relativo alle restrizioni del diritto d'accesso a favore dei giornalisti. La disposizione non subisce modifiche materiali. Il criterio della pubblicazione nella parte redazionale di un mezzo di

156 DTF **138** III 425 consid. 5.4 s.; **123** II 534 consid. 2e
157 DTF **138** III 425 consid. 5.5

comunicazione resta invariato. Questo significa che sono contemplati soltanto i dati raccolti in vista della pubblicazione di un lavoro giornalistico nella parte redazionale di un mezzo di comunicazione[158]. Deve inoltre trattarsi di un mezzo di comunicazione pubblicato periodicamente. Ne fanno ad esempio parte giornali, riviste, trasmissioni radiofoniche o televisive, agenzie telegrafiche o servizi d'informazione in rete aggiornati continuamente e con una periodicità nota al pubblico[159].

9.1.6 Disposizioni speciali per il trattamento di dati da parte di persone private

Il capitolo 5 disciplina i diritti specifici nei confronti dei titolari privati del trattamento. Le disposizioni sul diritto d'accesso nel caso del trattamento di dati da parte di persone private concretizzano, in riferimento alla protezione dei dati, la tutela della personalità secondo l'articolo 28 CC e servono pertanto a realizzare il principio dell'autodeterminazione informativa nelle relazioni tra privati (cfr. art. 35 cpv. 1 e 3 Cost.). I tre articoli di questa sezione formano un'unità: l'articolo 26 D-LPD precisa le lesioni della personalità nell'ambito della protezione dei dati, l'articolo 27 D-LPD definisce i motivi giustificativi di una lesione e l'articolo 28 D-LPD disciplina le pretese giuridiche che possono essere fatte valere in seguito a una lesione della personalità a causa del trattamento di dati. Pur riprendendo in gran parte il diritto vigente, il D-LPD prevede alcuni adeguamenti redazionali per rendere le disposizioni più chiare e comprensibili.

La valutazione della LPD ha inoltre evidenziato che, soprattutto nel settore privato, le persone interessate fanno raramente valere i propri diritti, il che è dovuto principalmente ai costi che rischia di cagionare un processo[160]. Il presente avamprogetto intende ovviarvi adeguando il disciplinamento delle spese nel procedimento civile (cfr. n. 9.2.15).

Art. 26 Lesioni della personalità

Poiché l'articolo 28 CC non definisce il termine «lesioni della personalità», l'articolo 26 D-LPD lo precisa in riferimento alle lesioni in seguito al trattamento di dati.

Cpv. 1 Principio

Il capoverso 1 sancisce il principio secondo cui il trattamento di dati non deve ledere illecitamente la personalità delle persone interessate. Il tenore della disposizione resta invariato rispetto al diritto vigente. Il diritto di disporre dei propri dati personali, tutelato dal diritto all'autodeterminazione informativa, è spesso sensibilmente intaccato dal trattamento di dati. Il rispetto dei principi del trattamento di dati anche da parte dei titolari privati è perciò d'importanza fondamentale per la tutela

158 Barrelet Denis/Werly Stéphane, Droit de la communication, 2ª ed., Berna 2011, N 1769.
159 Barrelet Denis/Werly Stéphane, Droit de la communication, 2ª ed., Berna 2011, N 1420.
160 Cfr. pag. 90 seg. e 219 del rapporto finale del 10 mar. 2011 sulla valutazione della legge sulla protezione dei dati («Evaluation des Bundesgesetzes über den Datenschutz», disponibile soltanto in tedesco).

delle persone interessate, tanto più che una parte notevole dei trattamenti è effettuata da privati.

Cpv. 2 Presunzione di una lesione della personalità

Il capoverso 2 fa riferimento, tra le altre cose, al rispetto dei principi del trattamento di dati e presume una lesione della personalità segnatamente in tre casi.

Secondo la lettera a vi è lesione della personalità se sono trattati dati in violazione dei principi di cui agli articoli 5 e 7 D-LPD.

La lettera b prevede inoltre una lesione della personalità se sono trattati dati contro l'espressa volontà della persona interessata. Questa disposizione conferisce pertanto alla persona interessata il diritto di vietare esplicitamente a un titolare del trattamento di trattare determinati dati, senza che debbano essere soddisfatte le condizioni specifiche per un divieto (opting-out). Questa possibilità è prevista anche dalla legge vigente ed è ora richiesta anche dall'articolo 8 lettera d P-STE 108. Una manifestazione della volontà è espressa se risulta da un testo scritto od orale oppure da un segnale e la volontà risulta direttamente da tale testo o segnale. La persona interessata deve pertanto esprimere con un testo o con segnali che non è d'accordo con un determinato trattamento di dati. La manifestazione della volontà deve in quanto tale chiarire la volontà mediante il modo in cui è espressa. La persona interessata dovrebbe ad esempio disdire un servizio che implica il trattamento di dati o rilasciare una dichiarazione scritta od orale che indica al titolare del trattamento che non vuole che siano trattati i suoi dati. Una manifestazione «tacita» non è sufficiente. (cfr. il commento all'art. 5 cpv. 6 D-LPD, n. 9.1.3.1). Non è pertanto ad esempio sufficiente che la persona interessata non usufruisca semplicemente più di un servizio che implica il trattamento di dati.

Secondo la lettera c vi è una lesione della personalità se sono comunicati a terzi dati degni di particolare protezione.

L'elenco non è esaustivo e pertanto una lesione della personalità a causa del trattamento di dati può sussistere anche in altri casi. Per maggiore chiarezza e in conformità con l'articolo 28 CC, in cui la lesione della personalità e i motivi giustificativi sono trattati in due disposizioni separate che, da una parte, disciplinano la lesione illecita della personalità e, dall'altra, definiscono i casi in cui la lesione è lecita, nelle lettere b e c è stato tolto il riferimento alla giustificazione, analogamente a quanto fatto per la lettera a in occasione della revisione del 2003[161]. Il D-LPD disciplina i motivi giustificativi esclusivamente nell'articolo 27.

Cpv. 3 Assenza di lesione della personalità

Secondo il capoverso 3 non vi è invece lesione della personalità quando la persona interessata ha reso i dati accessibili a tutti e non si è opposta espressamente a un loro trattamento (per il termine «espressamente» si veda il commento al cpv. 2 lett. b). Questa regola, ripresa senza modifiche dal diritto vigente, è coerente, poiché in questo caso la libertà individuale di disporre dei propri dati personali non può essere lesa. Con l'espressione «di regola» si esprime che si tratta di una presunzione legale

[161] Cfr. DTF **136** II 508 consid. 5.2.3.

e non di una finzione. Ciò permette alla persona interessata di dimostrare, in un caso concreto, che ciononostante vi è una lesione della sua personalità. Questa possibilità è opportuna e importante perché la distinzione tra sfera privata e pubblica diventa sempre più difficile.

Art. 27 Motivi giustificativi

L'articolo 27 precisa i motivi giustificativi del trattamento di dati lesivo della personalità. Fatte salve piccole modifiche, la norma resta invariata rispetto al diritto vigente.

Cpv. 1 Principio

Il capoverso 1 sancisce il principio secondo cui qualsiasi lesione della personalità, ovvero qualsiasi trattamento di dati lesivo della personalità, è illecita se non è giustificata dal consenso della persona interessata, da un interesse preponderante privato o pubblico oppure dalla legge. La disposizione corrisponde all'articolo 28 capoverso 2 CC. In presenza del consenso della persona interessata o di una legge non si procede a una ponderazione degli interessi e non si applica il capoverso 2. Tra i motivi giustificativi previsti dalla legge si possono menzionare ad esempio l'obbligo di trattamento e l'obbligo di esame (p. es. art. 28 segg. della legge federale del 23 marzo 2001[162] sul credito al consumo o art. 3 segg. della legge del 10 ottobre 1997[163] sul riciclaggio di denaro) o l'obbligo di conservazione. La ponderazione degli interessi è invece necessaria in presenza di un interesse privato o pubblico. La persona interessata ha, tra le altre cose, l'interesse a salvaguardare la propria libertà di disporre dei dati, mentre il titolare o il responsabile del trattamento ha l'interesse a trattare i dati. Il capoverso 2 fornisce un elenco esemplare di trattamenti che possono rappresentare un interesse preponderante del titolare del trattamento. Una lesione della personalità è giustificata soltanto se l'interesse al trattamento prevale sugli interessi della persona interessata.

Cpv. 2 Interessi preponderanti del responsabile del trattamento

Il capoverso 2 precisa i casi in cui può sussistere un interesse preponderante del titolare del trattamento. La formulazione, che è la stessa del diritto vigente, chiarisce che non si tratta di motivi giustificativi assoluti. Come nel diritto vigente, è infatti determinante la ponderazione degli interessi nel singolo caso. Contrariamente al diritto vigente, la disposizione proposta parla di titolare e non più di responsabile del trattamento. L'adeguamento è dovuto all'introduzione del termine di titolare del trattamento. I motivi giustificativi di cui all'articolo 27 capoverso 2 sono tuttavia concepiti per persone che in quanto titolari possono decidere in merito allo scopo, ai mezzi e alla portata del trattamento dei dati. Gli altri convenuti possono far valere i motivi giustificativi di cui al capoverso 1. In virtù dell'articolo 8 capoverso 4 D-LPD, il responsabile del trattamento può far valere gli stessi motivi giustificativi del titolare del trattamento. La modifica non ha ripercussioni sulla legittimazione passiva.

162 RS **221.214.1**
163 RS **955.0**

L'elenco resta in gran parte invariato rispetto al diritto vigente. Non è esaustivo e pertanto anche altri motivi possono costituire un interesse preponderante del titolare del trattamento. Enumera varie finalità che giustificano il trattamento di dati e possono prevalere nei confronti degli interessi della persona interessata. In linea di massima l'elenco comprende tre gruppi di trattamenti: quelli per determinate attività economiche, quelli nell'ambito dei media e quelli per scopi impersonali, ad esempio di ricerca. In determinati casi la finalità del trattamento non è sufficiente per giustificare una lesione della personalità, poiché il trattamento deve soddisfare anche determinate condizioni affinché possa essere fatto valere il motivo giustificativo dell'interesse preponderante. Ciò vale in particolare in riferimento alle lettere b, c ed f. In questi casi, prima di ponderare gli interessi nel caso concreto, va dapprima verificato se il trattamento in questione soddisfa le condizioni specifiche. Se le condizioni specifiche non sono soddisfatte, il trattamento dei dati è giustificato soltanto se sussiste un motivo giustificativo di cui al capoverso 1. Qui appresso commentiamo solo le lettere c ed e, che hanno subito modifiche rispetto alla legge in vigore.

Cpv. 2 lett. c Valutazione del credito

Per quanto riguarda l'attività di servizi di informazioni commerciali, è importante innanzitutto segnalare la sentenza del Tribunale amministrativo federale A-4232/2015 del 18 aprile 2017 (Moneyhouse). Moneyhouse AG è una società che fornisce informazioni commerciali e riceve dati in forma elettronica da diverse fonti pubbliche e private. Questa moltitudine di dati personali è pubblicata sul sito www.moneyhouse.ch ed è usata per proporre diversi tipi di servizi, ad esempio un motore di ricerca di imprese e di persone. Mentre questo servizio è gratuito per gli utenti a condizione che si siano registrati sul sito, altri sono a pagamento e riservati ai cosiddetti «Premium user», ad esempio l'accesso a informazioni sulla solvibilità e la morale di pagamento o informazioni dettagliate su pagamenti mancati, sulle esecuzioni, sul registro fondiario e sulla situazione economica e fiscale, come pure servizi riguardanti profili di imprese. Per le offerte supplementari e l'accesso ai dati delle persone fisiche che non sono iscritte nel registro di commercio o in un elenco telefonico deve essere fatto valere un interesse giustificativo[164]. In riferimento agli abbonamenti Premium, soggetti a pagamento, il Tribunale amministrativo federale è giunto alla conclusione che Moneyhouse AG allestisce un profilo biografico delle persone. Ha osservato che si è pertanto in presenza di un trattamento del profilo della personalità e quindi il motivo giustificativo della verifica del credito di cui all'articolo 13 capoverso 2 lettera c LPD non è applicabile[165]. Per il Tribunale amministrativo federale non vi è né una base legale né è stato dimostrato l'espresso consenso delle persone interessate come motivo che giustifica l'allestimento di un profilo della personalità. Infine, anche la ponderazione degli interessi ha evidenziato che prevale l'interesse a tutelare la personalità delle persone interessate. Il Tribunale amministrativo federale ha pertanto constatato un trattamento illecito di profili della personalità, impartendo a Moneyhouse di chiedere il consenso espresso delle persone interessate, pena la cancellazione dei pertinenti dati nella misura in cui se ne possano dedurre informazioni su aspetti fondamentali della personalità[166]. Inoltre, il Tribunale amministrati-

164 TAF, A-4232/2015 del 18 apr. 2017, fatti A.a.
165 TAF, A-4232/2015 del 18 apr. 2017, consid. 5.3.
166 TAF, A-4232/2015 del 18 apr. 2017, consid. 5.5.

vo federale ha ordinato a Moneyhouse di effettuare un controllo annuale della sua banca dati attraverso la verifica del 5 per cento delle ricerche effettuare sul suo sito[167]. D'altronde, nell'ambito del rapporto in adempimento del postulato 16.3682 «Inquadrare le prassi delle società che forniscono dati sulla solvibilità», il nostro Consiglio esaminerà misure specifiche per le imprese che forniscono informazioni commerciali.

Il D-LPD tiene già conto di determinati timori legati all'attività delle imprese che forniscono informazioni commerciali. Affinché la verifica del credito possa essere considerata un interesse preponderante devono essere soddisfatte quattro condizioni. Rispetto al diritto vigente, la disposizione è leggermente più severa, in particolare per tenere conto del rischio elevato connesso a questo tipo di trattamento di dati.

I numeri 1 e 2 corrispondono al diritto vigente, salvo la sostituzione dell'espressione «profilo della personalità» con «profilazione». Anche in virtù del diritto vigente gli istituti che valutano il credito di una persona non possono trattare profili della personalità. Resta vietato anche il trattamento di dati degni di particolare protezione. Ne fanno parte anche i dati sui perseguimenti amministrativi e penali, poiché terzi non hanno neppure accesso al casellario giudiziale. Contrariamente a quanto proposto da diversi partecipanti alla consultazione, la LPT non può concedere ulteriori diritti agli istituti che forniscono informazioni economiche.

I numeri 3 e 4 sono nuovi.

Secondo il numero 3 i dati non possono risalire a oltre cinque anni addietro. Questo inasprimento è stato chiesto da vari partecipanti alla consultazione e appare giustificato tenendo conto dell'importanza della valutazione della solvibilità per la persona interessata. Anche il Tribunale amministrativo federale ha sottolineato che le esigenze poste alla qualità dei dati e quindi alla correttezza del trattamento di dati devono essere proporzionali al rischio di una lesione della personalità[168]. La quota di verifica del 5 per cento, molto modesta, impartita dal Tribunale amministrativo federale a Moneyhouse, mostra le difficoltà di tenere aggiornate simili banche dati. Per questo motivo riteniamo opportuno introdurre un disciplinamento generale della durata durante la quale possono essere utilizzati i dati. Tale limitazione può essere attuata mediante strumenti tecnici appositi (privacy by design, cfr. art. 6 D-LPD e il relativo commento), ad esempio la cancellazione automatica alla scadenza di un determinato periodo. La durata di conservazione di cinque anni si basa sull'articolo 8*a* capoverso 4 LEF secondo cui, per i terzi, il diritto di consultazione si estingue cinque anni dopo la chiusura del procedimento. I diritti degli istituti che forniscono informazioni economiche non devono essere più estesi.

Il numero 4 prevede che la persona interessata debba essere maggiorenne. Questa condizione è introdotta per migliorare la protezione dei minori, uno degli obiettivi della revisione della LPD. La portata di questa modifica dovrebbe essere limitata, viste le ristrette possibilità dei minori di esercitare i diritti civili.

167 TAF, A-4232/2015 del 18 apr. 2017, consid. 7.3.2.
168 TAF, A-4232/2015 del 18 apr. 2017, consid. 7.1.

Cpv. 2 lett. e Trattamento a scopo di ricerca, pianificazione o statistica

Le condizioni della lettera e relative al motivo giustificativo del trattamento di dati per scopi impersonali, in particolare nei settori della ricerca, pianificazione o statistica, sono state leggermente inasprite. L'utilizzazione di dati per tali scopi è ammessa soltanto se sono soddisfatte le condizioni di cui ai numeri 1–3. S'intende così rafforzare la tutela dei dati personali degni di particolare protezione, soprattutto in considerazione delle possibilità offerte da Big Data e dalla crescente digitalizzazione nella vita quotidiana, grazie alle quali è possibile trattare un numero sempre maggiore di dati personali degni di particolare protezione.

Secondo il numero 1, i dati devono essere resi anonimi non appena lo scopo del trattamento lo permette. Pertanto, quando non è più necessario disporre di dati personali per il trattamento a scopi di ricerca, pianificazione o statistica, questi devono essere resi anonimi. Questa condizione è soddisfatta se i dati sono comunicati sotto forma pseudonimizzata e la chiave per reidentificare la persona resta presso colui che ha trasmesso i dati (anonimizzazione di fatto).

Questo principio si evince già dall'articolo 5 capoverso 4 D-LPD. Secondo l'articolo 26 capoverso 2 lettera a D-LPD, la violazione di tale disposizione costituisce una lesione della personalità, che può essere giustificata da uno dei motivi di cui all'articolo 27 D-LPD. Grazie alla nuova disposizione dell'articolo 27 capoverso 2 lettera e numero 1 D-LPD, non sarà più possibile giustificare una violazione dell'articolo 5 capoverso 4 D-LPD con il trattamento a scopi di ricerca, pianificazione o statistica, a meno che non sia applicabile uno dei motivi giustificativi di cui all'articolo 27 capoverso 1 D-LPD.

I dati personali degni di particolare protezione comunicati a terzi devono essere comunicati in una forma che non permetta d'identificare le persone interessate (n. 2). Secondo l'articolo 26 capoverso 2 lettera c D-LPD, la comunicazione di dati personali degni di particolare protezione a terzi comporta una lesione della personalità, che può essere giustificata da uno dei motivi di cui all'articolo 27 D-LPD. Grazie alla nuova condizione del numero 2, non sarà più possibile giustificare la comunicazione di dati personali degni di particolare protezione in forma non anonimizzata con il motivo del trattamento a scopi di ricerca, pianificazione o statistica.

Infine, come finora, i risultati possono essere pubblicati soltanto in una forma che non permetta d'identificare le persone interessate (n. 3).

Art. 28 Pretese giuridiche

L'articolo 28 disciplina le pretese giuridiche che le persone interessate possono far valere nei confronti di persone private.

Cpv. 1 Rettifica

Secondo il capoverso 1 la persona interessata può chiedere di rettificare dati personali inesatti. Questo diritto è attualmente previsto dall'articolo 5 capoverso 2 LPD. Nel D-LPD è unito in un unico articolo a tutte le altre pretese giuridiche. La rettifica può consistere sia nell'integrazione dei dati mancanti o nella cancellazione dei dati inesatti ed eventualmente nella loro sostituzione con quelli esatti.

Visto che il diritto alla rettifica è sancito in un capoverso a sé stante, ne risulta chiaramente che esso sussiste a prescindere da una lesione della personalità secondo l'articolo 26 D-LPD. Neanche i motivi giustificativi di cui all'articolo 27 possono essere fatti valere. Il capoverso 1 prevede invece due eccezioni che escludono la rettifica.

Secondo la lettera a non si può chiedere di rettificare i dati se una disposizione legale ne vieta la modifica. Si pensi agli obblighi legali di trattamento e di conservazione secondo cui i titolari privati del trattamento devono lasciare inalterati i dati.

La lettera b permette una ponderazione degli interessi in riferimento a dati trattati unicamente a scopo di archiviazione e che rispondono a un interesse pubblico di lasciare questi dati inalterati. Questa eccezione contempla, ad esempio, le biblioteche private.

Cpv. 2 Azioni

Il capoverso 2 contiene il riferimento alle azioni secondo l'articolo 28 e seguenti CC, già previsto dal diritto vigente. In analogia all'articolo 28 capoverso 1 CC, la disposizione elenca i singoli diritti specifici che la persona interessata può far valere. Per maggiore chiarezza il D-LPD li suddivide in un elenco. Quest'ultimo precisa, in riferimento al trattamento dei dati, in particolare l'azione per proibire una lesione e quella per farla cessare di cui all'articolo 28*a* capoverso 1 numeri 1 e 2 CC. Secondo la lettera a, la persona interessata può chiedere di proibire il trattamento dei dati personali. Secondo la lettera b può chiedere di far cessare la comunicazione dei dati a terzi e secondo la lettera c può chiedere di rettificare, cancellare o distruggere i dati.

Mentre nel diritto vigente è previsto soltanto implicitamente, nel D-LPD il diritto alla cancellazione è stato formulato esplicitamente, in conformità con i requisiti dell'articolo 8 lettera e P-STE 108. Il regolamento (UE) 2016/679 contiene un disciplinamento analogo. Il diritto alla cancellazione corrisponde, nel settore della protezione dei dati, al «diritto all'oblio» come lo si evince in generale dalla protezione della personalità del diritto civile[169]. Pertanto anche in Svizzera sarebbe possibile una decisione analoga a quella emessa dalla Corte di giustizia europea nei confronti di Google[170]. Il diritto all'oblio non vale tuttavia in modo assoluto[171]. La giurisprudenza sulla protezione dei dati, infatti, pondera in linea di principio gli interessi della persona i cui dati sono trattati e il diritto alla libertà d'opinione e d'informazione, dal quale risulta spesso un interesse a conservare o utilizzare le informazioni. Tale interesse può ad esempio sussistere nel caso di archivi o biblioteche, il cui compito è raccogliere, rendere accessibili, conservare e presentare al pubblico i documenti senza alterarli. La ponderazione degli interessi nel singolo caso è possibile e necessaria in virtù dell'articolo 28 capoverso 2 D-LPD e del rinvio agli articoli 28 e seg. CC, di modo che nel testo di legge non è stato necessario inserire clausole specifi-

169 Cfr. in particolare DTF **109** II 353; DTF **111** II 209 e DTF **122** II 449.
170 Cfr. la sentenza nella causa C-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos [AEPD], Mario Costeja González) del 13 mag. 2014, ECLI:EU:C:2014:317.
171 DTF **111** II 209 consid. 3c.

che[172]. L'Incaricato avrebbe auspicato l'introduzione di un diritto esplicito alla cancellazione («diritto all'oblio»).

Cpv. 3 Menzione del carattere contestato

Il capoverso 3 prevede la menzione del carattere contestato dei dati personali, ripresa senza modifiche dal diritto vigente. Se non può essere dimostrata né l'esattezza né l'inesattezza dei dati personali, la persona interessata può chiedere di aggiungere una menzione che ne rilevi il carattere contestato. La disposizione va valutata alla luce del fatto che l'inesattezza di determinati fatti, soprattutto se sono connessi a giudizi di valore, non può sempre essere dimostrata in modo adeguato. Con la menzione del carattere contestato la persona interessata usufruisce almeno di una protezione giuridica parziale.

Cpv. 4 Comunicazione a terzi o pubblicazione

Alla stregua del diritto vigente, il capoverso 4 prevede il diritto di chiedere che la rettifica, la distruzione, il divieto di trattamento o di comunicazione a terzi nonché la menzione del carattere contestato dei dati siano comunicati a terzi o pubblicati. Questa regola concretizza l'articolo 28*a* capoverso 2 CC nell'ambito della protezione dei dati.

È invece abrogata la disposizione riguardante la procedura semplificata per le domande in esecuzione del diritto d'accesso. La disposizione è divenuta obsoleta in seguito all'entrata in vigore del Codice di procedura civile, nel quale sono inserite tutte le disposizioni legate alle procedure civili (art. 12 cpv. 4 CPC). Il CPC disciplina la procedura applicabile (art. 243 cpv. 2 lett. d D-CPC) e il foro giuridico (art. 20 lett. d D-CPC).

9.1.7 Disposizioni speciali per il trattamento di dati da parte di organi federali

Art. 29 Controllo e responsabilità in caso di trattamento congiunto di dati personali

Rispetto all'articolo 16 LPD, l'articolo 29 D-LPD subisce poche modifiche.

L'articolo 16 capoverso 1 LPD è abrogato. La responsabilità dell'organo federale che tratta dati personali si evince dalla definizione di «titolare del trattamento» (art. 4 lett. i D-LPD).

Per gli stessi motivi, l'articolo 29 D-LPD rinuncia all'espressione «regolare in modo specifico». Inoltre, secondo il D-LPD, se un organo federale tratta dati congiuntamente ad altre autorità o a privati, il Consiglio federale ha l'obbligo, e non soltanto la facoltà, di disciplinare i dettagli relativi ai controlli e alle responsabilità in materia di protezione dei dati. Questa modifica attua l'articolo 21 della direttiva

[172] L'art. 38 non prevede la possibilità di ponderare gli interessi, per cui è stata inserita una riserva nel suo cpv. 5.

(UE) 2016/680. L'articolo 26 del regolamento (UE) 2016/679 prevede una regola analoga.

Art. 30 Basi legali

Per tenere conto delle critiche della dottrina relative alla distinzione tra le deroghe di cui all'articolo 17 capoverso 2 LPD e all'articolo 19 capoverso 2 LPD, l'articolo 30 capoverso 2 D-LPD disciplina le basi legali per il trattamento di determinati dati personali, mentre il capoverso 4 fissa le deroghe ai requisiti posti alla base legale.

Cpv. 1 Base legale

Il capoverso 1 riprende il principio dell'articolo 17 capoverso 1 LPD, secondo cui gli organi federali possono trattare dati personali soltanto se esiste una pertinente base legale, fatte salve determinate eccezioni.

Cpv. 2 Base legale in una legge in senso formale

Come nel diritto vigente, il capoverso 2 lettera a sancisce che per il trattamento di dati personali degni di particolare protezione è necessaria una base in una legge in senso formale.

Secondo la lettera b, gli organi federali sono autorizzati alla profilazione ai sensi dell'articolo 4 lettera f D-LPD soltanto se lo prevede una base in una legge in senso formale. La disposizione sostituisce l'articolo 17 capoverso 2 LPD secondo cui i profili della personalità possono essere trattati soltanto se lo prevede esplicitamente una legge in senso formale. In considerazione del rischio di ingerenza nei diritti fondamentali delle persone interessate, riteniamo che per la profilazione debba essere prevista una base legale di livello equivalente a quella per il trattamento di dati particolarmente degni di protezione. Come illustrato qui appresso nel commento al capoverso 3, la condizione di una base in una legge in senso formale non è assoluta. Spetterà pertanto al legislatore decidere in ciascun settore se sia necessaria una base legale formale in una legge specifica o se sia sufficiente una base in una legge in senso materiale. Può infatti darsi che in determinati casi una profilazione non comporti rischi per i diritti fondamentali della persona interessata.

Secondo il capoverso 2 lettera c è necessaria una base in una legge in senso formale se lo scopo o il tipo del trattamento di dati può comportare una grave ingerenza nei diritti fondamentali della persona interessata. Questa fattispecie non è esplicitamente prevista dall'articolo 17 capoverso 2 LPD, ma non costituisce di per sé una novità poiché l'articolo 36 capoverso 1 Cost. sancisce che le restrizioni gravi dei diritti fondamentali devono fondarsi su una base legale prevista da una legge in senso formale. La lettera c è tuttavia necessaria poiché in varie leggi federali sono abrogati il termine «profilo della personalità» e le pertinenti basi legali. Riteniamo infatti che l'abrogazione del suddetto termine non deve comportare un abbassamento del livello della base legale.

Una grave ingerenza nei diritti fondamentali delle persone interessate può risultare dalle finalità del trattamento di dati personali (primo caso di applicazione della lettera c). In certi ambiti infatti, gli organi federali devono eventualmente trattare determinati dati personali al fine di valutare, ad esempio, la pericolosità di una persona, il

suo potenziale per esercitare una funzione, l'idoneità a svolgere un compito legale oppure il suo modo di vivere. A seconda delle finalità perseguite dall'organo federale, il trattamento può costituire, a prescindere dal tipo di dati trattati, una grave ingerenza nei diritti fondamentali della persona interessata. Se ciò è il caso è pertanto necessario prevedere per tali trattamenti una base legale dello stesso livello di quella prevista per il trattamento di dati degni di particolare protezione.

Una grave ingerenza nei diritti fondamentali della persona interessata può risultare dal tipo di trattamento (secondo caso di applicazione della lett. c). Si tratta soprattutto delle decisioni individuali automatizzate secondo l'articolo 19 capoverso 1 D-LPD. Non tutte le decisioni individuali automatizzate presentano un rischio elevato per la persona interessata e pertanto in alcuni casi è sufficiente una base legale in una legge in senso materiale. Tuttavia, se la decisione individuale automatizzata si basa su una dati degni di particolare protezione, è in linea di massima necessaria una base legale in una legge in senso formale. Questo disciplinamento permette inoltre di rispettare i requisiti dell'articolo 11 della direttiva (UE) 2016/680.

Cpv. 3 Deroghe all'esigenza di una base in una legge formale

Questa disposizione autorizza il Consiglio federale ad adottare una base legale in senso materiale per il trattamento di dati degni di particolare protezione e le profilazioni se sono soddisfatte due condizioni cumulative. Secondo la prima (lett. a) il trattamento deve essere indispensabile per l'adempimento di un compito definito in una legge in senso formale. Affinché questa condizione sia soddisfatta, il legislatore deve precisare nella legge la natura dei compiti che richiedono il trattamento di dati personali. La seconda condizione (cpv. 3 lett. b) è nuova e ha il vantaggio di circoscrivere in maniera più precisa la portata del capoverso 3 rispetto all'articolo 17 cpv. 2 lett. a LPD. Quest'ultimo è applicabile solo eccezionalmente, il che può comportare che il margine di apprezzamento a disposizione possa indurre a supporre casi eccezionali anche laddove non ne esistono i presupposti.

L'abbassamento del livello della base legale è opportuno in particolare per i dati personali degni di particolare protezione eccezionalmente trattati nell'ambito degli affari del Consiglio federale, dei dipartimenti e degli uffici (p. es. decisioni su ricorsi, casi di responsabilità dello Stato, affari relativi al personale federale). Anche per questi trattamenti, secondo il vigente articolo 17 capoverso 1 LPD, sarebbe necessaria una base in una legge in senso formale. Per contro, secondo l'articolo 30 capoverso 3 D-LPD sarà in futuro sufficiente una base in una legge in senso materiale se il trattamento è indispensabile per l'adempimento di un compito definito in una legge in senso formale e non comporta rischi particolari per i diritti fondamentali della persona interessata. Se queste condizioni sono soddisfatte e l'accesso ai dati in questione è fortemente limitato, in futuro sarà in linea di massima sufficiente una base in una legge in senso materiale.

Cpv. 4 Deroghe

Questa disposizione prevede una deroga all'esigenza di una base legale (cpv. 1–3) se è soddisfatta una delle condizioni di cui alle lettere a–c.

La lettera a prevede una decisione del Consiglio federale di autorizzare eccezionalmente un organo federale a trattare dati personali senza una base legale. Corrisponde all'eccezione prevista dall'articolo 17 capoverso 2 lettera b LPD.

Secondo la lettera b gli organi federali possono trattare dati personali senza una pertinente base legale se, nel caso specifico, la persona interessata vi ha acconsentito conformemente all'articolo 5 capoverso 6 D-LPD o ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento. Questa disposizione corrisponde sostanzialmente all'eccezione prevista dall'articolo 17 capoverso 2 lettera b LPD.

Infine, la lettera c è una nuova deroga, non prevista dall'articolo 17 capoverso 2 LPD e corrisponde all'articolo 10 lettera b della direttiva (UE) 2016/680 e all'articolo 6 paragrafo 1 lettera d del regolamento (UE) 2016/679. Secondo la disposizione gli organi federali possono trattare dati personali se è necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole.

Art. 31 Trattamento automatizzato di dati personali nell'ambito di sistemi pilota

Le modifiche rispetto all'articolo 17*a* LPD non hanno lo scopo di indebolire le condizioni applicabili quando un organo federale prevede un trattamento automatizzato di dati nell'ambito di un progetto pilota prima dell'entrata in vigore di una legge in senso formale, ma sono unicamente tese a ridurre la densità normativa. Infatti, dalla sua entrata in vigore, gli organi federali hanno fatto poche volte uso di questa norma. Inoltre, alcune disposizioni dell'articolo 17*a* LPD possono essere riprese nella futura ordinanza d'esecuzione.

Le condizioni previste ai capoversi 1 e 2 sono identiche a quelle dell'articolo 17*a* capoverso 1 LPD, salvo che «profili della personalità» è sostituito da «altri trattamenti ai sensi dell'articolo 30 capoverso 2 lettere b e c». Inoltre, nella lettera c si precisa che la fase sperimentale è necessaria «in particolare per ragioni tecniche». Questa modifica è dovuta all'abrogazione dell'articolo 17*a* capoverso 2 LPD, che enumera i casi in cui una fase sperimentale può essere considerata indispensabile per trattare determinati dati. Per le ragioni indicate sopra, questi casi possono essere disciplinati in un'ordinanza d'esecuzione.

I capoversi 3 e 4 corrispondono al diritto in vigore, fatte salve l'abrogazione del termine «profili della personalità» e alcune modifiche redazionali.

Art. 32 Comunicazione di dati personali

L'articolo 32 D-LPD mantiene il principio sancito dall'articolo 19 LPD, secondo cui gli organi federali hanno il diritto di comunicare dati personali se ne esistono i fondamenti giuridici, ma precisa che la nozione di fondamento giuridico corrisponde alla base legale di cui all'articolo 30 capoversi 1–3 D-LPD. Da questa precisazione si evince che l'articolo 32 non rinvia alle eccezioni previste dall'articolo 30 capoverso 4 D-LPD. Pertanto, i casi in cui gli organi federali sono autorizzati a comunicare dati personali in assenza di una base legale sono elencati in modo esaustivo

all'articolo 32 capoverso 2 lettere a–e D-LPD. Questa modifica tiene conto delle critiche della dottrina riguardo alla delimitazione tra le eccezioni previste dall'articolo 17 capoverso 2 LPD e quelle elencate dall'articolo 19 capoverso 2 LPD.

I «dati personali» del capoverso 1 comprendono anche i dati degni di particolare protezione. Qualora per il trattamento di determinate categorie di dati personali (dati personali particolarmente degni di protezione) o per determinati tipi di trattamenti (profilazione, trattamenti ai sensi dell'art. 30 cpv. 2 lett. c) l'articolo 30 richieda una base in una legge in senso formale, ciò vale anche per le prescrizioni relative alla comunicazione di tali dati personali. La comunicazione di dati personali è di per sé un'operazione delicata e pertanto non è privo di importanza il modo in cui i dati comunicati vengono acquisiti. Se pertanto la comunicazione avviene successivamente a uno dei tipi di trattamento particolarmente delicati, ciò deve essere previsto da una legge in senso formale. Le deroghe previste dal capoverso 2 sono applicabili anche quando un organo federale prevede di comunicare questo tipo di dati.

L'eccezione prevista dal capoverso 2 lettera a è ampliata rispetto al diritto vigente. In assenza di una base legale, un organo federale è autorizzato a comunicare dati in un caso specifico non soltanto, come finora, quando tali dati sono indispensabili per l'adempimento dei compiti legali del destinatario, ma anche quando la comunicazione è indispensabile per l'adempimento dei compiti legali dell'organo federale che intende comunicare i dati.

La lettera c è una nuova eccezione non prevista dall'articolo 19 capoverso 1 LPD ed è inserita anche nell'articolo 30 capoverso 4 lettera c D-LPD.

L'articolo 32 capoverso 3 D-LPD corrisponde all'articolo 19 capoverso 1bis LPD, salvo un singolo adeguamento. L'adeguamento intende migliorare il coordinamento tra la LTras e la LPD: in riferimento alla condizione dell'interesse pubblico preponderante alla comunicazione dei dati (art. 29 cpv. 3 lett. b D-LPD) va chiarito che tale condizione si applica non solo addizionalmente (alternativamente), ma anche indipendentemente dall'articolo 32 capoversi 1 e 2. Si propone di sostituire, nella frase introduttiva dell'articolo 32 capoverso 3 D-LPD, l'espressione «anche» (nella versione tedesca «auch», assente nella versione francese) con «inoltre / darüber hinaus / en outre», ponendola all'inizio della frase per evidenziare che il capoverso 3 costituisce una base legale supplementare a quelle previste dal capoversi 1 e 2.

L'articolo 32 capoverso 4 D-LPD non subisce modifiche rispetto all'articolo 19 capoverso 2 LPD. Restano pertanto valide le spiegazioni del messaggio del nostro Consiglio del 23 marzo 1988[173].

Per contro, l'esigenza della base legale per le «procedure di richiamo» nel settore pubblico (art. 19 cpv. 3 LPD) è abrogata poiché nell'era digitale appare ormai obsoleta. Questa modifica non indebolisce la protezione dei dati personali poiché la comunicazione deve sempre avvenire conformemente alle disposizioni sulla protezione dei dati. Le modifiche delle leggi speciali che si rendono necessarie in seguito all'abrogazione dell'articolo 19 capoverso 3 dovranno essere fatte man mano in occasione delle revisioni di tali leggi.

I capoversi 5 e 6 corrispondono ai capoversi 3bis e 4 dell'articolo 19 LPD.

173 FF **1988** II 353, in particolare pag. 410.

Art. 33 Opposizione alla comunicazione di dati personali

Questa disposizione resta invariata rispetto al diritto vigente (art. 20 LPD), fatti salvi alcuni adeguamenti redazionali. Nella versione tedesca l'espressione «Sperrung der Bekanntgabe» è sostituita da «Widerspruch gegen die Bekanntgabe» in adeguamento alla terminologia europea.

Secondo l'Incaricato, oltre che alla comunicazione di dati, il diritto all'opposizione dovrebbe applicarsi anche al trattamento di dati.

Art. 34 Offerta di documenti all'Archivio federale

La disposizione corrisponde all'articolo 21 LPD e non subisce modifiche materiali.

Art. 35 Trattamento di dati per scopi di ricerca, pianificazione e statistica

La disposizione corrisponde in gran parte all'articolo 22 LPD.

Inoltre, nel capoverso 1 è introdotta una nuova lettera b, secondo cui l'organo federale deve comunicare i dati personali degni di particolare protezione a persone private in una forma che non permetta d'identificare le persone interessate. La modifica intende migliorare la tutela dei dati degni di particolare protezione. La condizione è soddisfatta anche se la comunicazione avviene in forma pseudonimizzata e la chiave per reidentificare la persona resta presso colui che ha trasmesso i dati (anonimizzazione di fatto).

Il capoverso 2 è inoltre modificato in riferimento ai rinvii agli articoli 5 capoverso 3, 30 capoversi 2 e 32 capoverso 1 D-LPD.

Art. 36 Attività di diritto privato di organi federali

La disposizione corrisponde all'articolo 23 capoverso 1 LPD. L'articolo 23 capoverso 2 LPD può essere abrogato, poiché il D-LPD prevede lo stesso sistema di sorveglianza per i privati e gli organi federali.

Art. 37 Pretese e procedura

Rispetto all'articolo 25 LPD, l'articolo 37 D-LPD subisce alcune modifiche illustrate qui appresso.

Cpv. 1 Richieste

Questa disposizione disciplina le richieste che la persona interessata può rivolgere all'organo federale e resta invariata rispetto all'articolo 25 capoverso 1 LPD.

Cpv. 2 Altre richieste

Nella legge vigente il diritto della persona interessata di esigere la cancellazione dei propri dati si evince implicitamente dall'articolo 25 LPD. Per rispettare i requisiti dell'articolo 8 lettera e P-STE 108 e dell'articolo 16 della direttiva (UE) 2016/680, tale diritto è menzionato esplicitamente nell'articolo 37 capoverso 2 lettere a e b. L'articolo 17 del regolamento (UE) 2016/679 prevede anch'esso, a determinate con-

dizioni, il diritto della persona interessata di richiedere la cancellazione dei propri dati («diritto all'oblio»). Lo stesso diritto è previsto dall'articolo 28 D-LPD, al fine di applicare le stesse regole ai titolari del trattamento privati e pubblici (cfr. n. 9.1.6). La situazione giuridica concreta resta tuttavia immutata.

Nel capoverso 2 lettera a, rispetto all'articolo 25 capoverso 3 lettera a LPD è cancellata l'ultima parte del periodo, relativa al divieto della comunicazione a terzi, poiché l'opposizione a tale comunicazione è disciplinata in modo esaustivo dall'articolo 33 D-LPD[174]. A differenza dei diritti di cui all'articolo 37, l'opposizione di cui all'articolo 33 D-LPD non è connessa al trattamento illecito.

Nella lettera b del presente capoverso è tuttavia mantenuta la possibilità della persona interessata di esigere dall'organo federale di pubblicare la decisione sull'opposizione alla comunicazione secondo l'articolo 33. Anche se l'articolo 33 non lo prevede, è ragionevole che la persona interessata lo possa esigere almeno nel caso di una comunicazione illecita.

Cpv. 3 Limitazione del trattamento

Con la limitazione del trattamento, il capoverso 3 prevede un provvedimento meno radicale rispetto alla cancellazione o distruzione dei dati contestati.

Questo disciplinamento corrisponde all'articolo 16 paragrafo 3 della direttiva (UE) 2016/680, secondo cui, anziché cancellare i dati, il titolare del trattamento può limitarne il trattamento quando l'esattezza dei dati personali è contestata dalla persona interessata e l'esattezza o l'inesattezza non può essere accertata o se i dati devono essere conservati a fini probatori.

L'articolo 18 del regolamento (UE) 2016/679 va oltre, poiché prevede che la persona interessata ha il diritto di limitare il trattamento dei dati.

Il P-STE 108 non prevede invece la limitazione del trattamento.

Il capoverso 3 va interpretato in modo tale che i dati possono essere ulteriormente trattati, ma soltanto per determinati scopi. Non si tratta quindi di escludere qualsiasi trattamento di dati. Conformemente alla considerazione 47 della direttiva (UE) 2016/680, la limitazione del trattamento va intesa in modo tale che l'organo federale può trattare i dati in questione soltanto per lo scopo che ne ha impedito la cancellazione. Il capoverso 3 prevede quattro costellazioni.

Secondo il capoverso 3 lettera a, l'organo federale deve limitare il trattamento dei dati personali se la persona interessata ne contesta l'esattezza e non può essere dimostrata né la loro esattezza né l'inesattezza. In tal caso l'organo federale può trattare i dati contestati esclusivamente allo scopo di accertarne l'esattezza o l'inesattezza. Non appena accertata l'esattezza dei dati, l'organo federale può proseguire il trattamento senza limitazioni. Se tuttavia i dati personali si rivelano inesatti, l'organo federale deve cancellarli o distruggerli, sempreché non siano applicabili le lettere b o c.

174 Cfr. Bangert Jan, Kommentar zu Art. 25/25bis DSG, in: Maurer-Lambrou Urs/Blechta Gabor (a c. di), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3a ed., Basilea 2014, N 62 seg.

Secondo il capoverso 3 lettera b, l'organo federale deve limitare il trattamento se lo esigono interessi preponderanti di un terzo, ad esempio se la cancellazione o la distruzione dei dati impedirebbe a un terzo di far valere i propri diritti in giudizio. Ciò significa che i dati possono essere ancora trattati, ma soltanto affinché il terzo possa far valere i propri diritti. È escluso il trattamento per qualsiasi altro scopo.

Secondo il capoverso 3 lettera c, l'organo federale non deve cancellare o distruggere i dati se ciò potrebbe mettere a rischio un interesse preponderante pubblico, segnatamente la sicurezza interna o esterna della Svizzera.

Infine, il capoverso 3 lettera d stabilisce che l'organo federale non deve cancellare o distruggere i dati se ciò rischia di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo. In tal caso l'organo federale può continuare a trattare i dati, ma soltanto per lo scopo che ne ha impedito la cancellazione, ossia per proseguire un'indagine, un'istruzione o un procedimento.

Limitare il trattamento significa contrassegnare i dati contestati in modo tale che il loro futuro trattamento si limiti allo scopo che ne ha impedito la cancellazione o la distruzione. I dati devono essere contrassegnati in modo chiaro. In pratica ciò può significare trasferire temporaneamente i dati in un altro sistema di trattamento o impedire agli utenti l'accesso ai dati. Nei sistemi di trattamento automatico dei dati la limitazione del trattamento dovrebbe essere in linea di massima garantita da mezzi tecnici, affinché i dati non possano essere trattati ulteriormente e modificati per scopi diversi da quelli del capoverso 3.

Cpv. 4 Menzione del carattere contestato

Il capoverso 4 prevede la menzione del carattere contestato dei dati, riprendendo senza modifiche la disposizione dal diritto vigente (art. 25 cpv. 2 LPD). Se non può essere accertata né l'esattezza né l'inesattezza dei dati personali, l'organo federale deve aggiungervi una menzione che ne rilevi il carattere contestato.

Cpv. 5 Fondi di istituzioni pubbliche della memoria collettiva

Secondo il capoverso 5 la rettifica, cancellazione o distruzione di dati personali non può essere chiesta in riferimento ai fondi di biblioteche, istituti d'insegnamento, musei, archivi accessibili al pubblico e altre istituzioni pubbliche della memoria collettiva. Questa eccezione ha una portata limitata poiché molte di queste istituzioni sono rette dal diritto cantonale. La disposizione si riferisce a istituzioni pubbliche la cui attività si concentra soprattutto sulla raccolta, la messa a disposizione, la conservazione e la presentazione al pubblico di documenti di qualsiasi tipo (anche digitali). Una rettifica, cancellazione o distruzione sarebbe contraria a tali scopi specifici di trattamento nella misura in cui concerne gli archivi delle suddette istituzioni. Non è neppure applicabile la menzione del carattere contestato ai sensi del capoverso 4 del presente articolo. Infatti, i documenti di questi fondi intendono rispecchiare il passato, il che è possibile soltanto se essi sono conservati nella loro forma originale e quindi inalterati. Vi è un notevole interesse pubblico a tali fondi, che si evince dalla libertà d'informazione (art. 16 cpv. 3 Cost.).

Il secondo periodo del capoverso 5 permette alle persone interessate di chiedere che tali istituzioni limitino l'accesso ai dati controversi. A tal fine la persona interessata

deve tuttavia rendere credibile un interesse preponderante. Questa limitazione va considerata soprattutto in riferimento alla crescente tendenza a rendere accessibili a chiunque su Internet ampi fondi di istituzioni pubbliche della memoria collettiva. Ciò riduce il tempo necessario per ricerche mirate e nel contempo aumenta la cerchia di persone che ha accesso ai fondi in questione. Per questi casi la legge deve pertanto permettere una ponderazione accurata degli interessi: da una parte, l'interesse del pubblico a un accesso inalterato e illimitato ai documenti e, dall'altra, quello delle persone interessate a non rendere accessibili a tutti informazioni inesatte o che ledono la loro personalità. Come si evince dal primo periodo del capoverso 5, nel caso di archivi o altre istituzioni simili prevale in linea di massima l'interesse pubblico a un accesso libero e inalterato. Un interesse preponderante della persona interessata va invece presunto soltanto se il libero accesso ai dati che la riguardano comporta per lei notevoli svantaggi che potrebbero danneggiarla fortemente anche in futuro (p. es. nella sua carriera professionale). Questi svantaggi vanno inoltre confrontati con il valore archiviale dei dati controversi, risultante ad esempio dalla loro importanza storica oppure dal tipo o dal contenuto dei documenti. Occorre presumere un interesse preponderante della persona interessata in particolare se il valore archiviale dei dati e quindi l'importanza di un accesso illimitato appaiono esigui in relazione ai danni che potrebbero derivarne per la persona interessata. In tal caso quest'ultima può chiedere che l'istituzione limiti l'accesso alle informazioni controverse. Nel caso concreto la limitazione va impostata in modo tale da risultare proporzionata rispetto agli interessi in gioco. Spesso potrebbe bastare che un documento sia disponibile soltanto fisicamente nell'archivio e non più su Internet. In singoli casi si potrebbe rendere accessibile un documento soltanto a persone che ne hanno bisogno per la loro attività di ricerca o giornalistica.

Il capoverso 5 non si applica invece al trattamento di dati delle suddette istituzioni che non è in relazione con i loro fondi ed è effettuato per altri scopi, ad esempio per i conti utente delle biblioteche o i dossier del personale. Per questi trattamenti la persona interessata può far valere tutti i diritti di cui all'articolo 37.

Art. 38 Procedura in caso di comunicazione di documenti ufficiali che contengono dati personali

La disposizione corrisponde all'articolo 25bis LPD e resta invariata.

9.1.8 Incaricato

9.1.8.1 Organizzazione

Art. 39 Nomina e statuto

Cpv. 1 Procedura di nomina

La procedura di nomina dell'Incaricato di cui al capoverso 1 resta invariata, poiché è conforme alla direttiva (UE) 2016/680 e al P-STE 108. Il P-STE 108 non prevede disposizioni sulle modalità per l'elezione o la nomina dell'autorità di sorveglianza. L'articolo 43 della direttiva (UE) 2016/680 obbliga gli Stati Schengen a disciplinare

la procedura di nomina, lasciandoli liberi di scegliere tra la nomina da parte del Parlamento, del Governo, del presidente dello Stato o di un organo indipendente. L'articolo 53 del regolamento (UE) 2016/679 prevede la stessa soluzione per gli Stati membri dell'Unione europea.

Abbiamo esaminato la proposta di vari partecipanti alla consultazione di prevedere l'elezione da parte del Parlamento. Per i motivi esposti qui appresso riteniamo tuttavia che tale modifica non sia opportuna. La procedura attuale offre garanzie sufficienti per l'indipendenza dell'Incaricato nei confronti dell'Esecutivo, poiché l'Assemblea federale può rifiutarsi di approvare la nomina da parte del nostro Consiglio. Non siamo neppure convinti che l'elezione da parte del Parlamento rafforzi l'indipendenza dell'Incaricato, dato che potrebbe essere influenzata da gruppi di interesse. Inoltre, la nomina da parte del nostro Consiglio, su riserva dell'approvazione del Parlamento, permette che l'Incaricato continui a essere aggregato, sotto il profilo amministrativo, alla Cancelleria federale. Ciò non sarebbe invece più possibile in caso di elezione da parte del Parlamento. Se non dovesse più far parte dell'Amministrazione federale, per l'Incaricato potrebbe rivelarsi più difficile assolvere la vigilanza sugli organi federali e indurli a partecipare a un'inchiesta. Se fosse eletto dal Parlamento, l'Incaricato dovrebbe essere indipendente anche sotto il profilo finanziario, alla stregua ad esempio del Controllo federale delle finanze.

Cpv. 3 Statuto

Il primo periodo del capoverso 3 concretizza l'indipendenza dell'Incaricato, precisando che non deve ricevere né sollecitare istruzioni da un'autorità o da un terzo. Tale modifica tiene conto dell'articolo 12bis paragrafo 4 P-STE 108 e dell'articolo 42 paragrafi 1 e 2 della direttiva (UE) 2016/680, che ha lo stesso tenore dell'articolo 52 paragrafi 1 e 2 del regolamento (UE) 2016/679.

Cpv. 2, 4 e 5

Queste disposizioni rimangono invariate rispetto al diritto vigente (art. 26 cpv. 2, 4 e 5 LPD).

L'Incaricato ritiene che, vista la sua funzione di vigilanza, il disciplinamento relativo al suo preventivo andrebbe adeguato a quello previsto per il Controllo federale delle finanze.

Art. 40 Rinnovo e cessazione del mandato

Secondo il diritto vigente, il mandato dell'Incaricato può essere rinnovato un numero indefinito di volte. Questo principio è modificato con il capoverso 1, al fine di attuare i requisiti dell'articolo 44 paragrafo 1 lettera e della direttiva (UE) 2016/680. Secondo quest'ultimo gli Stati Schengen devono disciplinare l'eventuale rinnovabilità e, se del caso, il numero di rinnovi del mandato del membro o dei membri di ciascuna autorità di controllo. Secondo la suddetta disposizione gli Stati Schengen possono quindi scegliere se e quante volte rinnovare il mandato dell'autorità di controllo. L'articolo 54 paragrafo 1 lettera e del regolamento (UE) 2016/679 contiene un disciplinamento analogo.

Conformemente al margine di manovra concesso dall'articolo 44 della direttiva (UE) 2016/680, proponiamo che l'Incaricato possa essere rinominato due volte. Potrà pertanto rimanere in carica al massimo per 12 anni. Con questo disciplinamento intendiamo rafforzare la sua indipendenza. Il timore di non essere rinominato non deve costituire un freno all'adempimento dei suoi compiti legali. Il rapporto di lavoro si estingue automaticamente se durante il suo mandato l'Incaricato raggiunge l'età di cui all'articolo 21 della legge federale del 20 dicembre 1946[175] sull'assicurazione per la vecchiaia e per i superstiti (LAVS; art. 10 cpv. 1 della legge del 24 marzo 2000[176] sul personale federale [LPers] in combinato disposto con l'art. 14 cpv. 1 LPers).

I capoversi 2, 3 e 4 restano sostanzialmente invariati rispetto all'articolo 26*a* LPD.

Art. 41 Attività accessorie

L'articolo 41 rende più severe le condizioni per l'esercizio di un'attività accessoria da parte dell'Incaricato. La disposizione attua l'articolo 42 paragrafo 3 della direttiva (UE) 2016/680, che ha lo stesso tenore dell'articolo 52 paragrafo 3 del regolamento (UE) 2016/679. La disposizione si applica soltanto all'Incaricato, il supplente e la segreteria sottostanno alla LPers.

Mentre l'articolo 26*b* LPD si limita a prescrivere che il Consiglio federale può autorizzare l'Incaricato a esercitare un'altra attività, sempreché questa non pregiudichi la sua indipendenza e la sua reputazione, l'articolo 41 capoverso 1 primo periodo D-LPD sancisce il principio secondo cui l'Incaricato non può esercitare alcuna attività lucrativa supplementare. Il secondo periodo precisa che non può neppure esercitare una funzione al servizio della Confederazione o di un Cantone. Il termine «Cantone» va inteso in senso lato e comprende anche i Comuni, i distretti, i circondari e gli enti di diritto pubblico. Inoltre, il secondo periodo del capoverso 1 dispone che l'Incaricato non può essere membro della direzione, del consiglio di amministrazione, dell'ufficio di vigilanza o di revisione di un'impresa commerciale, a prescindere dal fatto che la sua attività sia remunerata o no.

Il capoverso 2 limita la portata del capoverso 1 e prevede che a determinate condizioni il nostro Consiglio può autorizzare l'Incaricato a esercitare un'attività accessoria. La decisione è pubblicata.

Art. 42 Autocontrollo dell'Incaricato

Questa disposizione obbliga l'Incaricato ad adottare misure di controllo adeguate, in particolare in riferimento alla sicurezza dei dati personali, affinché in seno alla sua autorità sia garantita l'esecuzione conforme delle norme federali sulla protezione dei dati. Nella futura ordinanza, il nostro Consiglio preciserà le misure da adottare.

175 RS **831.10**
176 RS **172.220.1**

9.1.8.2 Inchiesta per violazione delle disposizioni sulla protezione dei dati

Art. 43 Inchiesta

Secondo il diritto vigente la procedura si distingue a seconda che riguardi l'attività di sorveglianza dell'Incaricato nel settore privato o nel settore pubblico. Mentre l'articolo 27 LPD stabilisce che l'Incaricato ha il compito di sorvegliare il trattamento dei dati da parte degli organi federali, secondo l'articolo 29 capoverso 1 lettere a–c LPD egli accerta i fatti nei confronti di un privato quando i metodi di trattamento possono ledere la personalità di un numero considerevole di persone, quando devono essere registrate collezioni di dati in virtù dell'articolo 11*a* LPD o quando sussiste l'obbligo d'informare secondo l'articolo 6 capoverso 3 LPD. Le competenze di sorveglianza dell'Incaricato nei confronti del settore privato non sono attualmente conformi ai requisiti del P-STE 108. Infatti, l'articolo 12bis di tale Convenzione non limita i casi in cui l'autorità di controllo può esercitare i suoi poteri investigativi e d'intervento presso il titolare del trattamento.

Cpv. 1 Apertura dell'inchiesta

Secondo l'articolo 43 capoverso 1 D-LPD l'Incaricato avvia un'inchiesta, d'ufficio o a querela di parte, nei confronti di un organo federale o una persona privata se degli indizi lasciano presumere che un trattamento di dati potrebbe essere contrario alle disposizioni sulla protezione dei dati. La denuncia può essere presentata da un terzo o dalla persona interessata. Entrambi non sono tuttavia parti del procedimento (cfr. art. 47 cpv. 2 D-LPD a contrario). Se è la persona interessata ad aver sporto denuncia, l'Incaricato deve tuttavia informarla sul seguito dato alla denuncia e sull'esito di un'eventuale inchiesta (cpv. 5). La persona interessata deve far valere i suoi diritti con i rimedi giuridici applicabili: può proporre un'azione d'innanzi a un giudice civile se il titolare del trattamento è un privato oppure può impugnare la decisione dell'organo federale responsabile; questo disciplinamento corrisponde al diritto vigente.

Cpv. 2 Rinuncia all'apertura di un'inchiesta

L'Incaricato può rinunciare ad aprire un'inchiesta se la violazione delle disposizioni sulla protezione dei dati è di poca importanza, ad esempio se un'associazione sportiva o culturale invia un messaggio di posta elettronica a tutti i suoi membri senza celare l'identità dei destinatari. Il capoverso 2 può anche essere applicato se l'Incaricato ritiene che è sufficiente fornire consulenza al titolare del trattamento per ovviare a una situazione poco problematica.

Cpv. 3 Obblighi di collaborare

Il capoverso 3 disciplina l'obbligo di collaborare della persona privata e dell'organo federale, riprendendo il disciplinamento previsto dagli articoli 27 capoverso 3 e 29 capoverso 2 LPD. Secondo la disposizione, la parte del procedimento deve fornire all'Incaricato tutte le informazioni e i documenti necessari per l'inchiesta. Il secondo periodo del capoverso 3 stabilisce che il diritto di rifiutare informazioni è retto dagli articoli 16 e 17 PA. L'articolo 16 capoverso 1 PA rinvia all'articolo 42 capoversi 1 e

3 della legge del 4 dicembre 1947[177] di procedura civile federale, secondo cui le persone interrogate possono rifiutarsi di deporre su fatti la cui rivelazione le esporrebbe a procedimento penale. Si tratta delle persone che devono serbare i segreti secondo gli articoli 321bis e 321ter CP. Un medico può ad esempio rifiutarsi di fornire all'Incaricato i dati relativi ai suoi pazienti se questi ultimi non vi acconsentono. Lo stesso vale per gli avvocati e i loro clienti. Anche l'articolo 90 del regolamento (UE) 2016/679 prevede che gli Stati membri possono adottare norme specifiche per stabilire i poteri delle autorità di controllo in relazione ai titolari del trattamento o ai responsabili del trattamento che sono soggetti, ai sensi del diritto degli Stati membri, al segreto professionale o a un obbligo di segretezza equivalente.

Art. 44 Competenze

Questa disposizione soddisfa i requisiti dell'articolo 12bis paragrafo 2 lettera a P-STE 108, secondo cui l'autorità di controllo deve disporre di poteri d'indagine e d'intervento. Anche secondo l'articolo 47 paragrafo 1 della direttiva (UE) 2016/680, gli Stati membri devono disporre per legge che l'autorità di controllo abbia poteri d'indagine effettivi, segnatamente il potere di ottenere dal titolare del trattamento l'accesso a tutti i dati personali oggetto del trattamento e a tutte le informazioni necessarie per l'adempimento dei suoi compiti. L'articolo 58 paragrafo 1 lettere e ed f del regolamento (UE) 2016/679 prevede una norma analoga.

Cpv. 1 Misure investigative

Le misure investigative di cui al capoverso 1 possono essere attuate se è stata aperta un'indagine e se il privato o l'organo federale non ottempera all'obbligo di collaborare. In altre parole, l'Incaricato può ordinare le misure di cui alle lettere a–d soltanto se i tentativi di ottenere la collaborazione del titolare del trattamento sono stati vani.

L'elenco delle misure di cui al capoverso 1 è analogo a quello dell'articolo 12 PA e non è esaustivo. L'Incaricato ha in particolare il diritto di accedere a tutte le informazioni, i documenti, i registri delle attività di trattamento e i dati personali necessari per l'inchiesta (lett. a) o di chiedere l'accesso ai locali o agli impianti (lett. b). Come tutte le autorità federali deve rispettare le norme vigenti, in particolare quelle relative alla protezione dei dati e alla tutela del segreto di fabbricazione e d'affari. Sottostà inoltre al segreto d'ufficio secondo l'articolo 22 LPers. È pertanto garantito il trattamento confidenziale dei dati personali ai quali l'Incaricato ha accesso nell'adempimento del suo compito di sorveglianza, in particolare quando informa la persona che ha sporto denuncia sul risultato di un'eventuale indagine (art. 43 cpv. 4 D-LPD) o quando pubblica il suo rapporto d'attività secondo l'articolo 51 D-LPD.

Cpv. 2 Provvedimenti cautelari

Questa disposizione conferisce all'incaricato la competenza di ordinare provvedimenti cautelari per la durata dell'inchiesta e farli eseguire da un'autorità federale o da organi di polizia cantonali o comunali. Secondo il vigente articolo 33 capoverso 2 LPD, qualora nell'ambito dell'accertamento dei fatti nei confronti di una persona

177 RS **273**

privata o di un organo federale constati che le persone interessate rischiano di subire un pregiudizio non facilmente riparabile, l'Incaricato può chiedere provvedimenti cautelari al presidente della corte del Tribunale amministrativo federale competente in materia di protezione dei dati. Dato che l'articolo 45 D-LPD conferisce poteri decisionali all'Incaricato, per ordinare provvedimenti cautelari non è più necessario l'intervento del Tribunale amministrativo federale e la pertinente disposizione può pertanto essere stralciata. La procedura di ricorso contro i provvedimenti cautelari è retta dagli articoli 44 e seguenti PA. L'effetto sospensivo del ricorso è retto dall'articolo 55 PA.

In considerazione dell'articolo 45 del regolamento (UE) 2016/679, le nuove competenze d'inchiesta dell'Incaricato sono un elemento fondamentale per garantire che la Commissione europea rinnovi o mantenga la decisione di adeguatezza nei confronti della Svizzera.

Art. 45 Provvedimenti amministrativi

L'articolo 45 D-LPD attua l'articolo 47 paragrafo 2 della direttiva (UE) 6016/680 e dà seguito alle raccomandazioni della valutazione Schengen di conferire competenze decisionali all'Incaricato. L'articolo 58 paragrafo 2 del regolamento (UE) 2016/679 elenca tutti i provvedimenti correttivi che l'autorità di controllo deve poter ordinare. Oltre ai provvedimenti previsti dall'articolo 47 paragrafo 2 della direttiva (UE) 2016/680, l'autorità di controllo può in particolare infliggere sanzioni amministrative (art. 58 cpv. 2 lett. i) e ordinare la sospensione dei flussi di dati verso un destinatario in un Paese terzo o verso un'organizzazione internazionale (lett. j).

L'articolo 45 D-LPD è ampiamente conforme all'articolo 12bis paragrafo 2 lettera c P-STE 108.

Tuttavia, proponiamo di non conferire all'Incaricato la competenza di infliggere sanzioni amministrative, bensì di attribuirgli quella di ordinare provvedimenti amministrativi, la cui inosservanza può essere perseguita penalmente (art. 57 D-LPD).

L'articolo 45 D-LPD lascia all'Incaricato un grande margine d'apprezzamento, poiché si tratta di una disposizione potestativa e quindi l'Incaricato non è tenuto ad adottare provvedimenti amministrativi. La disposizione comprende due categorie di provvedimenti.

La prima categoria è costituita da una serie di provvedimenti contro i trattamenti di dati che violano le disposizioni sulla protezione dei dati (cpv. 1, 2 e 4) e vanno da un semplice ammonimento, all'ordine di distruggere i dati (cpv. 1), fino al divieto di comunicare dati all'estero (cpv. 2). Il disciplinamento si basa sul principio di proporzionalità. Invece di ordinare la sospensione del trattamento, l'Incaricato può ad esempio ordinarne la modifica e limitare il provvedimento soltanto alla sua parte problematica. Se durante l'inchiesta la parte coinvolta ha adottato i provvedimenti necessari per ristabilire il rispetto delle disposizioni sulla protezione dei dati, l'Incaricato può limitarsi a pronunciare un ammonimento (cpv. 4).

La seconda categoria di provvedimenti riguarda i casi in cui non sono stati rispettati prescrizioni d'ordine o obblighi nei confronti della persona interessata (cpv. 3). L'Incaricato può in particolare ordinare che il titolare del trattamento proceda a una

valutazione d'impatto sulla protezione dei dati conformemente all'articolo 20 (lett. d) o comunichi alla persona interessata le informazioni di cui all'articolo 23 (lett. g). L'elenco del capoverso 3 non è esaustivo.

L'Incaricato informa della sua decisione soltanto le parti oggetto dell'inchiesta. Se del caso, informa il pubblico conformemente all'articolo 51 capoverso 2 D-LPD. Il provvedimento pronunciato deve essere motivato in maniera sufficiente, poiché il titolare del trattamento deve poter essere in particolare in grado di identificare i trattamenti cui si applica la decisione dell'Incaricato. Le parti oggetto della procedura d'inchiesta possono presentare ricorso conformemente alle disposizioni generali sull'organizzazione giudiziaria federale (cfr. art. 46 D-LPD). Se del caso, l'Incaricato può comminare una pena per l'inosservanza del provvedimento ordinato (art. 57).

Art. 46 Procedura

Secondo il capoverso 1, la procedura d'inchiesta e quella per le decisioni di cui agli articoli 44 e 45 D-LPD sono rette dalla PA. La persona privata o l'organo federale che è parte della procedura d'inchiesta ha il diritto di essere sentito (art. 29 segg. PA).

Il capoverso 2 precisa che hanno qualità di parte soltanto l'organo federale o la persona privata contro cui è stata aperta un'inchiesta. Di conseguenza solo loro possono presentare ricorso contro le decisioni e i provvedimenti dell'Incaricato (art. 42 e 43 D-LPD). La persona interessata non ha qualità di parte, neppure nel caso in cui l'Incaricato ha avviato un'inchiesta su sua denuncia. Se intende far valere le sue pretese nei confronti del titolare privato del trattamento deve agire in giudizio conformemente all'articolo 28 D-LPD, ossia dinanzi al giudice civile competente. Nel settore pubblico, la persona interessata deve agire contro l'organo federale responsabile (art. 37 D-LPD), impugnando la decisione di quest'ultimo dinanzi alla competente autorità di ricorso. La procedura è invariata rispetto al diritto vigente.

Secondo il capoverso 3, l'Incaricato può impugnare le decisioni del Tribunale amministrativo federale relative ai ricorsi, analogamente a quanto previsto dai vigenti articoli 27 capoverso 6 e 29 capoverso 4 LPD.

Art. 47 Coordinamento

Determinate autorità federali sorvegliano privati od organizzazioni esterne all'Amministrazione federale. L'Ufficio federale della sanità pubblica (UFSP), ad esempio, sorveglia le assicurazioni malattia, l'Autorità federale di vigilanza sui mercati finanziari (FINMA) sorveglia le banche o altri fornitori di servizi finanziari. L'espressione «organizzazioni esterne all'Amministrazione federale» corrisponde a quella dell'articolo 1 capoverso 2 lettera e PA.

Nel quadro di una procedura di sorveglianza, che può eventualmente sfociare in una decisione dell'autorità competente, possono sorgere questioni inerenti alla protezione dei dati. Per tenere conto di questo fatto, secondo il capoverso 1 la pertinente autorità di sorveglianza deve invitare l'Incaricato a esprimere il suo parere. Se anche l'Incaricato ha aperto un'inchiesta ai sensi dell'articolo 43 D-LPD contro la medesima parte, questi e l'autorità di sorveglianza devono coordinarsi a due livelli (cpv. 2):

da una parte per accertare se le due procedure possano essere condotte parallelamente o se una delle due debba essere sospesa o abbandonata e, dall'altra, per definire il contenuto delle rispettive decisioni nel caso di una conduzione parallela. In caso di conflitti di competenza decide il nostro Consiglio (art. 9 cpv. 3 PA). Il coordinamento deve essere garantito in modo rapido e semplice. Le unità interessate vanno informate sull'esito del coordinamento e sulla legislazione applicabile, affinché sappiano quanto prima quali siano i loro diritti e doveri.

9.1.8.3 Assistenza amministrativa

Art. 48 Assistenza amministrativa tra autorità svizzere

Questa nuova disposizione disciplina l'assistenza amministrativa tra l'Incaricato, da una parte, e le autorità federali e cantonali, dall'altra. Il vigente articolo 31 capoverso 1 lettera c LPD si limita infatti a conferire all'Incaricato il compito di collaborare con le autorità incaricate della protezione dei dati in Svizzera.

Il capoverso 1 sancisce il principio secondo cui le autorità federali e cantonali devono comunicare all'Incaricato le informazioni e i dati personali necessari all'adempimento dei suoi compiti legali. Si tratta di una norma standard sull'assistenza amministrativa prevista anche da molte altre leggi federali.

Secondo il capoverso 2, l'Incaricato comunica le informazioni e i dati di cui hanno bisogno alle autorità cantonali competenti in materia di protezione dei dati (lett. a), alle autorità penali competenti in caso di denuncia di un reato ai sensi dell'articolo 59 capoverso 2 D-LPD (lett. b) e alle autorità federali nonché alle autorità cantonali e comunali di polizia per l'esecuzione dei provvedimenti di cui agli articoli 44 capoverso 2 e 45 D-LPD (lett. c).

Le comunicazioni di cui ai capoversi 1 e 2 possono essere effettuate spontaneamente o su domanda.

Art. 49 Assistenza amministrativa alle autorità estere

Questa nuova disposizione disciplina l'assistenza amministrativa tra l'Incaricato e le autorità incaricate della protezione dei dati all'estero. Il vigente articolo 31 capoverso 1 lettera c LPD si limita infatti a conferire all'Incaricato il compito di collaborare con le suddette autorità.

La disposizione traspone nel diritto svizzero l'articolo 50 della direttiva (UE) 2016/680 ed è conforme agli articoli 15 e 16 P-STE 108. L'articolo 61 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

L'Incaricato avrebbe auspicato un'integrazione della disposizione che lo autorizzasse a disciplinare in una convenzione le modalità della cooperazione con le autorità estere incaricate della protezione dei dati. Il nostro Consiglio preferisce invece attenersi alla delega della competenza di cui all'articolo 61 D-LPD.

Cpv. 1 Condizioni

Secondo questa disposizione, l'Incaricato può, a determinate condizioni (lett. a–e), scambiare informazioni o dati personali con autorità estere incaricate della protezione dei dati ai fini dell'adempimento dei rispettivi compiti legali in materia di protezione dei dati.

Secondo la prima condizione (lett. a) tra la Svizzera e lo Stato estero deve essere garantita l'assistenza amministrativa nel settore della protezione dei dati. In secondo luogo, conformemente al principio della specialità, le informazioni e i dati personali possono essere utilizzati soltanto nell'ambito della procedura concernente la protezione dei dati personali su cui si fonda la domanda di assistenza amministrativa (lett. b). Se in seguito i dati sono usati in un procedimento penale si applicano i principi dell'assistenza internazionale in materia penale. La terza e la quarta condizione garantiscono la tutela del segreto professionale, d'affari e di fabbricazione (lett. c) e vietano di comunicare a terzi le informazioni e i dati personali senza il consenso dell'autorità mittente (lett. d). Infine, l'autorità destinataria deve impegnarsi a rispettare gli oneri e le limitazioni d'uso richiesti dall'autorità mittente (lett. e).

L'Incaricato può rifiutare la domanda di assistenza se ad esempio non sono rispettate le condizioni di cui all'articolo 13 D-LPD o se uno dei motivi previsti dall'articolo 32 capoverso 6 D-LPD si oppone alla comunicazione dei dati personali.

Cpv. 2 Comunicazione di dati personali

Il capoverso 2 lettere a–g stabilisce le informazioni che l'Incaricato può comunicare all'autorità estera per motivare la sua domanda di assistenza o per dare seguito alla domanda dell'autorità estera. Per comunicare l'identità delle persone interessate l'Incaricato necessita del consenso di ciascuna persona (lett. c n. 1). Al consenso si applicano i requisiti di cui all'articolo 5 capoverso 6 D-LPD. Senza il consenso l'identità può essere comunicata soltanto se è indispensabile per l'adempimento dei compiti legali dell'Incaricato o dell'autorità estera (lett. c n. 2). Queste condizioni corrispondono a quelle previste dall'articolo 32 capoverso 2 lettere a e b D-LPD.

Cpv. 3 Parere

Prima di trasmettere a un'autorità estera informazioni che potrebbero contenere segreti professionali, d'affari o di fabbricazione, l'Incaricato deve informare le persone fisiche o giuridiche titolari del segreto e invitarle a esprimere un parere. È tuttavia esentato da tale obbligo se ciò è impossibile o esige mezzi sproporzionati.

9.1.8.4 Altri compiti dell'Incaricato

Art. 50 Registro

La disposizione prevede che l'Incaricato tiene un registro delle attività di trattamento comunicategli dagli organi federali (art. 11 cpv. 4). Analogamente al diritto vigente, il registro va pubblicato.

Art. 51 Informazione

Il capoverso 1 corrisponde al vigente articolo 30 capoverso 1 LPD, eccetto che l'Incaricato dovrà presentare ogni anno un rapporto d'attività all'Assemblea federale e al nostro Consiglio.

Il capoverso 2 estende l'informazione attiva da parte dell'Incaricato. Quest'ultimo informa il pubblico sui suoi accertamenti e sulle sue decisioni, sempreché l'informazione sia d'interesse generale. Il secondo periodo dell'articolo 30 capoverso 2 LPD è abrogato. In quanto autorità indipendente, l'Incaricato può decidere autonomamente quali informazioni fornire al pubblico. I dati devono essere resi anonimi, salvo se sussiste un interesse pubblico preponderante alla loro pubblicazione (art. 32 cpv. 3 e 5 D-LPD). Si applicano inoltre le condizioni di cui all'articolo 32 capoverso 6 D-LPD.

L'obbligo dell'autorità di controllo di presentare un rapporto d'attività è previsto dall'articolo 49 della direttiva (UE) 2016/680 e dall'articolo 12bis paragrafo 5bis P-STE 108. L'articolo 59 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

Art. 52 Altri compiti

Rispetto al diritto in vigore (art. 31 LPD), l'elenco dei compiti conferiti all'Incaricato è completato al fine di attuare l'articolo 46 paragrafo 1 lettere d ed e della direttiva (UE) 2016/680. Questi nuovi compiti corrispondono anche alle esigenze dell'articolo 12bis numero 2 lett. e P-STE 108.

Secondo il capoverso 1, l'Incaricato ha in particolare il compito di informare, formare e consigliare nel settore della protezione dei dati gli organi federali e i privati. Il compito comprende anche manifestazioni informative o corsi di perfezionamento, soprattutto per i titolari del trattamento nel settore pubblico (lett. a). Un ulteriore compito è sensibilizzare alla protezione dei dati il pubblico e soprattutto le persone bisognose di particolare protezione quali i minori o le persone anziane (lett. c). L'Incaricato deve inoltre informare, su richiesta, le persone interessate in merito all'esercizio dei loro diritti (lett. d).

In virtù della lettera e, l'Incaricato deve essere consultato in merito a tutti i progetti di atti legislativi e di provvedimenti della Confederazione implicanti il trattamento di dati personali e non più soltanto in merito a quelli che tangono in maniera rilevante la protezione dei dati. Tale modifica corrisponde alla prassi attuale.

La lettera g stabilisce che l'Incaricato deve elaborare guide e strumenti per i titolari del trattamento, i responsabili del trattamento e le persone interessate Attualmente egli assolve questo compito nell'ambito della sua attività di consulenza (art. 28, 30 e 31 LPD)[178]. La disposizione precisa inoltre che nel farlo l'Incaricato tiene conto delle specificità di ciascun settore e della tutela delle persone particolarmente bisognose di protezione, quali i minori, le persone diversamente abili o quelle anziane.

178 P. es. la Guida al trattamento dei dati personali nella sfera medica, la Guida al trattamento dei dati personali in senso all'Amministrazione federale o la Guida al trattamento dei dati personali nell'ambito del lavoro.

Il capoverso 2 corrisponde all'articolo 31 capoverso 2 LPD.

Abrogazione dell'articolo 33 LPD

Questa disposizione può essere abrogata. Il capoverso 1, secondo il quale la protezione giuridica è retta dalle disposizioni generali sull'amministrazione della giustizia federale, ha in effetti solo una portata dichiaratoria. Il capoverso 2 è invece superfluo in virtù dell'articolo 44 capoverso 2 D-LPD.

9.1.8.5 Emolumenti

Art. 53

Secondo l'articolo 33 capoverso 1 OLPD, i pareri dell'Incaricato per privati sono sottoposti a emolumento e si applicano le disposizioni dell'ordinanza generale dell'8 settembre 2004[179] sugli emolumenti (OgeEm).

Il capoverso 1 sancisce nella legge il principio secondo cui l'Incaricato deve riscuotere dai privati un emolumento per determinati servizi, quali il parere in merito a un codice di condotta (lett. a), l'approvazione di clausole tipo di protezione dei dati e di norme vincolanti d'impresa (lett. b), la consultazione in seguito a una valutazione d'impatto sulla protezione dei dati (lett. c), i provvedimenti di cui agli articoli 44 capoverso 2 e 45 D-LPD (lett. d) e la consulenza su questioni inerenti alla protezione dei dati (lett. e). Dal capoverso 1 si evince, a contrario, che per un'inchiesta che si conclude senza l'ordine di provvedimenti cautelari o amministrativi non è riscosso un emolumento.

Il capoverso 2 incarica il Consiglio federale di determinare l'importo degli emolumenti. Conformemente all'articolo 46*a* capoverso 1 RVOG può prevedere emolumenti soltanto per i servizi di cui all'articolo 53 capoverso 1 D-LPD. Deve inoltre determinare l'importo della tariffa in modo tale che copra i costi dei servizi forniti (principio della copertura dei costi). Non è quindi previsto di finanziare mediante emolumenti l'intera attività dell'Incaricato, poiché vanno coperti soltanto i costi dei servizi di cui al capoverso 1. A seconda del servizio, il Consiglio federale può stabilire una tariffa forfettaria o una tariffa a ore.

Secondo il capoverso 3 il Consiglio federale può inoltre determinare i casi in cui è possibile rinunciare alla riscossione di un emolumento o ridurlo. È ad esempio possibile rinunciarvi se vi è un interesse pubblico preponderante al servizio e quest'ultimo contribuisce all'osservanza della protezione dei dati. L'articolo 3 capoverso 2 lettera a OgeEm prevede una soluzione simile. L'Incaricato può altresì differire, ridurre o rinunciare all'emolumento se il titolare o il responsabile del trattamento è una persona fisica oppure una piccola o media impresa.

Gli emolumenti sono riscossi soltanto presso le persone private. La consulenza alle autorità cantonali è retta dall'articolo 3 capoverso 1 OgeEm: l'Amministrazione federale non riscuote emolumenti dagli organi intercantonali, dai Cantoni e dai Comuni

179 RS **172.041.1**

per quanto gli stessi concedano il diritto di reciprocità. I servizi per gli organi della Confederazione e dei Cantoni sono forniti gratuitamente.

9.1.9 Disposizioni penali

In seguito alle critiche avanzate dai partecipanti alla consultazione, abbiamo rielaborato in modo radicale le disposizioni penali.

In sede di consultazione è stata chiesta l'introduzione di sanzioni amministrative finanziarie (rinviando al regolamento [UE] 2016/279). In Svizzera, tuttavia, le sanzioni amministrative finanziarie a carattere penale costituiscono un'eccezione. Tradizionalmente sono contemplate nei settori in cui le imprese sottostanno a una sorveglianza di diritto amministrativo perché esercitano un'attività economica per la quale necessitano di una concessione o autorizzazione oppure ricevono sussidi dello Stato (p. es. nel settore postale, o per i giochi in denaro). Erano inoltre state introdotte nel diritto sui cartelli, quando il CP non prevedeva ancora la punibilità delle imprese. Dato che le sanzioni amministrative finanziarie sono di carattere penale, devono essere rispettate determinate garanzie della procedura penale. Tuttavia la procedura amministrativa, che è in linea di massima applicata, non disciplina tali questioni. Nel caso di tali sanzioni, inoltre, una colpa di terzi è imputata direttamente a un'impresa, cosa che il legislatore ha rifiutato introducendo la punibilità dell'impresa secondo l'articolo 102 CP: la responsabilità secondo l'articolo 102 CP non è una responsabilità causale o per rischio[180], bensì la responsabilità per carente organizzazione. Con l'introduzione di sanzioni amministrative finanziarie nella LPD questa decisione di fondo nell'ambito del diritto penale verrebbe fortemente relativizzata per mezzo del diritto amministrativo.

Nel settore della protezione dei dati questo tipo di sanzioni sarebbe inoltre particolarmente arrischiato. Il campo d'applicazione personale della LPD è molto più ampio rispetto a quello delle leggi relative a settori in cui sono tradizionalmente previste sanzioni amministrative finanziarie e in cui l'attività commerciale è esercitata da imprese. Nonostante si rivolga anche a grandi imprese, la LPD contempla anche piccole e medie imprese e persone fisiche. In assenza di un diritto procedurale codificato per le sanzioni amministrative a carattere penale, vi sarebbe anche il rischio di pregiudicare i diritti procedurali delle persone fisiche, soprattutto perché nel diritto penale accessorio vi sono differenze procedurali tra persone giuridiche e persone fisiche[181]. Riassumendo, l'introduzione nella LPD di sanzioni amministrative finanziarie creerebbe una grande incertezza giuridica (non solo nel settore della protezione dei dati), il che non è sostenibile.

Intendiamo pertanto basarci su strutture consolidate che si sono affermate nella prassi. In Svizzera il rispetto di obblighi di diritto amministrativo è garantito dal diritto penale amministrativo e dal diritto penale accessorio. I destinatari di queste norme sono le persone fisiche. Benché l'obbligo di diritto amministrativo incomba

180 Messaggio concernente la modifica del CP (Disposizioni generali), FF **1999** II 1669, n. 217.421 e DTF **142** IV 333.

181 In merito al principio «nemo tenetur» in relazione alle persone giuridiche nel diritto penale accessorio cfr. DTF **142** IV 207, 215 seg., 222 seg. e DTF **140** II 384, 393.

all'impresa, la sua violazione è imputata ai dirigenti (cfr. art. 29 CP e art. 6 DPA[182]). Il timore, espresso in sede di consultazione, che possa essere punito un collaboratore qualsiasi dell'impresa è pertanto infondato. La sanzione con provvedimenti penali significa anche che gli utili realizzati con reati previsti dalla LPD e gli strumenti del reato possono essere confiscati in virtù delle disposizioni del CP (art. 69 segg. CP). Inoltre è previsto che l'Incaricato non può pronunciare sanzioni penali perché altrimenti la sua organizzazione dovrebbe essere radicalmente modificata e ampliata. Per questi motivi proponiamo di mantenere il sistema di perseguimento penale vigente.

Rispetto al diritto vigente, le disposizioni penali della LPD devono essere inasprite. Come chiesto dal P-STE 108 (art. 10) e dalla direttiva (UE) 2016/680 (art. 50) le sanzioni devono essere dissuasive. Pene troppo miti potrebbero portare l'UE a non ritenere più adeguata la normativa svizzera. Gli elementi fondamentali del sistema di sanzioni proposto sono i seguenti:

- si rinuncia a punire la violazione di un obbligo per negligenza, in conformità con le recenti decisioni del Parlamento (p. es. disegno di legge sui giochi in denaro[183]). L'Incaricato avrebbe invece auspicato che fosse punibile anche la negligenza;
- gli obblighi di diritto amministrativo sono stati precisati e la punibilità è stata limitata agli obblighi fondamentali;
- in compenso all'Incaricato è conferita la competenza di ordinare il rispetto degli obblighi previsti dalla LPD con commutazione di una pena in caso di inosservanza. Questo modello è molto diffuso nel diritto penale accessorio (p. es. nella legge del 22 giugno 2007[184] sulla vigilanza dei mercati finanziari [LFINMA]) e corrisponde al meccanismo dell'articolo 292 CP. Se necessario, l'Incaricato può partecipare al procedimento penale cantonale in qualità di parte;
- abbiamo fissato l'importo della multa massima a 250 000 franchi, soprattutto per avvicinare il diritto svizzero al regolamento (UE) 2016/679. Sarebbe tuttavia discutibile aumentare ulteriormente l'importo massimo della multa per le persone fisiche soltanto perché si ritiene che la multa sia troppo bassa per dissuadere le imprese. Le disposizioni penali del D-LPD sono destinate soprattutto alle persone fisiche, in particolare ai dirigenti (cfr. art. 29 CP e art. 6 DPA). Va osservato che ad esempio la LFINMA commina la multa fino a 250 000 franchi per le violazioni di un obbligo per negligenza (art. 44 segg. LFINMA), ma l'inosservanza di una decisione con la multa fino a 100 000 franchi (art. 48 LFINMA). L'Incaricato è invece del parere che le multe non siano abbastanza dissuasive, soprattutto per quanto riguarda l'ammontare;
- come finora, la violazione dell'obbligo di discrezione è considerata una contravvenzione;

182 Cfr. DTF **142** IV 315
183 Cfr. FF **2015** 6989
184 RS **956.1**

– se i dati sono trattati da un'impresa, gli obblighi derivanti dalla LPD incombono ai suoi dirigenti, che sono tenuti per legge a garantire il rispetto degli obblighi in seno all'impresa[185]. Pertanto, conformemente agli articoli 29 CP e 6 DPA, la violazione di un obbligo o l'inosservanza di una decisione dell'Incaricato rivolta all'impresa sono imputate ai dirigenti dell'impresa e non a un semplice collaboratore;
– se la multa non supera 50 000 franchi, in applicazione dell'articolo 7 DPA possono essere multate direttamente le imprese. Teniamo così anche conto delle critiche avanzate in sede di consultazione.

Art. 54 Violazione degli obblighi di informare, di concedere l'accesso e di collaborare

L'articolo 54 D-LPD riprende l'articolo 34 LPD, eccetto l'articolo 34 capoverso 2 lettera a che disciplina obblighi non più previsti dal D-LPD. Per contro la disposizione si riferisce anche al nuovo obbligo di informare in caso di decisione individuale automatizzata (art. 19 D-LPD).

Il capoverso 1 lettera a punisce chi fornisce intenzionalmente informazioni inesatte oppure anche informazioni incomplete dando l'impressione che siano complete. Il rifiuto di fornire un'informazione non è invece punibile secondo la lettera a, bensì secondo la lettera b. Tuttavia, la persona privata che, contrariamente ai fatti, sostiene di non disporre di informazioni sulla persona interessata, è punibile in virtù del capoverso 1 lettera a.

Il capoverso 1 lettera b si applica ai casi in cui una persona privata omette del tutto di informare la persona interessata conformemente agli articoli 17 capoverso 1 e 19 capoverso 1 o di fornirle le informazioni di cui all'articolo 17 capoverso 2. Non è invece punibile la persona privata che appellandosi agli articoli 18 o 25 sostiene di non essere tenuta a informare la persona interessata. In tal caso, infatti, la persona interessata sa che vengono trattati dati che la riguardano. È pertanto in grado di far valere i suoi diritti e avviare un procedimento civile in cui si decide se il rifiuto o la limitazione del diritto d'accesso o dell'obbligo d'informare sia giustificato o meno[186].

Il capoverso 2 riprende l'articolo 34 capoverso 2 lettera b LPD, che punisce chi fornisce intenzionalmente all'Incaricato, durante l'inchiesta, informazioni false o nega intenzionalmente la collaborazione.

La violazione di questi obblighi continua a essere considerata una contravvenzione, ma la multa massima prevista, pari a 250 000 franchi, è notevolmente più elevata rispetto al diritto vigente. L'importo effettivo sarà fissato tenendo conto della situazione economica dell'autore (art. 106 cpv. 3 CP in combinato disposto con l'art. 47 CP). In casi di poco conto può essere punita con la multa l'impresa invece della persona responsabile. Inoltre, conformemente all'articolo 52 CP si può prescindere dal procedimento penale o dalla punizione in casi di lieve entità.

185 DTF **142** IV 315
186 Cfr. anche FF **1988** II 353, in particolare pag. 424.

Art. 55 Violazione degli obblighi di diligenza

Questa disposizione è nuova poiché il D-LPD prevede una serie di obblighi che non sono contemplati dalle disposizioni penali vigenti. È possibile proteggere in modo efficace la personalità e i diritti fondamentali delle persone interessate soltanto se i titolari e i responsabili del trattamento rispettano tutti i loro obblighi. Per indurre questi ultimi a rispettare le disposizioni sulla protezione dei dati, proponiamo questa integrazione delle disposizioni penali.

Per sua natura, la disposizione ha per oggetto innanzitutto le persone con il potere di impartire istruzioni, poiché la competenza decisionale per l'adempimento di questi obblighi è un compito dirigenziale (cfr. anche art. 29 CP).

Art. 56 Violazione dell'obbligo di discrezione

Dall'entrata in vigore della LPD la tecnologia dell'informazione e della comunicazione ha registrato immensi progressi e la sua importanza è notevolmente aumentata. Anche in seguito alla diffusione massiccia degli smartphone, un numero sempre maggiore di dati è memorizzato e trattato da un numero sempre maggiore di persone in un numero sempre maggiore di sistemi. Alla luce di questa situazione appare opportuno estendere la tutela del segreto a tutti i tipi di dati personali. Il fattore determinante è che si tratti di dati segreti. Ciò corrisponde agli articoli 320 e 321 CP, poiché anche in questi casi il criterio determinante è che l'informazione in questione sia segreta. Si applica pertanto la nozione materiale del segreto prevista dal diritto penale[187]. Sussiste un segreto tutelato dal diritto penale se il fatto in questione non è di pubblico dominio, se il detentore del segreto ha un interesse degno di protezione a limitarne la diffusione e anche la relativa volontà. Non rientra quindi nella fattispecie qualsiasi rivelazione di dati personali. Il termine «rivelare» corrisponde a quello degli articoli 320 e 321 CP e istituisce pertanto coerenza per quanto riguarda l'atto in questione[188]

L'articolo 56 D-LPD colma le lacune dovute alla cerchia limitata di autori prevista dagli articoli 320 e 321 CP (reati speciali) e prevede pertanto l'obbligo di discrezione anche per persone non contemplate dagli articoli 320 e 321 CP. La violazione dell'obbligo di discrezione è una contravvenzione (perseguibile a querela di parte) ed è punito con la multa fino a 250 000 franchi.

Il capoverso 2 estenda la punibilità agli ausiliari (trattamento di dati per conto del titolare) e alle persone che svolgono una formazione. L'estensione corrisponde alla LPD vigente e di fatto anche al disciplinamento previsto dall'articolo 321 CP («ausiliari»). Con l'adozione del messaggio concernente la legge sulla sicurezza delle informazioni[189], il nostro Consiglio ha sottoposto al Parlamento una pertinente modifica dell'articolo 320 CP.

187 Stefan/Jean-Richard-dit-Bressel Marc, in: Trechsel/Pieth (a c. di), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurigo/San Gallo 2013, art. 162 CP N 2.

188 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (Hrsg.), (a c. di), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurigo/San Gallo 2013, art. 320 CP N 8 e art. 321 CP N 23 seg.

189 FF **2017** 2563, in particolare pagg. 2613 seg. e 2689 segg.

La rivelazione può essere giustificata dal consenso della persona autorizzata. Si applicano per analogia le regole generali e i principi sviluppati dalla giurisprudenza e dalla dottrina in relazione all'articolo 321 numero 2 CP[190].

Nella prassi possono sorgere questioni di concorrenza in particolare in riferimento agli articoli 320 (agenti della Confederazione) e 321 CP (avvocati, medici, ecc.). Tuttavia questo succede già nel diritto vigente, per cui tale concorrenza non dovrebbe porre problemi degni di nota.

Art. 57 Inosservanza di decisioni

Abbiamo inserito l'articolo 57 dopo la procedura di consultazione. Disposizioni analoghe sono molto diffuse nel diritto penale accessorio della Confederazione. Da una parte, l'articolo compensa l'abrogazione di numerose disposizioni penali previste dall'avamprogetto. D'altro canto, la disposizione tiene conto delle questioni in merito al principio *nulla poena sine lege* sollevate in sede di consultazione. Le stesse questioni sarebbero sorte anche in riferimento a sanzioni amministrative poiché queste ultime hanno carattere penale. La soluzione proposta permette di formulare la pertinente disposizione del D-LPD in una forma generale, senza entrare in conflitto con le esigenze di precisione poste a una disposizione di diritto penale. Inoltre, questa soluzione agevola il lavoro delle competenti autorità di perseguimento penale e tiene quindi conto delle critiche in parte espresse in sede di consultazione.

L'articolo 57 D-LPD permette all'Incaricato di ordinare il rispetto degli obblighi secondo il D-LPD (cfr. art. 45 cpv. 3 D-LPD) comminando una pena in caso di inosservanza. Il vantaggio di questo modello è che nella decisione l'obbligo può essere precisato in modo tale che il destinatario non possa avere dubbi su cosa deve fare od omettere di fare. Ciò agevola anche il compito delle autorità cantonali di perseguimento penale, che, in caso di inosservanza e a querela dell'Incaricato, devono accertare i fatti e pronunciare una sentenza o emanare un decreto d'accusa.

Se la decisione dell'Incaricato riguarda un'impresa, si applica la punibilità del dirigente secondo l'articolo 29 CP: la responsabilità dell'impresa circa l'obbligo alla base dell'inosservanza punibile è addossato alla persona fisica. In questo modo teniamo conto delle critiche espresse in parte in sede di consultazione.

Art. 58 Contravvenzioni commesse nell'azienda

Questa disposizione riprende il disciplinamento previsto dagli articoli 6 e 7 DPA. È necessario un rinvio esplicito perché in linea di massima la DPA non è applicabile nella fattispecie.

L'articolo 6 capoverso 2 DPA consente di applicare la responsabilità del padrone d'azienda anche nell'ambito della LPD. Infatti, nella maggior parte dei casi gli obblighi della LPD sono rivolti al padrone d'azienda[191]. L'articolo 6 capoverso 2 svolge pertanto un ruolo analogo all'articolo 29 CP e addossa la responsabilità penale ai dirigenti dell'impresa ossia alle persone che hanno la competenza di deci-

190 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (Hrsg.), (a c. di), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurigo/San Gallo 2013, art. 321 CP N 28.
191 Cfr. DTF **142** IV 315

dere e di impartire istruzioni. Questo permette di addossare in modo oggettivo la responsabilità penale in un'impresa.

L'importo massimo della multa fino al quale è possibile, secondo l'articolo 7 DPA, punire l'azienda in vece della persona fisica è aumentato a 50 000 franchi. L'adeguamento è necessario poiché nella LPD il limite massimo della multa non è di 10 000 franchi (art. 106 cpv. 1 CP), bensì di 250 000 franchi.

Art. 59 Competenze

Analogamente a quanto previsto dal diritto vigente, il perseguimento e il giudizio dei reati competono ai Cantoni.

L'Incaricato ha il diritto di sporgere denuncia e può partecipare al procedimento cantonale in qualità di accusatore privato (art. 118 segg. CPP). Può quindi impugnare i decreti di abbandono e ricorrere contro le sentenze cantonali, se appare opportuno nell'interesse dell'applicazione uniforme della LPD. Non può invece ricorrere contro i decreti d'accusa e l'entità della pena, il che d'altronde non è necessario in considerazione dei suoi compiti.

Art. 60 Prescrizione dell'azione penale

Secondo l'articolo 109 CP, l'azione penale per le contravvenzioni si prescrive in tre anni. Le inchieste in materia di protezione dei dati richiedono la conoscenza delle pertinenti tecnologie e possono essere onerose. Per evitare che i procedimenti penali nel settore della protezione dei dati siano votati all'insuccesso a causa del termine di prescrizione troppo breve, proponiamo di prolungare tale termine a cinque anni.

9.1.10 Conclusione di trattati internazionali

Art. 61

Questa disposizione sostituisce l'articolo 36 capoverso 5 LPD, troppo vago rispetto ai principi in vigore per la delega di competenze. La presente disposizione precisa che il nostro Consiglio può concludere trattati internazionali con uno o più soggetti di diritto internazionale (Stati, organizzazioni internazionali) in due casi. Secondo la lettera a, può concludere trattati internazionali concernenti la cooperazione internazionale tra le autorità incaricate della protezione dei dati. Si tratta di accordi di cooperazione sul tipo dell'Accordo del 17 maggio 2013[192] tra la Confederazione Svizzera e l'Unione europea concernente la cooperazione in merito all'applicazione dei rispettivi diritti della concorrenza. Secondo la lettera b, il nostro Consiglio può inoltre concludere trattati internazionali sul riconoscimento reciproco della protezione adeguata in caso di comunicazione internazionale di dati.

192 RS **0.251.268.1**. Va osservato che in questo caso la competenza per la conclusione non era stata conferita al nostro Consiglio.

Gli altri capoversi dell'articolo 36 LPD sono abrogati: i capoversi 1 e 4 sono superflui poiché la prassi di prescrivere esplicitamente che il nostro Consiglio debba emanare le disposizioni d'esecuzione è stata abbandonata. Può essere abrogato anche il capoverso 3, secondo cui il nostro Consiglio può prevedere deroghe agli articoli 8 e 9 LPD per quanto concerne le informazioni fornite dalle rappresentanze diplomatiche e consolari svizzere all'estero. Infine, il capoverso 6 è obsoleto, poiché il nostro Consiglio non ha mai fatto uso della sua competenza di disciplinare il modo di porre al sicuro le collezioni i cui dati, in caso di guerra o di crisi, possono mettere in pericolo la vita o l'integrità fisica delle persone interessate.

9.1.11 Disposizioni finali

Abrogazione dell'articolo 37 LPD

In sede di consultazione è emerso che l'articolo 37 LPD è superfluo e deve quindi essere abrogato. Oggi tutti i Cantoni dispongono di disposizioni sulla protezione dei dati che garantiscono una protezione adeguata in conformità con la Convenzione STE 108 e il suo protocollo aggiuntivo.

Art. 62 Abrogazione e modifica di altri atti normativi

L'abrogazione e la modifica di altri atti normativi sono commentate al numero 9.2.

Art. 63 Disposizioni transitorie relative agli obblighi del titolare del trattamento

Secondo il capoverso 1, durante due anni a partire dall'entrata in vigore della nuova LPD, l'obbligo di informare sulla raccolta di dati personali è retto dal diritto anteriore. Durante due anni i titolari privati del trattamento dovranno pertanto informare solo in merito alla raccolta di dati particolarmente degni di protezione (cfr. art. 14 LPD). L'obbligo di informare in caso di profili della personalità, previsto dal diritto vigente, decade, poiché secondo il nuovo diritto questo tipo di dati non esiste più. Gli organi federali dovranno continuare a informare della raccolta di dati personali le persone interessate conformemente al vecchio diritto (cfr. art. 18 LPD), salvo che sia applicabile l'articolo 63 capoverso 2 D-LPD.

Secondo il capoverso 2, durante due anni a partire dall'entrata in vigore della nuova legge, gli articoli 6 e 17–21 si applicano soltanto ai trattamenti di dati ai sensi degli articoli 1 e 2 della direttiva (UE) 2016/680. Per i titolari privati del trattamento e gli organi federali che trattano dati al di fuori del campo d'applicazione della direttiva (UE) 2016/680, questi articoli si applicano soltanto due anni dopo l'entrata in vigore della nuova legge. Questo disciplinamento intende dare ai titolari del trattamento abbastanza tempo per prepararsi all'adempimento dei nuovi obblighi. Nel campo d'applicazione della direttiva (UE) 2016/680, gli articoli sono invece validi sin dall'entrata in vigore della nuova legge.

Art. 64 Disposizioni transitorie relative ai trattamenti

L'articolo 64 prevede varie regole transitorie per i trattamenti.

Cpv. 1

Il capoverso 1 riguarda i trattamenti di dati conclusi al momento dell'entrata in vigore della nuova LPD. Si tratta di trattamenti eseguiti completamente secondo il vecchio diritto e che non continuano dopo l'entrata in vigore di quello nuovo. Questi trattamenti continuano a essere retti dal diritto anteriore. Pertanto i trattamenti conclusi leciti secondo il diritto anteriore non possono diventare illeciti al momento dell'entrata in vigore della nuova LPD. Ciò non vale tuttavia per il diritto d'accesso (art. 23–25 D-LPD); al momento dell'entrata in vigore della nuova LPD esso sarà retto esclusivamente dal nuovo diritto, anche in riferimento a dati e a trattamenti di dati eseguiti secondo il vecchio diritto.

Cpv. 2

Il capoverso 2 riguarda i trattamenti di dati avviati secondo il diritto anteriore e che continuano anche dopo l'entrata in vigore del nuovo diritto, per i quali quest'ultimo ha tuttavia inasprito le condizioni. Si pensi ad esempio al caso in cui secondo il nuovo diritto si è in presenza di una lesione della personalità perché sono state modificate le condizioni del motivo giustificativo. In linea di massima questi trattamenti possono proseguire per due anni senza adeguamenti. In questo lasso di tempo il titolare del trattamento deve provvedere affinché questi trattamenti diventino conformi al nuovo diritto.

Il capoverso due non riguarda gli obblighi di cui agli articoli 6, 20 e 21 D-LPD, che sono contemplati dal capoverso 3.

Cpv. 3

Il capoverso 3 riguarda i trattamenti di dati avviati secondo il diritto anteriore e che continuano anche dopo l'entrata in vigore del nuovo diritto. A questi trattamenti non si applicano gli articoli 6, 20 e 21 D-LPD, a condizione che lo scopo del trattamento resti immutato e non siano raccolti nuovi dati. In questo caso i trattamenti possono proseguire senza soddisfare le condizioni dell'articolo 6. Inoltre, per questi dati non si deve procedere successivamente a una valutazione d'impatto sulla protezione dei dati. Questo disciplinamento è dovuto in particolare al fatto che gli obblighi di cui agli articoli 6, 20 e 21 vanno adempiuti soprattutto prima dell'inizio del trattamento dei dati. Occorre evitare che i titolari del trattamento siano tenuti ad adempiere questi obblighi posteriormente e quindi retroattivamente.

Se non sono soddisfatte le condizioni di cui al capoverso 3, gli obblighi previsti dagli articoli 6, 20 e 21 si applicano anche ai trattamenti avviati secondo il diritto anteriore e che continuano anche dopo l'entrata in vigore del nuovo diritto. Ad eccezione del campo d'applicazione della direttiva (UE) 2016/680), queste disposizioni esplicano tuttavia effetto soltanto due anni dopo l'entrata in vigore della nuova LPD. I titolari del trattamento hanno quindi due anni di tempo per soddisfare questi obblighi.

Cpv. 4

Il capoverso 4 riguarda tutti i trattamenti di dati che non rientrano nei capoversi 1–3. Ne fanno parte in particolare i trattamenti avviati dopo l'entrata in vigore della nuova LPD, ma anche quelli leciti sia secondo il diritto anteriore che secondo quello nuovo. A questi trattamenti il nuovo diritto si applica a partire dall'entrata in vigore delle pertinenti disposizioni.

Art. 65 Disposizione transitoria relativa a procedure in corso

Per garantire la certezza del diritto e il rispetto del principio della buona fede, questa disposizione stabilisce che le inchieste dell'Incaricato in corso al momento dell'entrata in vigore della nuova legge e i ricorsi pendenti contro decisioni di prima istanza emanate prima della sua entrata in vigore sono retti dal vecchio diritto. Ciò riguarda sia le disposizioni materiali sulla protezione dei dati sia le competenze dell'Incaricato e le altre norme procedurali applicabili.

Art. 66 Disposizione transitoria relativa ai dati su persone giuridiche

L'abrogazione della protezione dei dati relativi a persone giuridiche nel D-LPD e la limitazione del termine «dati personali» secondo l'articolo 4 lettera a D-LPD alle informazioni relative a una *persona fisica* identificata o identificabile, ha diverse ripercussioni per il trattamento di dati da parte di organi federali. In particolare, in seguito a queste novità, le basi legali federali che autorizzano gli organi federali a trattare e pubblicare dati personali non saranno in futuro applicabili al trattamento e alla pubblicazione di dati relativi a *persone giuridiche*. In base al principio della legalità sancito dall'articolo 5 capoverso 1 Cost., qualsiasi attività dello Stato – e quindi anche qualsiasi trattamento di dati da parte dello Stato – deve fondarsi su una base legale (cfr. anche gli art. 13 cpv. 2, 27 e 36 Cost.). Per questo motivo il disegno introduce nella LOGA una serie di disposizioni che disciplinano il trattamento di dati relativi a persone giuridiche da parte degli organi federali (cfr. n. 9.2.8). Vanno menzionati in particolare l'articolo 57*r* D-LOGA, che istituisce una base legale generale per il trattamento di dati relativi a persone giuridiche da parte degli organi federali, e l'articolo 57*s* D-LOGA, che – analogamente all'articolo 32 D-LPD riguardante la comunicazione di dati personali – contiene i requisiti delle basi legali per la comunicazione di dati relativi a persone giuridiche. A differenza dell'articolo 57*r* D-LOGA, l'articolo 57*s* D-LOGA non costituisce pertanto una base legale per la comunicazione di dati specifici da parte degli organi federali e quindi anche in futuro la comunicazione di dati relativi a persone giuridiche dovrà fondarsi su una base legale in una legge speciale. L'adeguamento di tutte le basi legali attualmente in vigore (che in seguito agli adeguamenti previsti dal D-LPD saranno nella maggior parte dei casi applicabili soltanto alle persone fisiche) nell'ambito del presente progetto non sarebbe appropriato, poiché allungherebbe notevolmente il disegno di legge e il messaggio. Riteniamo pertanto più opportuno rivedere in modo approfondito le disposizioni sulla protezione dei dati delle leggi speciali dopo il dibattito parlamentare sul presente progetto, verificando se le disposizioni che si riferiscono al trattamento di dati relativi a persone giuridiche da parte di organi federali debbano essere mantenute oppure adeguate o abrogate. Affinché nel frattempo non sorgano

lacune giuridiche, l'articolo 66 D-LPD prevede una disposizione transitoria per gli organi federali, secondo cui le suddette disposizioni federali (in leggi sia in senso formale che in senso materiale) sui dati relativi a persone giuridiche continuano ad applicarsi durante cinque anni a partire dall'entrata in vigore del D-LPD. In particolare per la comunicazione di dati relativi a persone giuridiche, durante questo periodo gli organi federali potranno quindi basarsi sulle basi legali del diritto anteriore.

Solo in alcuni singoli casi, in cui, per motivi pratici e inerenti alla certezza del diritto, appare già ora opportuno, le disposizioni delle leggi speciali sui dati relativi a persone giuridiche sono adeguate nell'ambito del presente disegno. Sono adeguati i seguenti atti normativi:

- LTras (cfr. n. 9.2.7: art. 3 cpv. 2, 9, 11, 12 cpv. 2 e 3, 15 cpv. 2 lett. b);
- LOGA (cfr. n. 9.2.8: art. 57*h*^{bis}, 57*h*^{ter},. 57*i*, 57*j*, 57*k* frase introduttiva,. 57*l* rubrica e frase introduttiva, 57*r*, 57*s* e 57*t*);
- legge federale del 16 dicembre 2005[193] sull'abilitazione e la sorveglianza dei revisori (cfr. n. 9.2.12: art. 15*b*);
- legge del 9 ottobre 1992[194] sulla statistica federale (cfr. n. 9.2.24: art. 5 cpv. 2 lett. a e 4 lett. a, 14 cpv. 1, 14*a* cpv. 1, 15 cpv. 1, 16 cpv. 1 e 19 cpv. 2);
- legge del 17 giugno 2005[195] contro il lavoro nero (cfr. n. 9.2.56: art. 17 rubrica, cpv. 1, 2 e 4, nonché 17*a*);
- legge del 3 ottobre 2003[196] sulla Banca nazionale (cfr. n. 9.2.66: art. 16 cpv. 5 e 49*a*);
- legge federale del 19 marzo 1976[197] su la cooperazione allo sviluppo e l'aiuto umanitario internazionali (cfr. n. 9.2.69: art. 13*a* cpv. 1);
- legge federale del 30 settembre 2016[198] sull'energia (cfr. n. 13.7: art. 56 cpv. 1, 58 rubrica, cpv. 1 e 3 nonché 59 cpv. 1 e 2) e la legge sull'approvvigionamento[199] elettrico da modificare in seguito alla legge federale del 30 settembre sull'energia (cfr. n. 13.7: art. 17*c* cpv. 1 e 27 cpv. 1).

Art. 67 Disposizione transitoria relativa alla certificazione

Secondo l'articolo 12 capoverso 2 D-LPD, il nostro Consiglio emana disposizioni sul riconoscimento delle procedure di certificazione e sull'introduzione di un marchio di qualità inerente alla protezione dei dati. La disposizione è ripresa dal vigente articolo 11 capoverso 2 LPD. Il nostro Consiglio adeguerà soprattutto gli atti normativi vigenti, in particolare l'ordinanza del 28 settembre 2007[200] sulle certificazioni in

193 RS **221.302**
194 RS **431.01**
195 RS **822.41**
196 RS **951.11**
197 RS **974.0**
198 FF **2016** 6921
199 RS **734.7**; cfr. FF **2016** 6921
200 RS **235.13**

materia di protezione dei dati e l'ordinanza del 17 giugno 1996[201] sull'accreditamento e sulla designazione. Visto il carattere tecnico di tali ordinanze e il poco tempo a disposizione per elaborare tutte le disposizioni d'esecuzione, riteniamo ragionevole prevedere un termine transitorio di due anni. Durante tale periodo si applica il diritto anteriore.

9.2 Commento alle modifiche degli altri atti normativi

L'abrogazione e la modifica di altri atti normativi necessarie in seguito al D-LPD sono disciplinate nell'allegato D-LPD.

9.2.1 Abrogazione della legge federale del 19 giugno 1992 sulla protezione dei dati

Essendo il D-LPD una revisione totale, la LPD vigente va abrogata.

9.2.2 Modifica terminologica in determinate leggi federali

In seguito alla soppressione dell'espressione «collezione di dati» nel D-LPD devono essere adeguate anche le leggi settoriali in cui questa ricorre. Inoltre, l'espressione «titolare della collezione di dati» è sostituita con «titolare del trattamento».

Il D-LPD abroga l'espressione «profilo della personalità» e introduce quella di «profilazione». Come indicato nel commento all'articolo 4 lettera f D-LPD, le due nozioni non sono identiche, poiché la profilazione implica una valutazione di determinate caratteristiche personali basata su un trattamento dei dati automatizzato, segnatamente mediante un algoritmo.

L'abrogazione dell'espressione «profilo della personalità» comporta la necessità di adeguare delle disposizioni previste in alcune leggi federali e che autorizzano gli organi federali a trattare profili della personalità.

In una parte di queste leggi federali basta semplicemente sopprimere il riferimento al profilo della personalità, poiché, in effetti, in determinati settori le basi legali che autorizzano gli organi federali ad allestire tali profili non sono mai state applicate. In altre leggi, commentate qui di seguito, l'espressione va sostituita con «profilazione» oppure adeguata, tenendo conto della nuova esigenza prevista all'articolo 30 capoverso 2 lettere b e c D-LPD.

201 RS **946.512**

9.2.3 Legge federale del 16 dicembre 2015[202] sugli stranieri

Art. 101

L'espressione «profilo della personalità» è soppressa. Confronta il commento al numero 9.2.2.

Art. 104 cpv. 4

Il rinvio al D-LPD è aggiornato.

Art. 105 cpv. 1

In virtù di questa disposizione, dati personali possono essere comunicati all'estero a condizione che lo Stato o l'organismo in questione garantisca una protezione dei dati equivalente a quella svizzera. Le condizioni applicabili alle suddette comunicazioni devono essere uniformi nel diritto federale. Occorre dunque prevedere un rinvio all'articolo 13 D-LPD.

Art. 111d cpv. 1 e 2

Questa disposizione disciplina la comunicazione di dati personali nel quadro degli accordi d'associazione a Schengen. Il capoverso 1 disciplina la comunicazione di dati personali alle autorità competenti di uno Stato terzo prevedendo un rinvio agli articoli 13 e 14 D-LPD. Gli adeguamenti delle eccezioni di cui al capoverso 2 tengono conto del nuovo tenore dell'articolo 14 capoverso 1 lettere a, c e d D-LPD.

Art. 111f, secondo periodo

Questa disposizione può essere abrogata poiché l'obbligo del titolare del trattamento di fornire alla persona interessata le informazioni disponibili sull'origine dei dati è previsto all'articolo 23 capoverso 2 lettera e D-LPD.

9.2.4 Legge del 26 giugno 1998[203] sull'asilo

Art. 96 cpv. 1, art. 99a cpv. 2 lett. a, art. 100 cpv. 2 e art. 102 cpv. 1, terzo periodo, e 2

L'espressione «profilo della personalità» è soppressa. Confronta il commento al numero 9.2.2.

Art. 98 cpv. 1

Confronta il commento all'articolo 105 D-LStr al numero 9.2.3.

202 RS **142.20**
203 RS **142.31**

Art. 99 cpv. 6

L'espressione «titolare della collezione di dati» è sostituita con «titolare del trattamento» e il rinvio al D-LPD è aggiornato.

Art. 102c cpv. 1 e 2

Confronta il commento all'articolo 111*d* capoversi 1 e 2 D-LStr (n. 9.2.3).

Art. 102e, secondo periodo

Confronta il commento all'articolo 111*f,* secondo periodo D-LStr (n. 9.2.3).

9.2.5 Legge federale del 20 giugno 2003[204] sul sistema d'informazione per il settore degli stranieri e dell'asilo

Art. 4 cpv. 2

L'espressione «profilo della personalità» è soppressa. Confronta il commento al numero 9.2.2.

Art. 6 e 7 cpv. 2

I rinvii al D-LPD sono stati adeguati.

Art. 15 Comunicazione all'estero

In questa disposizione occorre adeguare i rinvii agli articoli 13 e 14 D-LPD.

Art. 16 Obbligo di vigilanza delle autorità cantonali della protezione dei dati

Questa disposizione va adeguata in quanto l'articolo 37 LDP è abrogato.

9.2.6 Legge federale del 26 giugno 1998[205] sull'archiviazione

Art. 11 cpv. 1

L'espressione «profilo della personalità» è soppressa per le ragioni illustrate al numero 9.2.2. Il termine di protezione di 50 anni è applicato soltanto agli archivi classificati in base a nomi di persona e contenenti dati personali degni di particolare protezione. Per gli altri dati personali, il termine di protezione è di 30 anni.

204 RS **142.51**
205 RS **152.1**

Art. 15, titolo e cpv. 1

La disposizione va adeguata poiché per quanto riguarda il diritto d'informazione la legge sull'archiviazione rinvia completamente alla LPD. L'adeguamento garantisce che il suddetto rinvio comprenda pure le condizioni di cui all'articolo 16 D-LPD.

9.2.7 Legge federale del 17 dicembre 2004[206] sulla trasparenza

Art. 3 cpv. 2

Dato che in futuro la LPD sarà applicabile soltanto ai dati di persone fisiche, per motivi di certezza giuridica è necessario precisare, nel capoverso 2, il rinvio al D-LPD sostituendo «dati» con «dati personali», in sintonia con la terminologia dell'articolo 4 lettera a.

Art. 9 Protezione dei dati personali e dei dati su persone giuridiche

A seguito dell'abrogazione della protezione dei dati delle persone giuridiche nel D-LPD e della limitazione del concetto di dati personali, nell'articolo 4 lettera a D-LPD, alle informazioni relative a una persona fisica identificata o identificabile, per motivi di certezza giuridica è necessario chiarire nell'articolo 9 D-LTras che anche i documenti ufficiali contenenti dati personali di persone giuridiche vanno se possibile resi anonimi prima della consultazione (cpv. 1; cfr. il commento al n. 9.1.11). Per la medesima ragione, nel capoverso 2 occorre precisare il rinvio nel senso che le domande di accesso a documenti non anonimizzati vanno valutate in base all'articolo 32 D-LPD per quanto riguarda i dati personali e in base all'articolo 57*s* LOGA per i dati su persone giuridiche.

Art. 11 Diritto di essere consultati

Secondo l'articolo 11 capoverso 1 LTras, l'autorità consulta la persona interessata se una domanda d'accesso concerne documenti ufficiali che contengono dati personali. In virtù del nuovo campo d'applicazione del D-LPD, l'obbligo dell'autorità di consultare la persona interessata non è più garantito. Pertanto è necessario adeguare l'articolo 11 capoverso 1 LTras affinché il diritto legale di essere sentiti delle persone giuridiche rimanga garantito nel caso in cui l'autorità prenda in considerazione di concedere l'accesso secondo l'articolo 7 capoverso 2 LTras (cfr. anche il commento al n. 9.1.11).

Il nuovo tenore dell'articolo 11 capoverso 1 stabilisce l'obbligo dell'autorità di consultare i terzi interessati se prende in considerazione di accordare l'accesso a un documento ufficiale la cui pubblicazione potrebbe ledere la sfera privata di tali terzi. Il concetto di sfera privata vale anche per persone giuridiche, per cui l'autorità è obbligata a consultarle se l'accesso a un documento ufficiale che intende accordare può ledere la sfera privata di persone giuridiche (p. es. la loro reputazione).

206 RS **152.3**

La limitazione dell'obbligo di consultazione di persone i cui dati personali sono contenuti in un documento ufficiale ai casi in cui il fatto di rendere accessibili i dati potrebbe ledere la sfera privata di queste persone concerne anche le persone fisiche. In tal modo si tiene conto dell'attuale giurisprudenza del Tribunale federale, secondo cui l'autorità può rinunciare a consultare terzi se non vi è manifestamente il rischio che il fatto di rendere accessibili i dati di persone fisiche (o di persone giuridiche) non potrà ledere la sfera privata di queste persone[207].

La modifica dell'articolo 11 capoverso 2 è puramente redazionale.

Art. 12 cpv. 2, secondo periodo, e cpv. 3

L'adeguamento dell'articolo 11 capoverso 1 D-LTras richiede la modifica dell'articolo 12 capoversi 2, secondo periodo, e 3, applicandolo a documenti ufficiali che se resi accessibili potrebbero ledere la sfera privata di terzi.

Art. 15 cpv. 2 lett. b

Per i motivi suesposti è necessario integrare l'articolo 15 capoverso 2 con una lettera b secondo cui l'autorità deve pronunciare una decisione se, diversamente da quanto raccomandato dall'Incaricato, intende accordare l'accesso a un documento ufficiale che se reso accessibile potrebbe ledere la sfera privata di terzi.

Art. 18, frase introduttiva

Il rinvio al D-LPD è stato aggiornato.

9.2.8 Legge del 21 marzo 1997 1997[208] sull'organizzazione del Governo e dell'Amministrazione

Osservazione preliminare in merito agli articoli 57h–57h^{ter}

Situazione di partenza: basi legali dei sistemi di gestione degli affari

L'articolo 57*h* LOGA costituisce la base legale formale per i sistemi GEVER delle singole unità amministrative. In virtù del capoverso 3 il nostro Consiglio ha emanato l'ordinanza GEVER del 30 novembre 2012[209].

Con Acta Nova, il nuovo sistema GEVER dell'Amministrazione federale (programma GENOVA) che viene attualmente sviluppato come standard e introdotto progressivamente nell'Amministrazione federale centrale e in singole unità di quella decentrale (p. es. presso l'Incaricato; entro l'inizio del 2020, le singole unità amministrative avranno accesso ai sistemi GEVER di altre unità amministrative per svolgere processi sovradipartimentali (p. es. consultazioni degli uffici, affari del Consiglio federale). Ciò permette di semplificare i processi e di evitare passaggi da un

207 Cfr. la sentenza del TF 1C_50/2015 del 2 dic. 2015, consid. 6.3.
208 RS **172.010**
209 RS **172.010.441**

sistema all'altro: la documentazione per le consultazioni degli uffici non dovrà ad esempio più essere inviata per mail, ma sarà sufficiente inviare un riferimento all'incarto in questione e le unità amministrative consultate potranno lavorare direttamente su un documento principale. In futuro si punta a svolgere tramite GEVER anche altri processi lavorativi riguardanti numerose unità amministrative (p. es. acquisti, programmi di legislatura, obiettivi del Consiglio federale, rapporti di gestione). La licenza acquisita nel quadro della commessa OMC consente di introdurre e gestire il nuovo sistema GEVER nell'Amministrazione federale sia centrale che decentrale.

Nel quadro di soluzioni di governo elettronico, anche servizi cantonali, comunali e privati (imprese, cittadini) dovranno poter accedere in modo mirato e chiaramente delimitato al nuovo sistema GEVER. È stata pertanto acquisita una licenza che consente tali accessi illimitati senza ulteriori costi.

Necessità di adeguare le basi legali

Nel messaggio del 25 agosto 1999[210] concernente l'istituzione e l'adeguamento di basi legali per il trattamento di dati personali, relativamente all'articolo 57*h* LOGA il nostro Consiglio ha affermato: *«La disposizione proposta non contempla i sistemi di registrazione utilizzati in comune dai diversi organi federali e che contengono dati personali ai quali tali organi hanno accesso. Per questi sistemi è necessario istituire una base legale specifica, segnatamente per disciplinare la comunicazione regolare dei dati personali degni di particolare protezione o dei profili della personalità mediante una procedura di richiamo, conformemente all'articolo 19 capoversi 1 e 3 LPD.»*

Secondo l'articolo 19 capoverso 3, primo periodo LPD, gli organi federali possono permettere l'accesso a dati personali mediante una procedura di richiamo, qualora ciò sia previsto esplicitamente. In virtù del secondo periodo, *dati personali degni di particolare protezione* come pure *profili della personalità* possono essere resi accessibili mediante una procedura di richiamo soltanto qualora lo preveda esplicitamente una legge *in senso formale*. Questa disposizione è abrogata nel quadro della revisione della LPD.

Nell'ambito dei processi generali che concernono numerosi dipartimenti o unità amministrative (procedure di consultazione, affari del Consiglio federale, procedure di pianificazione, progetti d'acquisto), i dati degni di particolare protezione vengono trattati soltanto in rari casi eccezionali (per quanto concerne gli affari del Consiglio federale sono p. es. decisioni su ricorsi, casi di responsabilità dello Stato, decisioni e rapporti su divieti d'attività secondo la legge federale del 21 marzo 1997[211] sulle misure per la salvaguardia della sicurezza interna [LMSI], affari del personale). A ben vedere, secondo il vigente articolo 17 capoverso 1 LPD anche questo trattamento richiede una base legale formale. In futuro, invece, si prevede che sarà sufficiente un'ordinanza se il trattamento è indispensabile per l'adempimento di un compito definito in una legge in senso formale e non comporta rischi particolari per i diritti fondamentali della persona interessata (cfr. art. 30 cpv. 3 D-LPD).

210 FF **1999** 7979, in particolare pag. 7983.
211 RS **120**

Già oggi, l'effettiva base legale per il trattamento di dati personali deve in linea generale risultare dal diritto speciale. Il vigente articolo 57*h* LOGA costituisce unicamente la base legale necessaria in virtù dell'articolo 19 capoverso 3 LPD (da abrogare) per comunicare mediante una procedura di richiamo dati personali degni di particolare protezione.

Dato che l'articolo 57*h* LOGA presenta una stretta correlazione con il diritto generale in materia di protezione dei dati e lo concretizza in un settore importante per il trattamento di dati da parte dell'Amministrazione federale, è opportuno un adeguamento nel quadro della revisione della LPD. Per ragioni di trasparenza, il passaggio fondamentale dal principio dello stoccaggio di dati a un approccio fondato sui processi del trattamento di dati nell'ambito dei sistemi GEVER andrebbe messo in risalto in una base legale opportunamente adeguata.

A seguito dell'abrogazione della protezione dei dati delle persone giuridiche nel D-LPD e della limitazione del concetto di dati personali nell'articolo 4 lettera a D-LPD alle informazioni relative a una persona fisica identificata o identificabile, per motivi di certezza giuridica negli articoli 57*h*^{bis} e 57*h*^{ter} occorre chiarire che queste disposizioni sono applicabili anche ai dati di persone giuridiche (cfr. il commento al n. 9.1.11).

Art. 57h Gestione

Il vigente articolo 57*h* va ripartito su tre disposizioni. Esso comprende sia norme concernenti la tenuta di sistemi di gestione degli affari, sia norme relative al trattamento di dati personali in tali sistemi. Questi due elementi vanno separati e disciplinati in due disposizioni diverse.

Capoverso 1: oggigiorno l'Amministrazione federale centrale non può fare a meno di sistemi elettronici di gestione degli affari (sistemi GEVER; cfr. in particolare art. 1 cpv. 1 dell'ordinanza GEVER del 30 novembre 2012[212] [O GEVER]). I sistemi GEVER servono in particolare per svolgere gli affari in modo conforme al diritto, orientato ai processi e trasparente (art. 1 cpv. 2 O GEVER). Il tenore della presente disposizione va dunque ampliato leggermente rispetto a quello vigente. In questi sistemi non sono trattati unicamente affari nel senso procedurale ma vi sono anche registrati documenti a lungo termine (p. es. in vista della documentazione dell'attività amministrativa conformemente all'art. 22 dell'ordinanza del 25 novembre 1998[213] sull'organizzazione del Governo e dell'Amministrazione [OLOGA] e della successiva archiviazione). Se del caso, questa funzione documentativa dei sistemi GEVER potrà essere ampliata ulteriormente.

212 RS **172.010.441**. L'art. 1 cpv. 1 dell'O GEVER ha il seguente tenore: «In linea di massima i documenti pertinenti a un affare dell'Amministrazione federale sono trattati in sistemi di gestione elettronica degli affari (sistemi GEVER). Sono considerati pertinenti a un affare i documenti necessari per comprovare l'attività amministrativa ai sensi dell'art. 22 dell'ordinanza del 25 nov. 1998 sull'organizzazione del Governo e dell'amministrazione (OLOGA).» Cfr. anche i commenti nel messaggio del CF dell'11 set. 2015 concernente il finanziamento di un prodotto GEVER standardizzato e della sua introduzione nell'Amministrazione federale centrale, FF **2015** 5691.

213 RS **172.010.1**

Anche il sistema EXE-BRC, che serve in particolare allo svolgimento di affari del Consiglio federale, costituisce un sistema di gestione degli affari ai sensi di questa disposizione.

Le suddette unità dell'Amministrazione federale sono in linea di massima uffici. Per via della sua struttura organizzativa il Dipartimento federale degli affari esteri (DFAE) dispone però di un unico sistema GEVER.

Il *capoverso 2* dispone che le unità dell'Amministrazione federale centrale o decentrale responsabili dei pertinenti sistemi GEVER possono concedere un accesso limitato ai propri sistemi di gestione degli affari ad altre autorità federali (p. es. altre unità dell'Amministrazione federale centrale e decentrale, ai Servizi del Parlamento o ai Tribunali federali), nonché a servizi esterni all'Amministrazione federale (p. es. servizi cantonali o conferenze intercantonali). Ciò intende consentire di svolgere in questi sistemi numerosi affari (p. es. consultazioni degli uffici, affari del CF, acquisti o procedure di rendiconto; cfr. più in alto) e semplificare la collaborazione interdipartimentale.

In tal modo, in futuro in tanti casi non sarà più necessario inviare i documenti tramite la posta elettronica e pertanto sarà possibile proteggere meglio da accessi non autorizzati le procedure e le informazioni su cui queste si fondano.

Art. 57h^{bis} Trattamento di dati personali e di dati relativi a persone giuridiche

Sostanzialmente, il *capoverso 1* corrisponde al vigente articolo 57*h* capoverso 1, ultimo periodo LOGA, che descrive gli scopi per i quali dati personali e dati relativi a persone giuridiche possono essere trattati nei sistemi di gestione degli affari. In tal modo si preserva questa concretizzazione, necessaria dal punto di vista della protezione dei dati. Essa si evince dagli articoli 4 capoverso 3 e 17 capoverso 1 LPD (cfr. art. 5 cpv. 3 e 30 cpv. 1 D-LPD). La base legale per il trattamento (in particolare la raccolta e la comunicazione) dei dati personali o dei dati relativi a persone giuridiche deve tuttavia sempre risultare dal diritto speciale. La presente disposizione consente il trattamento da un punto di vista orientato ai processi.

Il rinvio alle basi legali per la comunicazione al *capoverso 2* chiarisce esplicitamente che queste devono risultare dal diritto speciale. In tal caso, i dati possono essere comunicati concedendo l'accesso (pertinentemente delimitato) al sistema GEVER dell'unità amministrativa prevalentemente responsabile.

Il *capoverso 3* corrisponde al vigente articolo 57*h* capoverso 1, secondo periodo LOGA con una lieve modifica redazionale relativa all'eliminazione dell'espressione «profili della personalità» nel quadro della revisione della LPD. A seguito dell'abrogazione della protezione dei dati relativi alle persone giuridiche nel D-LPD occorre qui esplicitare che i sistemi di gestione degli affari possono contenere anche dati su persone giuridiche degni di particolare protezione (ossia dati concernenti perseguimenti e sanzioni di natura amministrativa e penale o segreti professionali, d'affari e di fabbricazione; cfr. art. 57*r* cpv. 2 e il commento al n. 9.1.11).

Il *capoverso 4* è in sé di natura declaratoria: il principio secondo cui l'accesso va limitato risulta direttamente dal principio della proporzionalità (art. 5 cpv. 2 Cost., art. 4 cpv. 2 LPD e art. 5 cpv. 2 D-LPD). Il competente organo federale è responsa-

bile per la limitazione dell'accesso. La pertinente formulazione assoluta del vigente articolo 57*h* capoverso 2, che concede l'accesso «soltanto» ai collaboratori dell'organo federale interessato, è per contro inadeguata. Le possibilità d'accesso fondate sui processi comporteranno regolarmente la possibilità di un accesso «esterno», ad esempio anche a metadati che potrebbero contenere nomi, numeri di telefono e indirizzi di posta elettronica di collaboratori dell'amministrazione.

I futuri sistemi di GEVER prevedono la possibilità di un disciplinamento degli accessi basato sui ruoli nonché una codificazione sistematica dei dati e offrono pertanto opportunità sufficienti per attuare questa disposizione nella prassi. I dettagli andranno disciplinati nell'ordinanza (cfr. i vigenti art. 6 segg O GEVER); eventualmente anche i requisiti di sicurezza che devono soddisfare le persone e le organizzazioni esterne all'Amministrazione federale alle quali è concesso l'accesso al sistema.

*Art. 57h^ter^* Disposizioni d'esecuzione

Sostanzialmente, l'articolo 57*h^ter^* corrisponde al vigente articolo 57*h* capoverso 2 LOGA. La disposizione di delega autorizza pure le unità dell'Amministrazione federale decentrale a prevedere regole speciali concernenti le condizioni che devono soddisfare i sistemi da utilizzare.

Con la licenza federale Acta Nova, di recente acquisizione, la Confederazione può ora fornire il nuovo sistema GEVER anche alle unità decentralizzate dell'Amministrazione federale senza costi di licenza supplementari. A medio e lungo termine occorre dunque garantire che queste unità lavorino con lo standard federale al fine di risparmiare costi e semplificare la collaborazione elettronica tra le diverse unità amministrative.

Art. 57i Rapporto con altre leggi federali

Per motivi di certezza giuridica all'articolo 57*i* occorre chiarire che la riserva di altre leggi federali prevista in questa disposizione è applicabile anche al trattamento di dati su persone giuridiche (cfr. il commento al n. 9.1.11).

Art. 57j Principi

A seguito dell'abrogazione della protezione dei dati relativi a persone giuridiche nel D-LPD e della delimitazione, all'articolo 14 lettera a D-LPD, della definizione di dati personali a informazioni relative a una persona fisica identificata o identificabile, per motivi di certezza giuridica occorre esplicitare anche nell'articolo 57*j* capoversi 1 e 2 che queste disposizioni sono applicabili anche ai dati su persone giuridiche (cfr. il commento al n. 9.1.11). I dati relativi a persone giuridiche degni di particolare protezione ai sensi del capoverso 2 comprendono i perseguimenti e le sanzioni di natura amministrativa e penale nonché i segreti professionali, d'affari e di fabbricazione (cfr. art. 57*r* cpv. 2).

Nel capoverso 2 è inoltre eliminata l'espressione «profili della personalità». Confronta il n. 9.2.2.

Art. 57k, frase introduttiva

La definizione di «dati personali» è integrata con «dati su persone giuridiche». Confronta i commenti precedenti e quelli al n. 9.1.11.

Art. 57l, rubrica, frase introduttiva e lett. b n. 4

La definizione di «dati personali» nella rubrica e nella frase introduttiva è integrata con «dati su persone giuridiche». Confronta il commento precedente e quello al n. 9.1.11.

L'espressione «collezioni di dati» alla lettera b numero 4 è sostituita con «infrastruttura elettronica». Confronta il n. 9.1.11.

Art. 57r Trattamento di dati su persone giuridiche

A seguito dell'abrogazione della protezione dei dati personali delle persone giuridiche, le basi legali previste dal diritto federale che autorizzano gli organi federali a trattare dati personali non si applicano più se tali organi trattano dati concernenti persone giuridiche. L'articolo 5 Cost. esige però che l'attività dello Stato sia retta dalla legge. Inoltre, qualsiasi compito di un organo che potrebbe ledere la sfera privata di una persona giuridica (art. 13 Cost.) o limitare la sua libertà economica (art. 27 Cost.) deve rispettare le esigenze di cui all'articolo 36 Cost. (esigenza di una base legale, esistenza di un interesse pubblico preponderante e rispetto del principio della proporzionalità). Riteniamo di conseguenza necessario creare una base legale generale che autorizzi gli organi federali a trattare dati, anche degni di particolare protezione, concernenti persone giuridiche, a condizione che l'adempimento dei loro compiti lo esiga e che questi ultimi siano descritti in una legge in senso formale (cpv. 1). L'espressione «organi federali» si riferisce alla definizione legale di cui all'articolo 4 lettera h D-LPD, che comprende ad esempio anche le unità amministrative decentralizzate.

Nel capoverso 2 è definita la nozione di dati su persone giuridiche degni di particolare protezione, che comprende dunque i dati relativi a perseguimenti e sanzioni di natura amministrativa o penale (lett. a) e quelli relativi a segreti professionali, d'affari o di fabbricazione (lett. b).

Art. 57s Comunicazione di dati concernenti persone giuridiche

Cpv. 1 Comunicazione di dati su persone giuridiche

Questa disposizione sancisce il principio secondo cui gli organi federali possono comunicare dati concernenti persone giuridiche soltanto se lo prevede una base legale. Quest'ultima può essere un trattato internazionale, una legge in senso formale o un'ordinanza. Questo principio generale corrisponde a quello di cui all'articolo 32 capoverso 1 D-LPD relativo alla comunicazione di dati personali.

Cpv. 2 Esigenza di una base in una legge in senso formale

Questa disposizione prevede che gli organi federali possano comunicare dati su persone giuridiche degni di particolare protezione, ossia dati concernenti perseguimenti

o sanzioni penali e amministrativi oppure segreti professionali, commerciali o di fabbricazione, soltanto se lo prevede una base legale in una legge in senso formale. La comunicazione di tali informazioni può in effetti costituire una restrizione grave dei diritti fondamentali di una persona giuridica ai sensi dell'articolo 36 capoverso 1, secondo periodo Cost. È dunque necessaria una base in una legge in senso formale.

Cpv. 3 Deroghe

Il capoverso 3 prevede una deroga all'esigenza di una base legale ai sensi dei capoversi 1 e 2 se una delle condizioni previste alle lettere a–c è adempiuta. Questa disposizione corrisponde alle eccezioni previste dall'articolo 32 capoverso 2 lettere a, b ed e D-LPD.

I capoversi 4–6 corrispondono a quanto previsto all'articolo 32 capoversi 3, 5 e 6 D-LPD.

Art. 57t Diritti delle persone giuridiche

Invece di introdurre esplicitamente un diritto d'accesso o di rettifica retto prettamente dalla legislazione in materia di protezione dei dati, riteniamo che il diritto procedurale applicabile costituisca una norma sufficiente per garantire i diritti delle persone giuridiche risultanti dall'articolo 13 capoverso 2 Cost. Pertanto, nel quadro di una procedura amministrativa di prima istanza, le persone giuridiche possono esaminare gli atti ai sensi degli articoli 26 e seguenti PA, esercitare il diritto di essere sentite ai sensi degli articoli 29 e seguenti PA e, se del caso, di impugnare la decisione pronunciata dall'autorità competente. Infine, le persone giuridiche possono far valere l'articolo 25*a* PA, secondo cui chiunque abbia un interesse degno di protezione può esigere che l'autorità competente pronunci una decisione impugnabile per atti materiali che si fondano sul diritto pubblico federale e che tangono diritti od obblighi. In tal modo le persone giuridiche ottengono il diritto alla rettifica o alla distruzione dei loro dati.

9.2.9 Legge del 24 marzo 2000[214] sul personale federale

Art. 27 cpv. 2, frase introduttiva e lett. b

L'espressione «profilo della personalità» è soppressa. Confronta il numero 9.2.2.

È d'uopo segnalare che l'articolo 27 è stato modificato nel quadro della revisione del 16 giugno 2017 della legge federale sull'istituto amministratore dei fondi di compensazione AVS, AI e IPG[215]. Le disposizioni di coordinamento (cfr. n. 13.7) dovranno tenere conto del nuovo tenore di questa disposizione e dell'abrogazione dell'espressione «profili della personalità».

214 RS **172.220.1**
215 FF **2017** 3627

Art. 27d cpv. 2, frase introduttiva, e 4, frase introduttiva

L'espressione «profilo della personalità» è soppressa. Confronta il numero 9.2.2.

9.2.10 Legge del 17 giugno 2005[216] sul Tribunale amministrativo federale

Art. 35 lett. b

Questa disposizione può essere abrogata dato che il D-LPD conferisce all'Incaricato la competenza decisionale (art. 44 e 45 D-LPD).

9.2.11 Codice civile[217]

Art. 45a cpv. 3 n. 3

L'articolo 45*a* capoverso 3 numero 3 D-CC[218] incarica il Consiglio federale di disciplinare, con la partecipazione dei Cantoni, la vigilanza sul registro elettronico dello stato civile. Si tratta in particolare di modificare l'articolo 83 dell'ordinanza del 28 aprile 2004[219] sullo stato civile (OSC), ispirandosi ad esempio alla soluzione prevista all'articolo 55 capoverso 1 dell'ordinanza N-SIS dell'8 marzo 2013[220]. Quest'ultima dispone che le autorità cantonali di protezione dei dati e l'Incaricato collaborino attivamente nel quadro delle loro rispettive competenze ed esercitino una vigilanza coordinata sul trattamento dei dati personali. Per quanto riguarda la vigilanza sul registro elettronico dello stato civile, l'Incaricato e le autorità cantonali di protezione dei dati non devono intaccare la competenza del giudice di modificare i dati litigiosi (art. 42 CC).

È d'uopo segnalare che l'articolo 45*a* CC è stato modificato nel quadro della revisione del CC del 16 aprile 2014[221]. Le disposizioni di coordinamento (cfr. n. 13.7) dovranno tenere conto del nuovo tenore di questa disposizione ed effettuare le necessarie modifiche.

216 RS **173.32**
217 RS **210**
218 Cfr. il messaggio concernente la modifica del Codice civile svizzero (Atti dello stato civile e registro fondiario), FF **2014** 3059.
219 RS **211.112.2**
220 RS **362.0**
221 FF **2014** 3095

9.2.12 Legge del 16 dicembre 2005[222] sui revisori

Art. 15b Trattamento di dati personali e di dati su persone giuridiche

Per l'adempimento dei suoi compiti legali, l'Autorità federale di sorveglianza dei revisori (ASR) tratta numerosi dati relativi a persone fisiche e giuridiche, che acquisisce in particolare nel quadro degli obblighi d'informazione e di notificazione (art. 15*a* della legge sui revisori [LSR]), dei suoi controlli (art. 16 LSR) e dell'assistenza amministrativa (art. 22 segg. LSR). Tali dati comprendono dati generali come le informazioni di contatto e d'identificazione di un richiedente o di un titolare nonché dati concreti rilevanti per l'abilitazione e la sorveglianza (p. es. dati relativi alle formazioni e alla carriera professionale, estratti dal casellario giudiziale, dati concernenti procedimenti penali o amministrativi importanti oppure procedimenti di responsabilità civile o amministrativa, informazioni sull'organizzazione e l'esercizio di revisori o sull'esecuzione di servizi di revisione). Per motivi di certezza giuridica l'articolo 15*b* D-LSR esplicita che per l'adempimento dei suoi compiti legali l'ASR può trattare dati personali e dati su persone giuridiche, inclusi quelli degni di particolare protezione. I dati su persone giuridiche degni di particolare protezione comprendono segnatamente i dati relativi ai suddetti procedimenti nonché i segreti professionali, aziendali e di fabbricazione (cfr. il commento al n. 9.2.8).

9.2.13 Legge federale del 24 marzo 2000[223] sul trattamento di dati personali in seno al Dipartimento federale degli affari esteri

Art. Art. 1, secondo periodo

Questa disposizione può essere abrogata poiché superflua.

Art. 2 cpv. 1 e 2, primo periodo

Il capoverso 1 va modificato a seguito dell'abrogazione dell'espressione «collezione di dati». Cionondimeno la base legale che autorizza i servizi competenti del DFAE a trattare dati personali rimane la medesima.

Il capoverso 2 subisce due modifiche: da un lato occorre eliminare l'espressione «collezione di dati», dall'altro l'espressione «profili della personalità» va sostituita con «dati personali al fine di valutare l'idoneità delle persone per le missioni di cui al capoverso 1».

Art. 5 cpv. 1, frase introduttiva e cpv. 3

L'espressione «collezione di dati» è soppressa (cfr. il numero 9.2.2). Nella versione tedesca, l'espressione «administrative und strafrechtliche Massnahmen» è adeguata alla terminologia dell'articolo 4 lettera c n. 5 D-LPD.

222 RS **221.302**
223 RS **235.2**

Art. 6 lett. a

L'espressione «collezione di dati» è soppressa (cfr. il numero 9.2.2).

È d'uopo segnalare che la legge federale del 24 marzo 2000 sul trattamento di dati personali in seno al Dipartimento federale degli affari esteri è attualmente in revisione. La consultazione relativa all'avamprogetto del 28 giugno 2017 si conclude il 20 ottobre 2017. Determinati termini di questa legge dovranno eventualmente essere adeguati alla nuova terminologia della futura LPD.

9.2.14 Legge federale del 19 dicembre 1986[224] contro la concorrenza sleale

Art. 22 cpv. 2, secondo periodo

Il rinvio all'articolo 6 LPD va adeguato alla nuova numerazione del D-LPD (art. 13 e 14).

9.2.15 Codice di procedura civile[225]

Le modifiche del Codice di procedura civile (CPC) proposte sono state in linea di massima ben accolte in sede di consultazione.

Art. 20 lett. d: Foro

L'articolo 20 D-CPC disciplina il foro competente per le azioni civili in materia di protezione dei dati, in particolare le azioni in esecuzione del diritto di consultazione e di cancellazione secondo l'articolo 16 D-LPD, le azioni in esecuzione del diritto d'accesso secondo l'articolo 23 D-LPD e le azioni secondo l'articolo 28 D-LPD.

Esenzione dalle spese processuali

Dalla valutazione della LPD è emerso che le persone interessate sono poco inclini a esercitare i loro diritti e non li fanno valere per vie legali, in particolare nel settore privato[226]. Questa situazione, dovuta al rischio di dover assumere i costi, riduce notevolmente l'efficacia della LPD. Quale conseguenza, nell'ambito della LPD manca inoltre una prassi giudiziaria differenziata che concretizzi le disposizioni e garantisca maggiore certezza giuridica.

Per permettere alle persone interessate di far valere più facilmente in giudizio le loro pretese in materia di protezione dei dati occorre pertanto soprattutto esentare dalle spese processuali i procedimenti di diritto civile secondo la LPD, come è già previsto in altri ambiti (p. es. procedimento secondo la legge federale del 24 marzo 1995

224 RS **241**
225 RS **272**
226 Cfr. pag. 90 seg. e 219 del rapporto finale del 10 mar. 2011 sulla valutazione della legge sulla protezione dei dati («Evaluation des Bundesgesetzes über den Datenschutz», disponibile soltanto in tedesco).

sulla parità dei sessi [LPar] o controversie secondo il diritto del lavoro fino a un valore litigioso di 30 000 franchi o controversie derivanti dalla legge del 17 dicembre 1993[227] sulla partecipazione). In tal modo si riduce notevolmente il rischio economico per le persone interessate. Dato che la maggior parte delle pretese in materia di protezione dei dati non costituiscono controversie secondo il diritto patrimoniale, non è opportuno introdurre un valore litigioso come nel diritto del lavoro. In considerazione del numero di casi finora trattati è però improbabile che la modifica faccia aumentare repentinamente il numero di casi portati in giudizio o la disponibilità in tal senso. Tanto più che, se soccombe, la persona interessata è sempre tenuta a versare le spese ripetibili e ad assumersi i propri costi processuali. Inoltre, in caso di malafede o temerarietà processuali, le spese processuali possono essere addossate a una parte anche nelle procedure gratuite (art. 115 CPC).

Art. 99 cpv. 3 lett. d

Per le procedure secondo la LPD, il disegno propone di eliminare l'obbligo – di cui all'articolo 99 capoverso 1 CPC – dell'attore di prestare cauzione per le spese ripetibili su richiesta del convenuto. In tal modo si intende ridurre ulteriormente l'onere finanziario per l'attore.

Ciò riguarda procedure ordinarie concernenti azioni di diritto civile secondo l'articolo 28 D-LPD. La modifica proposta agevola in particolare l'avvio di questo tipo di azioni, finora praticamente mai promosse. Se alle procedure secondo l'articolo 243 capoverso 2 lettera d CPC è applicata la procedura semplificata, anche il diritto vigente e immodificato esenta tali procedure dall'obbligo di prestare cauzione per le spese ripetibili (cfr. art. 99 cpv. 3 CPC).

Art. 113 cpv. 2 lett. g

Il CPC va completato affinché con la modifica non vengano assegnate spese processuali neanche nelle procedure di conciliazione condotte in virtù della LPD, obbligatorie nella procedura ordinaria così come in quella semplificata (art. 197 CPC). Ciò è previsto dal diritto vigente per determinate controversie come ad esempio quelle in materia di locazione e affitto di abitazioni e di locali commerciali o quelle secondo la legge sulla partecipazione (cfr. art. 113 cpv. 2 CPC).

L'esenzione dalle spese processuali riduce il rischio che in caso di promovimento di un'azione la persona interessata si veda addossare le spese in tutte le azioni di diritto civile secondo la LPD. Tanto più che nella procedura di conciliazione non sono in linea di massima assegnate spese ripetibili (art. 113 cpv. 1, primo periodo CPC). Vanno in linea di principio assunte personalmente le spese per la propria rappresentanza legale, a meno che non sia stato chiesto il gratuito patrocinio.

Art. 114 lett. f

Il CPC va completato affinché nelle procedure decisionali condotte in virtù della LPD non vengano assegnate spese processuali, come è già il caso ad esempio nelle con-

[227] RS **822.14**

troversie secondo la legge sulla parità dei sessi o la legge sulla partecipazione oppure in quelle secondo il diritto del lavoro fino a un valore litigioso di 30 000 franchi.

Grazie a questo nuovo disciplinamento, le procedure decisionali sono esentate dalla spese processuali e quindi si riduce il rischio economico per la persona interessata. Le spese ripetibili sono invece assegnate conformemente ai principi usuali (art. 104 segg. CPC).

Art. 243 cpv. 2 lett. d: Procedura applicabile

Analogamente al diritto d'accesso, i diritti secondo l'articolo 16 D-LPD possono essere fatti valere con procedura semplificata. Questa modifica è necessaria in quanto l'articolo 16 D-LPD è nuovo.

Art. 407d: Disposizione transitoria

Per quanto riguarda il diritto transitorio, una volta entrate in vigore, le nuove disposizioni procedurali saranno applicabili a tutte le procedure, anche a quelle pendenti. In particolare, anche per queste procedure non dovranno più essere fornite garanzie e non saranno più addossate spese processuali (art. 113 cpv. 2 lett. g e art. 114 lett. f D-CPC).

9.2.16 Legge federale del 18 dicembre 1987[228] sul diritto internazionale privato

Art. 130 cpv. 3

Come precedentemente illustrato (cfr. n. 9.2.2), l'evoluzione tecnica ha reso obsoleta la nozione di collezione di dati, peraltro quasi mai utilizzata negli ordinamenti giuridici di altri Stati. Anche il D-LPD si riferisce ora esclusivamente al trattamento di dati. È pertanto opportuno adeguare l'articolo 130 capoverso 3 della legge federale sul diritto internazionale privato (LDIP) laddove menziona il «luogo nel quale la collezione di dati è gestita o utilizzata».

L'articolo 130 D-LDIP continua a disporre che per le azioni intese a dare esecuzione al diritto d'informazione o d'accesso in relazione al trattamento di dati personali sono competenti i tribunali menzionati nell'articolo 129 LDIP. In Svizzera la persona interessata può pertanto intentare la causa a scelta in uno dei seguenti luoghi: nel domicilio o, in mancanza di questo, nella dimora abituale del titolare del trattamento, nel luogo della sede commerciale della stessa, nonché nel luogo dell'atto o nel luogo dell'evento. L'atto illecito ai sensi dell'articolo 129 LDIP consiste principalmente nel rifiuto di accordare un diritto d'informazione o d'accesso. Il luogo dell'atto è dunque il luogo dal quale avrebbe dovuto essere concesso il diritto d'informazione o d'accesso[229], di regola il luogo in cui il titolare del trattamento dei dati esercita l'atti-

228 RS **291**

229 Cfr. DTF **113** II 476 consid. 3 e DTF **125** III 346 consid. 4c/bb sul luogo dell'atto in caso di inadempimenti.

vità nel cui quadro ha luogo il trattamento di dati in questione. Il luogo dell'evento è il luogo in cui la persona interessata avrebbe dovuto ottenere il diritto d'informazione o d'accesso, di regola la sua dimora abituale[230].

Il presente disegno non menziona più la possibilità alternativa d'azione nel «luogo nel quale sono trattati i dati personali» contemplata dall'avamprogetto (il passaggio in questione intendeva sostituire la vigente alternativa di intentare un'azione «nel luogo nel quale la collezione di dati è gestita o utilizzata»). È presumibile che anche un diritto d'informazione o d'accesso fondato su un diritto straniero è principalmente diretto contro il titolare del trattamento dei dati (cfr. p. es. art. 15 del Regolamento [UE] 2016/679). In questo contesto, il luogo del trattamento dei dati va considerato il luogo in cui il titolare esercita l'attività nel cui quadro ha luogo il trattamento di dati in questione[231]. Tale luogo corrisponde al luogo dell'atto già menzionato nell'articolo 129 capoverso 1 LDIP (cfr. il paragrafo precedente). Di norma dovrebbe essere pure equiparabile a quello in cui ha sede commerciale la persona che tratta i dati[232], parimenti menzionato nell'articolo 129 capoverso 1 LDIP. Per alcuni autori, il tribunale competente nel luogo del trattamento dei dati risulta direttamente dal luogo dell'evento di cui all'articolo 129 capoverso 1 LDIP[233]. In questo contesto il passaggio ora abrogato non avrebbe prodotto alcun plusvalore ma unicamente confusione.

Alcuni partecipanti alla consultazione hanno chiesto l'introduzione di una frase a complemento dell'articolo 139 capoverso 3 LDIP. La disposizione vigente prevede che l'articolo 139 capoverso 1 LDIP, che disciplina il diritto applicabile alle lesioni della personalità, sia applicabile anche alle «pretese per lesione della personalità risultante da un trattamento di dati personali come pure per pregiudizio arrecato al diritto d'accesso ai dati personali». La frase completiva proposta avrebbe ad esempio il seguente tenore: «un luogo all'estero in cui si svolge il trattamento di dati ai sensi del capoverso 1 lettera c non può essere fatto valere solo perché i dati sono registrati nel Paese straniero in questione». Rinunciamo a una simile modifica ritenendola inutile. Il luogo dell'evento ai sensi del suddetto articolo 139 capoverso 1 lettera c va infatti determinato in relazione alla lesione fatta valere. Il luogo della mera registrazione dei dati entra pertanto in considerazione quale luogo dell'evento soltanto in casi specifici, ad esempio se si fa valere che le modalità di registrazione violano le disposizioni in materia di protezione dei dati[234]. In quest'ottica, un luogo

230 Cfr. Rosenthal David, in: Rosenthal David/Jöhri Yvonne (ed.), Handkommentar zum Datenschutzgesetz, Zurigo 2008, Art. 139 IPRG N 24; alle medesime conclusioni giungono Vischer Frank, in: ZK-IPRG, 2. A., Zurigo 2004, Art. 139 IPRG N 28; Umbricht Robert/Rodriguez Rodrigo/Krüsi Melanie, in: Honsell Heinrich/ Vogt Nedim Peter, Schnyder Anton K./Berti Stephen V. (ed.), BSK-IPRG, 3. A., Basilea 2013, Art. 130 IPRG N 11, e Bonomi Andrea, in: Bucher Andreas (ed.), CR-LDIP/CL, Art. 139 IPRG N 16; nel presente caso è pure possibile un collegamento con il domicilio usuale della persona interessata, come in Dasser Felix, in: BSK-IPRG, op. cit., Art. 139 IPRG N 43

231 Cfr. Dasser, in: BSK-IPRG, op. cit., Art. 139 IPRG N 45.

232 Rapporto del Consiglio federale dell'11 dic. 2015 sulla responsabilità civile dei provider, pag. 90 segg. (disponibile in tedesco e francese; il rinvio è alla versione tedesca).

233 Cfr. Bucher Andreas, Le premier amendement de la LDIP, in: Etudes de droit international en l'honneur de Pierre Lalive, Basilea 1993, pag. 8

234 Cfr. Rosenthal, Handkommentar zum Datenschutzgesetz, op. cit., Art. 139 IPRG N 22.

dell'evento ai sensi del capoverso 1 non può mai essere fondato unicamente sul fatto che i dati sono registrati nello Stato in questione. In considerazione di quanto precede, è assai poco probabile che il diritto del mero luogo di registrazione sia applicato nel caso di azioni in esecuzione di un diritto d'informazione o d'accesso.

9.2.17 Codice penale[235]

Art. 179novies Sottrazione di dati personali

Questa disposizione non sarà più applicata ai dati di persone giuridiche, che non saranno più soggette alla LPD. La disposizione transitoria dell'articolo 66 D-LPD non è applicabile. I riferimenti ai profili della personalità e alla collezione di dati vanno d'altra parte eliminati in conseguenza della loro soppressione nel D-LPD. Nella disposizione l'espressione «non liberamente accessibili» è inoltre sostituita con «non […] accessibili a chiunque».

Art. 179decies Usurpazione d'identità

La mozione Comte (14.3288), accolta dal Parlamento, incarica il nostro Consiglio di presentare una modifica del diritto penale che renda l'usurpazione d'identità, che costituisce una grave violazione della personalità, un reato a sé stante.

L'identità di una persona è definibile mediante diverse caratteristiche costitutive quali il nome, la provenienza, la sua immagine, la posizione sociale, familiare o professionale, nonché altri dati personali come la data di nascita, l'indirizzo Internet, il numero del conto o i cosiddetti *nickname*.

La proposta disposizione penale contro l'usurpazione d'identità protegge la personalità dell'individuo. Il diritto al rispetto e alla stima della propria identità deve essere protetto penalmente rendendo perseguibile l'usurpazione dell'identità in quanto parte della personalità. Dal punto di vista sistematico, la disposizione va collocata sotto il titolo dei delitti contro l'onore e la sfera personale riservata[236]. Intendiamo però rinunciare a sanzionare l'usurpazione dell'identità altrui fine a sé stessa o l'utilizzo di un'identità fittizia, poiché estenderebbe eccessivamente i limiti del diritto penale. L'autore deve invece agire con l'intenzione di causare un danno o di ottenere un vantaggio.

Il fenomeno e la problematica dell'usurpazione dell'identità altrui si sono accentuati e acuiti in seguito al diffuso utilizzo dei media elettronici e dei corrispondenti mezzi di comunicazione. Nella prassi la soglia che bisogna superare per esprimersi sui media sociali o agire tramite i mezzi di comunicazione elettronici utilizzando un nome altrui si è sensibilmente ridotta rispetto alle vie di comunicazione tradizionali. La disposizione penale proposta va tuttavia applicata indipendentemente dai mezzi impiegati per commettere il reato. Rientra dunque nel suo campo d'applicazione anche l'usurpazione tradizionale d'identità, ad esempio un'ordinazione scritta di

235 RS **311.0**
236 Art. 173 segg. CP

merci o una presa di contatto personale e orale per preparare la cosiddetta truffa del falso nipote. La disposizione non si applica dunque unicamente agli usurpatori che utilizzano un computer o un telefono.

Il danno per la vittima dell'usurpazione d'identità sancito nella disposizione penale deve raggiungere una certa gravità e può essere di natura materiale o immateriale. La forte rabbia che l'autore intende provocare nella persona interessata può già costituire un danno sufficiente[237].

Nel caso dell'usurpazione dell'identità altrui con l'intenzione di arrecare un danno o procacciarsi un vantaggio illecito, di norma si pone la questione dell'applicazione di ulteriori disposizioni relative ad altre fattispecie penali come la frode, la falsità in documenti o i reati contro l'onore. Nei casi in cui il carattere illecito dell'atto non è completamente coperto dall'altra fattispecie applicabile, per cui non è ancora considerato l'aspetto della lesione della personalità causata dall'usurpazione dell'identità, occorre presumere il concorso ideale di reati. Sono quindi applicabili entrambe le disposizioni penali. Se per esempio in una rete sociale A assume l'identità di B e diffama C, va applicata, oltre alla fattispecie della diffamazione, anche la nuova fattispecie dell'usurpazione d'identità. Solo in questo modo è possibile punire l'atto illecito commesso nei confronti di B e considerare le ripercussioni negative per B, come la perdita di reputazione, l'avvio di un procedimento o una rettifica dispendiosa e solo parzialmente efficace. Anche nel caso della sottrazione di dati personali[238] e della susseguente usurpazione dell'identità, sono applicate entrambe le disposizioni penali. Se l'usurpazione d'identità fa parte di una truffa volta a procacciarsi un vantaggio illecito, la fattispecie della truffa può anche comprendere la fattispecie dell'usurpazione d'identità (di norma precedente), che viene dunque pure punita.

La pena comminata deve essere appropriata al valore del bene giuridico protetto e all'illiceità dell'atto, poiché altrimenti il diritto penale perde credibilità ed efficacia preventiva. Il pericolo risultante dal fenomeno dell'usurpazione d'identità non va sottovalutato o minimizzato, in particolare nell'era digitale, anche se l'illiceità concreta dell'atto e le ripercussioni per la persona danneggiata non sono sempre gravi. Di conseguenza, la nuova fattispecie penale è considerata un delitto e punita con una pena detentiva fino a un anno o con una pena pecuniaria.

Conformemente all'articolo 14 CP sono fatti salvi e non sono quindi punibili gli atti permessi dalla legge e dunque leciti, ad esempio nel quadro di indagini di polizia e penali.

Art. 352 cpv. 2

Il titolo del D-LPD non deve più essere citato integralmente in quanto all'articolo 349*a* è stata introdotta l'abbreviazione (cfr. modifica del CP alla cifra II).

237 Per un elemento costitutivo d'infrazione identica nel quadro di un abuso d'autorità cfr. Heimgartner Stefan, in: Niggli/Wiprächtiger (ed.), Basler Kommentar, Strafrecht II, 3ª edizione, Basilea 2013, ad art. 312 CP n° 23.

238 Art. 179^{novies} CP

Art. 355a cpv. 1

L'espressione «profilo della personalità» è soppressa (cfr. il commento al n. 9.2.2).

Art. 365 cpv. 1

L'espressione «profilo della personalità» è soppressa (cfr. il commento al n. 9.2.2).

9.2.18 Legge federale del 22 marzo 1974[239] sul diritto penale amministrativo (DPA)

La DPA è applicata nei casi in cui il procedimento e il giudizio per un'infrazione punita dalla legislazione amministrativa federale sono demandati a un'autorità amministrativa della Confederazione (art. 1 e 2). Il nuovo tenore dell'articolo 2 capoverso 3 D-LPD richiede la modifica delle disposizioni speciali di protezione dei dati nella DPA. A tal fine è ripreso il disciplinamento previsto nel CPP, tenendo conto delle modifiche apportate dal presente progetto.

Art. 18a Raccolta di dati personali

Questa disposizione disciplina la trasparenza della raccolta di dati personali. Corrisponde alla regolamentazione prevista dall'articolo 95 CPP.

Art. 18b Trattamento di dati personali

Confronta per analogia il commento all'articolo 95*a* D-CPP (n. 9.3.2).

Art. 18c Comunicazione e utilizzazione di dati personali in procedimenti penali pendenti

Questa disposizione disciplina la comunicazione e l'utilizzazione di dati in procedimenti pendenti e corrisponde alla regolamentazione prevista all'articolo 96 CPP.

Art. 18d Diritti d'informazione durante la pendenza del procedimento

Questa disposizione disciplina i diritti d'informazione in procedimenti pendenti. Corrisponde alla regolamentazione prevista all'articolo 97 CPP.

Art. 18e Esattezza dei dati personali

Questa disposizione disciplina il requisito dell'esattezza dei dati. Corrisponde alla regolamentazione prevista all'articolo 98 CPP. Per quanto concerne il capoverso 2 si rinvia al commento all'articolo 98 capoverso 2 D-CPP (n. 9.3.2).

239 RS **313.0**

9.2.19 Procedura penale militare del 23 marzo 1979[240]

La giustizia militare è un'autorità giudiziaria indipendente (art. 1 della procedura penale militare [PPM]) e può essere assimilata alla nozione di «tribunale» ai sensi dell'articolo 2 capoverso 3 D-LPD. Diversamente dal CPP, la PPM non prevede però alcuna disposizione a sé stante sulla protezione dei dati. Riteniamo pertanto opportuno adeguare la legge riprendendo in buona parte il disciplinamento previsto nel CPP e tenendo conto delle modifiche apportate dal presente progetto.

Art. 25a Raccolta di dati personali

Questa disposizione disciplina la trasparenza della raccolta di dati personali. Corrisponde alla regolamentazione prevista all'articolo 95 CPP.

Art. 25b Trattamento di dati personali

Confronta per analogia il commento all'articolo 95*a* D-CPP (n. 9.3.2).

Art. 25c Comunicazione e utilizzazione di dati personali in procedimenti pendenti

Questa disposizione disciplina la comunicazione e l'utilizzazione di dati personali nel quadro di un procedimento pendente e corrisponde all'articolo 96 CPP.

Art. 25d Diritti d'informazione durante la pendenza del procedimento

Questa disposizione disciplina il diritto d'accesso nel quadro di un procedimento pendente. Corrisponde all'articolo 97 CPP.

Art. 25e Esattezza dei dati personali

Questa disposizione disciplina il requisito dell'esattezza dei dati e corrisponde all'articolo 98 CPP. Per quanto concerne il capoverso 2 si rinvia al commento all'articolo 98 capoverso 2 D-CPP.

9.2.20 Legge federale del 13 giugno 2008[241] sui sistemi d'informazione di polizia della Confederazione

Art. 3 cpv. 2, primo periodo

L'espressione «profili della personalità» è soppressa (cfr.n. 9.2.2.

240 RS **322.1**
241 RS **361**

Art. 5, rubrica, e cpv. 2

Riteniamo che il capoverso 2 possa essere abrogato. L'affidamento del trattamento a un responsabile, anche se finalizzato al controllo e alla manutenzione informatica, è retto esclusivamente dall'articolo 8 D-LPD. Pertanto occorre adeguare anche la rubrica.

Art. 7 cpv. 1

Il rinvio al D-LPD è stato aggiornato.

9.2.21 Legge del 4 ottobre 1991[242] sui PF

Art. 36a cpv. 1, primo periodo, e art. 36b cpv. 1 e 5, secondo periodo, e art. 36c cpv. 2

L'espressione «profilo della personalità» è soppressa (cfr.n. 9.2.2.

All'articolo 36*c* capoverso 2 è inoltre aggiornato il rinvio al D-LPD.

9.2.22 Legge del 17 giugno 2011[243] sulla promozione dello sport

Art. 21 cpv. 3, frase introduttiva

L'espressione «profilo della personalità» è soppressa (cfr. n. 9.2.2).

Art. 25 cpv. 1, frase introduttiva e cpv. 4

L'espressione «profilo della personalità» è soppressa (cfr. n. 9.2.2). Il capoverso 4 disciplina la comunicazione di dati personali alle autorità competenti di uno Stato terzo prevedendo un rinvio agli articoli 13 e 14 D-LPD.

9.2.23 Legge federale del 19 giugno 2015[244] sui sistemi d'informazione della Confederazione nel campo dello sport

Art. 1 cpv. 1, frase introduttiva

L'espressione «profilo della personalità» è soppressa (cfr. n. 9.2.2).

242 RS **414.110**
243 RS **415.0**
244 RS **415.1**

Art. 4

Questa disposizione disciplina il trattamento di dati per lavori ai sistemi d'informazione e può essere abrogata. L'affidamento a terzi di un trattamento di dati, anche a scopi di controllo e manutenzione informatica, è disciplinato esclusivamente dall'articolo 8 D-LPD.

Art. 9, frase introduttiva, art. 14, frase introduttiva, art. 18, frase introduttiva, art. 22, frase introduttiva, art. 26, frase introduttiva, art. 32, frase introduttiva

L'espressione «profilo della personalità» è soppressa (cfr. n. 9.2.2).

9.2.24 Legge federale del 9 ottobre 1992[245] sulla statistica federale

A seguito dell'abrogazione della protezione dei dati personali di persone giuridiche, per motivi di certezza giuridica occorre modificare alcune disposizioni della legge sulla statistica federale (cfr. il commento al n. 9.1.11). Riteniamo che nel settore della statistica debba essere garantita la medesima protezione dei dati per le persone fisiche e quelle giuridiche. Alcuni termini sono inoltre adeguati alla nuova terminologia della futura LDP.

Art. 5 cpv. 2 lett. a e 4 lett. a

L'espressione «dati personali» è sostituita con «dati personali o dati su persone giuridiche».

Art. 7 cpv. 2

L'espressione «collezione di dati» è sostituita con «banca dati» (cfr. i commenti al numero 9.2.2). Il rinvio all'articolo 22 LPD deve essere adeguato alla nuova numerazione del D-LPD (art. 35).

Art. 10 cpv. 4 e 5, secondo periodo

Nel capoverso 4 l'espressione «dati provenienti dalle loro collezioni» è sostituita con «dati provenienti dalle loro banche dati».

Nel capoverso 5, secondo periodo, il rinvio al D-LPD è stato aggiornato.

Art. 12 cpv. 2

L'espressione «collezione di dati» è sostituita con «banche dati».

245 RS **431.01**

Art. 14 cpv. 1

L'espressione «la persona interessata» è sostituita con «la persona fisica o giuridica interessata».

Art. 14a cpv. 1, secondo periodo

Dopo «dati personali degni di particolare protezione» è aggiunta l'espressione «dati su persone giuridiche degni di particolare protezione». L'espressione «profili della personalità» è sostituita con «le caratteristiche essenziali di una persona fisica».

Art. 15 cpv. 1

L'espressione «dati personali» è sostituita con «dati personali o dati su persone giuridiche». Il principio della sicurezza dei dati deve valere per entrambe le categorie di persone.

Art. 16 cpv. 1

A seguito dell'abrogazione della protezione dei dati concernenti le persone giuridiche occorre precisare che la futura LPD sarà applicabile esclusivamente al trattamento di dati personali su persone fisiche.

Art. 19 cpv. 2, frase introduttiva

L'espressione «dati personali» è sostituita con «dati personali o dati su persone giuridiche».

9.2.25 Legge federale del 18 giugno 2010[246] sul numero d'identificazione delle imprese

Art. 3 cpv. 1 lett. d e art. 5 cpv. 1 lett. b

L'espressione «collezione di dati» è sostituita con «banche dati». (cfr. n. 9.2.2).

9.2.26 Legge del 18 dicembre 1992[247] sulla Biblioteca nazionale

Art. 2 cpv. 2 e art. 7

Concerne unicamente il testo tedesco. L'espressione «Datensammlung» è sostituita con «Datenbank» negli articoli 2 capoverso 2 e 7.

246 RS **431.03**
247 RS **432.21**

9.2.27 Legge federale del 16 marzo 2012[248] sulla circolazione delle specie di fauna e di flora protette

Art. 23 cpv. 2, primo periodo

Il diritto vigente prescrive da un lato che i dati possono essere comunicati mediante procedura di richiamo se la legislazione estera corrispondente garantisce un'adeguata tutela della personalità delle persone interessate, e, dall'altro, che il Consiglio federale designa gli Stati nonché le organizzazioni sovranazionali e internazionali che garantiscono tale tutela. Al fine di assicurare un disciplinamento uniforme nel diritto federale occorre rinviare all'articolo 13 D-LPD.

9.2.28 Legge federale del 16 dicembre 2005[249] sulla protezione degli animali

Art. 20c cpv. 1, frase introduttiva

L'espressione «profilo della personalità» è soppressa. Confronta il numero 9.2.2.

9.2.29 Legge militare del 3 febbraio 1995[250]

Art. 31 cpv. 2, secondo periodo

L'articolo 31 capoverso 1 prevede che i militari abbiano a disposizione servizi di consulenza e assistenza medica, spirituale, psicologica e sociale nell'ambito del servizio militare. In considerazione della natura di questi compiti occorre sopprimere l'espressione «profili della personalità».

Art. 99 cpv. 2, primo periodo, e 3 lett. d

A seguito della natura dei compiti del servizio informazioni dell'esercito, al capoverso 2, primo periodo, occorre sostituire l'espressione «profili della personalità» con «dati personali che permettono di valutare il grado di pericolosità di una persona». Questa modifica adempie l'esigenza di una base legale di cui all'articolo 30 capoverso 2 lettera b D-LPD.

Nel capoverso 3 lettera d l'espressione «collezione di dati» è sostituita con «attività di trattamento di dati». Confronta il numero 9.2.2.

Art. 100 cpv. 2, primo periodo

L'espressione «profilo della personalità» è soppressa. Si veda il commento al numero 9.2.2.

248 RS **453**
249 RS **455**
250 RS **510.10**

Art. 146

L'espressione «profilo della personalità» è sostituita con «dati personali che permettono di valutare il grado di pericolosità di una persona».

9.2.30 Legge del 5 ottobre 2007[251] sulla geoinformazione

Art. 11 Protezione dei dati

Il capoverso 1 corrisponde al vigente articolo 11 della legge sulla geoinformazione (LGI), che dispone che la futura LPD si applicherà a tutti i geodati di base di diritto federale che costituiscono dati personali. Secondo il messaggio del 6 settembre 2006[252], «ciò fa sì che per tutti i geodati di base di diritto federale è applicata una regolamentazione unitaria della protezione dei dati (quella della Confederazione), indipendentemente dal fatto che i geodati di base con riferimento a persone siano elaborati da un'autorità della Confederazione, di un Cantone o di un Comune oppure da un privato che agisce su mandato pubblico. Per quanto concerne i geodati di base di diritto federale che sottostanno alla potestà sui dati dei Cantoni o dei Comuni e costituiscono dati personali, la vigilanza sulla protezione dei dati continua a incombere alle autorità cantonali o comunali di vigilanza sulla protezione dei dati, nonostante l'applicabilità della legge federale sulla protezione dei dati».

Nella misura in cui i geodati di base di diritto federale costituiscono dati personali, in virtù dell'articolo 11 D-LPD essi devono figurare nel registro delle attività di trattamento. Dato che la maggior parte dei geodati di base di diritto federale consente di stabilire un collegamento indiretto con il proprietario tramite la geometria del terreno, il numero dell'immobile e i dati pubblici del registro fondiario, la Confederazione e i Cantoni dovrebbero integrare nei registri delle attività di trattamento circa 50 delle circa 190 raccolte di geodati di base. Dal punto di vista della protezione dei dati ciò sarebbe poco sensato poiché tutti i geodati di base di diritto federale sono già elencati nell'allegato dell'ordinanza del 21 maggio 2008[253] sulla geoinformazione. Sono inoltre per lo più accessibili al pubblico in virtù di una legge speciale. Per questo motivo il capoverso 2 autorizza il nostro Consiglio a escludere l'inserimento dei geodati di base nel registro delle attività di trattamento, a condizione che il rischio di ingerenza nei diritti fondamentali della persona interessata sia limitato.

Il nuovo capoverso 3 dispone che il nostro Consiglio può definire per i geodati di base di diritto federale diversi livelli di autorizzazione vincolanti che considerano tutti gli aspetti della protezione dei dati, di particolari obblighi di mantenimento del segreto e del principio della trasparenza. Questa disposizione esecutiva, vigente dall'entrata in vigore del diritto in materia di geoinformazione nel 2008, si è dimostrata efficace e va sancita nella legge. I livelli di autorizzazione concernono l'accesso di terzi e di autorità a geodati. Eccezioni al diritto d'accesso della persona

251 RS **510.62**
252 FF **2006** 7165, in particolare pag. 7201.
253 RS **510.620**

interessata ai propri dati sono ammissibili unicamente alle condizioni di cui all'articolo 24 D-LPD.

9.2.31 Legge federale del 3 ottobre 2008[254] sui sistemi d'informazione militari

Art. 1 cpv. 1, frase introduttiva, e 3

Nel capoverso 1, frase introduttiva, l'espressione «profili della personalità» può essere sostituita con «dati personali». I dati personali che possono essere trattati sono infatti elencati nelle disposizioni legali applicabili al pertinente sistema d'informazione.

Nel capoverso 3 è stato aggiornato il rinvio al D-LPD.

Art. 10 lett. c

La terminologia va adeguata a quella dell'articolo 4 lettera c numero 2 D-LPD.

Art. 11 cpv. 2

Per la combinazione di determinati dati, l'articolo 11 prevede una limitazione del trattamento dei dati. L'espressione «profili della personalità» è definita diversamente come dati la cui combinazione consente di valutare le caratteristiche essenziali della personalità. Il capoverso 2 fissa un termine di conservazione massima per questo tipo di dati.

9.2.32 Legge federale del 13 dicembre 1996[255] sul materiale bellico

Art. 30 cpv. 2, secondo periodo

Nell'ambito dell'esecuzione della legge sul materiale bellico, l'Ufficio centrale per la repressione delle attività illegali concernenti materiale bellico collabora alla prevenzione di reati e notifica alle autorità di perseguimento penale competenti le infrazioni alle disposizioni della legge. Secondo l'articolo 30 capoverso 2, secondo periodo, l'Ufficio centrale è a tal fine autorizzato a trattare dati personali, compresi i dati personali degni di particolare protezione e i profili della personalità, nella misura e per il periodo richiesti dall'esecuzione dei suoi compiti. Vista la natura dei compiti dell'Ufficio federale, l'espressione «profili della personalità» va sostituita con «dati che permettono di valutare il pericolo che una persona commetta infrazioni alla presente legge».

254 RS **510.91**
255 RS **514.51**

9.2.33 Legge federale del 20 giugno 1997[256] sulle armi

Art. 32e cpv. 1 e 2

Confronta l'articolo 111*d* capoversi 1 e 2 D-LStr (n. 9.2.3).

Art. 32g, secondo periodo

Confronta l'articolo 111*f,* secondo periodo D-LStr (n. 9.2.3).

9.2.34 Legge federale del 4 ottobre 2002[257] sulla protezione della popolazione e sulla protezione civile

Art. 72 cpv. 1, seconda frase introduttiva e lett. a e b, nonché 1bis

Il diritto in vigore prevede che l'autorità federale competente può allestire profili della personalità, in particolare per accertare il potenziale per funzioni di quadro dei militi della protezione civile e dei partecipanti ai corsi. L'espressione «profili della personalità» va dunque sostituita al capoverso 1 con «i dati personali che permettono di valutare l'attribuzione della funzione di base o di accertare il potenziale per funzioni di quadro» e al capoverso 1bis con «dati personali che permettono di valutare il potenziale per funzioni di quadro o di specialista».

9.2.35 Legge federale del 7 ottobre 2005[258] sulle finanze della Confederazione

Art. 60c cpv. 1, frase introduttiva e cpv. 3

L'espressione «profilo della personalità» deve essere soppressa (cfr. n. 9.2.2).

9.2.36 Legge del 28 giugno 1967[259] sul Controllo delle finanze

Art. 10 cpv. 3

Questa modifica concerne solo il testo tedesco. L'espressione «Datensammlung» deve essere soppressa nel primo periodo e sostituita con «System» nel secondo periodo.

256 RS **514.54**
257 RS **520.1**
258 RS **611.0**
259 RS **614.0**

9.2.37 Legge federale del 18 marzo 2005[260] sulle dogane

Art. 38 cpv. 2

La decisione di tassazione di cui al capoverso 1 può essere resa sotto forma di decisione individuale automatizzata ai sensi dell'articolo 19 D-LPD. Conformemente all'articolo 19 capoverso 4 D-LPD, l'organo federale deve designare questa decisione come tale affinché la persona interessata possa riconoscere che è stata resa in maniera automatizzata.

Art. 103 cpv. 1, frase introduttiva e cpv. 2

L'identità può essere accertata mediante il rilevamento dei dati genetici. Questa disposizione era finora contenuta nell'articolo 226 capoverso 3 lettera b numero 1 dell'ordinanza del 1° novembre 2006[261] sulle dogane e viene ora trasposta nella legge.

Art. 110 cpv. 1 e 2

Nel capoverso 1 l'espressione «profilo della personalità» è soppressa. Gli scopi previsti al capoverso 2 del diritto vigente sono d'ora innanzi previsti al capoverso 1.

Il primo periodo del nuovo capoverso 2 prevede unicamente che l'AFD può a tal fine gestire sistemi d'informazione.

Il secondo periodo del capoverso 1 è nuovo. Abilita l'AFD a procedere a profilazioni per adempiere i compiti di cui al capoverso 1 ad eccezione della lettera d. L'AFD tratta e analizza in maniera automatizzata dati personali allo scopo di allestire delle analisi dei rischi che consentono di effettuare controlli più mirati. Per questa attività l'AFD necessita di una base legale formale.

Art. 110a cpv. 3 lett. b

L'espressione «profilo della personalità» deve essere soppressa (cfr. n. 9.2.2).

Art. 112 cpv. 2, frase introduttiva, 4 lett. b e 6, secondo periodo

L'espressione «profilo della personalità» deve essere soppressa nella frase introduttiva del capoverso 2 (cfr. n. 9.2.2).

Nel capoverso 2 occorre inoltre prevedere una base legale per la comunicazione di dati personali risultanti da una profilazione (cfr. il commento all'art. 32 D-LPD al n. 9.1.7).

Il capoverso 4 lettera b può essere abrogato poiché non più applicabile.

Nel capoverso 6, secondo periodo, è stato aggiornato il rinvio al D-LPD.

260 RS **631.0**
261 RS **631.01**

Art. 113 e 114 cpv. 2

L'espressione «profilo della personalità» deve essere soppressa (cfr. n. 9.2.2).

In entrambe le disposizioni occorre inoltre prevedere una base legale per la comunicazione di dati personali risultanti da una profilazione (cfr. il commento all'art. 32 D-LPD al n. 9.1.7).

9.2.38 Legge del 12 giugno 2009[262] sull'IVA

Art. 76 cpv. 1, secondo periodo

Il diritto in vigore prevede che l'Amministrazione federale delle contribuzioni gestisca le necessarie collezioni di dati e gli strumenti per il trattamento e la conservazione. Questa disposizione può essere soppressa poiché superflua.

9.2.39 Legge del 21 marzo 1969[263] sull'imposizione del tabacco

Art. 18 cpv. 4

L'importo dell'imposta può essere stabilito sotto forma di decisione individuale automatizzata ai sensi dell'articolo 19 D-LPD. Conformemente all'articolo 19 capoverso 4 D-LPD, l'organo federale deve designare questa decisione come tale affinché la persona interessata possa riconoscere che è stata resa in maniera automatizzata.

9.2.40 Legge del 6 ottobre 2006[264] sull'imposizione della birra

Art. 17 cpv. 3, secondo periodo

Confronta il commento all'articolo 18 capoverso 4 del disegno della legge sull'imposizione del tabacco (n. 9.2.39).

262 RS **641.20**
263 RS **641.31**
264 RS **641.411**

9.2.41 Legge del 21 giugno 1996[265] sull'imposizione degli oli minerali

Art. 21 cpv. 2bis

Confronta il commento all'articolo 18 capoverso 4 del disegno della legge sull'imposizione del tabacco (n. 9.2.39).

9.2.42 Legge del 19 dicembre 1997[266] sul traffico pesante

Art. 11 cpv. 4

Confronta il commento all'articolo 18 capoverso 4 del disegno della legge sull'imposizione del tabacco (n. 9.2.39).

9.2.43 Legge federale del 21 marzo 2003[267] sull'energia nucleare

Art. 24 cpv. 2

Il diritto in vigore prevede che nell'ambito del controllo dell'affidabilità delle persone impiegate in funzioni essenziali per la sicurezza nucleare interna ed esterna possano essere elaborati dati personali particolarmente degni di protezione sulla salute e l'idoneità psichica, nonché dati rilevanti per la sicurezza sulla condotta di vita delle persone interessate. Il secondo periodo, secondo cui può essere compilata una raccolta di dati, può essere soppresso poiché superfluo.

9.2.44 Legge del 24 giugno 1902[268] sugli impianti elettrici

Art. 25a cpv. 2

L'espressione «conservare tali dati in forma elettronica» può essere soppressa poiché superflua.

265 RS **641.61**
266 RS **641.81**
267 RS **732.1**
268 RS **734.0**

9.2.45 Legge federale del 19 dicembre 1958[269] sulla circolazione stradale

Art. 76b cpv. 3, secondo periodo

L'espressione «profili della personalità» deve essere soppressa (cfr. n 9.2.2).

9.2.46 Legge federale del 20 dicembre 1957[270] sulle ferrovie

Art. 16a Trattamento di dati da parte dei titolari di una concessione

I rinvii del capoverso 1 agli articoli della futura LPD vanno adeguati. Il capoverso 1 della versione tedesca viene modificato in più punti al fine di allinearlo alle versioni italiana e francese.

L'espressione «profili della personalità» deve essere soppressa nel capoverso 2 (cfr. n 9.2.2).

Secondo il capoverso 3 la vigilanza sul trattamento di dati personali da parte dei titolari della concessione è retta dall'articolo 27 LPD. Questa disposizione può essere abrogata dato che il D-LPD non distingue più tra la vigilanza dell'Incaricato sui privati e quella sugli organi della Confederazione.

9.2.47 Legge del 20 marzo 2009[271] sul trasporto di viaggiatori

Art. 54 Trattamento di dati da parte dei titolari di una concessione

Si rinvia al commento sull'articolo 16*a* della legge sulle ferrovie (n. 9.2.46).

9.2.48 Legge del 4 ottobre 1963[272] sugli impianti di trasporto in condotta

Art. 47a cpv. 2

Si rinvia al commento sull'articolo 25*a* capoverso 2 della legge sugli impianti elettrici (n. 9.2.44).

269 RS **741.01**
270 RS **742.101**
271 RS **745.1**
272 RS **746.1**

9.2.49 Legge federale del 21 dicembre 1948[273] sulla navigazione aerea

Art. 107a cpv. 2, frase introduttiva, 4 e 5

L'espressione «profilo della personalità» nella frase introduttiva del capoverso 2 è soppressa. Ciò non ha conseguenze sulla base legale prevista alla lettera a numeri 1–3.

La modifica del capoverso 4 concerne soltanto il testo tedesco. L'espressione «Datensammlung» va sostituita con «Datenbeschaffung».

Al capoverso 5 l'espressione «profili della personalità» è soppressa. La comunicazione di dati personali ad autorità estere è possibile se le condizioni di cui all'articolo 13 D-LPD sono rispettate.

Occorre rinviare alla modifica del 16 giugno 2017 della legge sulla navigazione aerea[274]. Le disposizioni di coordinamento (cfr. n. 13.7) prevedono la soppressione dell'espressione «profili della personalità» nell'articolo 21*c* verso 1 lettera b.

9.2.50 Legge del 17 dicembre 2010[275] sulle poste

Art. 26 cpv. 1, 2, frase introduttiva, e 3, secondo periodo, nonché art. 28

L'espressione «profili della personalità» è soppressa (cfr. n 9.2.2).

9.2.51 Legge del 30 aprile 1997[276] sulle telecomunicazioni

Art. 13a cpv. 1, primo periodo, e art. 13b cpv. 1, secondo periodo, 2, frase introduttiva e 4, primo periodo

L'espressione «profili della personalità» è soppressa (cfr. n 9.2.2).

9.2.52 Legge federale del 24 marzo 2006[277] sulla radiotelevisione

Art. 69f cpv. 1, secondo periodo, e art. 88 cpv. 2

Secondo queste disposizioni, la vigilanza sul trattamento di dati personali da parte dell'organo di riscossione e dell'autorità di vigilanza è retta dalle disposizioni della LPD applicabili agli organi federali. L'espressione «e la relativa sorveglianza» va

273 RS **748.0**
274 FF **2017** 3661
275 RS **783.0**
276 RS **784.10**
277 RS **784.40**

soppressa in entrambe le disposizioni dato che il D-LPD non distingue più tra la vigilanza dell'Incaricato sui privati e quella sugli organi federali.

9.2.53 Legge federale del 30 settembre 2011[278] sulla ricerca umana

Art. 42 cpv. 2

La disposizione va modificata in quanto deve rinviare agli articoli 13 e 14 D-LPD e non più all'articolo 6 LPD.

9.2.54 Legge del 3 ottobre 1951[279] sugli stupefacenti

Art. 3f cpv. 1

L'espressione «profili della personalità» va soppressa (cfr. n 9.2.2).

Art. 18c, secondo periodo

Si rinvia al commento sull'articolo 111*f* secondo periodo D-LStr (n. 9.2.3).

9.2.55 Legge del 28 settembre 2012[280] sulle epidemie

Art. 60 cpv. 9, primo periodo

In questa disposizione vanno adeguati i rinvii alla LPD.

Art. 62 cpv. 1 e 3, frase introduttiva, nonché lett. a e d

L'articolo 62 disciplina la comunicazione di dati personali ad autorità estere. Le modifiche si allineano al nuovo disciplinamento previsto agli articoli 13 e 14 D-LPD.

9.2.56 Legge del 17 giugno 2005[281] contro il lavoro nero

Art. 17, rubrica, e cpv. 1, frase introduttiva, nonché cpv. 2 e 4

A seguito dell'abrogazione della protezione dei dati delle persone giuridiche occorre creare due basi legali distinte (cfr. anche il commento al n. 9.1.11). L'articolo 17

278 RS **810.30**
279 RS **812.121**
280 RS **818.101**
281 RS **822.41**

disciplinerà soltanto il trattamento di dati personali da parte delle competenti autorità cantonali. Nel capoverso 4 è stato aggiornato il rinvio al D-LPD.

Art. 17a Trattamento di dati su persone giuridiche

Questa disposizione abilita le competenti autorità cantonali a trattare dati su persone giuridiche.

9.2.57 Legge del 6 ottobre 1989[282] sul collocamento

Art. 33a cpv. 1, frase introduttiva e cpv. 3 nonché art. 35 cpv. 2, 3bis e 5 lett. d

Come emerge dal messaggio del 24 novembre 1999[283] concernente l'adeguamento e l'armonizzazione delle basi legali per il trattamento di dati personali nelle assicurazioni sociali, gli organi incaricati di applicare le diverse leggi in materia di assicurazioni sociali, tra cui in senso lato anche la legge sul collocamento (LC), sono chiamati a trattare costantemente una moltitudine di dati personali, necessari dal momento dell'assoggettamento all'assicurazione, per il calcolo e il prelievo dei contributi o dei premi, o ancora al momento della determinazione e della concessione delle prestazioni d'assicurazione. I dati personali trattati sono di natura molto diversa e vanno da semplici indicazioni sull'identità di una persona a informazioni di carattere confidenziale concernenti la salute o ancora fatti appartenenti alla sfera privata come l'età, il reddito, l'iter professionale, la storia famigliare e così via. A seconda della maniera in cui sono combinati, simili dati personali possono fornire un quadro generale della personalità di un individuo e costituire in tal modo un «profilo della personalità» ai sensi dell'articolo 3 lettera d LPD.

Il disegno di legge sopprime l'espressione «profili della personalità» e dunque anche la corrispondente base legale nell'articolo 33*a* LC. Riteniamo però necessario creare una base in una legge in senso formale per trattamenti che, come descritto precedentemente, possono fornire un quadro generale della personalità di un individuo (art. 30 cpv. 2 lett. b D-LPD). Nel settore delle assicurazioni sociali, trattamenti di dati di questo tipo possono causare una grave ingerenza nei diritti fondamentali della persona interessata. Proponiamo pertanto di aggiungere all'articolo 33*a* un nuovo capoverso 3 che autorizzi i competenti organi a trattare ai sensi del capoverso 1 dati personali che consentono di valutare la situazione personale ed economica del beneficiario di prestazioni di consulenza.

Art. 35b

La modifica concerne soltanto il testo francese. Il termine «fichier» è sostituito con «registre» (cfr. n 9.2.2).

282 RS **823.11**
283 FF **2000** 205

9.2.58 Legge federale del 20 dicembre 1946[284] su l'assicurazione per la vecchiaia e per i superstiti

Art. 49° cpv. 1, frase introduttiva

Il disegno di legge sopprime la nozione di «profilo della personalità» e dunque la relativa base legale prevista all'articolo 49*a*. Come nel caso della LC (cfr. n. 9.2.57), riteniamo però necessario creare una base in una legge in senso formale per trattamenti che possono fornire un quadro generale della personalità di un individuo (art. 30 cpv. 2 lett. c D-LPD). Simili trattamenti possono causare una grave ingerenza nei diritti fondamentali della persona interessata, soprattutto se comprendono anche dati medici degni di particolare protezione. Proponiamo dunque di aggiungere all'articolo 49*a* un nuovo capoverso 2 che autorizza gli organi competenti a trattare dati personali che permettono segnatamente di valutare la salute, la gravità dell'infermità fisica o psichica, i bisogni e la situazione economica dell'assicurato per adempiere i compiti di cui al capoverso 1.

9.2.59 Legge federale del 25 giugno 1982[285] sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità

Art. 85a cpv. 1, frase introduttiva, e 2

Confronta l'articolo 49*a* D-LAVS (n. 9.2.58).

9.2.60 Legge federale del 18 marzo 1994[286] sull'assicurazione malattie

Art. 84 cpv. 1, frase introduttiva, e 2

Si rinvia al commento sull'articolo 49*a* D-LAVS (n. 9.2.58).

Sostanzialmente si può rinviare ai commenti all'articolo 49*a* capoverso 2 D-LAVS (cfr. n. 9.2.58) anche per quanto riguarda il nuovo articolo 84 capoverso 2 della legge sull'assicurazione malattie. Rispetto alle altre assicurazioni sociali, nell'assicurazione malattie questa disposizione sarà applicata principalmente all'assicurazione dell'indennità giornaliera per malattia. Nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie (AOMS) e dei compiti degli assicuratori ad essa connessi, è prevedibile un'applicazione limitata di questa disposizione nel quadro dei compiti legali, ad esempio se sono necessari accertamenti supplementari in singoli casi come il rimborso di determinati farmaci (soprattutto con limitazione). Va sottolineato che i trattamenti delle categorie di dati menzionate al capoverso 2 con

284 RS **837.0**
285 RS **831.40**
286 RS **832.10**

finalità che vanno oltre l'esecuzione dell'AOMS e dell'assicurazione dell'indennità giornaliera per malattia è sempre inammissibile.

9.2.61 Legge federale del marzo 1981[287] sull'assicurazione contro gli infortuni

Art. 96 cpv. 1, frase introduttiva, e 2

Nella frase introduttiva al capoverso 1 è solamente soppressa la nozione di profili della personalità.

Secondo il nuovo capoverso 2, per adempiere i propri compiti gli organi di cui al capoverso 1 possono procedere alla profilazione ed emanare decisioni individuali automatizzate.

Diversamente dall'assicurazione malattie, l'assicurazione obbligatoria contro gli infortuni si basa sul principio delle prestazioni in natura. L'assicuratore è tenuto a fornire le prestazioni sanitarie in natura, a sue spese, diventando così debitore del fornitore di prestazioni[288]. Conformemente al principio delle prestazioni in natura, l'assicuratore offre al paziente un trattamento completo e adeguato piuttosto che rimborsare le spese contro fattura, come accade nell'assicurazione malattie (principio del rimborso delle spese).

Il principio delle prestazioni in natura consente tra l'altro all'assicuratore di partecipare alla scelta dell'entità, della natura e della durata delle prestazioni e dunque di ordinare le misure necessarie alla cura adeguata dell'assicurato (art. 48 cpv. 1 LAINF). Una cura adeguata può in determinati casi evitare il versamento di future rendite. Per poter determinare la cura adeguata, l'assicuratore deve però poter trattare i dati medici necessari. La profilazione gli permette ad esempio di identificare tempestivamente i casi complessi e di affidarli in modo mirato a un collaboratore specializzato.

Nell'insieme, la modifica del capoverso 2 non conferisce alcuna nuova competenza agli assicuratori contro gli infortuni, ma garantisce semplicemente che essi possano continuare ad assumere le loro competenze attuali.

9.2.62 Legge federale del 19 giugno 1992[289] sull'assicurazione militare

Art. 94a cpv. 1, frase introduttiva, e 2

Si rinvia al commento sull'articolo 96 D-LAINF (n. 9.2.61).

287 RS **832.20**
288 Maurer Alfred, Schweizerisches Unfallversicherungsrecht, 2ª ed., Berna 1989, pag. 523 segg.
289 RS **833.1**

9.2.63 Legge del 25 giugno 1982[290] sull'assicurazione contro la disoccupazione

Art. 96b cpv. 1, frase introduttiva, e 2 nonché 96c cpv. 2, frase introduttiva e 2bis

Si rinvia al commento sull'articolo 49*a* D-LAVS (n. 9.2.58).

9.2.64 Legge del 1° luglio 1966[291] sulle epizoozie

Art. 54a cpv. 3

L'espressione «profilo della personalità» è soppressa (cfr. n 9.2.2).

9.2.65 Legge del 20 giugno 1986[292] sulla caccia

Art. 22 cpv. 3 primo e secondo periodo

L'espressione «collezione elettronica di dati» è soppressa, mentre quella di «registrazioni elettroniche» è sostituita con «dati personali».

9.2.66 Legge del 3 ottobre 2003[293] sulla banca nazionale

Art. 14 cpv. 3

Per svolgere le sue attività legali e osservare l'evoluzione sui mercati finanziari la Banca nazionale raccoglie i dati statistici necessari (art. 14 cpv. 1 della legge sulla banca nazionale [LBN]). Al fine di contenere l'onere per le persone tenute a fornire i dati ed evitare per quanto possibile sovrapposizioni con rilevamenti di dati di altri servizi statistici e unità amministrative della Confederazione, nella raccolta dei dati statistici la Banca nazionale collabora con i servizi competenti della Confederazione, in particolare con l'Ufficio federale di statistica (UST) e l'Autorità federale di vigilanza sui mercati finanziari (FINMA), con le autorità competenti di altri Paesi e con le organizzazioni internazionali (art. 14 cpv. 2 LBN).

Nella prassi è ora emerso che il disciplinamento vigente non è sempre sufficiente. In alcuni casi, obblighi legali di mantenimento del segreto e il blocco dei dati impediscono la trasmissione di dati in forma non aggregata alla Banca nazionale: l'articolo 74 della legge del 12 giugno 2009[294] sull'IVA vieta la trasmissione di dati sull'IVA dall'Amministrazione federale delle contribuzioni (AFC) alla Banca nazio-

290 RS **837.0**
291 RS **916.40**
292 RS **922.0**
293 RS **951.11**
294 RS **641.20**

nale. Anche se l'AFC può mettere a disposizione dell'UST questi dati in forma non anonimizzata (art. 10 cpv. 4 e 5 della legge del 9 ottobre 1992[295] sulla statistica federale [LStat] in combinato disposto con l'art. 136 cpv. 2 dell'ordinanza del 27 novembre 2009 sull'IVA[296]), la trasmissione alla Banca nazionale è esclusa poiché la LBN non contiene alcuna disposizione analoga all'articolo 10 capoversi 4 e 5 LStat. Ne risulta che la Banca nazionale deve rilevare nuovamente presso le imprese dati di cui l'AFC già dispone, il che raddoppia l'onere per le imprese.

All'articolo 14 va dunque aggiunto un nuovo capoverso 3 che, analogamente alla LStat, stabilisce che l'AFC fornisce alla Banca nazionale, per l'adempimento dei compiti statistici, le basi e i risultati della sua attività statistica nell'ambito dell'imposta sul valore aggiunto e, se necessario, i dati sull'imposta sul valore aggiunto provenienti dalle sue raccolte di dati e rilevazioni. In tal modo è garantito che la Banca nazionale non debba rilevare nuovamente dati statistici nell'ambito dell'IVA di cui l'AFC già dispone, sgravando pertanto le imprese.

Al fine di garantire che terzi non possano accedere tramite la Banca nazionale a dati ai quali non avrebbero in altro modo accesso è esplicitamente stabilito che la Banca nazionale non può trasmettere a terzi dati che ha ottenuto dall'AFC in virtù del capoverso 3. Questa limitazione è applicabile indipendentemente dall'articolo 35 D-LPD anche alla comunicazione di dati a terzi per scopi impersonali, in particolare ricerca, pianificazione e statistica. La Banca nazionale non può neppure scambiare questi dati con la FINMA malgrado l'articolo 16 capoverso 4 LBN, con l'UST malgrado l'articolo 16 capoverso 4bis o con banche centrali straniere od organizzazioni e organismi internazionali malgrado gli articoli 50*a* e 50*b* LBN. Essa è per contro autorizzata a trasmettere dati in forma aggregata conformemente all'articolo 16 capoverso 3 LBN.

Art. 16 cpv. 4bis e 5

L'articolo 16 disciplina la confidenzialità sui dati trattati dalla Banca nazionale a fini statistici.

La Banca nazionale è tenuta a serbare il segreto sui dati raccolti (art. 16 cpv. 1 LBN), anche nei confronti delle autorità e organizzazioni internazionali con cui collabora a fini statistici. Secondo il diritto vigente essa può pertanto scambiare dati confidenziali unicamente con le competenti autorità svizzere di vigilanza sui mercati finanziari (art. 16 cpv. 4 LBN). A tutte le altre autorità nazionali ed estere, in particolare all'UST, la Banca nazionale può in linea di massima trasmettere i dati soltanto in forma aggregata (art. 16 cpv. 3 in combinato disposto con l'art. 14 cpv. 2 LBN). Le uniche eccezioni sono la FINMA, la Banca dei regolamenti internazionali e determinate organizzazioni e organismi internazionali, alle quali da poco tempo la Banca nazionale può trasmettere, a condizioni restrittive, informazioni non accessibili al pubblico, compresi i suoi dati statistici (art. 50*a* e 50*b* LBN).

295 RS **431.01**
296 RS **641.201**

Per analizzare l'evoluzione sui mercati finanziari, ottenere una visione d'assieme del traffico dei pagamenti, allestire la bilancia dei pagamenti o la statistica delle attività sull'estero, la Banca nazionale raccoglie dati statistici sull'attività di altre persone fisiche o giuridiche (art. 15 cpv. LBN). Proprio nell'ambito della bilancia dei pagamenti, le esigenze della Banca nazionale in materia di dati si sovrappongono in numerosi punti alle esigenze dell'UST. La mancanza di una base legale chiara per la comunicazione di dati tra la Banca nazionale e l'UST comporta pertanto per entrambi un onere molto maggiore per garantire la qualità dei loro rilevamenti. Non è possibile mettere a frutto le sinergie tra i singoli rilevamenti, il che conduce sia per la Banca nazionale e l'UST sia per le persone tenute a fornire i dati un onere supplementare inutile ed evitabile mediante uno scambio vicendevole di dati. A ciò si aggiunge il fatto che la Banca nazionale così come l'UST e altri servizi statistici sono obbligati a limitare il numero e il genere delle rilevazioni allo stretto necessario e a contenere per quanto possibile l'onere delle persone tenute a informare (art. 1 cpv. 1 dell'ordinanza del 18 marzo 2004[297] sulla Banca nazionale [OBN]). In particolare, la Banca nazionale rinuncia alla rilevazione di dati statistici qualora possa «procurarsi tempestivamente in altro modo dati di qualità equivalente» (art. 4 cpv. 3 OBN).

Per questi motivi, il nuovo capoverso 4bis autorizza la Banca nazionale a comunicare all'UST dati in forma non aggregata. Trattandosi di una eccezione al principio di cui al capoverso 3, secondo cui la Banca nazionale è autorizzata a trasmettere dati ad autorità nazionali ed estere e a organizzazioni internazionali soltanto in forma aggregata, la disposizione è applicabile unicamente se la comunicazione dei dati persegue scopi statistici e l'UST ha bisogno di tali dati per adempiere i propri compiti. Il nuovo capoverso chiarisce inoltre che l'UST non può trasmettere a terzi i dati ricevuti dalla Banca nazionale. Questo divieto vale anche per la trasmissione a scopi impersonali, indipendentemente dalla norma generale di cui all'articolo 35 D-LPD, ed esclude segnatamente anche la comunicazione di tali dati ad altre autorità o servizi statistici nazionali ed esteri. In tal modo si mira a impedire che terzi possano accedere tramite l'UST a dati ai quali non avrebbero in altro modo accesso.

Diversamente dalla Banca nazionale, in virtù dell'articolo 19 capoverso 2 LStat, l'UST è a determinate condizioni già oggi autorizzato a comunicare dati personali in forma non aggregata per scopi di statistica. Questo principio vale per i dati del Registro delle imprese e degli stabilimenti (RIS), ma solo in modo limitato: in base all'articolo 10 capoverso 5 LStat, l'UST non può infatti trasmettere alla Banca nazionale i dati sull'IVA contenuti nel RIS. Con il nuovo articolo 14 capoverso 3 LBN è pertanto creata la base legale affinché l'AFC possa mettere direttamente a disposizione della Banca nazionale i dati sull'IVA per scopi statistici.

La modifica dell'articolo 16 capoverso 5 costituisce un adeguamento risultante dalla modifica del campo d'applicazione del D-LPD. Dato che in futuro la LPD sarà applicabile unicamente ai dati di persone fisiche, per motivi di certezza giuridica è necessario precisare il rinvio al D-LPD.

297 RS **951.131**

Art. 49a Trattamento di dati personali e di dati su persone giuridiche

In adempimento dei suoi compiti pubblici, la Banca nazionale tratta una gran quantità di dati di persone giuridiche e in parte anche fisiche. Queste informazioni sugli attori del mercato finanziario e sulle imprese costituiscono un presupposto fondamentale per l'esercizio dei suoi compiti legali. Nei settori della statistica (art. 14–16 LBN) e stabilità del sistema finanziario (art. 16*a* LBN), la Banca nazionale dispone di una base legale esplicita per il trattamento di dati. Per motivi di certezza giuridica, l'articolo 49*a* chiarisce che per adempiere i propri compiti legali, la Banca nazionale può trattare dati personali, compresi quelli degni di particolare protezione, e dati su persone giuridiche.

9.2.67 Legge del 10 ottobre 1997[298] sul riciclaggio di denaro

Art. 29 cpv. 2, secondo periodo

L'espressione «profili della personalità» è soppressa (cfr. n. 9.2.2).

Art. 33 Principio

Il rinvio al D-LPD è stato aggiornato.

Art. 34 rubrica e cpv. 1–3

Nella rubrica nonché nei capoversi 1 e 2 l'espressione «collezioni di dati» è sostituita con «banche dati» e «banche dati e incarti».

Nel capoverso 3 è stato aggiornato il rinvio al D-LPD.

9.2.68 Legge del 22 giugno 2007[299] sulla vigilanza dei mercati finanziari

Art. 23 Trattamento di dati

Il disegno di legge sopprime l'espressione «profilo della personalità» e dunque la relativa base legale prevista all'articolo 23. Nel quadro dei suoi compiti di vigilanza, la FINMA tratta dati personali di ogni tipo. L'esercizio della vigilanza sul mercato finanziario presuppone informazioni complete sugli assoggettati e sugli attori del mercato finanziario. I dati trattati comprendono anche dati degni di particolare protezione. Lo scopo del trattamento può inoltre comportare una grave ingerenza nei diritti fondamentali, soprattutto nella libertà economica. Per questo motivo proponiamo l'adeguamento della base legale in senso formale per il trattamento di dati da parte della FINMA, al fine di tenere conto dell'esigenza di cui all'articolo 30 capoverso 2 D-LPD. I trattamenti di dati possono essere affidati a specialisti incaricati

298 RS **955.0**
299 RS **956.1**

dalla FINMA secondo l'articolo 14 capoverso 4 LFINMA nonché a fornitori di prestazioni impiegati in base al diritto privato (cpv. 1 e 2).

La natura dei suoi compiti fa sì che la FINMA riceva tantissimi dati da parte degli istituti assoggettati e di altri terzi. Per poter identificare, in base a questa enorme quantità di dati, un eventuale condotta scorretta dal punto di vista del diritto in materia di vigilanza, la FINMA non può evitare di trattare dati nel quadro di una profilazione. In particolare nell'ambito della vigilanza sul mercato (p. es. al fine di accertare un possibile insider trading o una manipolazione del mercato), la FINMA è confrontata con una gran quantità di dati relativi agli scambi commerciali e alle transazioni, che devono essere analizzati e valutati in maniera automatizzata in relazione alle persone interessate. Per garantire l'efficacia della vigilanza, la FINMA deve dunque poter trattare i pertinenti dati nel quadro di una profilazione (cpv. 3).

Come finora, la FINMA disciplina i dettagli in un'ordinanza (cpv. 4).

Art. 23a Elenco pubblico

Questa disposizione corrisponde all'articolo 23 capoverso 2 del diritto in vigore.

9.2.69 Legge federale del 19 marzo 1976[300] su la cooperazione allo sviluppo e l'aiuto umanitario internazionali

Art. 13a cpv. 1, frase introduttiva e lett. g

La frase introduttiva del capoverso 1 contempla il trattamento di dati di persone fisiche e giuridiche. Dato che il D-LPD abroga la protezione dei dati personali delle persone giuridiche, occorre adeguare la frase introduttiva (cfr. il commento al n. 9.1.11).

La lettera g con l'espressione «profili della personalità» è abrogata (cfr. il n. 9.2.2).

Occorre segnalare che questa disposizione è abrogata nell'avamprogetto del 28 giugno 2017 concernente la legge federale del 24 marzo 2000 sul trattamento di dati personali da parte del DFAE (cfr. n. 9.2.13).

9.2.70 Legge federale del 24 marzo 2006[301] sulla cooperazione con gli Stati dell'Europa dell'Est

Art. 15 cpv. 2, frase introduttiva

L'espressione «profili della personalità» è soppressa (cfr. il n. 9.2.2).

300 RS **974.0**
301 RS **974.1**

Occorre segnalare che questa disposizione è abrogata nell'avamprogetto del 28 giugno 2017 concernente la legge federale del 24 marzo 2000 sul trattamento di dati personali da parte del DFAE (cfr. n. 9.2.13).

9.3 Commento alle modifiche delle leggi federali che attuano i requisiti della direttiva (UE) 2016/680

Le modifiche che figurano in più testi di legge sono commentate un'unica volta; successivamente si rinvia a tale commento.

9.3.1 Codice penale[302]

Al fine di trasporre i requisiti della direttiva (UE) 2016/680, il presente progetto prevede d'introdurre un certo numero di disposizioni di protezione dei dati applicabili agli scambi di dati effettuati nell'ambito della cooperazione di polizia. Con alcune eccezioni, le suddette disposizioni non sono quindi applicabili soltanto alle autorità federali ma anche a quelle cantonali. In questo ambito la Confederazione ricorre alla sua competenza legislativa poiché il settore della cooperazione internazionale in materia penale è retto dal diritto federale. Se la Costituzione attribuisce in un determinato settore la competenza legislativa alla Confederazione, il legislatore può anche emanare norme di protezione dei dati applicabili alle autorità cantonali incaricate di applicare il diritto federale.

Art. 349a Basi legali

Questa disposizione attua gli articoli 8 e 10 della direttiva (UE) 2016/680, che in sostanza prevedono che un trattamento di dati rientrante nel campo d'applicazione di tale atto è lecito soltanto se esiste una base legale o, in assenza di questa, in certi casi specifici elencati nelle due disposizioni. In assenza di una base legale, le competenti autorità federali hanno il diritto di comunicare dati unicamente nei casi previsti dall'articolo 349*a* lettere a e b. Per contro, le autorità federali competenti non possono basarsi sull'articolo 32 capoverso 2 lettere a, b ed e D-LPD per comunicare dei dati, poiché tale disposizione non è compatibile con i requisiti di cui agli articoli 8 e 10 della direttiva (UE) 2016/680.

Art. 349b Parità di trattamento

Questa disposizione attua l'articolo 9 capoversi 3 e 4 della direttiva (UE) 2016/680, che sancisce la parità di trattamento tra le autorità degli Stati Schengen e le autorità nazionali di perseguimento penale. L'articolo 349*b* corrisponde alla soluzione scelta dal legislatore federale all'articolo 6 LSIS. La comunicazione di dati ad autorità di uno Stato Schengen è soggetta alle medesime condizioni di protezione dei dati di

[302] RS **311.0**

quella a un'autorità nazionale. L'adozione di nuove restrizioni legali rimane possibile, a condizione che il principio della parità di trattamento sia rispettato.

Art. 349c Comunicazione di dati personali a uno Stato terzo o a un organo internazionale

Questa disposizione attua gli articoli 35–38 della direttiva (UE) 2016/680, che consentono agli Stati Schengen di trasmettere dati personali a uno Stato terzo o a un organo internazionale soltanto se sono adempiute determinate condizioni cumulative.

L'articolo 349*c* s'ispira alla sistematica e al contenuto degli articoli 13 e 14 D-LPD, fatte salve certe modifiche legate ali requisiti degli articoli 35–38 della direttiva (UE) 2016/680.

Cpv. 1

Il capoverso 1 sancisce il principio secondo cui nessun dato può essere comunicato all'autorità competente di uno Stato che non è vincolato alla Svizzera da uno degli accordi d'associazione a Schengen (Stato terzo) o a un organo internazionale, qualora la personalità della persona interessata possa subirne grave pregiudizio, dovuto in particolare all'assenza di una protezione adeguata. La disposizione contempla unicamente gli Stati non vincolati da uno degli accordi d'associazione a Schengen.

Cpv. 2

Il capoverso 2 definisce i casi in cui uno Stato terzo o l'organo internazionale garantiscono un livello di protezione dei dati adeguato. Si tratta di un elenco esaustivo di condizioni alternative. Se una di queste condizioni è realizzata non vi è più alcun ostacolo legato alla protezione dei dati che si opponga alla comunicazione di dati a uno Stato terzo o a un organo internazionale.

In virtù del capoverso 2 lettera a, la legislazione dello Stato terzo garantisce una protezione adeguata dei dati se l'Unione europea l'ha constatato tramite decisione. L'organo competente in materia è la Commissione europea. La decisione di adeguatezza è presa conformemente all'articolo 36 della direttiva (UE) 2016/680. Il capoverso 2 lettera a si distingue dall'articolo 13 capoverso 1 D-LPD, secondo cui il Consiglio federale deve esaminare se lo Stato in questione garantisce una protezione adeguata. L'autorità che intende comunicare dei dati a uno Stato terzo nel quadro della cooperazione di polizia e giudiziaria instaurata da Schengen deve osservare le decisioni della Commissione europea sull'adeguatezza. Negli altri settori, il titolare del trattamento si basa sulla constatazione del Consiglio federale. Questa differenza di disciplinamento non conduce in linea di massima a una situazione d'incertezza giuridica, poiché già attualmente l'Incaricato pubblica un elenco degli Stati che garantiscono una protezione dei dati. Tale elenco corrisponde nella sostanza alle decisioni della Commissione europea sull'adeguatezza.

Il capoverso 2 lettere b e c prevede altri due casi in cui l'autorità competente può considerare che la trasmissione non minacci gravemente la personalità degli interessati. Una comunicazione di dati è pertanto lecita se la protezione dei dati è garantita da un trattato internazionale (lett. b) o da garanzie specifiche (lett. c). Il capoverso 2 lettera b corrisponde all'articolo 13 capoverso 2 lettera a D-LPD. Sono considerati

«trattati internazionali» non soltanto gli accordi internazionali conclusi con uno Stato terzo o un organo internazionale nel campo della cooperazione di polizia e che soddisfano le esigenze poste dalla direttiva (UE) 2016/680, ma anche le convenzioni internazionali in materia di protezione dei dati ratificate dallo Stato destinatario. Il capoverso 2 lettera c corrisponde all'articolo 13 capoverso 2 lettera c D-LPD. In virtù di questa disposizione, l'autorità competente può comunicare dei dati a uno Stato terzo o a un organo internazionale che fornisce garanzie specifiche per la protezione adeguata della persona interessata.

Cpv. 3

Secondo il capoverso 3, se l'autorità competente è un'autorità federale, questa comunica all'Incaricato le categorie di comunicazioni di dati personali effettuate in virtù del capoverso 2 lettera c. L'Incaricato non deve essere informato in merito a tutte le comunicazioni, ma piuttosto sulle categorie di comunicazioni effettuate in virtù di tale disposizione. Secondo il capoverso 3, secondo periodo, ogni comunicazione va documentata, il che permette all'Incaricato di effettuare gli accertamenti necessari e se del caso pronunciare un divieto ai sensi dell'articolo 45 capoverso 2 D-LPD.

Cpv. 4 e 5

Per il caso in cui non può essere garantita una protezione adeguata ai sensi del capoverso 2, il capoverso 4 presenta un elenco esaustivo delle eccezioni. Se una di queste è applicabile, l'autorità è liberata dal divieto di comunicare dati personali allo Stato terzo o all'organo internazionale che non garantiscono una protezione adeguata. Questa disposizione traspone i requisiti dell'articolo 38 della direttiva (UE) 2016/680. Come risulta dalla considerazione 72 di tale atto, queste deroghe dovrebbero essere interpretate in maniera restrittiva ed escludere trasferimenti frequenti, completi e strutturali di dati personali nonché trasferimenti di dati su larga scala, limitandoli ai dati strettamente necessari.

Il capoverso 4 lettera a dispone che dati personali possono essere comunicati se nel caso specifico ciò risulta necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo. In virtù della lettera b, la comunicazione è pure possibile se necessaria per prevenire una minaccia imminente e grave per la sicurezza pubblica di uno Stato Schengen o di uno Stato terzo.

Il capoverso 4 lettere c e d prevede due altre eccezioni, applicabili però soltanto a condizione che un interesse degno di protezione e preponderante della persona interessata non vi si opponga. L'espressione «prevenire, accertare o perseguire un reato» corrisponde al campo d'applicazione della direttiva (UE) 2016/680, che disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali «a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali». Nel quadro delle lettere b e c l'autorità deve ponderare gli interessi. Se giunge alla conclusione che l'interesse degno di protezione della persona interessata prevale sugli interessi del perseguimento penale, ad esempio se la comunicazione potrebbe mettere in pericolo la vita della persona interessata, l'autorità deve rinunciare ad avvalersi delle eccezioni previste alle lettere c e d. Se l'autorità compe-

tente è un'autorità federale, questa deve comunicare all'Incaricato la comunicazione di dati secondo il capoverso 4 (cpv. 5).

Art. 349d Comunicazione a uno Stato terzo o a un organo internazionale di dati personali provenienti da uno Stato Schengen

Questa disposizione attua i requisiti dell'articolo 35 paragrafo 1 lettere c ed e nonché paragrafo 2 della direttiva (UE) 2016/680, secondo cui gli Stati Schengen devono provvedere affinché i dati ricevuti da uno Stato Schengen possano essere comunicati a uno Stato terzo o a un organo internazionale soltanto se sono soddisfatte determinate condizioni cumulative. Questa disposizione è applicata alle autorità svizzere che hanno ricevuto dati da uno Stato Schengen nel quadro di una procedura di cooperazione di polizia e che intendono comunicarli a uno Stato terzo o a un organo internazionale ai fini dell'assistenza. Fatte salve alcune modifiche, l'articolo 349*d* corrisponde all'articolo 6*b* LSIS, soppresso per ragioni di sistematica.

Una comunicazione è possibile unicamente se le tre condizioni cumulative del capoverso 1 sono soddisfatte. Conformemente ai principi della finalità e della proporzionalità, la comunicazione deve essere necessaria per la prevenzione, l'accertamento e il perseguimento di un reato e l'autorità destinataria deve essere competente in materia (cpv. 1, frase introduttiva e lett. a). Lo Stato Schengen presso il quale sono stati raccolti i dati deve inoltre dare il suo consenso preliminare (lett. b) e infine lo Stato terzo o l'organo internazionale deve garantire una protezione adeguata ai sensi dell'articolo 349*c* (lett. c).

Il capoverso 2 prevede un'eccezione all'obbligo di ottenere il consenso preliminare dello Stato Schengen che ha raccolto i dati. In virtù delle lettere a e b, i dati possono essere comunicati se nel caso specifico il consenso preliminare dello Stato Schengen non può essere ottenuto in tempo utile e se la comunicazione è indispensabile per prevenire una minaccia imminente e grave alla sicurezza pubblica di uno Stato Schengen o di uno Stato terzo oppure per salvaguardare gli interessi essenziali di uno Stato Schengen. Si tratta di condizioni cumulative. Se dei dati sono comunicati in virtù del capoverso 2, l'autorità competente deve informare senza indugio lo Stato Schengen interessato (cpv. 3).

Art. 349e Comunicazione di dati personali a un destinatario domiciliato in uno Stato terzo

Questa disposizione attua l'articolo 39 della direttiva (UE) 2016/680, che autorizza gli Stati Schengen a permettere, in casi singoli e specifici, all'autorità di trasferire dati personali direttamente a un destinatario stabilito in uno Stato terzo. Questa norma contempla i casi in cui è urgente trasmettere dati all'estero, ad esempio per proteggere la vita di qualcuno che rischia di essere vittima di un reato o per evitare la commissione imminente di un crimine o di un atto di terrorismo[303].

Secondo la definizione dell'articolo 3 paragrafo 10 della direttiva (UE) 2016/680, per «destinatario» si intende una persona fisica o giuridica, un'autorità pubblica o un altro organismo cui sono comunicati dati personali.

303 Consid. 73 della direttiva (UE) 2016/680

Cpv. 1

In virtù del capoverso 1, i dati personali possono essere comunicati a un destinatario stabilitosi in uno Stato terzo soltanto se sono soddisfatte tre condizioni cumulative. Le comunicazioni di dati in virtù dell'articolo 349*e* devono rimanere casi eccezionali.

La prima condizione figura nella frase introduttiva del capoverso 1. L'autorità competente deve innanzitutto accertare l'impossibilità di comunicare i dati all'autorità competente dello Stato terzo tramite i consueti canali della cooperazione di polizia, in particolare a causa di una situazione d'urgenza.

In virtù della seconda condizione (cpv. 1 lett. b), la comunicazione deve essere necessaria per l'adempimento di un compito legale dell'autorità che comunica i dati, ovverossia compiti nei settori della prevenzione, dell'accertamento o del perseguimento di un reato. La comunicazione deve inoltre essere indispensabile. La possibilità di avvalersi dell'articolo 349*e* non deve d'altronde costituire una soluzione facile per l'autorità competente. La comunicazione è indispensabile unicamente se è una *conditio sine qua non* per l'adempimento del compito legale dell'autorità.

Infine, nessun interesse degno di protezione e preponderante della persona interessata deve opporsi alla comunicazione (cpv. 1 lett. b). L'autorità deve dunque ponderare gli interessi per determinare se prevalga l'interesse pubblico minacciato o quello della persona interessata.

Cpv. 2

Il capoverso 2 dispone che l'autorità competente comunichi i dati personali al destinatario con l'espresso divieto di utilizzarli per scopi diversi da quelli fissati dall'autorità. Si tratta di una concretizzazione del principio del vincolo alla finalità.

Cpv. 3

Secondo il capoverso 3, l'autorità competente informa senza indugio l'autorità competente dello Stato terzo in merito a qualsiasi comunicazione di dati personali, a condizione che questa informazione sia considerata appropriata. L'autorità non è tenuta a farlo ad esempio se è a conoscenza di casi di violazione dei diritti dell'uomo commessi dall'autorità competente dello Stato terzo in questione (consid. 73 della direttiva [UE] 2016/680).

Cpv. 4 e 5

Secondo il capoverso 4, se l'autorità competente è un'autorità federale, questa deve informare senza indugio l'Incaricato sulle comunicazioni di dati effettuate in virtù dell'articolo 349*e*. Contrariamente all'obbligo previsto all'articolo 349*c* capoverso 5, l'Incaricato deve essere informato in merito a tutte le comunicazioni e non solo alle categorie di comunicazioni. Le comunicazioni devono inoltre essere documentate (cpv. 5), il che permette all'Incaricato di effettuare le verifiche necessarie e se del caso di pronunciare un divieto di comunicazione in virtù dell'articolo 45 capoverso 2 D-LPD.

Art. 349f Esattezza dei dati personali

I capoversi 1, 2 e 5 mettono in atto l'articolo 7 paragrafi 2 e 3 della direttiva (UE) 2016/680, che in sostanza prevede che le competenti autorità debbano verificare la qualità dei dati prima di trasmetterli e fornire, nella misura del possibile, le informazioni che consentono all'autorità destinataria di valutare l'esattezza dei dati.

Il capoverso 1 s'ispira all'articolo 98 capoverso 1 CPP, che dispone che le autorità penali competenti rettifichino i dati personali inesatti.

Il capoverso 2 riprende l'articolo 98 capoverso 2 CPP precisando che, in caso di rettifica di dati personali incompleti, l'autorità competente non deve informarne soltanto l'autorità a cui ha trasmesso tali dati ma anche quella da cui li ha ricevuti.

Il capoverso 3 corrisponde all'articolo 12 OLPD.

Il capoverso 4 lettera a attua l'articolo 6 della direttiva (UE) 2016/680, che obbliga il titolare del trattamento a operare, nella misura del possibile, una distinzione tra i dati personali delle diverse categorie di interessati. Questa disposizione tiene conto del fatto che con l'avanzare della procedura la categoria in cui rientrano le persone interessate può cambiare. In effetti, secondo la considerazione 31 della suddetta direttiva, il trattamento di dati nei settori della cooperazione giudiziaria e di polizia implica necessariamente diverse categorie di persone interessate tra le quali conviene, nella misura del possibile, distinguere. La frase introduttiva del capoverso 4 lascia un certo margine di manovra all'autorità competente. In certi casi questa distinzione potrebbe non essere possibile, ad esempio se i fatti non consentono ancora di determinare se una persona è un testimone del reato o se vi ha partecipato come autore o complice.

Il capoverso 4 lettera b attua l'articolo 7 paragrafo 1 della direttiva (UE) 2016/680, secondo cui i dati personali fondati su fatti vanno distinti, nella misura del possibile, da quelli fondati su valutazioni personali[304].

Il capoverso 5 libera l'autorità dall'obbligo di informare il destinatario qualora le informazioni previste ai capoversi 2 o 3 siano deducibili dai dati personali stessi o dalle circostanze. Questa disposizione s'ispira alla soluzione prevista all'articolo 12 OLPD.

Art. 349g Verifica della liceità del trattamento

Questa disposizione attua l'articolo 17 della direttiva (UE) 2016/680, che obbliga gli Stati Schengen a prevedere per la persona interessata il diritto di chiedere all'autorità di controllo in materia di protezione dei dati di verificare la liceità di un trattamento di dati che la concernono, in caso di restrizione degli obblighi d'informazione o dei diritti della persona interessata di chiedere l'accesso ai suoi dati, la limitazione del trattamento oppure la rettifica o la cancellazione dei dati che la concernono. L'articolo 349*g* s'ispira alla soluzione prevista all'articolo 8 LSIP, tenendo conto delle modifiche apportate dal presente disegno (cfr. il n. 9.3.7).

304 Consid. 30 della direttiva (UE) 2016/680

Secondo il capoverso 1, nei casi previsti alle lettere a–c la persona interessata può chiedere all'Incaricato di verificare che gli eventuali dati che la concernono siano trattati conformemente al diritto. Vista la sistematica del titolo quarto del libro terzo CP, la persona interessata può avvalersi dell'articolo 349*g* soltanto per i trattamenti di dati rientranti nel campo d'applicazione del titolo quarto, ossia nel settore dell'assistenza in materia di polizia o in quello della cooperazione internazionale di polizia. Una verifica può inoltre essere richiesta soltanto nei confronti di un'autorità federale soggetta alla sorveglianza dell'Incaricato (cpv. 2), ad esempio fedpol o la Polizia giudiziaria federale.

L'Incaricato comunica l'esito della sua verifica alla persona interessata sempre nella stessa forma e conformemente al tenore previsto dal capoverso 3. La comunicazione non è impugnabile (cpv. 5).

Se l'Incaricato decide di aprire un'inchiesta nei confronti dell'autorità federale, la persona interessata non è parte del procedimento (art. 46 cpv. 2 D-LPD) e non può dunque ricorrere a rimedi giuridici contro le eventuali misure amministrative pronunciate dall'Incaricato (art. 45 D-LPD).

Art. 349h Inchiesta

Questa disposizione attua gli articoli 52 e 53 della direttiva (UE) 2016/680, che obbligano gli Stati Schengen a prevedere per la persona interessata il diritto di proporre reclamo all'autorità di controllo in materia di protezione dei dati e, se del caso, di interporre ricorso contro la decisione della suddetta autorità.

Secondo l'articolo 43 capoverso 1 D-LPD l'Incaricato può, d'ufficio o a querela, aprire un'inchiesta nei confronti di un organo federale se degli indizi lasciano presumere che un trattamento di dati potrebbe essere contrario alle disposizioni sulla protezione dei dati. La persona interessata può sporgere denuncia ma non ha qualità di parte nel procedimento (art. 43 cpv. 4 *a contrario* nonché art. 46 cpv. 2 D-LPD). Dato che la Svizzera è tenuta a riprendere e mettere in atto i requisiti della direttiva (UE) 2016/680, occorre introdurre un'eccezione a questo principio, ma unicamente per quanto riguarda i trattamenti di dati effettuati da un'autorità federale nel quadro di una procedura di cooperazione di polizia. In virtù dell'articolo 349*h* capoverso 1, la persona interessata che rende verosimile che uno scambio di dati personali che la concernono potrebbe violare le disposizioni sulla protezione dei dati (p. es. in relazione alle condizioni applicabili alla comunicazione di dati a uno Stato terzo o a un organo internazionale [art. 349*c* D-CP]) può dunque chiedere all'Incaricato di aprire un'inchiesta. Se la persona interessata non è in grado di rendere verosimile la violazione, l'Incaricato può dichiarare irricevibile la richiesta. Il capoverso 2 precisa che un'inchiesta può essere aperta unicamente nei confronti di un'autorità federale soggetta alla sorveglianza dell'Incaricato (cfr. il commento all'art. 349*g* cpv. 2 D-CP). Se del caso, l'Incaricato può ordinare provvedimenti cautelari o amministrativi nei confronti dell'autorità federale in questione (art. 44 e 45 D-LPD). L'Incaricato deve notificare la sua decisione all'autorità federale in questione e alla persona interessata, indicando loro i mezzi di ricorso.

Art. 355a cpv. 4

Il capoverso 4 è nuovo e precisa che gli scambi di dati personali con Europol sono equiparati a uno scambio con un'autorità competente di uno Stato Schengen (art. 349*b*). Secondo la considerazione 71 della direttiva (UE) 2016/680, gli accordi di cooperazione conclusi tra Europol e uno Stato terzo costituiscono un criterio determinante per valutare il livello di protezione dei dati dello Stato in questione. Si può dunque presumere che il legislatore dell'UE consideri che le prescrizioni di Europol in materia di protezione dei dati offrano una protezione adeguata.

Art. 355f e 355g

Queste disposizioni erano state introdotte in occasione del recepimento da parte della Svizzera della decisione quadro 2008/977/GAI.

L'articolo 355*f* CP disciplina la comunicazione di dati da uno Stato Schengen a uno Stato terzo o a un organo internazionale nel settore della cooperazione giudiziaria nell'ambito degli accordi di associazione a Schengen. Questa disposizione può essere abrogata poiché, per ragioni di sistematica, tale categoria di comunicazioni è disciplinata nel D-AIMP.

Contrariamente alla decisione quadro 2008/977/GAI, la direttiva (UE) 2016/680 non disciplina più la comunicazione di dati personali provenienti da uno Stato Schengen a una persona privata. L'articolo 355*g* può dunque essere abrogato.

9.3.2 Codice di procedura penale[305]

Art. 95a Trattamento di dati personali

La lettera a attua i requisiti di cui all'articolo 6 della direttiva (UE) 2016/680, che disciplina la distinzione tra differenti categorie di persone interessate. Questa disposizione tiene conto della problematica legata al possibile cambiamento delle categorie di persone interessate conseguente all'avanzamento della procedura. Secondo l'articolo 6 della direttiva (UE) 2016/680 si tratta ad esempio di distinguere tra indiziati e condannati, vittime e persone che alcuni fatti autorizzano a considerare potenziali vittime di reato o ancora altre parti quali i testimoni o le persone informate sui fatti. Per il legislatore europeo questa disposizione è particolarmente importante per i trattamenti di dati personali effettuati nel quadro della cooperazione di polizia o giudiziaria in materia penale, che implica necessariamente il trattamento di dati concernenti diverse categorie di persone interessate. Come risulta dalla considerazione 31 della suddetta direttiva, questa disposizione mira a garantire il diritto alla presunzione di innocenza (art. 10 cpv. 1 CPP).

La lettera a prescrive che l'autorità competente debba adottare le misure adeguate per distinguere nella misura del possibile le diverse categorie di persone interessate, disponendo di un certo margine di manovra. In effetti è possibile che in certi casi tale distinzione non possa essere effettuata, ad esempio se i fatti non consentono

[305] RS **312.0**

ancora di determinare se una persona è un testimone del reato o se vi ha partecipato come autore o complice.

La lettera b traspone i requisiti dell'articolo 7 della suddetta direttiva, che concerne la distinzione tra dati personali e verifica della qualità dei dati. Il paragrafo 1 obbliga gli Stati Schengen a distinguere nella misura del possibile i dati personali fondati su fatti da quelli fondati su valutazioni personali. Come risulta dalla sistematica dell'articolo 7, la disposizione concretizza il principio dell'esattezza e non può essere interpretato in maniera troppo restrittiva. In effetti la considerazione 30 della direttiva precisa che «… In particolare nei procedimenti giudiziari, le dichiarazioni contenenti dati personali sono basate sulla percezione soggettiva delle persone e non sempre sono verificabili. Il requisito dell'esattezza non dovrebbe pertanto riferirsi all'esattezza di una dichiarazione ma al semplice fatto che è stata rilasciata.» Le autorità penali mirano ad accertare la verità materiale al fine di garantire la giurisdizione penale. L'articolo 95*a* lettera b D-CPP mira al medesimo obiettivo. Il principio dell'esattezza vale in effetti per tutti i tipi di trattamento nella misura in cui i titolari del trattamento hanno, come tutte le persone coinvolte, un interesse preponderante che siano trattati esclusivamente dati attuali e pertinenti. L'articolo 143 CPP, che costituisce un caso d'applicazione dell'articolo 95*a* lettera b D-CPP, disciplina lo svolgimento dell'interrogatorio e al capoverso 5 dispone che con domande e obiezioni formulate in modo chiaro l'autorità penale deve mirare ad ottenere una deposizione completa e a chiarire le contraddizioni. Infine, riteniamo che l'articolo 95*a* non influisca sul giudizio di un giudice o sul decreto d'accusa emesso da un pubblico ministero. In effetti, allorquando il giudice o il pubblico ministero determina il movente dell'autore dell'infrazione o ne considera la situazione personale, la personalità o le circostanze attenuanti, non si tratta di una valutazione personale ma di elementi che fanno parte integrante della motivazione del giudizio o del decreto d'accusa e che non devono essere presentati separatamente.

Art. 98 cpv. 2

L'articolo 98 disciplina il requisito dell'esattezza dei dati.

Per quanto concerne la modifica apportata al capoverso 2 si rinvia al commento all'articolo 349*f* capoverso 2 D-CP (n. 9.3.1).

9.3.3 Assistenza internazionale in materia penale del 20 marzo 1981[306]

Il D-LPD non si applica alle procedure di assistenza giudiziaria (art. 2 cpv. 3 D-LPD). Il presente disegno introduce dunque nell'AIMP un nuovo capitolo 1*b* sulla protezione dei dati che attua i requisiti della direttiva (UE) 2016/680. In effetti, i trattamenti di dati personali effettuati nel quadro di una procedura di assistenza giudiziaria rientrano nel campo d'applicazione della normativa europea.

306 RS **351.1**

Il capitolo 1*b* non si applica soltanto alle autorità federali (p. es. l'UFG o il Ministero pubblico della Confederazione) ma anche alle autorità cantonali che collaborano a una procedura di assistenza giudiziaria o incaricate di decidere su una domanda di cooperazione dello Stato estero (art. 1 cpv. 1 AIMP). In questo caso la Confederazione si avvale della sua competenza di legiferare poiché il settore della cooperazione internazionale in materia penale è retto dal diritto federale.

Le pretese in materia di protezione dei dati sono trattate nel quadro della procedura di assistenza giudiziaria pendente e sottostanno ai medesimi rimedi di diritto.

Art. 11b Diritto d'accesso nel quadro di una procedura pendente

Questa disposizione accorda alle persone oggetto di una domanda di assistenza internazionale in materia penale il diritto di esaminare i dati personali e mette dunque in atto i requisiti della direttiva (UE) 206/680 (art. 14 e 18).

Secondo il capoverso 1, oltre ai propri dati personali, le persone interessate devono ricevere tutte le informazioni elencate alle lettere a–e, ossia lo scopo e la base legale del trattamento (lett. a), la durata di conservazione dei dati personali o, se ciò non è possibile, i criteri per determinare tale durata (lett. b), i destinatari o le categorie di destinatari (lett. c), le informazioni disponibili sulla provenienza dei dati personali (lett. d), nonché le informazioni necessarie per far valere i suoi diritti (lett. e). L'autorità competente deve ad esempio comunicarle che le sue pretese in materia di protezione dei dati sono trattate nel quadro della procedura di assistenza giudiziaria pendente e sottostanno ai medesimi rimedi di diritto.

Il diritto d'accesso della persona interessata non è tuttavia assoluto. Secondo il capoverso 2, la competente autorità può negare, limitare o posporre l'informazione in presenza di uno dei motivi di cui all'articolo 80*b* capoverso 2 o se una delle condizioni elencate alle lettere a–c è adempiuta. L'autorità deve motivare la decisione di negare l'accesso in modo da non divulgare le informazioni sulle quali si fonda tale decisione.

Art. 11c Restrizione del diritto d'accesso applicabile alle domande di arresto ai fini dell'estradizione

Questa disposizione introduce una restrizione del diritto d'accesso applicabile ai dati personali trattati nel quadro delle domande di arresto ai fini dell'estradizione. Si tratta di un disciplinamento del cosiddetto «diritto d'accesso indiretto» che s'ispira alla soluzione prevista all'articolo 8 LSIP adeguandolo alle modifiche apportatevi dal presente disegno (cfr. n. 9.3.7). L'articolo 11*c* tiene pure conto dell'articolo 17 della direttiva (UE) 2016/680, che obbliga gli Stati Schengen a prevedere il diritto della persona interessata di chiedere, in caso di restrizione del suo diritto d'accesso, all'autorità di controllo in materia di protezione dei dati di verificare la liceità di un trattamento di dati che la concernono.

Cpv. 1

Il capoverso 1 determina l'autorità, ossia l'UFG, cui compete rispondere a una persona che desidera sapere se uno Stato estero ha presentato alla Svizzera una doman-

da di arresto ai fini dell'estradizione nei suoi confronti. Qualsiasi altra autorità federale o cantonale confrontata con tale domanda non può trattarla e deve trasmetterla senza indugio all'UFG.

Cpv. 2–6

Secondo il capoverso 2, la persona che chiede all'UFG se ha ricevuto una domanda di arresto ai fini dell'estradizione di uno Stato estero riceve una risposta sempre identica, ossia che nessun dato che la concerne è trattato in modo illecito e che può chiedere all'Incaricato se gli eventuali dati che la concernono sono trattati conformemente al diritto. La persona interessata non viene quindi a sapere se nei suoi confronti è stata presentata una domanda di arresto ai fini dell'estradizione. Attualmente la situazione relativa al diritto d'accesso diretto della persona interessata non è soddisfacente. In effetti, un tale diritto permetterebbe in linea di massima a chiunque di sapere se è ricercato. Il diritto d'accesso può essere rifiutato, ma una simile decisione deve essere motivata. Il semplice fatto di rifiutare l'informazione può però suggerire al richiedente che egli è effettivamente oggetto di una domanda d'arresto ai fini dell'estradizione. Con l'introduzione di un diritto d'accesso indiretto il disegno di legge mira a evitare che persone ricercate possano venire a sapere in quali Paesi possono recarsi senza correre il rischio di farsi arrestare ai fini dell'estradizione. Il disciplinamento previsto all'articolo 11*c* è inoltre di durata limitata. Infatti, se è arrestata in Svizzera la persona interessata può avvalersi di tutti i diritti conferitigli dall'AIMP nel quadro della procedura d'estradizione.

Come indicato sopra, la persona interessata ha il diritto di chiedere all'Incaricato di verificare la liceità del trattamento (cpv. 2). Questa soluzione costituisce un buon compromesso tra l'interesse della persona in questione alla protezione della sua sfera privata e l'interesse pubblico a non mettere a rischio il perseguimento penale di uno Stato estero. Le comunicazioni dell'Incaricato sono formulate in maniera sempre identica: egli comunica alla persona interessata che nessun dato che la concerne è trattato in modo illecito oppure che in caso di errori nel trattamento dei dati personali ha aperto un'inchiesta conformemente all'articolo 43 D-LPD. Questa disposizione va interpretata e applicata alla stregua di altri diritti d'accesso indiretti del diritto federale, in particolare quelli previsti negli articoli 8 LSIP e 18 capoverso 4 LMSI.

In virtù del capoverso 3, l'Incaricato esegue la verifica chiesta limitandosi a controllare la liceità del trattamento dal punto di vista delle esigenze della protezione dei dati e non per quanto riguarda il rispetto delle condizioni applicabili alla cooperazione internazionale in materia penale. Se constata un errore nel trattamento dei dati può ordinare all'UFG di porvi rimedio. Ciò potrebbe essere il caso se la sicurezza del trattamento non è garantita o se autorità o terzi non autorizzati hanno accesso ai dati.

I capoversi 3–6 sono identici alle corrispondenti disposizioni dell'articolo 349*g* D-CP (cfr. n. 9.3.1).

Cpv. 7

Il capoverso 7 dispone che in deroga al capoverso 2 l'UFG può, d'intesa con lo Stato richiedente, fornire alla persona interessata le informazioni richieste.

Art. 11d Diritto di rettifica e cancellazione di dati personali

Questa disposizione disciplina i diritti di rettifica e cancellazione della persona oggetto di una domanda di cooperazione internazionale in materia penale. Attua i requisiti della direttiva (UE) 2016/680 (art. 16 e 18).

In virtù del capoverso 1, la persona oggetto di una domanda di cooperazione internazionale in materia penale può esigere dalla competente autorità che i suoi dati personali trattati in violazione dell'AIMP siano rettificati o cancellati, segnatamente se sono inesatti. Può ad esempio chiedere che dati personali concernenti la sua identità (cognome e nome, sesso, data di nascita, nazionalità, luogo di nascita) siano corretti e completati. Il principio dell'esattezza vale per tutti i tipi di trattamento, in quanto le autorità, così come tutte le persone coinvolte, hanno un interesse preponderante che siano trattati unicamente dati attuali e pertinenti. Spetta alla persona interessata dimostrare l'inesattezza dei dati personali. Il diritto di rettifica e cancellazione non vale tuttavia per tutti i dati personali. In particolare non è possibile esigere la rettifica o la cancellazione del contenuto materiale di dati personali acquisiti a scopi probatori o relativi a reati sui quali si fonda la domanda di cooperazione internazionale in materia penale. Secondo il capoverso 4, infatti, la verifica dell'esattezza dei dati personali compete alla pertinente autorità estera. La persona oggetto di una domanda di cooperazione internazionale non può dunque contestare l'esattezza dei dati presso la competente autorità dello Stato richiesto; se del caso deve contestarla presso la competente autorità dello Stato richiedente.

Il capoverso 2 prevede una misura meno radicale: invece di cancellare i dati personali, a determinate condizioni la competente autorità può limitarne il trattamento. Questa misura significa che il trattamento dei dati rimane possibile, ma unicamente se persegue determinati scopi. Come emerge dalla considerazione 47 della direttiva (UE) 2016/680, la limitazione del trattamento va interpretata nel senso che l'autorità può trattare i dati in questione soltanto per gli scopi che hanno impedito la loro cancellazione. Il capoverso 2 prevede tre fattispecie.

Secondo il capoverso 2 lettera a, la competente autorità limita il trattamento dei dati personali se la persona interessata contesta l'esattezza dei dati personali e la loro esattezza o inesattezza non può essere dimostrata. In questo caso la limitazione del trattamento significa che l'autorità può trattare i dati personali controversi soltanto allo scopo di determinarne l'esattezza o l'inesattezza. L'autorità può ad esempio comunicarli all'autorità estera che glieli ha trasmessi perché ne verifichi l'esattezza. Una volta che quest'ultima è stata dimostrata, l'autorità può proseguire il trattamento dei dati senza alcuna limitazione. Se invece i dati personali risultano essere inesatti, l'autorità deve cancellarli, a meno che non siano applicabili le lettere b o c.

Il capoverso 2 lettera b dispone che l'autorità competente deve limitare il trattamento dei dati se è necessario per proteggere interessi preponderanti, in particolare quelli di cui all'articolo 80*b* capoverso 2. In questo caso l'autorità deve limitare il trattamento nel senso che può continuare a trattare i dati personali soltanto agli scopi che ne hanno impedito la cancellazione. Può dunque comunicarli all'autorità estera per salvaguardare interessi preponderanti.

In virtù del capoverso 2 lettera c, la competente autorità può limitare il trattamento dei dati se la cancellazione dei dati personali rischia di compromettere una procedura di cooperazione internazionale in materia penale o la procedura estera su cui si fonda la domanda di cooperazione in materia penale. In questo caso i dati personali possono essere comunicati a un'autorità estera poiché la loro cancellazione ostacolerebbe lo svolgimento corretto della procedura.

Il capoverso 3 dispone che la competente autorità debba avvisare immediatamente l'autorità che le ha trasmesso o messo a disposizione i dati personali o alla quale li ha comunicati in merito alle misure adottate secondo i capoversi 1 e 2

Il capoverso 4, infine, dispone che la verifica dell'esattezza di dati personali acquisiti a scopi probatori o relativi a reati sui quali si fonda la domanda di cooperazione internazionale in materia penale compete alla pertinente autorità estera. L'obiettivo dell'assistenza giudiziaria internazionale in materia penale è che uno Stato esegua misure adeguate volte ad agevolare il perseguimento e la repressione di reati in un altro Stato. Sono dunque avviati due procedure: da un lato il procedimento penale estero e dall'altro la procedura di assistenza giudiziaria dinanzi alla competente autorità. La seconda procedura è al servizio della prima. L'esattezza dei dati personali acquisiti a scopi probatori (p. es. estratti bancari, registrazioni o verbali dell'interrogatorio di testimoni) o relativi a reati sui quali si fonda la domanda di cooperazione internazionale in materia penale (p. es. i fatti, la qualifica dei reati, la qualità della persona coinvolta nel procedimento penale) non potrebbe essere verificata dalla competente autorità dello Stato richiesto nel quadro di una procedura di assistenza. L'obiettivo del procedimento penale estero è infatti proprio la determinazione dell'esattezza o dell'inesattezza dei dati personali. Conformemente alla massima dell'istruzione, la competente autorità penale è tenuta d'ufficio ad acquisire tutti i fatti pertinenti per la qualifica dell'atto e il giudizio a favore o sfavore dell'indagato. È in questo contesto che l'esattezza dei dati personali acquisiti a scopi probatori o relativi a reati sui quali si fonda la domanda di cooperazione internazionale in materia penale deve essere verificata.

Art. 11e Parità di trattamento

Questa disposizione disciplina la parità di trattamento delle autorità degli Stati Schengen e delle autorità nazionali in materia di protezione dei dati. Essa attua l'articolo 9 capoversi 3 e 4 della direttiva (UE) 2016/680.

Quest'ultimo va interpretato in combinazione con l'articolo 60 della medesima direttiva, secondo cui rimangono impregiudicate le disposizioni specifiche contenute in atti giuridici dell'Unione europea che sono entrati in vigore prima dell'adozione della direttiva (UE) 2016/680 e che disciplinano il trattamento tra Stati membri (cfr. anche la consid. 94). Secondo questa interpretazione, la dichiarazione congiunta della Svizzera e dell'Unione europea in merito all'articolo 23 capoverso 7 dell'Accordo del 29 maggio 2000[307] relativo all'assistenza giudiziaria in materia penale tra gli Stati membri dell'UE è fatta salva.

307 Accordo tra la Confederazione Svizzera, l'Unione europea e la Comunità europea, riguardante l'associazione della Svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen concluso il 26 ottobre 2004; RS **0.362.31**.

L'articolo 11*e* rispetta il principio della specialità ai sensi dell'articolo 67 AIMP. Secondo tale principio le informazioni e i documenti ottenuti mercé l'assistenza non possono essere usati nello Stato richiedente né a scopo d'indagine né come mezzi di prova in procedimenti vertenti su fatti per cui l'assistenza è inammissibile.

Per il rimanente si rinvia al commento all'articolo 349*c* D-CP (n. 9.3.1).

Art. 11f Comunicazione di dati personali a uno Stato terzo o a un organo internazionale

Questa disposizione disciplina la comunicazione di dati a uno Stato terzo o a un organo internazionale. Il suo tenore corrisponde sostanzialmente a quello dell'articolo 349*c* D-CP. Contrariamente al capoverso 3 di quest'ultimo, l'articolo 11*f* non prevede tuttavia per le autorità federali un obbligo di comunicare all'Incaricato le categorie di comunicazioni di dati personali effettuate conformemente all'articolo 11*f* capoverso 2 lettera c o le comunicazioni di dati personali effettuate in virtù del capoverso 3. Questa differenza è giustificata dal fatto che all'Incaricato non compete la sorveglianza dei trattamenti di dati effettuati nel quadro di una procedura di assistenza giudiziaria internazionale in materia penale (cfr. il commento all'art. 3 cpv. 2 lett. e D-LPD). Per il rimanente si rinvia per analogia al commento all'articolo 349*d* D-CP (n. 9.3.1).

Art. 11g Comunicazione a uno Stato terzo o a un organo internazionale di dati personali provenienti da uno Stato Schengen

Questa disposizione disciplina la comunicazione di dati provenienti da uno Stato Schengen a uno Stato terzo o a un organo internazionale. Il tenore di questa disposizione corrisponde in sostanza a quello dell'articolo 349*d* D-CP. Tuttavia, in deroga al capoverso 1 lettera a di quest'ultimo, l'articolo 11*g* capoverso 1 lettera a contempla anche l'ipotesi che i dati ricevuti da uno Stato Schengen siano comunicati a uno Stato terzo per eseguire una decisione penale, il che rientra nell'assistenza giudiziaria. Per il rimanente si rinvia per analogia al commento relativo all'articolo 349*d* D-CP (n. 9.3.1).

Art. 11h Procedura di comunicazione di dati personali

Questa disposizione disciplina le modalità applicabili alle comunicazioni di dati personali. Corrisponde all'articolo 349*f* cpv. 3–5 D-CP (cfr. il relativo commento al n. 9.3.1).

9.3.4 Legge federale del 22 giugno 2001[308] sulla cooperazione con la Corte penale internazionale

Art. 2a Protezione di dati personali

Al fine di trasporre i requisiti della direttiva (UE) 2016/680 è necessario introdurre in questa legge un rinvio agli articoli 11*b*–11*d* e 11*f*–11*h* D-AIMP. L'articolo 11*e* è escluso da tale rinvio poiché disciplina la parità di trattamento tra le autorità degli Stati Schegen e non è dunque applicabile alla Corte penale internazionale.

9.3.5 Legge federale del 3 ottobre 1975[309] relativa al Trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale

Art. 9a Protezione di dati personali

Al fine di trasporre i requisiti della direttiva (UE) 2016/680 è necessario introdurre in questa legge un rinvio agli articoli 11*b,* 11*d* e 11*f*–11*h* D-AIMP.

9.3.6 Legge federale del 7 ottobre 1994[310] sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati

Art. 13 cpv. 2

Al fine di attuare i requisiti della direttiva (UE) 2016/680 è necessario adeguare l'articolo 13 capoverso 2 introducendovi un rinvio agli articoli 349*a*–349*h* D-CPP.

9.3.7 Legge federale del 13 giugno 2008[311] sui sistemi d'informazione di polizia della Confederazione

Art. 7 cpv. 2

Il capoverso 2 fa salvo anche il nuovo articolo 8*a* D-LSIP.

308 RS **351.6**
309 RS **351.93**
310 RS **360**
311 RS **361**

Art. 8 Restrizione del diritto d'accesso concernente il sistema di trattamento dei dati relativi ai reati federali

Questo articolo deve essere modificato poiché in virtù del D-LPD l'Incaricato non emana più raccomandazioni, bensì può aprire un'inchiesta ai sensi dell'articolo 43 D-LPD e se del caso ordinare misure amministrative in virtù degli articoli 44 e 45 D-LPD.

Il capoverso 1 rimane immutato rispetto al diritto vigente.

Il capoverso 2 è modificato dal punto di vista redazionale.

Il capoverso 3 è modificato in quanto la proposizione «che ha inviato a fedpol una raccomandazione ai sensi dell'articolo 27 LPD affinché tali errori vengano corretti» è sostituito da «che ha aperto un'inchiesta conformemente all'articolo 43 LPD». Inoltre, visto che gli articoli 44 e 45 D-LPD conferiscono all'Incaricato competenze decisionali, l'intervento del Tribunale amministrativo federale previsto dal secondo periodo della LSIP vigente non è più necessario e la pertinente disposizione può essere abrogata.

Il vigente capoverso 4 può essere abrogato. Il rinvio all'articolo 43 D-LPD è sufficiente. Secondo il nuovo capoverso 4, sulla base dell'inchiesta l'Incaricato può emanare una decisione (art. 45 D-LPD) che fedpol può impugnare.

Il capoverso 5 prevede che le comunicazioni di cui ai capoversi 2 e 3 abbiano sempre il medesimo tenore e che non vengano motivate, nonché che la comunicazione di cui al capoverso 3 non sia impugnabile.

Il capoverso 6 riprende senza modifiche il vigente capoverso 7.

Il capoverso 7 riprende il capoverso 8 vigente ma è modificato in quanto, se le condizioni sono soddisfatte, l'Incaricato può anche ordinare, e non più solo raccomandare, a fedpol di fornire alla persona interessata le informazioni richieste.

Art. 8a Restrizione del diritto d'accesso in caso di segnalazioni in vista dell'arresto ai fini dell'estradizione

Questa disposizione introduce una restrizione del diritto d'accesso in caso di segnalazioni in vista dell'arresto ai fini dell'estradizione che figurano in uno dei sistemi enumerati all'articolo 2 LSIP. Se la domanda della persona interessata non concerne uno di questi sistemi, secondo l'articolo 11*c* capoverso 1 D-AIMP fedpol è tenuto a trasmetterla all'UFG.

Per il rimanente si rimanda al commento all'articolo 11*c* D-AIMP (n. 9.3.3).

9.3.8 Legge del 12 giugno 2009[312] sullo scambio di informazioni con gli Stati Schengen

Art. 2 cpv. 3

Il rinvio agli articoli 6*a*–6*c* LSIS è sostituito con un rinvio agli articoli 349*a*–349*h* D-CP.

Art. 6a–6c

Gli articoli 6*a*–6*c* LSIS sono stati inseriti nella legge per attuare la decisione quadro 2008/977/GAI. Al fine di ridurre la densità normativa della legislazione federale, il nostro Consiglio propone di abrogare questa disposizione e introdurre un rinvio agli articoli 349*a*–349*h* D-CPP.

10 Entrata in vigore

È previsto che il Consiglio federale determini l'entrata in vigore della futura legge.

Come indicato al numero 2.2, la Svizzera ha un termine massimo di due anni a contare dalla data della notifica da parte dell'UE per recepire e attuare la direttiva (UE) 2016/680 nel suo ordinamento giuridico. La direttiva le è stata notificata il 1° agosto 2016 e pertanto il suddetto termine decade il 1° agosto 2018. Riteniamo che, pur essendo possibile, la soluzione di prevedere due diverse entrate in vigore per i settori pubblico e privato (innanzitutto per gli organi federali e a una data successiva per le persone private) non è opportuna. Il regolamento (UE) 2016/679 è infatti applicabile agli Stati membri dell'UE dal 25 maggio 2018 (art. 99). È nell'interesse della Svizzera che il presente disegno di legge entri in vigore il più rapidamente possibile fatte salve determinate disposizioni transitorie. In tal modo è possibile rispettare in linea di massima il termine di due anni previsto dagli obblighi di Schengen per la trasposizione della direttiva (UE) 2016/680.

11 Ripercussioni

Le ripercussioni del disegno e del recepimento della direttiva sono strettamente connesse e non sono pertanto illustrate separatamente.

312 RS **362.2**

11.1 Ripercussioni finanziarie e sull'effettivo del personale della Confederazione

11.1.1 Ripercussioni finanziarie e sull'effettivo del personale dell'Incaricato

Il disegno di legge introduce una serie di misure che comportano nuovi compiti per l'Incaricato. Le misure risultano in parte dalle esigenze del diritto europeo (P-STE 108, direttiva (UE) 2016/680 e regolamento (UE) 2016/679) e sono necessarie affinché la Svizzera possa continuare a garantire una protezione dei dati adeguata in rapporto agli standard dell'UE e adempiere i suoi obblighi risultanti dall'Accordo di associazione a Schengen. Alcune misure soddisfano un'esigenza dell'economia e mirano a facilitare alle imprese l'applicazione della legge. Dato che considerato l'esteso campo d'applicazione della direttiva (UE) 2016/679 (art. 3) numerose imprese svizzere vi saranno prevedibilmente assoggettate, è importante che il disegno non ne differisca troppo. A prescindere dalla questione della decisione di adeguatezza, per motivi di economicità e certezza giuridica le imprese devono infatti sviluppare una condotta aziendale ed emanare prescrizioni interne molto simili indipendentemente dall'assoggettamento al diritto europeo o nazionale.

A seguito dei suoi nuovi compiti, l'Incaricato necessita risorse di personale e informatiche supplementari. Va sottolineato che l'Unione europea ritiene che l'assegnazione di risorse sufficienti all'Incaricato costituisce un elemento importante per quanto riguarda sia la decisione di adeguatezza sia la trasposizione dell'acquis di Schengen. L'obbligo di attribuire alle autorità di controllo risorse sufficienti – di centrale importanza per la loro indipendenza – è difatti sancito in tutti gli atti normativi europei (art. 12bis cpv. 5 P-STE 108, art. 42 cpv. 4 della direttiva [UE] 2016/680 e art. 52 cpv. 4 del regolamento [EU] 2016/679). Per valutare l'adeguatezza della protezione dei dati si analizza anche l'effettiva attuazione delle misure. La prossima valutazione Schengen, nel 2018, comprenderà anche questo aspetto. Il gruppo delle autorità di controllo per SIS II si è recentemente rivolto alla Commissione europea, al Parlamento europeo e al Consiglio dell'UE chiedendo di garantire che le autorità di controllo ottengano realmente risorse finanziarie e di personale adeguate ai loro compiti legali.

11.1.1.1 Fabbisogno di personale

Il fabbisogno di personale supplementare dell'Incaricato non è statico né lineare e evolverà con il tempo. All'inizio i codici di condotta sottopostigli saranno probabilmente pochi, dato che le categorie professionali necessiteranno di tempo per elaborarle. Numerose misure sono inoltre collegate tra loro, cosicché il lavoro svolto per adottare una misura in un settore potrà servire anche in un altro settore. In relazione ai codici di condotta, ad esempio, la consultazione dell'Incaricato, che incoraggerà un comportamento conforme alla legge, contribuirà prevedibilmente a ridurre la necessità di aprire inchieste. Anche i compiti di controllo preventivi dell'Incaricato aumenteranno il rispetto della legislazione, riducendo a loro volta le inchieste. Al fine di valutare il più esattamente possibile il reale fabbisogno dell'Incaricato, pro-

poniamo dunque, da un lato, di accordare le risorse di personale in maniera scaglionata (cfr. la tabella) e, dall'altro, di valutare nuovamente il fabbisogno dopo al massimo cinque anni dall'entrata in vigore della legge.

È difficile effettuare stime precise. Abbiamo pertanto tentato di illustrare le ipotesi alla base della sua valutazione per ogni nuovo compito comportante un fabbisogno di personale supplementare. Questo modo di procedere è utile anche in vista della valutazione del fabbisogno in un ritmo quinquennale. Col tempo, infatti, il fabbisogno potrebbe ridursi in alcuni settori. Se possibile e conformemente al principio della copertura dei costi, i nuovi posti saranno finanziati tramite gli emolumenti (art. 53 D-LPD).

Secondo le stime, il fabbisogno di personale supplementare dell'Incaricato ammonta a dieci posti (giuristi e informatici nella classe di salario 24 per un totale di 1 800 000 franchi) distribuiti come segue.

– Secondo l'articolo 10 D-LPD, le associazioni professionali e dell'economia nonché gli organi federali possono sottoporre all'Incaricato dei *codici di condotta*. L'Incaricato deve esprimersi in merito e pubblicare il suo parere. L'elaborazione di codici di condotta da parte delle categorie professionali e i relativi pareri dell'Incaricato sono intesi consentire l'autoregolazione nel settore privato. I codici di condotta possono precisare la legge e dunque essere attuati specificatamente al settore d'attività[313]. Rispondono a un'esigenza di certezza giuridica identificato nella valutazione d'impatto della regolamentazione (cfr. n. 1.8).

  Sebbene non siano vincolanti, a lungo termine i codici di condotta miglioreranno l'applicazione della legge e ridurranno in tal modo il numero delle inchieste avviate dall'Incaricato. Coloro che sottopongono il loro codice di condotta all'Incaricato saranno inoltre esonerati, a determinate condizioni, dall'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (art. 20 cpv. 5 D-LPD). Anche l'Incaricato ne risulterà sgravato, in quanto in seguito non dovrà più essere previamente consultato (art. 21 D-LPD).

  La promozione dell'autoregolazione è una misura contemplata dal regolamento (UE) 2016/679 (art. 40). Diversamente dal D-LPD, l'atto normativo europeo prevede però che l'autorità di controllo approvi il codice, che in tal modo assume un carattere vincolante per i titolari che vi aderiscono. Abbiamo rinunciato ad adottare una simile soluzione, che avrebbe comportato costi maggiori dato che l'Incaricato avrebbe dovuto approvare i codici mediante una decisione impugnabile.

  Il numero di codici di condotta sottoposti annualmente all'Incaricato è stimato a dieci. L'onere lavorativo connesso varierà a seconda della complessità e della lunghezza del codice. È tuttavia ipotizzabile che la valutazione dei codici impiegherà in media una persona a tempo pieno. Prevediamo che nel primo anno saranno presentati pochi codici, dato che dovranno prima essere elaborati, e riteniamo che dopo qualche anno il numero di codici diminuirà

313 Cfr. p. es. il codice di condotta dell'Union française du marketing del 17 mar. 2005 all'indirizzo: www.cnil.fr/sites/default/files/typo/document/projet-codeUFMD.pdf.

poiché il numero di organizzazioni autorizzate è limitato. Per questo motivo sono stati previsti un posto a metà tempo per il primo e il quinto anno e un posto a tempo pieno per il secondo, il terzo e il quarto anno, nell'ipotesi che questi tre saranno gli anni più carichi.

Il posto potrà presumibilmente essere finanziato per circa il 60 per cento tramite gli emolumenti. Dato che la promozione dell'autoregolazione risponde a un interesse pubblico, in determinati casi l'Incaricato può rinunciare alla riscossione degli emolumenti in applicazione dell'articolo 3 capoverso 2 lettera a OgeEm.

– Secondo l'articolo 13 capoverso 2 lettere d ed e D-LPD, per la comunicazione di dati personali all'estero i titolari devono far approvare all'Incaricato *clausole tipo* e *norme vincolanti d'impresa* volte a garantire una protezione dei dati appropriata. L'approvazione da parte dell'Incaricato soddisfa un'esigenza del diritto europeo (art. 12bis cpv. 2 lett. b P-STE 108 e art. 46 cpv. 2 lett. b e d nonché art. 47 del regolamento [UE] 2016/679). L'Incaricato deve quindi esaminare i documenti sottopostigli e se del caso approvarli. Ciò costituisce un elemento centrale per garantire una protezione appropriata dei dati ai fini della decisione di adeguatezza dell'UE e dell'adempimento delle esigenze del P-STE 108. L'Incaricato statuirà in merito all'approvazione tramite decisione. Come i codici di condotta, anche questo controllo preventivo da parte dell'Incaricato contribuirà a migliorare il rispetto delle norme sulla protezione dei dati e a lungo termine ridurrà le inchieste aperte.

  Il numero di clausole tipo e norme vincolanti d'impresa sottoposte all'Incaricato è stimato a una ventina all'anno. L'onere lavorativo dipenderà principalmente dalla complessità e lunghezza dei documenti. È ipotizzabile che il loro esame impiegherà una persona a tempo pieno, ma che il fabbisogno di personale per svolgere questo nuovo compito diminuirà con il passare del tempo, dato che il numero di clausole tipo e norme vincolanti d'impresa che devono essere emanate è limitato. Il posto potrà presumibilmente essere finanziato per circa il 60 per cento tramite gli emolumenti. Anche qui, in determinati casi l'Incaricato potrà rinunciare alla riscossione degli emolumenti in applicazione dell'articolo 3 capoverso 2 lettera a OgeEm.

– Secondo l'articolo 21 D-LPD, l'Incaricato deve essere previamente consultato se da una valutazione d'impatto sulla protezione dei dati (art. 20 D-LPD) emerge che il trattamento previsto presenterebbe un rischio elevato per la personalità o i diritti fondamentali della persona interessata qualora il titolare del trattamento non adottasse alcuna misura. Più precisamente, l'Incaricato deve essere consultato se il titolare ritiene che il rischio non possa essere contenuto mediante misure ragionevoli in considerazione delle tecnologie disponibili e dei costi d'implementazione. L'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati è un'esigenza del diritto europeo (art. 8bis cpv. 2 P-STE 108, art. 27 della direttiva [UE] 2016/680 e art. 35 del regolamento [UE] 2016/679). La consultazione preventiva dell'autorità di controllo nell'ambito della protezione dei dati è esplicitamente prevista nella direttiva (UE) 2016/680 (art. 28) e del regolamento (UE) 2016/679 (art. 36).

A seguito di questo nuovo compito l'Incaricato deve esaminare approfonditamente le valutazioni d'impatto sottopostegli, i trattamenti di dati previsti e le misure proposte dai titolari e prendere posizione in merito entro un termine (prorogabile di un mese) di due mesi. Se ha obiezioni deve proporre misure adeguate. Si tratta di una procedura obbligata e sovente complessa per la quale devono essere impiegati un giurista e un informatico. Con la progressiva evoluzione dell'economia digitale, i trattamenti di dati che potrebbero comportare un rischio elevato per la personalità o i diritti fondamentali delle persone interessate sono destinati ad aumentare di numero e complessità, cosicché anche lo strumento della valutazione dell'impatto sulla protezione dei dati crescerà d'importanza.

Il numero di esami è stimato va da dieci a quindici all'anno. Questo nuovo compito richiederà tre posti supplementari. In considerazione del fatto che per due anni dopo l'entrata in vigore l'articolo 21 D-LPD sarà applicabile unicamente ai trattamenti di dati secondo gli articoli 1 e 2 della direttiva (UE) 2016/680 (art. 63 cpv. 2 D-LPD), proponiamo di creare, allo scadere di tale termine, due dei tre posti supplementari per l'esame delle valutazioni d'impatto. Il posto supplementare a partire dall'entrata in vigore della legge è motivato dal fatto che l'Incaricato deve definire le procedure interne per questo nuovo compito al fine di essere operativo al momento opportuno (informatica, istruzioni). Data la complessità dello strumento della valutazione d'impatto, occorre inoltre svolgere un importante lavoro di sensibilizzazione presso i titolari del trattamento. A lungo termine le misure dovrebbero promuovere un'applicazione corretta della legge e ridurre il numero di inchieste avviate dall'Incaricato. I posti necessari dovrebbero poter essere finanziati quasi interamente mediante gli emolumenti.

– Mentre secondo il diritto vigente i casi in cui può farlo sono limitati (art. 29 LPD), con il disegno di legge l'Incaricato apre un'*inchiesta* se indizi lasciano presumere una violazione delle disposizioni sulla protezione dei dati. In casi di poca importanza può rinunciare ad aprire un'inchiesta (art. 43 cpv. 2 D-LPD). Mentre attualmente è unicamente autorizzato a emanare raccomandazioni, in futuro potrà pronunciare decisioni vincolanti, ad esempio anche vietando un trattamento di dati (art. 43 segg. D-LPD), ed esaminare le comunicazioni di violazione della sicurezza dei dati ai sensi dell'articolo 22 D-LPD. Queste nuove competenze rispondono a esigenze del diritto europeo (art. 7 cpv. 2 e 12bis cpv. 2 lett. a e c P-STE 108, art. 30 e 47 della direttiva [UE] 2016/680 e art. 33 e 58 cpv. 1 lett. b e cpv. 2 del regolamento [UE] 2016/679) e sono dunque molto importanti per la decisione di adeguatezza nonché per l'adempimento dei requisiti del P-STE e della direttiva (UE) 2016/680. È d'uopo ricordare che già nel quadro della valutazione di Schengen del 2014 (cfr. n. 1.2.2.3) gli esperti europei hanno raccomandato alla Svizzera di attribuire all'Incaricato competenze decisionali.

L'Incaricato sarà chiamato a svolgere altri compiti di vigilanza previsti nel quadro della cooperazione Schengen in materia penale. Su richiesta della persona i cui diritti sono stati limitati (art. 349*g* D-CP e 11*c* D-AIMP) dovrà ad esempio in particolare verificare la conformità legale del trattamento dei dati.

Il numero delle inchieste che saranno svolte dall'Incaricato è stimato da 15 a 20 all'anno, mentre quello delle comunicazioni di violazioni della sicurezza dei dati da cinque a dieci all'anno. L'adempimento di questi nuovi compiti richiederà tre posti supplementari per un team interdisciplinare di due giuristi e un informatico. Reputiamo però che questo fabbisogno dovrebbe diminuire dopo un paio d'anni poiché è presumibile che con il tempo i titolari conosceranno bene le disposizioni vigenti e le applicheranno correttamente. Le decisioni dell'Incaricato e le eventuali sanzioni penali delle autorità cantonali produrranno inoltre prevedibilmente incentivi positivi. Per questi motivi proponiamo di ridurre l'effettivo dopo quattro anni (ossia 2022–2023) da tre a due posti e mezzo.

Dato che riguardano compiti di vigilanza propriamente detti, questi posti potranno essere finanziati tramite gli emolumenti soltanto nella misura del 30 per cento. Segnaliamo tuttavia di aver rinunciato a introdurre sanzioni amministrative considerate le maggiori risorse che un simile regime richiederebbe a causa delle garanzie procedurali supplementari ad esso connesse.

– L'articolo 49 D-LPD disciplina l'*assistenza amministrativa* tra l'Incaricato e le autorità estere incaricate della protezione dei dati. In considerazione del carattere sempre più transfrontaliero dei trattamenti di dati, la cooperazione tra le autorità nazionali di protezione dei dati è indispensabile e costituisce un'esigenza del diritto europeo (art. 12bis cpv. 7 e 13 segg. P-STE 108, art. 46 cpv. 1 lett. h e 50 della direttiva [UE] 2016/680 e art. 57 cpv. 1 lett. g e 61 del regolamento [UE] 2016/679). Il fabbisogno di personale supplementare ammonterà prevedibilmente a un posto, per il quale non è previsto alcun autofinanziamento.

– Il nuovo *Privacy Shield* tra la Svizzera e gli USA (cfr. n. 5) richiede parimenti risorse supplementari. Le ripercussioni finanziarie per l'Incaricato in questo settore sono già state annunciate al nostro Consiglio l'11 gennaio 2017, quando ha preso atto del nuovo quadro legale per la comunicazione di dati personali dalla Svizzera a imprese con sede negli Stati Uniti.

  Per l'Incaricato il Privacy Shield comporta determinati compiti di cooperazione. Deve ad esempio inoltrare i reclami delle persone interessate alla Federal Trade Commission, al Department of Commerce o al mediatore del Department of State e le domande di informazioni a quest'ultimo. Dato che negli Stati Uniti i trattamenti di dati sono sempre più esternalizzati e che in Svizzera oggigiorno il ricorso a servizi di imprese americane come Facebook, Google o Apple è sempre più diffuso, è ipotizzabile che il numero di reclami e domande che l'Incaricato dovrà trattare aumenterà fortemente. In due casi le imprese certificate secondo il Privacy Shield devono collaborare con l'Incaricato: se dati relativi alle risorse umane di imprese svizzere sono trattati, devono cooperare con l'Incaricato in tutte le questioni inerenti alla protezione dei dati. Le imprese possono scegliere volontariamente questa forma di cooperazione anche al di fuori del trattamento di dati delle risorse umane.

In collaborazione con la SECO, infine, l'Incaricato deve verificare annualmente la qualità delle misure concordate nel quadro del Privacy Shield a protezione della personalità delle persone interessate e redigere un rapporto.

Il fabbisogno di posti supplementari è stimato a un posto, non finanziabile tramite gli emolumenti.

Il fabbisogno di personale supplementare non può essere compensato internamente, in particolare dato che con la crescente digitalizzazione, indipendentemente dal progetto di revisione, all'Incaricato è stato attribuito un numero sempre maggiore di compiti, che l'eliminazione di alcuni compiti connessa con l'abrogazione dell'obbligo di notificare le collezioni di dati nel settore privato non riuscirà a controbilanciare.

Come menzionato all'inizio, il fabbisogno di personale dell'Incaricato si modificherà nel corso del tempo a seconda dei compiti. L'evoluzione dinamica del fabbisogno di personale è illustrata nella seguente tabella, strutturata secondo gli anni. Il fabbisogno sarà sottoposto a nuova valutazione al più tardi nel 2023. A fini di completezza, la tabella comprende anche il fabbisogno di personale dell'UFG (cfr. n. 11.1.2 per maggiori informazioni).

	2018–19	2019–20	2020–21	2021–22	2022–23	Finanziato tramite emolumenti
Esame dei codici di condotta	0,5	1	1	1	0,5	~ 60 %
Approvazione delle clausole tipo e delle norme vincolanti d'impresa sulla protezione dei dati	1	1	1	1	1	~ 60 %
Esame delle valutazioni d'impatto sulla protezione dei dati	1	1	3	3	3	~ 90 %
Inchieste / esame delle comunicazioni di violazioni della sicurezza dei dati	3	3	3	3	2,5	~ 30 %
Assistenza amministrativa	1	1	1	1	1	–
Compiti nel quadro del Swiss-US Privacy Shield	1	1	1	1	1	–
Totale posti presso l'Incaricato	7,5	8	10	10	9	
Totale posti UFG	1	1	1	1	1	
Totale globale	**8,5**	**9**	**11**	**11**	**10**	

11.1.1.2 Fabbisogno in materia d'informatica

Nel quadro della sua indipendenza, l'Incaricato necessita un budget minimo orientato all'adempimento dei suoi compiti per coprire le sue spese d'investimento e d'esercizio nel settore informatico. Per poter garantire un esercizio efficiente e possibilmente economico ricorre già oggi ai servizi di sostegno (informatica, finanze, personale, logistica) della Cancelleria federale (CaF). Ha peraltro deciso di ricorrere alle prestazioni informatiche standard della Confederazione, così da contribuire a un adempimento economico dei suoi compiti senza mettere in causa la sua indipendenza. Nonostante tutti gli sforzi, l'attuale budget di circa 300 000 franchi per il fabbisogno in materia d'informatica non è più sufficiente per attuare la nuova LPD.

Come l'economia, anche l'Amministrazione federale utilizza e sviluppa numerose applicazioni che trattano grandi quantità di dati. L'Incaricato deve dunque accertarsi che i dati personali siano anonimizzati o pseudonimizzati in modo da escludere con sufficiente probabilità, secondo lo stato attuale della tecnica, la ricostruzione dell'identità delle persone. Di norma, oggigiorno le moderne applicazioni per il trattamento di dati personali non sono più fornite per un'installazione locale bensì rese accessibili tramite Internet. Lo sviluppo della digitalizzazione obbliga l'Incaricato a svolgere i suoi accertamenti concernenti un'eventuale violazione della protezione dei dati in modo più dinamico e a concludere i suoi controlli più rapidamente e con un onere maggiore.

La sempre maggiore digitalizzazione richiede di conseguenza mezzi informatici supplementari affinché l'Incaricato possa assumere i suoi nuovi compiti:

Compito	Investimenti informatici (in fr.)	Esercizio, manutenzione, assistenza, gestione degli aggiornamenti (in fr.)	Perizie esterne, questioni specifiche (in fr.)
	2019	*Annualmente dal* 2020	Annualmente dal 2019
Infrastrutture e sistemi di test Servono a verificare se il trattamento di dati svolto dalle imprese e dalle amministrazioni rientrano nel diritto in materia di protezione dei dati	200 000.–	105 000.–	
Consultazione di esperti esterni Consultazione mirata di specialisti informatici esterni in considerazione dell'aumento della raccolta, del trattamento e dello scambio di dati personali			60 000.–

Compito	Investimenti informatici (in fr.)	Esercizio, manutenzione, assistenza, gestione degli aggiornamenti (in fr.)	Perizie esterne, questioni specifiche (in fr.)
	2019	*Annualmente dal* 2020	Annualmente dal 2019
Sviluppo dei mezzi di comunicazione e di lavoro elettronici (servizi web) per informazioni e consultazioni	240 000.–	85 000.–	
Totale degli investimenti informatici unici	440 000.–		
Totale delle spese informatiche annualmente ricorrenti		190 000.–	60 000.–

Occorre acquisire sistemi di test per esaminare se i trattamenti di dati svolti da imprese e organi federali rientrano nel campo d'applicazione del diritto in materia di protezione dei dati. L'esame si dovrà concentrare sui servizi, sui prodotti e sui processi commerciali che presentano un potenziale di pericolo per la sfera privata. A tale scopo sono necessarie misure di protezione speciali, per cui gli esami saranno effettuati in ambienti virtuali sicuri tramite un normale accesso Internet. In tal modo sarà tra l'altro possibile risalire allo scambio di dati delle applicazioni e dei prodotti via Internet (p. es. portali web, integrazione di reti sociali e webtracking nei siti Internet, trattamenti di dati su apparecchi mobili).

A seguito delle crescenti esigenze tecnologiche in materia di protezione dei dati e dell'aumento degli apparecchi mobili che raccolgono dati tramite sensori per trasmetterli via Internet a centri informatici, in determinate situazioni l'autorità della Confederazione preposta alla protezione dei dati dovrà consultare esperti esterni. Dato l'elevato grado di dinamismo delle tecnologie dell'informatica e della comunicazione, l'acquisizione e il mantenimento attivo di conoscenze specifiche non sarebbe opportuno. Sebbene la consultazione di specialisti sia necessaria per singoli accertamenti, l'esternalizzazione generale degli accertamenti a terzi non è possibile per motivi di confidenzialità.

L'ampliamento dei mezzi di comunicazione e di lavoro elettronici (applicazioni web) è inteso permettere all'autorità della Confederazione preposta alla protezione dei dati di agire in maniera preventiva e consultiva conformemente alle nuove prescrizioni legali. Ciò comprende in particolare l'assistenza in rete alle valutazioni d'impatto sulla protezione dei dati, il ricevimento e trattamento delle comunicazioni relative alle violazioni della sicurezza dei dati e l'analisi delle garanzie nel quadro dello scambio di dati personali con l'estero nonché l'utilizzo di strumenti volti a promuovere norme di condotta conformi alla protezione dei dati. Occorre pure mettere in atto un sistema di allerta e di annuncio (p. es. sistemi di notifica o registri di trattamenti dei dati) per la denuncia – anche anonima – di violazioni delle prescrizioni in materia di protezione dei dati. Andranno riprese tutte le soluzioni e applicazioni già disponibili nell'Amministrazione federale.

Gli investimenti unici in materia di tecnologie informatiche e delle comunicazioni, inclusi i costi dell'attuazione della nuova LPD, sono attualmente stimati a 440 000 franchi. L'acquisizione delle infrastrutture informatiche, delle applicazioni e dei servizi necessari comporterà spese supplementari annuali di 105 000 franchi. Le spese supplementari annuali per la consultazione di specialisti informatici ammonterà a 60 000 franchi.

Secondo la pianificazione, le nuove soluzioni saranno sviluppate e introdotte entro il 2020 e dovranno essere rinnovate dopo cinque anni.

11.1.2 Ripercussioni finanziarie e sull'effettivo del personale dell'UFG

L'esame della protezione dei dati garantita da uno Stato estero o da un organismo internazionale (art. 13 cpv. D-LPD) spetterà all'UFG, che dovrà verificare l'esistenza di una legislazione o di una regolamentazione interna che garantisca una protezione dei dati adeguata, così come la sua applicazione. Dovrà in particolare esaminare i testi normativi, la giurisprudenza e la dottrina in materia, nonché effettuare singoli viaggi all'estero e prevedere una cooperazione con altre autorità quali la Commissione europea e il comitato preposto alla riveduta Convenzione STE 108. Prevediamo che questo nuovo compito richiederà la creazione di un posto di giurista nella classe di salario 25 per un costo annuale di 192 900 franchi, inclusi i contributi del datore di lavoro. Questi costi non possono essere finanziati internamente, a differenza dei costi per l'installazione del posto di lavoro. A ciò si aggiungono 50 000 franchi per costi professionali e mandati esterni.

Nel quadro dei suoi accertamenti il nostro Consiglio si fonderà per quanto possibile su fonti disponibili (in particolare le valutazioni svolte nell'ambito della Convenzione STE 108 o dalla Commissione europea). Il numero degli Stati da esaminare dovrebbe aumentare in futuro. Si tratta inoltre di un processo dinamico che non va sottovalutato. L'elenco pubblicato dal nostro Consiglio acquisirà d'altronde nuovo valore e il Governo si assumerà la responsabilità per l'esame dell'adeguatezza della protezione dei dati dello Stato esaminato.

11.2 Ripercussioni per i Cantoni e i Comuni

La ratifica del protocollo d'emendamento della Convenzione STE 108 da parte della Svizzera vincola pure i Cantoni. Le sue disposizioni devono essere trasposte nel diritto svizzero conformemente alla ripartizione costituzionale delle competenze. Lo stesso vale per le disposizioni della direttiva (UE) 2016/680.

Ulteriori ripercussioni per i Cantoni e i Comuni risultano dal fatto che, in virtù delle competenze attribuitegli dalla nuova legge, l'Incaricato può fare appello agli organi di polizia cantonali e comunali per le sue misure investigative. È inoltre prevista l'assistenza amministrativa tra l'Incaricato e le autorità cantonali di protezione dei dati.

L'aumento delle disposizioni penali, in particolare l'introduzione di un'infrazione per inosservanza di una decisione dell'Incaricato, non dovrebbe comportare un incremento importante dei procedimenti penali cantonali. Le decisioni dell'Incaricato sono infatti impugnabili. L'inosservanza successiva al passaggio in giudicato dovrebbe limitarsi a pochi casi isolati.

11.3 Ripercussioni informatiche

Il disegno di legge ha un certo numero di ripercussioni sui trattamenti automatizzati dei dati. Il titolare del trattamento deve in particolare garantire che la persona interessata sia informata su tutte le raccolte di dati in Internet che la concernono o su una decisione individuale automatizzata nei suoi confronti. Inoltre, se intende eseguire dei trattamenti che presentano certi rischi deve effettuare una valutazione d'impatto sulla protezione dei dati personali e comunicare all'Incaricato i rischi e le misure prese in considerazione. Il titolare del trattamento deve altresì di norma adottare le misure adeguate per attuare il principio della protezione fin dalla progettazione e tenere un registro dei suoi trattamenti. Deve infine notificare all'Incaricato e, se del caso, anche alla persona interessata determinati casi di violazione della protezione dei dati personali.

Le ripercussioni informatiche per gli organi federali sono più limitate sotto diversi aspetti. Gli obblighi di allestire una valutazione d'impatto e di rispettare di norma il principio della protezione dei dati fin dalla progettazione hanno infatti poche conseguenze pratiche, poiché l'organo federale è già oggi tenuto ad annunciare senza indugio al responsabile della protezione dei dati da esso designato o, in mancanza di tale responsabile, all'Incaricato ogni progetto di trattamento automatizzato di dati personali, affinché le esigenze della protezione dei dati siano immediatamente prese in considerazione (art. 20 cpv. 2 OLPD).

L'articolo 25 della direttiva (UE) 2016/680 obbliga gli Stati Schengen a disporre che determinati trattamenti siano registrati in sistemi di trattamento automatizzato. Secondo questa disposizione, la verbalizzazione deve permettere di determinare i trattamenti effettuati e di stabilire il motivo, la data e l'ora di una consultazione o di una comunicazione di dati personali nonché, nella misura del possibile, l'identità della persona che ha consultato o comunicato i dati e quella del destinatario della comunicazione. Riteniamo che i sistemi di trattamento automatizzati impiegati dagli organi federali nell'ambito della cooperazione penale instaurata da Schengen rispettino le esigenze della normativa europea. Non si può tuttavia escludere che nel quadro di una futura valutazione della Svizzera in materia di protezione dei dati gli esperti europei giungano a un'altra conclusione e raccomandino al nostro Paese di adottare le misure tecniche necessarie affinché la verbalizzazione operata dal sistema di trattamento automatico esaminato fornisca tutte le informazioni previste dall'articolo 25 della direttiva (UE) 2016/680. L'attuazione di una simile raccomandazione avrebbe delle ripercussioni finanziare che al momento non sono quantificabili. L'obbligo per gli organi federali di annunciare le loro attività di trattamento all'Incaricato, infine, non ha ripercussioni pratiche poiché corrisponde in sostanza al

vigente obbligo di notificare le collezioni di dati previsto dall'articolo 11*a* capoverso 2 LPD.

Il registro delle collezioni di dati tenuto dall'Incaricato deve essere adeguato poiché, una volta entrata in vigore la nuova legge, non vi saranno più registrate le attività di trattamento dei privati ma solo quelle degli organi federali.

11.4 Ripercussioni per l'economia

Il disegno mira a rafforzare la protezione dei dati, in particolare migliorando la trasparenza dei trattamenti e il controllo delle persone interessate sui loro dati. Con il continuo sviluppo di nuove tecnologie è in effetti sempre più difficile sapere chi raccoglie dati su una persona e a quale scopo e chi ne è il destinatario. Il disegno intende inoltre migliorare la sorveglianza dell'applicazione e del rispetto delle disposizioni federali sulla protezione dei dati, conferendo poteri decisionali all'Incaricato e garantendo in tal modo una migliore tutela della sfera privata delle persone interessate.

Il disegno punta inoltre a facilitare i flussi transfrontalieri di dati garantendo la possibilità di scambiare dati tra un Paese e l'altro. Nell'ambito dello scambio di dati nel settore privato, gli Stati membri dell'UE considerano infatti la Svizzera un Paese terzo. Attualmente, la Svizzera beneficia di una decisione d'adeguatezza della Commissione[314], secondo la quale il diritto elvetico offre un livello di protezione dei dati adeguato. In virtù di questa decisione, una comunicazione di dati tra un'impresa privata ubicata sul territorio di uno Stato membro e un privato in Svizzera è equiparata a una comunicazione di dati all'interno dell'UE. La decisione della Commissione può tuttavia essere revocata in qualsiasi momento, come previsto dall'articolo 46 paragrafi 4 e 5 del regolamento (UE) 2016/679. Il disegno ha dunque anche l'obiettivo di adeguare il diritto federale ai requisiti europei in modo tale che la Svizzera possa continuare a beneficiare di una decisione d'adeguatezza dell'UE. La ratifica del protocollo d'emendamento della Convenzione STE 108 dovrebbe facilitare globalmente i flussi transfrontalieri di dati tra la Svizzera e i Paesi dell'UE nonché i Paesi che, pur non essendo membri dell'UE, hanno aderito alla Convenzione. È presumibile che la ratifica costituisca una condizione essenziale affinché l'UE riconosca alla nostra legislazione un livello di protezione adeguato (art. 45 del regolamento [UE] 2016/679).

Adeguando la protezione dei dati agli standard europei, il disegno rafforza la fiducia dei consumatori nel trattamento dei loro dati personali, in particolare nel quadro delle transazioni effettuate per via elettronica. Da questo punto di vista il disegno può generare ripercussioni positive non solo per i consumatori ma anche per le imprese, che in tal modo resteranno competitive e potrebbero approfittare di nuove possibilità commerciali soprattutto nel settore del commercio elettronico. I costi

314 GU L 215 del 25.8.2000, pag. 1

necessari per la realizzazione dei nuovi obblighi per i titolari del trattamento dovrebbero essere ampiamente compensati da queste ripercussioni positive.

Occorre parimenti considerare che le imprese svizzere che offrono servizi negli Stati membri dell'UE devono già osservare il regolamento (UE) 2016/679 per via del suo ampio campo d'applicazione territoriale. Per queste imprese il D-LPD non comporta spese supplementari in quanto prevede misure simili a quelle del regolamento europeo.

L'intervento dello Stato è limitato allo stretto necessario, con l'idea di responsabilizzare i titolari del trattamento incoraggiandoli a rispettare i codici di condotta oppure a ricorrere allo strumento della certificazione. È inoltre lasciata una grande autonomia agli attori economici che, grazie a misure volontarie come l'elaborazione di clausole tipo di protezione dei dati personali o di norme vincolanti d'impresa precedentemente approvate dall'Incaricato, possono assicurarsi dell'esistenza di una protezione adeguata dei dati nel quadro dei flussi transfrontalieri. Le agevolazioni apportate dopo la procedura di consultazione, in particolare in materia di obblighi di comunicazione, dovrebbero limitare gli oneri amministrativi.

11.5 Ripercussioni per la società e la sanità pubblica

Per affrontare le sfide sociali rappresentate dalle nuove tecnologie, il disegno prevede in particolare di rafforzare i poteri di sorveglianza dell'Incaricato, come pure di attribuirgli il compito di sensibilizzare il pubblico, in particolare le persone vulnerabili come i minori o gli anziani, in merito alla protezione dei dati.

La nuova legislazione migliora anche la posizione dei consumatori e delle persone vulnerabili.

Non ha per contro alcuna ripercussione sanitaria diretta, eccetto il fatto che il rafforzamento della protezione vale anche per i trattamenti di dati medici.

11.6 Ripercussioni per la parità tra i sessi

Il disegno non ha alcuna ripercussione per la parità tra i sessi.

11.7 Ripercussioni per l'ambiente

Il disegno non ha alcuna ripercussione per l'ambiente.

12 Programma di legislatura e strategie nazionali del Consiglio federale

12.1 Rapporto con il programma di legislatura

Il progetto di legge è annunciato nel messaggio del 27 gennaio 2016[315] sul programma di legislatura 2015–2019.

12.2 Rapporto con le strategie nazionali del Consiglio federale

Il progetto è conforme alla Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) e alla Strategia Open Government Data Svizzera. Fa d'altronde parte del catalogo di misure adottato per l'attuazione della Strategia Svizzera digitale (cfr. n. 0).

13 Aspetti giuridici

13.1 Costituzionalità

13.1.1 Competenza per l'approvazione dello scambio di note relative al recepimento della direttiva (UE) 2016/680

Secondo l'articolo 54 capoverso 1 Cost., gli affari esteri competono alla Confederazione e quindi a quest'ultima compete anche la conclusione di trattati internazionali. In virtù dell'articolo 166 capoverso 2 Cost., l'Assemblea federale è in linea di massima competente per l'approvazione dei trattati. Il Consiglio federale può concludere autonomamente dei trattati internazionali soltanto se vi è autorizzato da una legge o un trattato internazionale approvato dall'Assemblea federale oppure se si tratta di un trattato di portata limitata (art. 166 cpv. 2 Cost., art. 24 cpv. 2 LParl, art. 7*a* LOGA).

Nel presente caso manca un'autorizzazione speciale conferita al Consiglio federale da una legge o un accordo, dato che l'articolo 36 capoverso 5 LPD non è applicabile. D'altronde, la portata dello scambio di note tra la Svizzera e l'UE concernente il recepimento della direttiva (UE) 2016/680 non è limitata. Di conseguenza è l'Assemblea generale a essere competente per l'approvazione dello scambio di note.

Conformemente all'articolo 141 capoverso 1 lettera d Cost., i trattati internazionali sottostanno a referendum se sono di durata indeterminata e indenunciabili (n. 1), se prevedono l'adesione a un'organizzazione internazionale (n. 2) o se comprendono disposizioni importanti che contengono norme di diritto o per l'attuazione dei quali è necessaria l'emanazione di leggi federali (n. 3).

315 FF **2016** 981, in particolare pag. 1097.

Lo scambio di note tra la Svizzera e l'Unione europea concernente il recepimento della direttiva (UE) 2016/680 non rientra nel campo d'applicazione dell'articolo 141 capoverso 1 lettera d n. 1 e 2 Cost. Occorre dunque esaminare se questo accordo comprende disposizioni importanti che contengono norme di diritto o se per la sua attuazione è necessaria l'emanazione di leggi federali. Secondo l'articolo 22 capoverso 4 LParl sono considerate contenenti norme di diritto le disposizioni che, in forma direttamente vincolante e in termini generali ed astratti, impongono obblighi, conferiscono diritti o determinano competenze. D'altronde, secondo l'articolo 164 capoverso 1 Cost. tutte le disposizioni importanti che contengono norme di diritto devono essere emanate sotto forma di legge federale.

L'attuazione dello scambio di note tra la Svizzera e l'UE concernente il recepimento della direttiva (UE) 2016/680 implica diverse modifiche legislative. Pertanto, conformemente all'articolo 141 capoverso 1 lettera d numero 3 Cost. il relativo decreto federale d'approvazione sottostà al referendum in materia di trattati internazionali.

13.1.2 Competenza per l'approvazione del protocollo d'emendamento della Convenzione STE 108

L'articolo 4 P-STE 108 disciplina gli obblighi delle Parti. In virtù del paragrafo 1 ciascuna Parte deve adottare, nell'ambito del suo diritto interno, le misure necessarie per dare effetto alle disposizioni della Convenzione STE 108. Il paragrafo 2 dispone inoltre che tali misure devono essere adottate al più tardi al momento della ratifica o dell'adesione alla nuova Convenzione. Secondo l'articolo 25 non è ammessa alcuna riserva.

Il disegno è conforme al progetto di revisione della Convenzione STE 108. Non appena il suo protocollo d'emendamento sarà aperto alla firma, il nostro Consiglio potrà firmarlo e sottoporlo al Parlamento per approvazione. Per i motivi di cui al numero 13.1.1, il decreto federale concernente l'approvazione del protocollo d'emendamento della Convenzione STE 108 sottostà al referendum in materia di trattati internazionali in virtù dell'articolo 141 capoverso 1 lettera d numero 3 Cost.

13.1.3 Competenza legislativa della Confederazione

Come rilevato dal nostro Consiglio nel messaggio del 19 febbraio 2003 concernente la revisione della LPD e il decreto federale concernente l'adesione della Svizzera al Protocollo aggiuntivo alla Convenzione STE 108[316], la Costituzione federale non contiene alcuna norma che abilita espressamente la Confederazione a legiferare nel settore della protezione dei dati. L'articolo 13 Cost. sancisce il diritto di ognuno di essere protetto da un impiego abusivo dei suoi dati personali, ma si tratta di un diritto fondamentale che non attribuisce nuove competenze alla Confederazione. In virtù dell'articolo 35 capoversi 2 e 3 Cost., chi svolge un compito statale deve contribuire ad attuare i diritti fondamentali e le autorità devono provvedere affinché, per

316 FF **2003** 1885, in particolare pag. 1932.

quanto vi si prestino, siano realizzati anche nelle relazioni tra privati. In questo senso il progetto contribuisce ad attuare l'articolo 13 capoverso 2 Cost., sia nelle relazioni tra Stato e privati che in quelle tra privati. Il D-LPD concretizza le garanzie di cui all'articolo 13 capoverso 2 Cost. per le persone fisiche. Per il trattamento di dati delle persone giuridiche da parte degli organi federali, proponiamo di introdurre una regolamentazione minima nella LOGA.

Per quanto riguarda l'emanazione delle disposizioni di protezione dei dati applicabili al diritto privato, il legislatore può basarsi sulla competenza di legiferare nei settori del diritto civile (art. 122 Cost.), dell'esercizio dell'attività economica privata (art. 95 Cost.) e della protezione dei consumatori (art. 97 cpv. 1 Cost.).

Nel settore del diritto pubblico, il legislatore federale può fondarsi sulla competenza organizzativa conferitagli dall'articolo 173 capoverso 2 Cost. per emanare disposizioni di protezione dei dati applicabili alle autorità e ai servizi amministrativi.

La Costituzione federale riconosce ai Cantoni la piena autonomia in materia d'organizzazione e li abilita a legiferare sulla protezione dei dati nella loro sfera di competenza. La Confederazione ha quindi il diritto di emanare disposizioni di protezione dei dati applicabili ai settori pubblici cantonali o comunali soltanto negli ambiti in cui i Cantoni sono incaricati di eseguire il diritto federale, il quale deve a sua volta ovviamente essere fondato su una norma costituzionale. In questo caso la Confederazione deve tuttavia evitare di ingerire nelle competenze cantonali in materia di organizzazione. Il disegno rispetta questo limite. I settori nei quali estende la protezione dei dati concernono i trattamenti di dati effettuati da organi cantonali in esecuzione del diritto federale oppure quelli effettuati da organi federali insieme a organi cantonali. Il disegno, infine, abroga l'articolo 37 LPD (esecuzione da parte dei Cantoni).

13.2 Compatibilità con gli impegni internazionali della Svizzera

Il disegno è compatibile con gli impegni internazionali della Svizzera (cfr. in particolare n. 1.2, 1.3, 2, 3, 4 e 9.3). Le permette di ratificare non appena possibile il protocollo d'emendamento della Convenzione STE 108 (cfr. n. 3.2 e 3.3) nonché di rispettare l'impegno di attuare e applicare tutti gli sviluppi dell'acquis di Schengen, assunto nel quadro dell'Accordo di associazione a Schengen con l'UE (cfr. n. 1.2.2.3, 2.2–2.4 e 9.3).

L'articolo 61 della direttiva (UE) 2016/680 dispone che gli accordi internazionali relativi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, conclusi dagli Stati membri anteriormente all'entrata in vigore della direttiva e conformi al diritto dell'Unione applicabile anteriormente a tale data, restano in vigore fino alla loro modifica, sostituzione o revoca[317].

317 Consid. 95.

Il disegno non ha ripercussioni neppure sulla dichiarazione comune della Svizzera e dell'UE relativa all'articolo 23 paragrafo 7 della Convenzione del 29 maggio 2000[318] relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea. L'articolo 60 della direttiva (UE) 2016/680 prevede che le disposizioni contenute in atti giuridici dell'UE entrati in vigore prima della direttiva medesima rimangono impregiudicate.

13.3 Forma dell'atto

Il progetto del nostro Consiglio comprende due progetti di legge:

- il disegno di decreto federale che approva lo scambio di note tra la Svizzera e l'UE concernente il recepimento della direttiva (UE) 2016/680,
- un disegno di atto mantello comprendente la revisione totale della legge federale sulla revisione totale della LPD con in allegato le necessarie modifiche di altre leggi federali (cifra I) nonché le necessarie modifiche di leggi federali che attuano la direttiva (UE) 2016/680 nel quadro degli impegni connessi all'associazione a Schengen (cifra II).

13.4 Subordinazione al freno delle spese

Il disegno non implica spese che sottostanno al freno delle spese (art. 159 cpv. 3 lett. b Cost.).

13.5 Conformità alla legge sui sussidi

Il disegno non prevede sussidi.

13.6 Delega di competenze legislative

Il disegno delega competenze legislative al nostro Consiglio segnatamente nelle disposizioni seguenti:

- art. 11 cpv. 5, 23 cpv. 6: il Consiglio federale può prevedere eccezioni agli obblighi di tenere un registro delle attività di trattamento nonché al diritto d'accesso della persona interessata e al principio della gratuità;
- art. 13 cpv. 3: il Consiglio federale può prevedere altre garanzie appropriate per comunicare dati personali all'estero;
- art. 29: se un organo federale tratta dati personali congiuntamente ad altri organi federali, a organi cantonali o a persone private, il Consiglio federale disciplina i controlli e la responsabilità in materia di protezione dei dati;

318 RS **0.362.31**

– art. 31: il Consiglio federale conserva la sua competenza di autorizzare, a determinate condizioni, il trattamento automatizzato di dati personali degni di particolare protezione nel quadro di progetti pilota;
– art. 53: il Consiglio federale può definire i casi in cui è possibile rinunciare alla riscossione di un emolumento o ridurlo.

13.7 Coordinamento con altre leggi federali

Nel quadro dei dibattiti parlamentari occorre modificare le seguenti leggi federali che entrano in vigore dopo l'adozione del presente messaggio.

– Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna: i nuovi articoli 23*b* e 23*c* entrano in vigore assieme alla legge federale del 25 settembre 2015[319] sulle attività informative. L'espressione «profilo della personalità» va sostituita con «dati personali» nell'articolo 23*b* capoverso 2 lettera c ed eliminata nella frase introduttiva dell'articolo 23*c* capoverso 2.
– Legge federale del 12 giugno 2009[320] concernente l'imposta sul valore aggiunto: l'Amministrazione federale delle contribuzioni (AFC) tratta e analizza in maniera automatizzata dati di persone fisiche (p. es. nel quadro di esecuzioni, attestati di carenza di beni, errori di calcolo, indicazioni nel settore delle dogane) al fine di allestire profili di rischio che consentano di effettuare i controlli fiscali in modo più mirato. A tale scopo necessita di una base in una legge in senso formale. Negli articoli 76 capoverso 1 e 76*a* capoverso 1 va eliminata l'espressione «profili della personalità». In sostituzione, l'AFC deve ottenere la competenza di effettuare profilazioni. L'articolo 76*a* capoverso 3 lettera g va abrogato. L'articolo 76*a* capoverso 2 va adeguato affinché l'AFC possa comunicare dati anche in seguito a una profilazione. L'articolo 76 va completato con un capoverso 1bis secondo cui l'Incaricato può accedere al sistema di trattamento dell'AFC per esercitare la sua attività di vigilanza.
– Legge federale del 25 settembre 2015 sulle attività informative: nell'articolo 44 capoverso 1 l'espressione «profili della personalità» va sostituita con «altri dati personali che permettono di valutare il grado di pericolosità di una persona». Nell'articolo 46 capoverso 1 l'espressione «collezione di dati» va sostituita con «banca dati». Nell'articolo 61 capoverso 2 il rinvio all'articolo 6 capoverso 2 LPD va sostituito con un rinvio all'articolo 13 capoverso 1 D LPD. Anche l'articolo 64 va modificato in diversi punti: il capoverso 2 va modificato dato che secondo il D-LPD l'Incaricato non emana più raccomandazioni ma è autorizzato a aprire un'inchiesta; il capoverso 3 può essere abrogato dato che non è più necessario un intervento del Tribunale amministrativo federale; l'articolo 4 va adeguato affinché in caso di errori nel trattamento dei dati o relativamente al differimento dell'informazione l'Inca-

319 FF **2015** 5925
320 RS **641.20**, modifiche del 30 sett. 2016 RU **2017** 3575

ricato possa obbligare mediante decisione il Servizio informazioni della Confederazione (SIC) a eliminarli; il capoverso 5 va adeguato affinché l'Incaricato possa decidere che il SIC informi immediatamente la persona interessata se le condizioni previste da tale capoverso sono adempiute. L'articolo 65 può essere abrogato analogamente all'articolo 64 capoverso 3; anche il rinvio all'articolo 65 capoverso 1 nell'articolo 66 capoverso 1 va eliminato. Infine, occorre adeguare la terminologia nell'articolo 78: l'espressione «detentore delle varie collezioni di dati» va sostituita con «titolare del trattamento»; l'espressione «collezione di dati» può essere sostituita con «sistemi d'informazione, banche dati e atti».

– Legge del 20 giugno 2014[321] sulla cittadinanza: questa legge entra in vigore il 1° gennaio 2018. Nell'articolo 44 l'espressione «profili della personalità» va sostituita con «dati personali che permettono di valutare l'idoneità del richiedente per la naturalizzazione».

– Legge militare del 3 febbraio 1995: il nuovo articolo 100 entra in vigore il 1° gennaio 2018[322]. Nel capoverso 3 lettera a l'espressione «profili della personalità» va sostituita con «dati personali che permettono di valutare il grado di pericolosità di una persona» e nella lettera b occorre rinviare agli articoli 13 e 14 D-LPD. Al capoverso 4 lettera c numero 2 l'espressione «collezioni di dati» va sostituita con «attività di trattamento di dati».

Nel quadro dei dibattiti parlamentari occorre inoltre formulare disposizioni per il coordinamento tra il disegno di legge e le seguenti leggi federali la cui entrata in vigore non è ancora stata fissata.

– Legge federale del 18 marzo 2016[323] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni: nell'articolo 14 l'espressione «profili della personalità» va abrogata. Nell'articolo 13 l'espressione «detentrici della collezione di dati» va sostituita con «titolari del trattamento».

– Modifica del 18 marzo 2016[324] della legge sugli agenti terapeutici: nell'articolo 62*a* l'espressione «profili della personalità» va eliminata.

– Legge del 17 giugno 2016[325] sul casellario giudiziale: nell'articolo 3 capoverso 1 l'espressione «titolare della collezione di dati» va sostituita con «titolare del trattamento». Nell'articolo 12 capoverso 2 l'espressione «collezione di dati» va sostituita con «banca dati». Nella versione francese, infine, all'articolo 25 capoverso 1 va eliminata l'espressione «fichier journal».

– Legge federale del 30 settembre 2016[326] sull'energia: a seguito dell'abrogazione della protezione dei dati delle persone giuridiche nel D-LPD e della restrizione del concetto di dati personali all'articolo 4 lettera a D-LPD a informazioni relative a una persona fisica identificata o identificabile, negli articoli 56 capoverso 1, 58, rubrica e capoversi 1 e 3 nonché 59, rubrica e

321 FF **2014** 4461
322 FF **2014** 6049
323 FF **2016** 1675
324 FF **2016** 1637
325 FF **2016** 4315
326 FF **2016** 6921

capoversi 1 e 2 occorre adeguare la terminologia al fine di chiarire che queste disposizioni sono applicabili anche ai dati di persone giuridiche. L'espressione «dati personali» va sostituita o integrata in tutte le suddette disposizioni con «dati personali e dati di persone giuridiche». La legge del 23 marzo 2007[327] sull'approvvigionamento elettrico, modificata in seguito alla modifica della legge sull'energia, va adeguata come segue: l'articolo 17*c* capoverso 1 va completato affinché la LPD sia applicabile per analogia anche al trattamento di dati di persone giuridiche. Nell'articolo 27 capoverso 1 l'espressione «dati personali» va sostituita con «dati personali e dati di persone giuridiche».

– Modifica del 16 giugno 2017 della legge del 24 marzo 2000[328] sul personale federale: nell'articolo 27 capoverso 2 l'espressione «profili della personalità» va eliminata.
– Modifica del 16 giugno 2017[329] della legge federale sulla navigazione aerea: nell'articolo 21*c* capoverso 1 lettera b l'espressione «profili della personalità» va eliminata.
– Legge federale del 18 marzo 2016[330] sulla registrazione delle malattie tumorali: nell'articolo 7 capoverso 2 l'espressione «detentore di una collezione di dati» va sostituita con «titolare del trattamento».

13.8 Coordinamento con altri progetti legislativi

Il disegno potrebbe influire sui seguenti progetti legislativi in revisione.

– Disegno di legge federale sui giochi in denaro (LGD)[331]: occorrerà modificare le basi legali relative ai profili della personalità.
– Disegno di legge federale sugli esami genetici sull'essere umano (LEGU).
– Disegno di legge federale sull'organizzazione dell'infrastruttura ferroviaria[332].
– Progetto di revisione della legge sulle telecomunicazioni[333]: il messaggio dovrebbe essere adottato alla fine dell'estate 2017. Se del caso occorrerà adeguare la terminologia relativa alla protezione dei dati alla nuova LPD.
– Progetto di revisione della legge sugli stranieri: il messaggio dovrebbe essere adottato nel corso dell'autunno 2017. Se del caso occorrerà adeguare la terminologia relativa alla protezione dei dati alla nuova LPD.

327 RS **734.7**; cfr. FF **2016** 6921
328 RS **172.220.1**; cfr. FF **2016** 297, in particolare pag. 306.
329 FF **2017** 3661
330 FF **2016** 1623
331 FF **2015** 6989
332 FF **2016** 8487
333 RS **784.10**

– Disegno del Codice civile (Atti dello stato civile e registro fondiario)[334]: occorrerà tenere conto del nuovo tenore dell'articolo 45*c* CC e se del caso adeguarlo.

– Avamprogetto di legge federale sul trattamento di dati personali in seno al Dipartimento federale degli affari esteri: occorrerà se del caso adeguare la terminologia ed eliminare l'espressione «profili della personalità».

– Disegno di modifica della legge sulla vigilanza dei mercati finanziari (modifica dell'atto nel quadro del disegno di legge sugli istituti finanziari)[335]: nell'articolo 13*a* va eliminata l'espressione «profili della personalità». Al capoverso 1 del medesimo articolo occorre inoltre aggiungere che la FINMA può trattare, oltre a quelli dei suoi impiegati, anche i dati di «candidati a un impiego». All'elenco esemplificante dei compiti della FINMA che comportano il trattamento di dati occorre aggiungere «le procedure di reclutamento». Occorre infine precisare che la FINMA può affidare il trattamento a degli specialisti.

334 FF **2014** 3095
335 FF **2015** 7525