Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Ufficio federale di giustizia UFG
Ambito direzionale Diritto pubblico
Settore Progetti e metodologia legislativi

21 dicembre 2016

Rapporto esplicativo concernente l'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

Indice

Compendio

La presente revisione si prefigge di rafforzare la protezione dei dati aumentando la trasparenza del trattamento 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. La revisione mira inoltre a migliorare l'applicazione e il rispetto delle norme federali sulla protezione dei dati. Infine, intende garantire e migliorare la competitività della Svizzera, agevolando in particolare la comunicazione di dati all'estero. Un elevato grado di protezione riconosciuto a livello internazionale è inoltre teso a promuovere lo sviluppo di nuovi settori economici nell'ambito della digitalizzazione della società.

Situazione iniziale e obiettivi della revisione

La revisione si fonda su una decisione del Consiglio federale di elaborare un progetto con due obiettivi. Da una parte occorre eliminare le lacune della legge sulla protezione dei dati sorte in seguito alla rapidissima evoluzione tecnologica. Dall'altra, è necessario tenere conto degli sviluppi nel Consiglio d'Europa e nell'Unione europea. Il progetto è previsto negli obiettivi del Consiglio federale per il 2016 e nel programma di legislatura 2015-2019. Negli anni passati la protezione dei dati è stata oggetto di numerosi interventi parlamentari, a testimonianza della volontà politica di migliorare la legislazione federale in tale settore.

Anche a livello internazionale la protezione dei dati assume sempre maggiore importanza. 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. Inoltre, il Consiglio d'Europa prevede di rivedere la Convenzione STE 108 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale e di adottarla all'inizio del 2017.

La presente revisione intende garantire che la legislazione federale sia compatibile con la Convenzione STE 108 riveduta, in modo da permettere alla Svizzera di firmarla quanto prima. Inoltre, il progetto di revisione riprende i requisiti della direttiva (UE) 2016/680 e permette pertanto alla Svizzera di adempiere agli obblighi risultanti da Schengen. La revisione mette altresì in atto le raccomandazioni dell'Unione europea elaborate nel quadro della valutazione di Schengen, tra cui in particolare quella di estendere le competenze dell'Incaricato federale della protezione dei dati e della trasparenza. Infine, il presente progetto intende adeguare in generale la legislazione svizzera sulla protezione dei dati ai requisiti del regolamento (UE) 2016/679. Insieme alla ratifica della revisione della Convenzione STE 108, tale adeguamento costituisce un presupposto per la futura decisione di adeguatezza. Con tale decisione la Commissione europea confermerebbe che la legislazione svizzera garantisce una protezione adeguata dei dati. La decisione di adeguatezza è di fondamentale importanza soprattutto per l'economia svizzera.

Contenuti essenziali del progetto

Conformemente alle norme europee e alla maggior parte degli ordinamenti giuridici esteri, il presente progetto abolisce la protezione dei dati delle persone giuridiche. Ciò agevola la comunicazione di dati all'estero, anch'essa migliorata.

In generale, il progetto migliora la trasparenza del trattamento di dati. L'obbligo di informare la persona interessata in occasione della raccolta dei 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. Deve altresì avere la possibilità di esporre il suo punto di vista. Sono infine estese le informazioni da fornire alla persona interessata quando questa fa valere il suo diritto d'accesso.

La presente revisione mira a promuovere l'autoregolamentazione dei titolari del trattamento, soprattutto attraverso raccomandazioni di buona prassi tese ad agevolare le attività dei titolari e migliorare il rispetto della legge. Le raccomandazioni possono essere elaborate sia dall'Incaricato federale della protezione dei dati e della trasparenza, che nel farlo deve coinvolgere anche le cerchie interessate, sia dalle cerchie interessate stesse, che devono poi farle approvare dall'Incaricato.

L'indipendenza e la posizione dell'Incaricato federale della protezione dei dati e della trasparenza 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 della protezione dei dati e della trasparenza non può infliggere sanzioni amministrative.

Oltre alla revisione della legge sulla protezione dei dati, sono necessari adeguamenti di varie legge federali. In particolare, occorre attuare i requisiti della direttiva (UE) 2016/680 nel Codice penale, nel Codice di procedura penale e nella legge federale sull'assistenza giudiziaria in materia penale, nonché adeguare alcune disposizioni della legge sullo scambio di informazioni con gli Stati Schengen.

1 Punti essenziali del progetto

1.1 Situazione iniziale a livello nazionale

1.1.1 Diritto in vigore

A livello federale la protezione dei dati è attualmente retta 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 (cpv. 2 lett. e).

La LPD sancisce innanzitutto 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 i dati possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge (art. 4 cpv. 3). 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 o l'organo federale che tratta i dati personali deve accertarsi della loro esattezza (art. 5).

La LPD disciplina poi 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 (qui appresso l'«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 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 particolare protezione o profili della personalità che la riguardano, fatte salve alcune deroghe. La LPD disciplina inoltre 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 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*). La comunicazione di dati a terzi è in linea di principio possibile soltanto se esiste una base legale (art. 19 cpv. 1). Gli organi federali possono permettere l'accesso a dati personali mediante una procedura di richiamo soltanto se ciò è previsto esplicitamente dalla 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

[1] RS **235.1**

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 regole contenute in leggi federali speciali, il trattamento dei 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 determinati settori).

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 Consiglio federale 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 Consiglio federale, 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 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]»[8].

Il 1° aprile 2015 il Consiglio federale 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.

---

2 BÜRO VATTER/INSTITUT FÜR EUROPARECHT, Evaluation des Bundesgesetzes über den Datenschutz - Schlussbericht, Berna 11 mar. 2011, https://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 Erano rappresentate le autorità federali seguenti: 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 rappresentati dalla Fédération romande des consommateurs.

8 https://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.

Il Consiglio federale ha deciso di porre in consultazione un avamprogetto di modifica unico sottostante a referendum (avamprogetto di legge federale sulla revisione della legge federale sulla protezione dei dati e la modifica di altri atti normativi relativi alla protezione dei dati, qui appresso «AP»). L'atto mantello è costituito, da una parte, da una cifra I che comprende la revisione totale della LPD (qui appresso AP-LPD») e, nell'allegato, gli adeguamenti necessari di altre leggi federali nonché, dall'altra, da una cifra II che contiene le modifiche di leggi federali necessarie per l'attuazione della direttiva (UE) 2016/680 nell'ambito degli obblighi di Schengen. Nel presente rapporto gli atti normativi modificati sono indicati con «AP» seguito dall'abbreviazione della legge in questione (cfr. n. 8.2. segg.).

1.1.3 Strategia Svizzera digitale

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

La nuova strategia intende permettere alla Svizzera di trarre maggior profitto dalla crescente digitalizzazione e di svilupparsi in modo ancora più dinamico come economia pubblica 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 le 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[9] che comprende le misure che l'Amministrazione federale deve mettere in atto. L'AP fa parte di tali misure (n. 1.2 e 1.7 del piano d'azione).

Nel quadro dell'elaborazione della Strategia, l'Ufficio federale delle comunicazioni (UFCOM) ha conferito alla Scuola universitaria di Berna l'incarico di redigere uno studio sulla problematica dei Big Data[10]. 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 dall'AP 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)[11]: 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 cyberspazio, migliorare la capacità di resistenza delle infrastrutture d'importanza vitale e ridurre i cyber-rischi legati in particolare alla criminalità, allo spionaggio e al sabotaggio informatici. L'attuazione della strategia compete al Dipartimento federale delle finanze (DFF).

Strategia Open Government Data Svizzera del 16 aprile 2014 (OGD)[12]: la strategia intende promuovere la pubblicazione di dati raccolti dall'Amministrazione sotto forma di Open Governement Data (OGD), ossia dati dell'Amministrazione pubblici 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.

---

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

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

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

12 https://www.isb.admin.ch/isb/it/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html.

Il Programma nazionale di ricerca 75 «Big Data» (PNR 75)[13]: nel 2015 il Consiglio federale ha avviato questo programma di ricerca, dotato di un budget di 25 milioni di franchi. Lo scopo è di 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 di megadati in diversi ambiti della società.

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 diritto civile, il diritto sulla proprietà intellettuale, la sicurezza degli oggetti, il diritto in materia di concorrenza, ecc.). I lavori della commissione saranno probabilmente conclusi non prima 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 Consiglio federale ha deciso di proseguire le attività avviate nel contesto del programma nazionale «Giovani e media»[14], realizzato dal 2011 al 2015. Il DFI (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 sulle condizioni generali per un'economia digitale: il rapporto affronta gli ambiti di fondamentale importanza per l'economia digitale, suddividendoli in cinque settori: mercato del lavoro, ricerca e sviluppo, sharing economy, finanza digitale e politica in materia di concorrenza. Il rapporto esaminerà questi settori e, laddove necessario, proporrà adeguamenti legislativi volti a creare una situazione positiva per l'economia digitale per mezzo di condizioni quadro economiche e politiche favorevoli.

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 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.
- 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.

[13] http://www.nfp75.ch/fr.

[14] http://www.giovaniemedia.ch/it/home.html

- 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 Consiglio federale ha parzialmente adempito il postulato con il rapporto del 9 dicembre 2011 concernente la valutazione della legge federale sulla protezione dei dati[15].
- 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 Consiglio federale 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 Consiglio federale ha parzialmente adempito il postulato con il rapporto del 9 dicembre 2011 concernente la valutazione della legge federale sulla protezione dei dati [16].
- Postulato Schwaab 12.3152 «Diritto all'oblio in Internet»: il Consiglio nazionale ha adottato l'intervento il 15 giugno 2012. Quest'ultimo incarica il Consiglio federale 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 della revisione della LPD (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**); tuttavia alcune misure tese ad adempire la mozione possono essere realizzate nell'ambito di questa revisione.
- Postulato Recordon 13.3989 «Violazioni della personalità riconducibili al progresso delle tecnologie dell'informazione e della comunicazione»: l'11 dicembre 2013 il Consiglio nazionale ha adottato il postulato, che incarica il Consiglio federale di stilare un rapporto sui rischi per i diritti della personalità 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 Consiglio federale 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 Consiglio federale di redigere un rapporto che permetta di definire l'identità digitale dei cittadini integrandola nella loro personalità giuridica attuale, che 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 29 ottobre 2014, il Consiglio nazionale ha adottato l'intervento che incarica il Consiglio federale 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. Il Consiglio federale è in particolare invitato a valutare se occorra adeguare la legislazione relativa al trasferimento della proprietà e alla protezione dei dati.

[15] FF **2012** 227, 231

[16] FF **2012** 227, 231

- Postulato Schwaab 14.3782 «Regole per la "morte digitale"»: l'intervento, accolto dal Consiglio nazionale il 12 dicembre 2014, incarica il Consiglio federale 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»: l'intervento, adottato dal Consiglio nazionale il 20 marzo 2015, ha lo stesso tenore del postulato Comte 14.4284 «Registrazioni video di privati. Migliorare la tutela della sfera privata».
- 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, incarica il Consiglio federale di elaborare un rapporto incentrato sui rischi dell'utilizzo di videocamere private installate sui droni e sugli occhiali connessi.
- Postulato Derder 15.4045 «Diritto all'utilizzo dei dati personali. Diritto alla copia»: il 18 dicembre 2015 il Consiglio nazionale ha adottato l'intervento che incarica il Consiglio federale di esaminare, redigendo un rapporto, in che misura i privati e l'economia potrebbero approfittare dell'ulteriore utilizzo dei loro dati personali. Il Consiglio federale deve in particolare valutare l'introduzione di un diritto della persona interessata di ottenere una copia di tali dati.
- Motion Béglé 16.3379 «Promuovere la Svizzera quale cassaforte digitale universale». La mozione incarica il Consiglio federale di mantenere, nell'ambito della revisione della LPD, la protezione dei dati delle persone giuridiche (n. 1) e l'articolo 11 che prevede la certificazione facoltativa (n. 2). L'autore della mozione ritiene che tali disposizioni garantiscano un livello ottimale di protezione dei dati, posizionando così la Svizzera come cassaforte digitale universale. Il Consiglio nazionale ha trattato la mozione il 30 settembre 2016, respingendo la richiesta numero 1 e approvando la numero 2.
- Postulato Béglé 16.3383 «Dati digitali. Informare le persone lese in caso di pirateria»: il postulato incarica il Consiglio federale 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 Consiglio federale 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 Consiglio federale di vagliare il miglior mezzo per favorire la riappropriazione dei dati personali da parte delle persone interessate. Il Consiglio federale non si è ancora espresso sul postulato. Nella sua risposta il Consiglio federale propone di accogliere il postulato precisando che il tema della riappropriazione del controllo sui dati personali va affrontato nell'ambito della «Strategia Svizzera digitale». Il 30 settembre 2016 il Consiglio nazionale ha accolto il postulato.

1.2 Situazione internazionale

1.2.1 Osservazione preliminare

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 online. Oltre al diritto alla sfera privata, che è garantito dall'articolo 13 della Costituzione federale, ma anche da diversi trattati internazionali vincolanti (art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[17], art. 17 del Patto internazionale relativo ai diritti civili e politici[18]), 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 ONU), la libertà di riunione (art. 22 Cost., art. 11 CEDU, art. 21 Patto II ONU) e d'associazione (art. 23 e 28 Cost., art. 11 CEDU, art. 22 Patto II ONU) o il diritto al rispetto della vita familiare (art. 14 Cost., art. 8 e 12 CEDU, art. 23 Patto II ONU).

Per quanto riguarda la limitazione della protezione della sfera privata occorre rinviare in particolare ai 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). Questi requisiti vanno interpretati in senso stretto. Pur concedendo regolarmente agli Stati parte un ampio margine di configurazione in riferimento alla legittimità delle finalità perseguite[19], 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 (p. es. abitudini alimentari, stato di salute, ecc.) 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[20] relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (qui appresso «direttiva 95/46/CE»). Tale direttiva è stata completata dalla decisione quadro 2008/977/GAI[21] del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (qui appresso «decisione quadro 2008/977/GAI»).

Nell'ambito del programma di Stoccolma[22], 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 intitolata «Un approccio globale alla protezione dei dati personali nell'Unione europea»[23], la Commissione europea ha concluso che

17 CEDU, RS **0.101**

18 Patto II ONU, RS **0.103.2**

19 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.

20 GU L 281 del 23.11.1995, pag. 31.

21 GU L 350 del 30.12.2008, pag. 60.

22 GU C 115, del 4.5.2010, pag. 1.

23 COM (2010) 609 final.

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[24] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (qui appresso «regolamento (UE) 2016/679»), che abroga la direttiva 95/46/CE (cfr. n. 4), e, dall'altra, della direttiva (UE) 2016/680/CE[25] 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 (qui appresso «direttiva (UE) 2016/680»), 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 del 26 ottobre 2004[26] 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 (qui appresso 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.

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. Siffatta decisione può essere revocata in qualsiasi momento.

Nella decisione di adeguatezza del 26 luglio 2000 la Commissione europea ha confermato che la Svizzera dispone di una protezione adeguata dei dati[27]. Tale decisione si fonda tuttavia sul livello di protezione definito dalla direttiva 95/46/CE. In futuro, l'esame dell'adeguatezza 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, la Svizzera deve assolutamente disporre di una legislazione conforme ai requisiti del suddetto regolamento.

1.2.2.3 Raccomandazioni in relazione con gli accordi di Schengen

Con l'associazione a Schengen, 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 regolarmente se gli Stati associati, e quindi anche la Svizzera, rispettano 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. Secondo tale rapporto, la legislazione svizzera sulla protezione dei dati è conforme ai requisiti dell'acquis di Schengen. Il rapporto di

---

[24] 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.

[25] 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

[26] RS **0.362.31**

[27] Decisione della Commissione del 26 lug. 2000 (GU L 215 del 25.8.2000, pag. 1).

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.

L'AP-LPD tiene conto delle raccomandazioni dell'Unione europea in quanto conferisce all'Incaricato la competenza di emanare decisioni (cfr. art. 41-43 AP-LPD). Per contro, il Consiglio federale ritiene 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 giuridica svizzera. Il Consiglio federale è 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

Il 28 gennaio 1981 il Consiglio d'Europa ha adottato il primo trattato internazionale sulla protezione dei dati: la Convenzione del 28 gennaio 1981[28] per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (qui appresso «Convenzione STE 108 »), ratificata dalla Svizzera il 2 ottobre 1997. La Convenzione è stata completata dal Protocollo aggiuntivo dell'8 novembre 2001[29] 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. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

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 STE 108 (qui appresso «P-STE 108»). I lavori del comitato ad hoc istituito dal Comitato dei Ministri si sono conclusi nel giugno 2016. Il protocollo di emendamento della Convenzione STE 108 sarà probabilmente adottato dal Comitato dei Ministri all'inizio del 2017 (cfr. qui appresso n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Il presente rapporto si basa sul progetto di modernizzazione della Convenzione (stato: settembre 2016)[30], 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. 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. In dicembre 2013 l'Assemblea generale ha adottato una risoluzione[31] 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 territorio nazionale e all'estero. Il rapporto è stato presentato in luglio 2014[32].

---

28 RS **0.235.1**

29 RS **0.235.11**

30 Il testo francese è reperibile all'indirizzo seguente: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Version%20consolidée%20convention%20108%20modernisée%20juillet%202016.pdf. Versioni in tedesco e in italiano fanno parte della documentazione per la consultazione.

31 Risoluzione 68/167 del 18 dic. 2013 disponibile in francese al seguente indirizzo: http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167

32 OHCHR «Le droit à la vie privée à l'ère du numérique», 2014.

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.

L'8 marzo 2016 il relatore speciale ha presentato il suo primo rapporto. Vi constata che l'assenza di una definizione universale di «sfera privata» è uno degli ostacoli principali alla sua protezione esaustiva. Nel contesto che ci interessa in questa sede, il rapporto osserva inoltre che il rischio della violazione del diritto alla sfera privata attraverso un uso abusivo di dati personali da parte di imprese private non sia ancora chiarito in modo definitivo[33]. 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[34]. Il relatore speciale ritiene pertanto necessario un dialogo internazionale sulla raccolta e il trattamento di dati personali da parte delle imprese e sulla loro comunicazione a servizi statali. Prevede pertanto di procedere a un'ampia consultazione delle imprese e della società civile entro il 2017 nell'ambito del progetto «Corporate online business models and personal data use»[35].

Inoltre, il relatore speciale constata che i consumatori sono sempre più consapevoli dei rischi per il diritto alla sfera privata; lo testimonia la rapida crescita del mercato di prodotti e servizi tesi a tutelare la sfera privata[36]. Il relatore è contrario a sviluppi nazionali che obbligano per legge le imprese a introdurre nei loro prodotti dei meccanismi che permettano posteriormente l'accesso ai dati criptati[37]. Infine, riconosce l'importanza del rapido sviluppo di prodotti protetti biometricamente e intende collaborare con la ricerca, le autorità di perseguimento penale, i servizi d'informazione e la società civile per individuare meccanismi di protezione materiali e giuridici[38].

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

Conformemente all'orientamento economico dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), le linee guida del 1980 sulla protezione dei dati[39], 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 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)[40], 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

---

33 HRC, Special Rapporteur Right to Privacy 2016, n. 9.

34 HRC, Special Rapporteur Right to Privacy 2016, n. 9.

35 HRC, Special Rapporteur Right to Privacy 2016, n. 9 e 46 seg.

36 HRC, Special Rapporteur Right to Privacy 2016, n. 50.

37 HRC, Special Rapporteur Right to Privacy 2016, n. 30 seg.

38 HRC, Special Rapporteur Right to Privacy 2016, n. 15 e 46(e).

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

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

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[41]. 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[42] (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 della revisione

Il presente progetto dà seguito al mandato conferito dal Consiglio federale 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 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. Il progetto figura anche tra gli obiettivi del Consiglio federale del 2016 e nel programma di legislatura 2015-2019 (n. 10.1) e attua numerosi interventi parlamentari illustrati al n. 1.1.5.

L'AP persegue diversi obiettivi che si completano a vicenda. Innanzitutto il progetto 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 avamprogetto 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 (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Gli esperti europei hanno infatti raccomandato alla Svizzera di conferire competenze decisionali all'Incaricato. 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. **Fehler! Verweisquelle konnte nicht gefunden werden.**). A tal fine la legislazione svizzera va adeguata al regolamento (UE) 2016/679, senza tuttavia attuarlo completamente.

Infine, la revisione intende adeguare la legislazione svizzera al 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 Consiglio federale ha deciso di anticipare le relative spiegazioni integrandole nel presente rapporto. In tal modo intende evitare la necessità di svolgere una seconda consultazione.

Riassumendo, conseguendo i suddetti obiettivi s'intende da una parte adeguare la legislazione svizzera all'attuale evoluzione tecnologica e, dall'altra, garantire che la Svizzera rispetti

[41] OCSE, Linee guida sulla protezione dei dati 2013, principi 16-18, 19 lett. g e 20-23.

[42] OCSE; Linee guida 2013, principio 16.

gli impegni risultanti dall'Accordo di associazione a Schengen e possa ratificare la Convenzione STE 108 rivista. Infine occorre assicurare 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 progetto 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 Revisione della legge sulla protezione dei dati

1.4.1 Punti essenziali della revisione

La revisione 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. L'avamprogetto 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 dell'avamprogetto di revisione. Alla stregua della legge vigente, anche l'AP-LPD deve trattare allo stesso modo tutte le tecnologie. In tal modo la legge non si preclude allo sviluppo tecnologico e non impedisce innovazioni. Poiché contrario al carattere tecnologicamente neutro dell'atto normativo, si rinuncia ad esempio al requisito della base legale formale per la «procedura di richiamo» nel settore pubblico.

Il terzo elemento fondamentale è la modernizzazione della terminologia, soprattutto per migliorare la compatibilità con il diritto europeo. 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» è estesa ai «dati genetici» e ai «dati biometrici che identificano un individuo in maniera univoca».

Il quarto elemento fondamentale è il miglioramento della trasmissione transfrontaliera di dati. La normativa applicabile alla comunicazione internazionale di dati viene parzialmente estesa. Permane comunque il principio secondo cui nessun dato può essere trasmesso all'estero in assenza di una protezione adeguata dei dati. Tuttavia, compete al Consiglio federale, e non più al titolare del trattamento, decidere se la legislazione di uno Stato terzo soddisfa tale condizione. In assenza di una tale legislazione, l'AP-LPD prevede diverse possibilità per garantire una protezione adeguata e permettere così lo stesso 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, secondo cui gli obblighi dei titolari del trattamento sono precisati e si basano maggiormente sulla protezione della persona interessata, è strettamente connesso al quinto. L'AP-LPD amplia l'obbligo di informare e i titolari sono tenuti a effettuare una valutazione d'impatto di determinati tipi di trattamento. 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 un maggiore 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 dei suoi omologhi all'estero, non avrà tuttavia il diritto di infliggere sanzioni amministrative; in compenso l'AP-LPD estende notevolmente la parte penale della legge.

1.4.2 Principali novità

1.4.2.1 Modifica del campo d'applicazione della nuova LPD

L'AP-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, 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.

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

L'AP-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. Sono inoltre previste eccezioni. L'avamprogetto introduce altresì l'obbligo d'informare in occasione di decisioni automatizzate (p. es. decisioni fondate unicamente su algoritmi, senza intervento umano) e il diritto della persona interessata di far valere in tal caso il suo punto di vista. Secondo l'avamprogetto, alla persona interessata che esercita il suo diritto d'accesso devono essere fornite informazioni più ampie.

I diritti della persona interessata sono definiti in modo più chiaro in diversi punti. Tra le altre cose, l'AP-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.

1.4.2.3 Incoraggiamento all'autoregolamentazione

La revisione intende incoraggiare l'autoregolamentazione e un comportamento responsabile dei titolari del trattamento. Per agevolare i loro compiti e garantire un maggiore rispetto della legge, l'Incaricato può emanare raccomandazioni di buona prassi. Dato che già oggi l'Incaricato pubblica sul proprio sito raccomandazioni generali, non si tratta di una competenza del tutto nuova. Tuttavia essa sarà estesa. Per l'elaborazione delle raccomandazioni, l'Incaricato deve coinvolgere le cerchie interessate. Queste possono anche elaborare raccomandazioni proprie e farle approvare dall'Incaricato.

Le raccomandazioni di buona prassi permetteranno di disporre di regole più precise nei settori che oggi sollevano numerose questioni, di precisare certe nozioni e le modalità di determinati diritti o obblighi, come pure di responsabilizzare i titolari del trattamento.

Le raccomandazioni di buona prassi non hanno carattere vincolante. Ma il titolare del trattamento che le osserva, rispetta le disposizioni di legge precisate dalle raccomandazioni.

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. L'AP-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 tutti i suoi omologhi europei, non può pronunciare sanzioni amministrative. L'importo massimo della multa è aumentato a 500 000 franchi; l'elenco degli atti punibili è adeguato ai nuovi obblighi dei titolari e dei responsabili del trattamento. L'AP-LPD introduce un reato passibile di pena in caso di violazione dell'obbligo di discrezione e prolunga il termine di prescrizione dell'azione penale per le contravvenzioni. In caso di contravvenzione commessa nell'azienda, le autorità di perseguimento penale – nello specifico i Cantoni – possono rinunciare, a determinate condizioni, a perseguire la persona responsabile e condannare in sua vece l'azienda al pagamento della multa.

1.5 Revisione di altre leggi

Nelle norme specifiche sulla protezione dei dati applicabili alla cooperazione giudiziaria e di polizia istituita da Schengen, l'AP 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 e quelli fondati su giudizi personali.

Inoltre, 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, l'AP 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.

Poiché i registri pubblici relativi ai rapporti di diritto privato non sono più esclusi dal campo d'applicazione della LPD, deve essere adeguata anche la legislazione federale sullo stato civile, in particolare per quanto riguarda il controllo del rispetto della protezione dei dati e i diritti delle persone interessate.

1.6 Altre misure esaminate

Nel contesto dei lavori di revisione, il Consiglio federale ha esaminato altre misure, decidendo alla fine di non integrarle nell'AP. Si tratta in particolare delle seguenti misure.

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

L'opzione di permettere all'Incaricato di emanare regole vincolanti è stata scartata. Anche se avrebbe il vantaggio che l'Incaricato potrebbe obbligare direttamente i destinatari, tale soluzione creerebbe un certo numero di problemi connessi al principio della legalità (delega di competenze all'Incaricato, densità normativa). Rispetto alla soluzione delle raccomandazioni di buona prassi, la procedura di emanazione di tali regole sarebbe inoltre più lenta, poiché occorrerebbe ogni volta seguire la procedura per l'emanazione delle ordinanze dell'Amministrazione federale. Infine, questa opzione lascerebbe poco margine di manovra alle cerchie interessate, il che potrebbe indurle a non rispettare le pertinenti regole.

1.6.2 Inversione dell'onere della prova

Il Consiglio federale ha rinunciato all'inversione dell'onere della prova secondo l'articolo 13*a* della legge federale del 19 dicembre 1986[43] sulla concorrenza sleale (LCSl), secondo cui il giudice può 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) ha evidenziato che le proposte di invertire l'onere della prova incontrano una forte opposizione.

[43] RS **241**

1.6.3 Applicazione collettiva del diritto

Con la revisione della LPD non viene introdotta una normativa sull'applicazione collettiva dei diritti (estensione del diritto delle azioni collettive e introduzione di un'azione o di un concordato collettivi) circoscritta alla protezione dei dati. Gli strumenti dell'applicazione collettiva del diritto saranno invece esaminati in un contesto più ampio e trasversale nell'ambito dell'attuazione della mozione 13.3931 Birrer-Heimo.

1.6.4 Diritto alla portabilità dei dati

Il Consiglio federale 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. Il Consiglio federale ritiene 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. La valutazione 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.

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

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

Il Consiglio federale ha valutato se conferire il compito di elaborare e approvare le raccomandazioni di buona prassi a una commissione extraparlamentare invece che all'Incaricato. La soluzione di affidare tale compito all'Incaricato ha tuttavia il vantaggio di non creare oneri amministrativi e finanziari supplementari e consente di intervenire rapidamente.

1.6.6 Modifica dell'organizzazione dell'autorità di controllo

Il Consiglio federale ha valutato l'opportunità di trasformare l'Incaricato in un'autorità collegiale, decidendo 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 o Spagna).

1.6.7 Introduzione di meccanismi speciali per gestire i conflitti

Il Consiglio federale 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.), l'istituzione di un ulteriore organo di conciliazione porterebbe a conflitti di competenza. Inoltre, l'introduzione di un organo aggregato all'Incaricato causerebbe costi notevoli, il che non è conforme all'attuale politica finanziaria del Governo.

1.7 Analisi d'impatto della regolamentazione

L'analisi d'impatto della regolamentazione (AIR) è uno strumento che permette di esaminare e illustrare gli impatti economici dei progetti legislativi della Confederazione. Si tratta di uno strumento vincolante, importante in particolare nel caso di messaggi, rapporti esplicativi e

proposte del Consiglio federale. Le basi legali dell'AIR si trovano agli articoli 170 Cost. e 141 capoverso 2 della legge federale del 13 dicembre 2002[44] sul Parlamento (LParl).

L'UFG e la Segreteria di Stato dell'economia (SECO) hanno incaricato l'impresa PwC di procedere a un'AIR[45] che possa fungere da base per valutare gli effetti della revisione. L'analisi si fonda soprattutto sui risultati di un sondaggio condotto online presso le imprese e su colloqui effettuati con specialisti della protezione dei dati. In generale, l'AIR giudica il progetto di revisione in modo molto 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.

1.7.1 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 nuovi timori nella popolazione e nuove minacce per la protezione dei dati. L'AP intende soprattutto migliorare la sorveglianza e la disponibilità dei dati come pure la trasparenza dei trattamenti. 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.

1.7.2 Ripercussioni del progetto per i diversi gruppi della società

Le modifiche previste dall'AP riguardano tutte le imprese che operano in Svizzera. Per l'AIR le imprese sono state suddivise secondo la loro «esposizione al diritto in materia di protezione dei dati» dovuta 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*

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 sono in generale poco toccate dalle misure previste dall'AP. L'impatto della revisione su questo segmento è quindi relativamente debole. 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 dall'AP[46].

1.7.3 Ripercussioni per l'economia in generale

Occorre distinguere gli effetti della revisione 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.

---

44 RS **171.10**

45 L'AIR è reperibile sul sito dell'Ufficio federale di giustizia: https://www.bj.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html.

46 Per una visione dettagliata dell'impatto di ciascuna misura, cfr. la tabella riassuntiva a pag. 50 e segg. del rapporto.

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 innanzitutto constatato che dalla revisione non risultano in linea di massima obblighi specifici per le persone interessate, anzi la loro posizione viene migliorata. 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 (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). 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.

1.7.4 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» è accolta con favore poiché permetterebbe un rapido adeguamento alle novità tecnologiche (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

1.7.5 Aspetti pratici dell'esecuzione

Per limitare i costi risultanti dalla revisione, 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, l'AP 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 del trattamento. 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, guide) e l'elaborazione di raccomandazioni di «buona prassi». 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 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 presidenza dell'Unione europea. 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. **Fehler! Verweisquelle konnte nicht gefunden werden.**), 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 effettuare una distinzione 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 determinati 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 (articolo 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, 46 e 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 pertanto 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 Consiglio federale 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, 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 Consiglio federale 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 nell'AP-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 nell'AP-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 nell'AP-LPD. Una parte di tali requisiti è prevista anche dal P-STE 108. Su scala federale, l'autorità di controllo nazionale competente per tutti i settori sottostanti al campo d'applicazione della LPD è in linea di massima 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. 8.3).

La tabella delle concordanze allegata al presente rapporto esplicativo elenca gli articoli corrispondenti dell'AP-LPD, del P-STE 108 e della direttiva (UE) 2016/680.

2.4 Principali modifiche legislative necessarie

Oltre alle modifiche della LPD, gli atti normativi federali da modificare sono i seguenti: il Codice penale (CP)[47], il Codice di procedura penale (CPP)[48], la legge federale del 20 marzo 1981[49] sull'assistenza internazionale in materia penale (AIMP), la legge federale del 3 ottobre 1975[50] relativa al trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale, la legge federale del 12 giugno 2009[51] sullo scambio di informazioni con gli Stati Schengen (LSIS) e la legge federale del 7 ottobre 1994[52] sugli Uffici

47 RS **311.0**
48 RS **312.0**
49 RS **351.1**
50 RS **351.93**
51 RS **362.2**
52 RS **360**

centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati (LUC). Le disposizioni della direttiva (UE) 2016/680 che devono essere trasposte nell'AP-LPD e nelle summenzionate norme sulla protezione dei dati specifiche a determinati settori sono indicate nei commenti ai singoli articoli.

Dato che molte leggi federali che riguardano il settore della polizia contengono disposizioni sulla protezione dei dati, ci si può chiedere se questa dispersione delle disposizioni sulla protezione dei dati 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 Progetto di revisione della Convenzione STE 108 (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 inoltre 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 il principio della protezione dei dati sin dalla progettazione e per impostazione predefinita (art. 8^{bis} 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 deve essere esteso. 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. 12^{bis}), 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 49 Stati che l'hanno ratificata, due non sono membri del Consiglio d'Europa (Uruguay, Maurizio). Inoltre, vari altri Stati non membri stanno per ratificarla (Marocco, Tunisia, Senegal). L'interesse da parte degli Stati extraeuropei alla ratifica della Con-

venzione potrebbe crescere visto che l'Unione europea considera tale ratifica un criterio determinante per la 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 firma del P-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 di dati all'estero). 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[53]. 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[54] fondata sulla valutazione della legge sulla protezione dei dati.

Quanto alla procedura di ratifica, l'articolo 4 della futura Convenzione 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).

Il contenuto dell'AP-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 nell'AP-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

[53] Il Consiglio federale ha in particolare dichiarato il suo sostegno ai lavori in corso nel Consiglio d'Europa nella risposta ai seguenti interventi parlamentari: Ip. Eichenberger 13.4209 («US-Swiss Safe Harbor Framework. Ripristino della fiducia nell'ambito dello scambio di dati con gli Stati Uniti»); Interrogazione Gross 13.1072 («Patto dell'ONU relativo ai diritti civili e politici. Integrazione della protezione dei dati»)

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 Paesi terzi o 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 un certo numero di 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

All'interno dell'Unione europea il regolamento (UE) 2016/679 sostituirà la direttiva 95/46/CE.

Le disposizioni del regolamento (UE) 2016/679 non sono vincolanti per la Svizzera. Tuttavia ciò non significa che nel nostro Paese non esplichino effetto nei settori in cui esso è considerato un Paese terzo. Il regolamento è importante soprattutto per il settore privato. Infatti, come osservato al n. **Fehler! Verweisquelle konnte nicht gefunden werden.**, la Commissione europea ha constatato mediante decisione[55] che la Svizzera garantisce un livello di protezione dei dati adeguato. Tale decisione può tuttavia essere revocata in qualsiasi momento. Se intende beneficiare anche in futuro di una decisione di adeguatezza dell'Unione europea, la Svizzera, in quanto Stato terzo, ha pertanto un 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. L'AP è teso a permettere di garantire un livello di protezione adeguato ai sensi del regolamento.

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

Gli esempi illustrati qui di seguito dimostrano che i Paesi europei non sono gli unici ad aver adottato leggi sulla protezione dei dati[56].

5.1 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[57]. L'autorità di controllo svolge un ruolo di sostegno, consulenza e sorveglianza. L'articolo 29 del decreto 1558/2001[58] le permette di emanare regole amministrative e procedure in relazione al registro delle banche di dati personali (qui appresso «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 della 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 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, vegliare 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. Secon-

---

55 GU L 215 del 25.8.2000, pag. 1.

56 Le seguenti informazioni si basano su una perizia dell'Istituto svizzero di diritto comparato del 3 ago. 2016.

57 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, reperibile all'indirizzo: http://www.jus.gob.ar/media/33481/ley_25326.pdf.

58 Decreto 1558/2001, Protección de los datos personales, reperibile all'indirizzo: http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

do 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.

5.2 Nuova Zelanda

In Nuova Zelanda la protezione dei dati è retta principalmente dal «Pricacy Act 1993»[59]. Attualmente è in corso una revisione di tale atto e il progetto dovrebbe essere posto in consultazione entro il 2016 e 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».

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)[60] 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.

[59] Il «Privacy Act 1993» è reperibile al seguente indirizzo: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

[60] Sono considerate «Agency» praticamente tutte le persone e organizzazioni che dispongono di dati personali.

5.3 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)[61].

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).

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.

5.4 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])[62], 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 APPO). 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 sospensio-

[61] Le pertinenti disposizioni di legge sono reperibili in inglese al seguente indirizzo: http://www.law.goper.kr/eng/engMain.do.

[62] L'APPI è reperibile in inglese al seguente indirizzo: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

ne o il blocco del trattamento, se esso è contrario al suo scopo o se i dati sono stati ottenuti illecitamente. 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.

5.5 Singapore

L'autorità di controllo è la «Personal data protection commission (PDPC)». È stata istituita nel 2013 in attuazione del «Personal Data Protection Act (PDPA)»[63], 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 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

[63] Il PDPA è reperibile 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

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 tale principio.

6 Attuazione

Nel quadro dell'analisi d'impatto della regolamentazione è stato suggerito di evitare, per quanto possibile, termini giuridici indefiniti. La legge sulla protezione dei dati 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. Ciononostante le raccomandazioni di buona prassi intendono soddisfare l'esigenza di termini più esatti e specifici.

Inoltre, per non sovraccaricare la legge con un disciplinamento troppo dettagliato, è previsto di adeguare l'ordinanza relativa alla legge sulla protezione dei dati.

Anche se l'AP 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.

Infine, nella misura in cui il recepimento della direttiva (UE) 2016/680 e l'approvazione 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.

7 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 Consiglio federale 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 Consiglio federale 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 Consiglio federale 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» nell'AP-LPD, il Consiglio federale intende 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 Consiglio federale è preferibile ricorrere alle raccomandazioni di buona prassi.
- Postulato Recordon 13.3989 «Violazioni della personalità riconducibili al progresso delle tecnologie dell'informazione e della comunicazione». Nel contesto dei lavori di revisione il

Consiglio federale ha esaminato le nuove minacce per i diritti della personalità. L'AP-LPD prevede misure per migliorare la tutela di tali diritti.

- Postulati Gruppo liberale radicale 14.4137 e Comte 14.4284 «Registrazioni video di privati. Migliorare la tutela della sfera privata». L'AP-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, che si riallaccia alle disposizioni sulla violazione del segreto e della sfera privata, offre una protezione più estesa.
- 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 Béglé 16.3383 «Dati digitali. Informare le persone lese in caso di pirateria». Secondo l'articolo 17 AP-LPD un trattamento non autorizzato di dati deve essere notificato all'Incaricato e, in determinate circostanze, anche alla persona interessata. Il contenuto della notifica 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. L'AP-LPD prevede diversi obblighi del titolare e del responsabile del trattamento che si applicano anche ai dati medici (art. 13, 15, 16, 17, 18 e 19) e soddisfano le richieste del postulato. Ulteriori misure, quali ad esempio la precisazione dei requisiti per il consenso (art. 4 cpv. 6) nonché l'elaborazione delle raccomandazioni di buona prassi, dovrebbero portare a una maggiore protezione anche per i dati medici.

I seguenti interventi parlamentari possono essere tolti parzialmente dal ruolo:

- Postulato Derder 14.3655 «Definire la nostra identità digitale e identificare le soluzioni per proteggerla». Il Consiglio federale 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. La questione dell'identità digitale può essere esaminata in modo più approfondito nell'ambito dei lavori del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati o nell'ambito della «Strategia Svizzera digitale».
- Postulato Schwaab 14.3739 «Control by design. Potenziare i diritti di proprietà per impedire le connessioni indesiderate». L'AP-LPD adempie parzialmente il postulato in quanto migliora la protezione delle persone interessate. L'oggetto del postulato oltrepassa tuttavia l'ambito dei lavori di revisione, poiché riguarda essenzialmente aspetti legati alla sicurezza dei prodotti e di Internet. Pertanto il Consiglio federale propone di adempiere il postulato nell'ambito dei lavori del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati.
- Postulato Schwaab 14.3782 «Regole per la "morte digitale"»: l'articolo 12 AP-LPD prevede il diritto di accedere ai dati di una persona deceduta e permette inoltre agli eredi di chiedere la cancellazione dei suoi dati. Pertanto l'AP-LPD attua alcune richieste fondamentali del postulato. Altre richieste andranno realizzate nell'ambito della revisione del diritto successorio.
- Postulato Derder 15.4045 «Diritto all'utilizzo dei dati personali. Diritto alla copia». Il Consiglio federale ritiene che nell'ambito della revisione della LPD non sia opportuno introdurre un diritto di portabilità dei dati (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- 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. 1.6.4), l'AP-LPD non prevede alcuna precisazione in merito alla riappropriazione dei dati personali. La questione sarà esaminata dal gruppo di esperti per il futuro del trattamento e della sicurezza dei dati o nell'ambito della «Strategia Svizzera digitale».

8 Modifiche di legge

8.1 Commento all'AP-LPD

8.1.1 Scopo, campo d'applicazione e definizioni

8.1.1.1 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 essa stessa se e a quale scopo possono essere trattati i dati che la riguardano[64].

La disposizione è modificata soltanto sotto il profilo redazionale con l'esplicita menzione che la protezione è limitata alle persone private. L'adeguamento è una conseguenza della modifica del campo d'applicazione (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

8.1.1.2 Art. 2 Campo d'applicazione

Il presente avamprogetto estende parzialmente il campo d'applicazione della legge sulla protezione dei dati, in particolare per soddisfare i requisiti del P-STE 108. Prevede ad esempio 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), e di abrogare le deroghe 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, l'AP-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[65].

Cpv. 1 Applicazione alle persone private

Secondo l'avamprogetto la legge sulla protezione dei dati si applica al trattamento di dati di persone fisiche da parte di privati e organi federali.

Rinuncia alla protezione dei dati di persone giuridiche

L'AP-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)[66], dalla LCSl, dalla legge federale del 9 ottobre 1992[67] sul diritto d'autore (LDA) 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[68]. 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. 5 AP-LPD), il che comporterà probabilmente un aumento della comunicazione all'estero. È infine importante osservare che la maggior parte degli esperti consultati nell'ambito dell'analisi d'impatto

---

64 DTF **140** I 2, consid. 9.1

65 Cfr FF 1988 II 353, 384 e MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 286 segg.

66 RS **210**

67 RS **231.1**

68 In merito alla questione cfr. DECHSLER CHRISTIAN, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, AJP 2016, pag. 80 segg., pag. 85–86.

della revisione della LPD si è detta favorevole a rinunciare alla protezione dei dati delle persone giuridiche[69]. Il Consiglio nazionale ha d'altronde respinto una mozione che proponeva di mantenere la protezione dei dati delle persone giuridiche (cfr. n. 0 Mozione Béglé 16.3379).

La legge del 17 dicembre 2004[70] 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 dell'AP-LPD consegue che l'accesso a documenti ufficiali che contengono informazioni 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. L'articolo 9 LTras non si applica più ai documenti che contengono dati di una persona giuridica. Per tutelare i diritti delle persone giuridiche nel caso in cui una domanda si riferisca a documenti ove la concessione dell'accesso potrebbe ledere la loro sfera privata, l'avamprogetto adegua alcune disposizioni della LTras (cfr. n. 8.2.5).

In seguito all'abrogazione della protezione dei dati delle persone giuridiche, queste non possono più far valere il diritto alla consultazione in virtù della AP-LPD. Possono tuttavia eventualmente chiedere di consultare i documenti pubblici in virtù della LTras, se tali documenti potrebbero contenere informazioni che le riguardano.

Capoverso 2 Deroghe al campo d'applicazione

Come sinora, la legge sulla protezione dei dati non si applica al trattamento di dati da parte di persone fisiche per uso esclusivamente personale (art. 2 cpv. 2 lett. a AP-LPD); l'adeguamento redazionale non contiene 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 (art. 2 cpv. 2 lett. b AP-LPD), per i motivi già illustrati nel messaggio del 23 marzo 1988[71] concernente la legge federale sulla protezione dei dati. Infine, la lettera d del capoverso 2 riprende la deroga per il Comitato internazionale della Croce Rossa (CICR), precisando tuttavia che l'eccezione vale per tutti i beneficiari istituzionali ai sensi della legge del 22 giugno 2007[72] sullo Stato ospite che godono dell'immunità in Svizzera. Va osservato che il CICR è escluso dal campo d'applicazione della legge sulla protezione dei dati anche perché è un'organizzazione internazionale.

Lettera c Deroghe per le autorità giudiziarie federali

Secondo il capoverso 2 lettera c è escluso dal campo d'applicazione anche il trattamento di dati personali da parte delle autorità giudiziarie federali indipendenti, nell'ambito della loro attività giurisdizionale.

La deroga è giustificata dato che sottoporre queste autorità alla sorveglianza dell'Incaricato significherebbe pregiudicare la separazione dei poteri e l'indipendenza della giustizia. Inoltre, in questo ambito i diritti delle parti e dei partecipanti al procedimento sono disciplinati esclusivamente dal diritto procedurale (p. es. per mezzo del diritto di consultare gli atti), che concede loro una tutela equivalente a quella della legge sulla protezione dei dati. Ciò vale soprattutto per i diritti delle parti di conoscere i dati che confluiscono nel procedimento e di rettificare determinati dati, nonché per il trattamento di dati nell'ambito di procedure giudiziarie in generale. Il diritto procedurale non disciplina infatti soltanto lo svolgimento dei procedimenti, bensì anche la tutela della personalità delle parti che forniscono dati per il procedimento. Inoltre, il diritto procedurale esplica effetti anche su procedimenti chiusi. Poiché devono coincidere con il risultato del procedimento, gli atti di un procedimento chiuso possono essere modificati soltanto conformemente al diritto procedurale (rettifica, spiegazione, revisione).

---

69 Cfr. pag. 46 AIR.

70 RS **152.3**

71 FF **1988** II 353, 381

72 RS **192.12**

Affinché la situazione degli atti non venga modificata posteriormente da elementi estranei al procedimento, il diritto procedurale prevede procedure specifiche per la cura degli atti. Riassumendo, il criterio determinante per l'applicabilità della legge sulla protezione dei dati, in particolare a procedimenti chiusi, è l'assenza, sotto il profilo processuale, di un rapporto individuale diretto con un procedimento. Ne consegue che la legge sulla protezione dei dati è applicabile al trattamento di dati da parte dei servizi amministrativi delle autorità giudiziarie federali, ad esempio al trattamento dei dati sul personale[73]. In questo ambito le autorità sottostanno alla sorveglianza dell'Incaricato (ma cfr. il capoverso 3).

A differenza del diritto vigente, il Consiglio federale propone di usare «attività giurisdizionale» invece di «procedimenti pendenti», poiché quest'ultima nozione non rende giustizia a tutti i tipi di procedimenti. In particolare, il termine di «litispendenza» esiste solo nel diritto di procedura civile.

Rientrano nella nozione di «autorità giudiziarie federali indipendenti» ad esempio il Ministero pubblico della Confederazione, la giustizia militare o le autorità di ricorso indipendenti secondo l'articolo 47 della legge federale del 20 dicembre 1968[74] sulla procedura amministrativa (PA). La deroga non riguarda invece le autorità cantonali poiché, se il diritto federale non prevede altrimenti, il loro trattamento di dati è disciplinato dal diritto cantonale sulla protezione dei dati. Se i dati personali sono trattati da un'autorità che non può essere designata un'«autorità giudiziaria federale indipendente», la presente deroga non si applica. Il trattamento di dati da parte delle autorità federali di polizia nell'ambito della procedura penale rientra pertanto nel campo d'applicazione dell'AP-LPD; sono tuttavia fatte salve le norme sulla protezione dei dati specifiche a determinati settori. Lo stesso vale per il trattamento di dati da parte di autorità federali nell'ambito di una procedura penale amministrativa. Va infine sottolineato che il nuovo tenore della deroga di cui alla lettera c non ha ripercussioni per le procedure amministrative di prima istanza, che, come sinora, rientrano nel campo d'applicazione della legge sulla protezione dei dati.

Abrogazione della deroga per i registri pubblici (art. 2 cpv. 2 lett d LPD)

Il Consiglio federale ritiene che questa deroga non sia compatibile con l'articolo 3 del P-STE 108. La modifica riguarda unicamente i registri pubblici relativi ai rapporti di diritto privato tenuti dalle autorità federali, ossia Infostar, Zefix, il registro aeronautico dell'Ufficio federale dell'aviazione civile e il registro dei marchi dell'Istituto federale della proprietà intellettuale. 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 sulla protezione dei dati non può impedire l'applicazione corretta e uniforme del diritto privato federale. L'abrogazione dell'articolo 2 capoverso 2 lettera d LPD non ha pertanto conseguenze per i registri seguenti.

- Il registro fondiario è un registro pubblico di competenza dei Cantoni. In virtù delle disposizioni federali sul diritto in materia di registro fondiario (art. 942 segg. CC, art. 955 CC e ordinanza del 23 settembre 2011[75] sul registro fondiario [ORF]), gli uffici del registro fondiario dei Cantoni devono tenere un registro fondiario. I Cantoni sono responsabili dei danni derivanti dalla tenuta dei registri (art. 955 CC).
- Nel settore dei trasporti la tenuta del registro del naviglio compete ai Cantoni (art. 1 e 4 dell'ordinanza del 16 giugno 1986[76] sul registro del naviglio). Alla tenuta del registro è applicabile l'ORF, salvo disposizioni contrarie della legislazione federale sul registro del naviglio.
- Secondo l'articolo 927 del Codice delle obbligazioni (CO) [77], ogni Cantone deve tenere un registro di commercio, designare l'ufficio incaricato della tenuta corretta e prevedere

[73] Cfr. FF **1988** II 383

[74] RS **172.021**

[75] RS **211.432.1**

[76] RS **747.111**

[77] RS **220**

un'autorità incaricata di esercitare la vigilanza su tale ufficio (art. 3 e 4 cpv. 1 dell'ordinanza del 17 ottobre 2007[78] sul registro di commercio).

- La tenuta del registro sulle esecuzioni e sui fallimenti compete ai Cantoni (art. 8 cpv. 1 della legge federale dell'11 aprile 1889[79] sulla esecuzione e sul fallimento).
- Il registro pubblico sulle riserve di proprietà è tenuto dagli uffici cantonali delle esecuzioni (art. 715 CC).

Capoverso 3 Tribunali della Confederazione

Secondo l'articolo 2 capoverso 3, la legge sulla protezione dei dati non si applica al trattamento di dati personali da parte dei tribunali della Confederazione nell'ambito della loro attività giurisdizionale. Questa eccezione si applica per i medesimi motivi illustrati in riferimento alle autorità giudiziarie federali indipendenti (cfr. il commento all'art. 2 cpv. 2 lett. c).

Il trattamento di dati personali da parte dei tribunali della Confederazione che rientra nel campo d'applicazione della legge sulla protezione dei dati non sottostà alla sorveglianza dell'Incaricato (art. 3 cpv. 3 secondo periodo AP-LPD). La deroga è giustificata dal fatto che l'AP-LPD conferisce all'Incaricato la competenza di emanare decisioni nei confronti di organi federali. Vi sarebbe quindi il pericolo che ciò pregiudichi l'indipendenza dei tribunali 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, i tribunali della Confederazione dovranno prevedere una forma propria di sorveglianza sulla protezione dei dati, la cui organizzazione rientra nella loro sfera di competenza ed è ancora oggetto di colloqui.

Capoverso 4 Sorveglianza sul Consiglio federale

Il capoverso 4 corrisponde all'articolo 27 capoverso 1 secondo periodo LPD, secondo cui la sorveglianza non può essere esercitata sul Consiglio federale. Tale principio resta invariato.

Inoltre, anche l'Assemblea federale non sottostà alla sorveglianza dell'Incaricato.

Campo d'applicazione territoriale

Al contrario di quanto previsto dal regolamento (UE) 2016/679 (art. 3), l'AP-LPD non contiene disposizioni specifiche relative al campo d'applicazione territoriale della legge. Il Consiglio federale ritiene che il diritto attuale permetta già in larga misura di applicare la LPD a situazioni che presentano aspetti internazionali. In virtù della teoria delle conseguenze ciò vale anche per il diritto pubblico[80].

Piuttosto che in riferimento al campo d'applicazione territoriale, le difficoltà si pongono nell'attuazione ed esecuzione delle decisioni, in particolare nel settore di Internet. Il Consiglio federale 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[81]. È invece preferibile una soluzione per mezzo di accordi di assistenza giudiziaria bi- o multilaterali che permettano l'invio postale diretto 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. Infine, il Consiglio federale osserva che l'obbligo di designare

78 RS **221.411**

79 RS **281.1**

80 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»).

81 http://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).

un recapito è previsto nella PA e nella legge del 17 giugno 2005[82] sul tribunale amministrativo federale.

8.1.1.3 Art. 3 Definizioni

Lettera a 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, per esempio grazie all'indicazione del suo nome, a un numero d'identificazione, ai dati relativi alla sua ubicazione, alla sua identità su Internet oppure a vari aspetti specifici riguardanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali. Come nel diritto attuale, la mera possibilità teorica che qualcuno possa essere identificato non è sufficiente per supporre che una persona sia identificabile. Occorre invece tenere conto di tutti i mezzi che possono essere ragionevolmente impiegati per identificare una persona. I mezzi tecnici a disposizione sono esaminati in relazione al dispendio di tempo e all'onere finanziario necessari per applicarli. Viste le tecnologie sempre più precise per analizzare i dati e il loro costante sviluppo, il confine tra dati personali e altri dati è tuttavia sempre più sfuocato. I dati in base ai quali oggi vi è una mera possibilità teorica di identificazione, potranno forse in futuro essere attribuiti a una persona identificabile.

Va osservato che la legge sulla protezione dei dati usa in linea di massima il termine «dati personali». All'interno dello stesso capoverso per gli stessi viene a volte usato, soprattutto nella versione tedesca, anche il termine «dati» se è ovvio che con tale termine s'intendono i dati personali. Negli altri casi, se si parla di «dati» si tratta di dati che non sono personali, come per esempio nel caso della profilazione.

Lettera c Dati personali degni di particolare protezione

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

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. k della legge federale dell'8 ottobre 2004[83] sugli esami genetici sull'essere umano).

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, quali l'immagine del viso o i dati dattiloscopici. Le fotografie rientrano quindi nella definizione dei dati biometrici soltanto quando sono trattate con una tecnica specifica che permette l'identificazione o l'autenticazione univoca di una persona.

Come nel P-STE 108 (art. 6 cpv. 1), nella direttiva (UE) 2016/680 (art. 10) e nel regolamento (UE) 2016/679 (art. 9), i dati degni di particolare protezione comprendono anche quelli sulla vita sessuale della persona interessata. Tali dati sono contemplati dal termine «sfera intima».

Lettera 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 cpv. 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.).

---

82 RS **173.32**

83 RS **810.12**

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

Lettera f Profilazione

Il Consiglio federale propone 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 1992, questa espressione non ha avuto molta importanza e, vista l'evoluzione tecnologica, appare oggi obsoleta. Nell'AP-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. Per profilazione s'intende quindi qualsiasi elaborazione di dati, personali o no, tesa ad analizzare le caratteristiche essenziali di una persona o predirne gli sviluppi. Quali esempi di caratteristiche personali che possono essere analizzate, l'AP-LPD menziona il rendimento professionale, la situazione economica, la salute, la sfera intima o gli spostamenti. La profilazione può ad esempio avere lo scopo di valutare l'idoneità di una persona a svolgere una determinata attività.

La definizione del termine comprende l'analisi di dati personali e di altri dati tenendo pertanto conto del fatto che, grazie all'evoluzione tecnologica (Big Data), è vieppiù possibile analizzare dati di carattere non personale in modo tale da ottenere dati personali. Non ha importanza che il titolare del trattamento proceda alla profilazione per scopi propri o di terzi. Inoltre, il termine comprende sia l'analisi automatizzata sia quella non automatizzata dei dati (per la delimitazione rispetto alla decisione individuale automatizzata si veda il n. **Fehler! Verweisquelle konnte nicht gefunden werden.**), poiché il grado di automatizzazione del trattamento (p. es. con o senza algoritmo) non è un criterio oggettivo per decidere quali attività richiedano una protezione particolare della persona interessata. È invece determinante che i dati siano trattati allo scopo di analizzare caratteristiche personali essenziali. In tal modo si evitano lacune della protezione nel passaggio da «profilo della personalità» a «profilazione». Inoltre, il nuovo termine permette di mettere a disposizione degli organi federali una base legale più precisa. Soltanto agli organi federali che praticano la profilazione è conferita la pertinente competenza.

I dati ottenuti grazie a una profilazione sono in linea di principio dati personali ai sensi dell'articolo 3 lettera a AP-LPD. A seconda del contenuto può trattarsi anche di dati degni di particolare protezione.

Lettera h Titolare del trattamento

L'AP-LPD introduce questa espressione per 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). Per «titolare del trattamento» s'intende la persona privata o l'organo federale che determina le finalità e i mezzi del trattamento di dati. Affinché si possa parlare di «titolare del trattamento» devono pertanto essere soddisfatti due criteri cumulativi: la persona privata o l'organo federale deve determinare, da una parte, le finalità del trattamento di dati e, dall'altra, i mezzi. Questa definizione si distingue quindi parzialmente da quella di «detentore di una collezione di dati», la quale non implica la realizzazione del secondo criterio. Il criterio determinante non è più quello di sapere chi decide in merito al contenuto della collezione, bensì chi decide in merito ai mezzi per il trattamento di dati previsto.

Lettera i 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).

Il contratto che vincola il titolare e il responsabile del trattamento può essere di natura diversa: può trattarsi di un mandato (art. 394 segg. CO), di un contratto di appalto (art. 363 segg.

CO) o di un contratto misto, a seconda degli obblighi del responsabile del trattamento. Un impiegato con un contratto di lavoro non è invece considerato un responsabile del trattamento nei confronti del suo datore di lavoro.

Termini immutati

I seguenti termini restano immutati o subiscono soltanto adeguamenti redazionali rispetto al diritto vigente: persona interessata (lett. b), comunicazione (lett. e) e organi federali (lett. g).

Termini abrogati

Sono abrogati i seguenti termini.

- Detentore di una collezione di dati: l'espressione è sostituita da «titolare del trattamento».
- Collezione di dati: l'AP-LPD rinuncia a questa definizione 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 pescano dati in diversi server per analizzare determinati aspetti della personalità di un individuo. Queste attività non sono contemplate dalle disposizioni della legge vigente, poiché queste ultime implicano la presenza di una collezione, come ad esempio il diritto d'accesso (art. 8 LPD) e l'obbligo d'informare (art. 14 LPD). Ma è proprio per questo tipo di attività che è necessaria maggiore trasparenza. Il Consiglio federale sottolinea 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[84].
- Legge in senso formale: l'AP-LPD sopprime questa definizione poiché non è necessaria.

8.1.2 Disposizioni generali di protezione dei dati

8.1.2.1 Art. 4 Principi

Capoversi 1 e 2 Liceità e principio di proporzionalità

I capoversi 1 e 2 relativi ai principi della liceità, della buona fede e della proporzionalità restano invariati, fatta salva una modifica redazionale nel capoverso 2 della versione francese.

Capoverso 3 finalità vincolanti 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 essere più conforme al testo del P-STE 108 (art. 5 n. 4 lett. b), l'AP-LPD sancisce che i dati devono essere raccolti per determinate finalità chiaramente riconoscibili da parte della persona interessata. Questa nuova formulazione non comporta modifiche materiali rispetto al diritto in vigore: la raccolta dei dati e 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 scopi vaghi, non definiti o imprecisi non sono ammessi. La determinatezza va giudicata secondo le circostanze, restando fermo l'obiettivo di garantire un equilibrio tra gli interessi delle persone interessate, del titolare o del responsabile del trattamento e della società in generale.

Sempre in adeguamento alla terminologia dei testi europei (art. 5 par. 4 lett. b del P-STE 108, art. 4 par. 1 lett. b della direttiva (UE) 2016/680 e art. 5 par. 1 lett. b del regolamento (UE) 2016/679), l'AP-LPD prevede nello stesso capoverso che i dati non possono essere trattati in modo incompatibile con le finalità iniziali. Il trattamento è incompatibile se la persona interessata può legittimamente considerarlo inatteso, inappropriato o contestabile. Si possono ipotizzare i casi seguenti:

[84] MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 563; BELSER URS, in: Maurer-Lambrou/Vogt (Hg.), Basler Kommentar, Datenschutzgesetz, 2. Aufl., Basilea 2006, art. 3 LPD N 32; GAAC 62.57.

- l'utilizzazione a fini pubblicitari di indirizzi ottenuti in occasione della raccolta di firme per una campagna politica;
- 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);
- la raccolta e l'utilizzazione, per l'invio di spam, di indirizzi di posta elettronica trasmessi da una persona per una determinata finalità[85];
- la raccolta da parte di un'impresa privata di indirizzi IP di titolari di collegamenti che offrono illecitamente opere da scaricare[86].

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[87]. Il trattamento 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).

Secondo il capoverso 4 i dati possono essere conservati in una forma che consenta l'identificazione delle persone interessate soltanto per la durata necessaria al conseguimento delle finalità per le quali sono trattate. Il Consiglio federale propone di menzionare esplicitamente questa condizione, che si evince già dal principio di proporzionalità (art. 4 cpv. 2 LPD), per conformità al P-STE 108 (art. 5 par. 1 lett. e), alla direttiva (UE) 2016/680 (art. 4 par. 1 lett. e) e al regolamento (UE) 2016/679 (art. 5 par. 1 lett. e). In singoli casi determinate finalità possono comportare una durata di conservazione non anonimizzata relativamente lunga. Ciò vale in particolare per gli archivi pubblici, che in virtù dei loro compiti legali possono conservare dati anche a lungo termine.

Capoverso 5 Esattezza

Il capoverso 5 dell'AP-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 dai testi europei (art. 5 del P-STE 108, art. 4 della direttiva [UE] 2016/680 e art. 5 del regolamento [UE] 2016/679). La modifica non comporta modifiche materiali. Anche in futuro ogni persona che tratta dati personali dovrà accertarsi che questi siano esatti e aggiornati (obbligo di accertamento). Se sono incompleti o non aggiornati i dati personali trattati vanno corretti e completati (obbligo di diligenza), altrimenti devono essere cancellati (obbligo di cancellazione). Tali obblighi valgono in linea di massima per tutte le persone che trattano dati e per tutti i tipi di trattamento, poiché è nell'interesse sia di dette persone sia di quelle interessate che i dati trattati siano aggiornati ed esatti.

In riferimento all'attività di archivi, musei, biblioteche e altre istituzioni della memoria collettiva tali obblighi 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[88] 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 di tali documenti. 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, ciò sia ritenuto esatto o meno. Questa attività specifica è di notevole interesse pubblico.

---

85 GAAC 69.106 consid. 5.6.

86 DTF **136** II 508 consid. 4.

87 MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 731.

88 RS **432.21**

In adeguamento alla terminologia dei suddetti atti europei, nel testo francese il termine «correct» è sostituito da «exact»; in tedesco e in italiano la terminologia è già conforme. Si precisa inoltre che i dati devono essere aggiornati. Ciò non comporta modifiche materiali, poiché anche secondo il diritto vigente i dati devono essere completati e aggiornati secondo le circostanze[89].

Capoverso 6 Consenso

Il primo periodo stabilisce che quando il trattamento di dati personali è subordinato al consenso della persona interessata, il consenso è valido soltanto se espresso liberamente e in modo inequivocabile dopo debita informazione della persona interessata. Il nuovo tenore permette di adeguare la legge al P-STE 108 (art. 5 par. 2) e al regolamento (UE) 2016/679 (art. 4, n. 11 e 6, par. 1, lett. a). Come nel diritto vigente, il consenso deve essere dato per un trattamento specifico o una categoria di trattamento specifica e comprendere l'intero scopo del trattamento. Con questa formulazione il consenso resta privo di regole formali e può essere dato anche mediante atti concludenti. Non vi è invece consenso se la persona si astiene da qualsiasi atto.

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. Nelle versioni francese e italiana del testo, i termini «explicite» ed «esplicito» sono sostituiti da «exprès» ed «espresso». Questa modifica permette di porre fine alle controversie dottrinali riguardanti la qualità del consenso[90] e di soddisfare i requisiti della P-STE 108 (art. 5 par. 2); il regolamento (UE) 2016/679 (art. 4 n. 11 e 6 par. 1 lett. a) prevede un disciplinamento analogo. Il consenso espresso deve risultare da una dichiarazione scritta (anche per via elettronica) o orale oppure mediante segnali appositi, ad esempio attivando una casella o cliccando su un pulsante (p. es. «prosegui») in un sito Internet, optando per determinati parametri tecnici nel caso di servizi di imprese che trattano informazioni oppure ricorrendo a un altro tipo di dichiarazione.

8.1.2.2 Art. 5 Comunicazione di dati all'estero

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 loro protezione adeguata (par. 2). Il paragrafo 3 di tale articolo definisce i casi in cui tale condizione è soddisfatta. Il disciplinamento previsto dall'articolo 5 costituisce anche un adeguamento al diritto dell'Unione europea (art. 45 segg. del regolamento (UE) 2016/679).

Capoverso 1 Principio

Il capoverso 1 riprende il principio sancito dall'articolo 6 capoverso 1 LPD, cancellando tuttavia «dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata». Si tratta di un adeguamento redazionale resosi necessario in seguito al nuovo capoverso 2.

Capoverso 2 Constatazione del Consiglio federale

Secondo il capoverso 2 possono essere comunicati dati all'estero se il Consiglio federale ha constatato che lo Stato estero dispone di una legislazione che garantisce una protezione adeguata dei dati. La disposizione conferisce esplicitamente al Consiglio federale la competenza di verificare l'adeguatezza della legislazione estera nel settore della 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[91], ricorrendo, se del caso, all'elenco degli

---

89 MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 753 seg.; cfr. anche FF **1988 353,** 390

90 Certi autori distinguono il consenso «esplicito» dagli atti concludenti, mentre altri ritengono che il consenso esplicito può risultare anche da un atto concludente, a condizione che l'intenzione della persona interessata sia chiara. Per un riassunto delle opinioni in merito a tale questione: VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16 nov. 2015.

91 FF **2003** 1885, 1910 seg.

Stati che soddisfano tale condizione pubblicato dall'Incaricato (art. 7 OLPD)[92]. Per garantire l'applicazione uniforme del capoverso 2, l'adeguatezza della legislazione estera sarà in futuro verificata dal Consiglio federale, che redigerà un elenco degli Stati la cui legislazione garantisce una protezione adeguata (cpv. 7). 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 Consiglio federale dovrà anche valutare il modo in cui tale Stato applica la legislazione. Il risultato della verifica sarà pubblicato in un'ordinanza del Consiglio federale inserita nella Raccolta sistematica del diritto federale. Tale 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 Consiglio federale è giunto alla conclusione che essa non soddisfa i requisiti per garantire una protezione adeguata. Con la revisione, l'elenco del Consiglio federale diventa un criterio legale vincolante per i titolari del trattamento che intendono comunicare dati all'estero, mentre l'elenco dell'Incaricato previsto dal diritto vigente è inteso come mero strumento ausiliario messo a disposizione dei titolari.

Se il Consiglio federale constata che la legislazione di uno Stato garantisce una protezione adeguata, la libera comunicazione di dati personali a tale Stato è consentita sia ai titolari privati del trattamento sia agli organi federali.

Capoverso 3 Assenza di una decisione del Consiglio federale

In assenza di una decisione del Consiglio federale ai sensi del capoverso 2, il capoverso 3 lettere a-d prevede che possono essere comunicati dati all'estero se è garantita una protezione appropriata dei dati. L'AP-LPD segue l'esempio dell'Unione europea usando due termini differenti nei capoversi 2 e 3. Il termine «adeguata» è riservato alla qualifica della legislazione estera.

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, bensì anche qualsiasi altro trattato internazionale che preveda lo scambio di dati tra gli Stati contraenti e che rispetti le condizioni della Convenzione STE 108. Può anche trattarsi di un trattato internazionale che il Consiglio federale ha concluso in virtù dell'articolo 56 lettera b AP-LPD.

Il capoverso 3 lettere b e c 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).

Capoverso 3 lettera b Garanzie specifiche

Secondo il capoverso 2 lettera b i dati possono essere trasferiti all'estero se sono previste garanzie specifiche di protezione e se queste sono state previamente comunicate all'Incaricato. Se ha obiezioni nei confronti delle garanzie specifiche, l'Incaricato deve informarne il titolare o il responsabile del trattamento entro 30 giorni dalla ricezione delle garanzie (cpv. 4). L'articolo 6 capoverso 2 dell'OLDP prevede la stessa cosa. Se l'Incaricato non ha obiezioni o se scade il relativo termine, il titolare del trattamento è autorizzato a trasmettere i dati all'estero. Come nel diritto vigente, spetta al titolare del trattamento dimostrare che ha preso tutti i provvedimenti necessari affinché sia garantita una protezione appropriata e il destinatario rispetti le garanzie. Il titolare del trattamento resta anche responsabile dei pregiudizi che potrebbero risultare da una violazione delle garanzie.

Come si evince dalla terminologia usata, le «garanzie specifiche» riguardano un caso specifico di comunicazione di dati all'estero e non le comunicazioni effettuate in forma standardiz-

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

zata. Nel settore privato tali garanzie possono essere clausole contrattuali convenute tra il titolare del trattamento e il destinatario. Nel settore pubblico l'organo federale che acconsente alla cooperazione può vincolare il suo consenso a condizioni inerenti alla protezione dei dati. Contrariamente alle garanzie standardizzate (cfr. lett. c), le garanzie specifiche che nel singolo caso garantiscono una protezione adeguata valgono solo per la comunicazione prevista nel relativo contratto. Se il titolare del trattamento intende comunicare altri dati deve in linea di principio fissare nuove garanzie.

Capoverso 3 lettera c Garanzie standardizzate

Secondo il capoverso 3 lettera c, i dati possono essere comunicati all'estero per mezzo di garanzie standardizzate. Tali garanzie possono essere elaborate dai privati o dalle cerchie interessate (n. 1) oppure stabilite o riconosciute dall'Incaricato (n. 2). Anche gli organi federali possono ricorrere a questo tipo di garanzie. Per «garanzie standardizzate» 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 da privati al quale le persone private possono aderire volontariamente.

Nel caso previsto al capoverso 3 lettera c numero 1, le garanzie 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 inoltre a quella prevista dall'articolo 12bis paragrafo 2 lettera b del P-STE 108. L'Incaricato dispone di un termine di 6 mesi per comunicare al titolare del trattamento se approva le garanzie (cpv. 5 primo periodo). Il periodo decorre dal momento in cui l'Incaricato riceve la documentazione completa, ossia tutte le informazioni necessarie per giudicare l'adeguatezza delle garanzie standardizzate. Si tratta di un termine ordinatorio e quindi, in caso di mancato rispetto, si applicano le prescrizioni della denegata giustizia. Il titolare del trattamento non può comunicare dati all'estero prima di aver ricevuto una pertinente decisione impugnabile dell'Incaricato (art. 5 PA).

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

Capoverso 3 lettera d Norme vincolanti d'impresa inerenti alla protezione dei dati

Secondo il capoverso 3 lettera d, i dati possono essere comunicati all'estero se la loro protezione è garantita da norme vincolanti d'impresa previamente approvate dall'Incaricato (n. 1) o da un'autorità incaricata della protezione dei dati all'estero (n. 2). 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 di norme vincolanti d'impresa è disciplinata dall'articolo 57 paragrafo 1 lettera s del regolamento (UE) 2016/679. Il capoverso 3 lettera d costituisce un inasprimento del diritto in vigore poiché le norme vincolanti d'impresa devono essere approvate dall'Incaricato. Quest'ultimo ha a disposizione un termine di sei mesi per comunicare all'impresa l'approvazione o meno delle norme vincolanti sottopostegli (cpv. 5). Prima dell'approvazione i dati non possono essere trasmessi all'estero. La decisione dell'Incaricato è impugnabile.

Se le norme vincolanti d'impresa sono state approvate da un'autorità estera incaricata della protezione dei dati (cpv. 3 lett. d n. 2), l'impresa con sede in Svizzera deve comunicarlo

all'Incaricato affinché questi possa esercitare i suoi compiti di sorveglianza (cpv. 6). Questa disposizione risponde alle necessità dei gruppi imprenditoriali con sedi in vari Paesi.

Le norme di cui al capoverso 3 lettera d devono essere «vincolanti» nel senso 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 in questione, 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 regole normative. Se necessario, nell'ordinanza d'esecuzione il Consiglio federale può definire i criteri che devono soddisfare le norme vincolanti d'impresa.

Capoverso 7 Pubblicazione dell'elenco

L'elenco del Consiglio federale è pubblicato (cpv. 7). Va osservato che la futura ordinanza d'esecuzione andrà regolarmente aggiornata. In altre parole, il Consiglio federale dovrà verificare periodicamente la legislazione degli Stati che figurano nell'elenco. Potrà fondarsi anche sulle valutazioni del Consiglio d'Europa e dell'Unione europea.

La violazione dell'articolo 5 è punita (art. 50 cpv. 2 lett. b e 41 cpv. 1 lett. a AP-LPD).

8.1.2.3 Art. 6 Comunicazione di dati all'estero in casi eccezionali

Capoverso 1 Casi eccezionali

Analogamente al diritto in vigore (art. 6 cpv. 2 LPD), l'articolo 6 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. Il consenso della persona interessata è valido se sono soddisfatte le condizioni di cui all'articolo 4 capoverso 6 AP-LPD. La persona interessata deve in particolare essere informata dei rischi della comunicazione dei dati.

La lettera b corrisponde all'articolo 6 capoverso 2 lettera c LPD.

La lettera c numero 1 corrisponde all'articolo 6 capoverso 2 lettera d LPD prima parte del periodo. 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 per motivi umanitari, 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 all'articolo 6 capoverso 2 lettera d LPD seconda parte del periodo, salvo che l'espressione «in giustizia», ritenuta troppo limitativa, è sostituita con «dinnanzi a un'autorità giudiziaria o amministrativa».

La lettera d precisa che la comunicazione è inoltre lecita se è necessaria per proteggere la vita o l'incolumità fisica 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. Visto che è stato abrogato l'articolo 2 capoverso 2 lettera d LPD riguardante i registri pubblici relativi ai rapporti di diritto privato, è necessario precisare 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.

Capoverso 2 Comunicazione all'Incaricato

Il capoverso 2 obbliga il titolare o il responsabile del trattamento a informare l'Incaricato quando comunica dati personali in virtù delle lettere b-d. La disposizione si applica sia ai titolari privati sia agli organi federali ed attua i requisiti dell'articolo 12 paragrafo 5 P-STE 108.

La violazione dell'articolo 6 è punita conformemente all'articolo 51 capoverso 1 lettera a AP-LPD.

8.1.2.4 Art. 7 Affidamento del trattamento a un responsabile

I capoversi 1, 2 e 4 contengono modifiche terminologiche resesi necessarie a causa delle nuove espressioni introdotte nell'AP-LPD (responsabile del trattamento, titolare del trattamento).

Secondo il capoverso 2 il titolare del trattamento dovrà in futuro assicurare che il responsabile del trattamento sia in grado di garantire, oltre alla sicurezza dei dati, anche i diritti della persona interessata. Questa estensione è resa necessaria dalla direttiva (UE) 2016/680 (art. 22 par. 1). Il Consiglio federale ritiene inoltre che una trasposizione unicamente negli ambiti contemplati da Schengen non abbia senso, tanto più che il regolamento (UE) 2016/679 (art. 28 par. 1) prevede la stessa regola. Il Consiglio federale ha inoltre la possibilità di definire in un'ordinanza ulteriori obblighi del responsabile del trattamento.

Secondo il nuovo capoverso 3, il responsabile del trattamento può conferire il trattamento a un terzo soltanto previo accordo scritto del titolare del trattamento. Può trattarsi di una dichiarazione generale di consenso, nel qual caso il responsabile del trattamento informa il titolare di qualsiasi modifica (aggiunta o sostituzione di mandatari), in modo da permettergli di presentare obiezioni. Si tratta di una condizione della direttiva (UE) 2016/680 (art. 22 cpv. 2) per il settore Schengen; il regolamento (UE) 2016/679 (art. 28 par. 2) prevede una disposizione analoga. Il Consiglio federale ha scelto di applicare la disposizione a tutti i casi di conferimento a un responsabile, il che permette di migliorare la trasparenza dei trattamenti e il controllo dei propri dati da parte delle persone interessate. Secondo l'articolo 13 capoverso 4, il titolare del trattamento che affida il trattamento a un responsabile è inoltre tenuto a informarne la persona interessata e comunicarle i dati o le categorie di dati trattati.

8.1.2.5 Art. 8 Raccomandazioni di buona prassi

Il carattere generale e tecnologicamente neutro delle disposizioni della LPD può comportare presso i titolari o i responsabili del trattamento e le persone interessate una grande incertezza in merito al giusto comportamento, soprattutto nel settore privato. Secondo il Consiglio federale è pertanto fondamentale prevedere la possibilità di fissare, a complemento della legge, regole più precise e dinamiche. Propone pertanto di formalizzare l'elaborazione e l'emanazione di raccomandazioni di buona prassi che permettano di prevedere soluzioni più precise nei settori che sollevano attualmente numerose questioni (p. es. videosorveglianza, cloud-computing o reti sociali) nonché di precisare determinate nozioni (p. es. il rischio elevato secondo l'art. 16 AP-LPD) e le modalità di determinati diritti e obblighi, come ad esempio le modalità del diritto di essere sentiti in caso di decisione individuale automatizzata (art. 15 e 20 cpv. 3 AP-LPD) o le modalità dell'obbligo d'informare (art 13 e 14 AP-LPD) e dell'obbligo di valutare l'impatto del trattamento (art. 16 AP-LPD). Le raccomandazioni possono essere emanate sia per il settore privato sia per quello pubblico.

L'elaborazione di regole di comportamento e la promozione dell'autoregolamentazione da parte degli Stati e dell'autorità di sorveglianza sono previste anche dagli articoli 40 e 57 paragrafo 1 lettera m del regolamento (UE) 2016/679.

Capoverso 1 Elaborazione da parte dell'Incaricato

Secondo il capoverso 1, l'Incaricato elabora raccomandazioni di buona prassi. L'idea di conferire tale compito a una commissione extraparlamentare è stata scartata nel corso dei lavori

preliminari (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Appare infatti chiaro che, visto il suo ruolo e la sua esperienza, l'Incaricato è la persona più adatta a svolgere questo compito in modo efficace. Le raccomandazioni possono precisare singoli aspetti della legge relativi in particolare alla trasparenza del trattamento dei dati, ai diritti delle persone interessate e agli obblighi del titolare e del responsabile del trattamento.

Si tratta di formalizzare ed estendere un'attività che l'Incaricato svolge in parte già nell'ambito dei suoi attuali compiti d'informazione e di consulenza (art. 28, 30 e 31 LPD). Nell'elaborare le raccomandazioni l'Incaricato deve coinvolgere le diverse cerchie interessate, quali l'economia, le associazioni dei consumatori o i pazienti. Deve inoltre tenere conto delle specificità dei settori del trattamento di dati come pure dell'elevato bisogno di tutela delle persone particolarmente vulnerabili, quali i minori, le persone disabili e quelle anziane.

Capoverso 2 Elaborazione da parte delle cerchie interessate

Secondo il capoverso 2, anche le cerchie interessate possono elaborare raccomandazioni di buona prassi oppure completare o modificare quelle dell'Incaricato. In seguito possono sottoporgliele per approvazione a. L'incaricato le approva se ritiene che siano rispettate le disposizioni sulla protezione dei dati (anche quelle di testi legislativi diversi dall'AP-LPD). Permettendo ai settori interessati di essere attivi e partecipare alla regolamentazione di un settore, il Consiglio federale intende favorire soluzioni specifiche concordate e largamente accettate nei singoli settori. Tali soluzioni sarebbero particolarmente utili nel settore di Internet (protezione dei dati nelle reti sociali, utilizzazione di cookie, ecc.), nel quale la regolamentazione statale spesso non è sufficiente per proteggere i diritti delle persone interessate.

Nel settore di Internet e delle telecomunicazioni gli ambienti interessati hanno adottato dei codici di comportamento che, anche se non riguardano specificamente il settore della protezione dei dati, in certi casi proteggono i diritti delle persone interessate anche in tale settore. Si tratta, da una parte, della nuova iniziativa settoriale dell'Associazione svizzera delle telecomunicazioni per la tutela dei giovani dai nuovi mass media e per la promozione delle competenze in materia di mass media nella società[93]. Per i firmatari l'iniziativa prevede determinati obblighi riguardanti il blocco di certi siti Internet e l'adozione di misure per migliorare la protezione dei giovani nei nuovi media. Inoltre, il 1° febbraio 2013 la Swiss Internet Industry Association (Simsa) ha adottato un Codice di condotta hosting (CCH)[94] destinato ai fornitori di servizi di hosting.

Capoverso 3 Pubblicazione

Secondo il capoverso 3 l'Incaricato pubblica, ad esempio sul proprio sito Internet, le raccomandazioni di buona prassi.

8.1.2.6 Art. 9 Rispetto delle raccomandazioni di buona prassi

Osservando le raccomandazioni di buona prassi, il titolare o il responsabile del trattamento rispetta automaticamente le disposizioni sulla protezione dei dati concretizzate da dette raccomandazioni (Art. 9 cpv. 1 AP-LPD). Questa disposizione intende chiarire che il rispetto delle raccomandazioni di buona prassi equivale materialmente al rispetto della legge. Nel contempo chiarisce anche la natura delle raccomandazioni, il cui compito è di concretizzare la legge.

Secondo il capoverso 2 le disposizioni sulla protezione dei dati possono anche essere rispettate in maniera diversa da quella prevista dalle raccomandazioni di buona prassi. Ciò evidenzia il carattere facoltativo delle raccomandazioni. Per rispettare la legge, i titolari del trattamento non sono tenuti a rispettare le raccomandazioni, bensì sono libere di farlo. Gli ambienti interessati possono prevedere una soluzione diversa al livello delle loro associazioni.

8.1.2.7 Art. 10 Certificazione

L'articolo 10 AP-LPD disciplina la certificazione facoltativa che figura attualmente all'articolo 11 LPD. L'AP-LPD estende la procedura di certificazione a tutti i tipi di trattamenti

[93] https://asut.ch/asut/resources/documents/initiative_sectorielle_protection_jeunesse_m%C3%A9dias.pdf.

[94] http://simsa.ch/_Resources/Persistent/2260a505424ef1e0c8100899a6f38a06e4a4ecff/130201-simsa-cch-public-f.pdf.

di dati. Oltre ai sistemi di trattamento dei dati (procedura, organizzazione) e ai prodotti (programmi, sistemi), sarà in futuro possibile certificare anche determinati servizi. L'estensione permette l'adeguamento al regolamento (UE) 2016/679, che prevede anch'esso la certificazione per tutte le operazioni di trattamento del titolare e del responsabile del trattamento (art. 42).

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[95].

8.1.2.8 Art. 11 Sicurezza dei dati

L'articolo 11 AP-LPD riprende l'articolo 7 LPD, con alcune modifiche redazionali. L'obbligo di garantire la protezione 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. La disposizione precisa che il titolare e il responsabile del trattamento devono proteggere i dati contro il trattamento illecito o la perdita mediante provvedimenti tecnici e organizzativi. Per perdita s'intende anche la distruzione dei dati.

Il suddetto obbligo può portare a diverse misure. Se del caso, i dati devono essere pseudonimizzati e criptati. Eventualmente vanno previste misure che garantiscano la confidenzialità e la completezza dei dati come pure la disponibilità del sistema e dei servizi di trattamento o assicurino che, in caso di guasto tecnico o materiale, l'accesso ai dati e ai sistemi sia nuovamente disponibile entro un termine ragionevole. Infine, è ipotizzabile l'obbligo di sviluppare procedure che permettano di verificare regolarmente l'efficienza delle misure tecniche e organizzative volte a garantire la sicurezza dei dati.

8.1.2.9 Art. 12 Dati di una persona deceduta

Alcuni elementi di questa norma relativa a una persona deceduta si trovano attualmente nell'articolo 1 capoverso 7 OLPD. Nel diritto vigente 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. Con la disposizione dell'ordinanza il diritto d'accesso è stato pertanto 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.

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 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 di terzi o della persona deceduta o che quest'ultima non l'abbia esplicitamente vietato. Altre questioni sollevate dal postulato, ad esempio quelle relative alla portabilità dei dati o a una loro possibile trasmissione per eredità, sono esaminate nell'ambito della revisione in corso del diritto successorio.

Capoverso 1 Consultazione

Secondo il capoverso 1, il titolare del trattamento deve concedere gratuitamente l'accesso ai dati di una persona deceduta se sussiste un interesse degno di protezione. Il capoverso 2 suppone tale interesse in determinate situazioni (cfr. sotto). La mera curiosità non è invece considerato un interesse degno di protezione. Parallelamente al diritto di consultazione secondo l'AP-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 permette loro di far valere i propri diritti patrimoniali nell'ambito della devoluzione dell'eredità (art. 601*a* AP-CC).

[95] 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 (SR **235.13**).

L'accesso va rifiutato se la persona deceduta lo ha espressamente vietato (lett. a); in tal modo si tiene conto della sua volontà. In virtù di un interesse preponderante della persona deceduta può in particolare essere negato l'accesso a dati personali degni di particolare protezione. Anche l'accesso agli atti di un medico o di un avvocato può essere rifiutato per tutelare gli interessi preponderanti della persona deceduta (lett. b); un eventuale segreto d'ufficio o professionale è tuttavia in linea di massima annullato dal capoverso 3.

La consultazione va inoltre negata se vi si oppongono interessi preponderanti di terzi (lett. b). I congiunti di cui all'articolo 1 cpv. 7 OLPD rientrano nel concetto di «terzi». Degli interessi di terzi fa parte anche la protezione della personalità. Occorre decidere nel singolo caso se gli interessi in questione siano preponderanti, tenendo conto, tra le altre cose, del significato che i dati rivestono per le persone in questione, del fatto che grazie alla consultazione si rendono noti dati relativi a dette persone e dello scopo della domanda di consultazione.

Capoverso 2 Presunzione dell'interesse

Secondo il *capoverso 2,* un interesse alla consultazione degno di protezione è presunto nel caso di parenti in linea diretta della persona deceduta o di persone che al momento del decesso erano coniugate, vivevano in unione domestica o convivevano di fatto con la persona deceduta. Questo significa che tali persone devono semplicemente dimostrare di aver avuto un legame di questo tipo con la persone defunta e non devono quindi provare un interesse degno di protezione.

Indipendentemente da questa presunzione resta possibile la ponderazione degli interessi di cui al capoverso 1 lettere a e b.

Capoverso 3 Titolari di un segreto

Il capoverso 3 revoca in linea di massima i segreti d'ufficio o professionali che potrebbero essere invocati contro una domanda di consultazione. Si pensi ad esempio a un figlio che vuole consultare i dati medici del padre deceduto; un medico non vi si potrebbe opporre facendo valere il segreto medico.

Gli interessi dei titolari alla tutela del proprio segreto d'ufficio o professionale possono essere considerati nell'ambito della ponderazione di cui al capoverso 1 lettera b.

Capoverso 4 Cancellazione

Secondo il capoverso 4, ogni erede può chiedere che il titolare del trattamento cancelli o distrugga gratuitamente i dati della persona defunta. Questo diritto è stato espressamente previsto soltanto per gli eredi e concepito in modo tale da permettere a ogni singolo erede di chiedere la cancellazione senza che sia necessario il consenso di tutti gli altri eredi. Ciò evita numerose difficoltà soprattutto sotto il profilo processuale. Inoltre, eventuali interessi contrastanti degli eredi possono essere ponderati. Infine, grazie a questa soluzione il diritto alla cancellazione sussiste anche se la comunità degli eredi si scioglie dopo la conclusione della devoluzione. La richiesta di cancellazione o distruzione va rifiutata se in vita la persona deceduta lo ha espressamente vietato (lettera a) o se vi si oppongono interessi preponderanti della persona deceduta o di terzi (lettera b).

Questo diritto sussiste a prescindere da una lesione della personalità o da un trattamento illecito dei dati da parte del titolare del trattamento.

Capoverso 5 Riserva di norme speciali

Questa disposizione prevede una riserva a favore di eventuali norme speciali in altre leggi federali. Sono pertanto fatte salve, ad esempio, le disposizioni della LTras, che disciplinano l'accesso ai documenti ufficiali dell'Amministrazione federale, o le norme speciali della legge del 26 giugno 1998[96] sull'archiviazione relative al termine di protezione dei dati personali nei documenti archiviati nell'Archivio federale.

[96] RS **152.1**

8.1.3 Obblighi del titolare e del responsabile del trattamento

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

8.1.3.1 Art. 13 Obbligo d'informare in occasione della raccolta di dati personali

Il nuovo articolo 13 AP-LPD disciplina l'obbligo di informare in occasione della raccolta di dati personali. Gli articoli 14 e 18*a* LPD sono così riuniti in un solo articolo. 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 simile.

L'obbligo di informare migliora la trasparenza del trattamento di dati, uno degli obiettivi fondamentali della revisione. Se non ne è informata, spesso la persona interessata non può sapere che vengono trattati dati che la riguardano. Inoltre, la persona interessata può far valere i propri diritti conformemente alla legge 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.

Capoverso 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 siano raccolti presso terzi. Il titolare del trattamento deve informare attivamente la persona interessata. Anche se non vi sono condizioni formali, va scelta una forma che sia consona allo scopo della trasparenza del trattamento dei dati. Per motivi probatori è inoltre raccomandabile documentare l'informazione o fornirla per scritto. L'informazione può essere fornita individualmente o in forma generale, ad esempio nelle condizioni generali di contratto o mediante una dichiarazione standardizzata relativa alla protezione dei dati su un sito Internet. Sono ipotizzabili anche simboli e pittogrammi, a condizione che contengano le informazioni necessarie. Le informazioni possono essere rese accessibili anche attraverso vari livelli (p. es. dapprima attraverso un simbolo, cliccando sul quale si possono ottenere informazioni più particolareggiate). Se si sceglie una forma generale, l'informazione deve tuttavia essere facilmente accessibile, completa e sufficientemente visibile e la persona interessata deve esservi resa attenta senza difficoltà, senza dover cercare o chiedere le pertinenti informazioni. Inoltre, le informazioni devono essere comprensibili, in modo da essere conformi allo scopo della trasparenza del trattamento dei dati.

Capoverso 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. Egli 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. Ne fanno parte l'identità e le coordinate di contatto del titolare del trattamento, i dati o le categorie di dati trattati e lo scopo del trattamento. Va inoltre comunicata – soprattutto da parte degli organi federali – l'eventuale base legale su cui si fonda il trattamento, di modo che la persona interessata possa far valere i suoi diritti. 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. Il titolare del trattamento deve fornire più o meno informazioni a seconda del tipo di dati trattati, della natura e della portata del trattamento. Questa flessibilità è necessaria perché la legge sulla protezione dei dati è applicabile a una moltitudine di trattamenti diversi. Un disciplinamento flessibile consente nel contempo di garantire che il titolare del trattamento non debba fornire informazioni inutili e che la persona interessata riceva solo le informazioni necessarie. Consente inoltre ai titolari del trattamento di concretizzare l'obbligo di informare nel loro settore specifico per mezzo di

raccomandazioni di buona prassi. Le persone interessate devono essere informate al più tardi al momento della raccolta dei dati, ad eccezione dei casi di cui al capoverso 5.

Capoverso 3 Comunicazione a terzi

Secondo il capoverso 3, se è prevista la comunicazione dei dati a terzi la persona interessata deve essere informata in merito ai destinatari o alle categorie di destinatari. Se conosce l'identità del destinatario, il titolare del trattamento deve comunicarla. Tale obbligo è valido anche se il destinatario si trova all'estero.

Capoverso 4 Conferimento del trattamento a un responsabile

Se il trattamento di dati personali è conferito a un responsabile, il titolare del trattamento deve comunicare alla persona interessata l'identità e i dati di contatto del responsabile nonché i dati o le categorie di dati che quest'ultimo tratterà. Tale obbligo è valido anche se i responsabili del trattamento si trovano all'estero.

Capoverso 5 Momento dell'informazione

Il capoverso 5 stabilisce il momento dell'informazione qualora i dati non siano raccolti presso la persona interessata. In tal caso quest'ultima deve essere informata al più tardi al momento della registrazione dei dati da parte del titolare del trattamento o, se non è prevista la registrazione, al momento della loro comunicazione a terzi. Il termine «registrazione» comprende, oltre alla procedura tecnica della registrazione in un sistema informatico, anche qualsiasi altra attività, successiva alla raccolta, con cui si prepara l'ulteriore utilizzo dei dati.

La violazione dell'obbligo di informare è punita (cfr. art. 50 cpv. 1 lett. a e b n. 1 e 2 AP-LPD).

8.1.3.2 Art. 14 Eccezioni all'obbligo di informare e limitazioni

L'articolo 14 AP-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. 3-5). Le due situazioni vanno nettamente separate. La disposizione riprende in gran parte le disposizioni del diritto vigente (art. 9, art. 14 cpv. 4 e 5 nonché 18*b* LPD), le quali, per motivi di chiarezza, vengono riunite in un solo articolo.

Capoversi 1 e 2 Eccezioni all'obbligo di informare

Secondo il capoverso 1*,* il titolare del trattamento è esentato dall'obbligo di informare se la persona interessata dispone già delle informazioni di cui all'articolo 13. Si può presumere che disponga già di tali informazioni se è stata informata precedentemente e nel frattempo le informazioni da comunicare non sono cambiate. Anche nel caso in cui essa stessa ha reso accessibili i suoi dati, la persona interessata è da considerarsi informata della raccolta dei dati, tuttavia devono eventualmente esserle fornite altre informazioni di cui all'articolo 13, necessarie per garantire la trasparenza del trattamento dei dati.

Secondo il capoverso 2 la persona interessata non deve essere informata in riferimento ai dati che non sono stati raccolti presso di lei, se la registrazione o la comunicazione dei dati è espressamente prevista dalla legge (cpv. 2 lett. a) o se l'informazione non è possibile o esige mezzi sproporzionati (cpv. 2 lett. b). Quest'ultima eccezione va interpretata in senso stretto. Il titolare del trattamento non può limitarsi a presumere che l'informazione sia impossibile o esiga mezzi sproporzionati, bensì deve in linea di massima prendere tutti i provvedimenti che, considerando le circostanze, si possono ragionevolmente esigere per ottemperare all'obbligo di informare. Solo quando tali provvedimenti si rivelano vani, il titolare del trattamento può presumere che l'informazione sia impossibile.

Capoversi 3 e 4 Limitazione dell'informazione

I capoversi 3 e 4 fissano le condizioni alle quali il titolare del trattamento può rinunciare alla comunicazione dell'informazione oppure limitarla o differirla. In tale contesto è in parte necessaria una ponderazione degli interessi anche a seconda del fatto che il titolare del trattamento sia un organo federale o un privato. L'elenco delle eccezioni è esaustivo e le disposizioni vanno in linea di massima interpretate in modo restrittivo. L'informazione dovrebbe essere limitata soltanto nella misura in cui ciò sia imprescindibile. Vanno ponderati il motivo

della limitazione e l'esigenza della trasparenza del trattamento dei dati. In linea di massima va scelta la soluzione più favorevole per la persona interessata e quella che, tenendo conto delle circostanze, garantisce nella misura del possibile il trattamento trasparente dei dati.

Secondo il capoverso 3 ogni titolare del trattamento può limitare o differire la comunicazione di informazioni o rinunciarvi, se lo prevede una legge in senso formale (lett. a). Si tratta soprattutto di disposizioni di diritto pubblico destinate agli organi federali, mentre per i privati disposizioni simili sono più rare. Una deroga all'obbligo d'informare è inoltre prevista se lo esigono interessi preponderanti di terzi (lett. b). È in particolare il caso allorquando insieme all'informazione sul trattamento dei dati la persona interessata riceve anche informazioni su terzi che potrebbero pregiudicare gli interessi di questi ultimi.

Il capoverso 4 disciplina le situazioni in cui determinati titolari del trattamento possono limitare o differire la comunicazione delle informazioni oppure rinunciarvi. Secondo il capoverso 4 lettera a, il titolare del trattamento può limitare o differire la comunicazione delle informazioni oppure rinunciarvi se lo esigono i suoi interessi preponderanti e a condizione che non comunichi i dati a un terzo. 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. Secondo il capoverso 4 lettera b, un organo federale può limitare o differire la comunicazione delle informazioni o rinunciarvi, se è necessario a causa di un interesse pubblico preponderante (n. 1). È considerato un interesse pubblico preponderante in particolare la sicurezza interna o esterna della Confederazione. Per «sicurezza esterna» s'intende, oltre al rispetto degli impegni di diritto internazionale, anche la cura di buoni rapporti con l'estero. L'organo federale può inoltre limitare o differire la comunicazione delle informazioni oppure rinunciarvi, se tale comunicazione rischia di compromettere un'indagine, un'istruzione o un procedimento amministrativo o giudiziario (n. 2). In tal modo s'intende impedire che in base alla legge sulla protezione dei dati si possano eludere le disposizioni sul diritto di essere sentito e su altri diritti previsti dalle leggi procedurali nonché ostacolare procedimenti amministrativi e giudiziari.

Capoverso 5 Comunicazione successiva delle informazioni

Secondo il capoverso 5, il titolare del trattamento è tenuto a comunicare le informazioni non appena cessa il motivo per limitare o differire la comunicazione dell'informazione o rinunciarvi. Questa regola non si applica se la comunicazione è impossibile o esige mezzi sproporzionati (cfr. il commento al cpv. 2).

8.1.3.3 Art. 15 Obbligo di informare e sentire la persona interessata in caso di decisione individuale automatizzata

L'articolo 15 AP-LPD prevede l'obbligo di informare e sentire 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 agli articoli 3 numero 3 e 11 della direttiva (UE) 2016/680. L'articolo 4 numero 3 in combinato disposto con l'articolo 22 del regolamento (UE) 2016/679 contiene una disposizione analoga. L'introduzione del nuovo termine è necessaria, poiché le decisioni individuali automatizzate sono vieppiù frequenti in tutti i rami dell'economia e sono a volte prese sulla base di dati errati.

Capoverso 1 Informazione

Secondo il capoverso 1 il titolare del trattamento deve informare la persona interessata nel caso di una decisione individuale automatizzata che abbia per lei effetti giuridici o ripercussioni notevoli. Ciò significa che il titolare deve informare la persona interessata su una decisione individuale automatizzata e per quest'ultima deve risultare chiaro che si tratta di una siffatta decisione.

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 concreta nei confronti della persona interessata. Una decisione individuale automatizzata può sussistere anche nel caso in cui essa venga successivamente comunicata da una persona fisica che tuttavia non può più influire sulla decisione. 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. Una decisione individuale automatizzata esplica effetti giuridici per la persona interessata se incide direttamente sul suo statuto giuridico. Per ripercussioni notevoli s'intendono le conseguenze effettive di una certa gravità di una decisione individuale automatizzata. Sono ipotizzabili diversi casi di decisioni individuali automatizzate. Si è ad esempio in presenza di una siffatta decisione se le condizioni di un contratto di leasing (interessi, durata del contratto, termini di pagamento, ecc.) sono esclusivamente il risultato di una valutazione automatica della situazione finanziaria della persona interessata oppure se un'assicurazione contro le malattie si rifiuta di concludere un contratto con una determinata persona fondandosi esclusivamente sull'analisi del suo stato di salute per mezzo di un algoritmo. Anche le multe per infrazioni alla circolazione stradale inviate esclusivamente in base a un immagine del conducente in questione sono da considerarsi decisioni individuali automatizzate.

Una decisione individuale automatizzata può fondarsi anche su una profilazione ai sensi dell'articolo 3 lettera f AP-LPD. Per essere in presenza di una decisione individuale automatizzata non è tuttavia per forza necessaria una profilazione; i due termini non coincidono. Il criterio determinante è il processo automatico. La profilazione non è per forza il risultato di un processo automatico, mentre la decisione individuale automatizzata sì. Un altro criterio sono le ripercussioni per la persona interessata. Nel caso della decisione individuale automatizzata, in seguito al trattamento viene presa una determinata decisione. Nel caso della profilazione i dati sono analizzati per un determinato scopo senza che l'analisi debba obbligatoriamente avere ripercussioni dirette sulla persona interessata.

Capoverso 2 Diritto di essere sentiti

Secondo il capoverso 2 il titolare del trattamento deve dare alla persona interessata la possibilità di esprimersi in merito alla decisione individuale automatizzata e ai dati trattati. Il diritto di essere sentita intende garantire, insieme all'obbligo di informare, che la persona interessata non sia oggetto di decisioni prese senza intervento umano. La persona interessata deve in particolare avere la possibilità di esprimere il suo punto di vista sul risultato della decisione e sui dati su cui si fonda la decisione. S'intende così impedire che essa subisca un danno giuridico o di fatto perché il trattamento si fonda su dati incompleti, non aggiornati o errati. Ciò è anche nell'interesse del titolare del trattamento, poiché decisioni individuali automatizzate non corrette hanno 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. L'obbligo di informare e sentire la persona interessata non intacca tuttavia la libertà contrattuale. Se il titolare del trattamento non rispetta l'obbligo di sentire la persona interessata, questa può far valere il suo diritto con una domanda d'accesso ai sensi dell'articolo 20.

La legge non fissa il momento dell'informazione o quello in cui la persona interessata deve essere sentita. Quest'ultima può quindi essere informata e sentita 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 ricorrere a un rimedio giuridico, a condizione che ciò non comporti per lei ulteriori costi (p. es. spese procedurali).

Capoverso 3 Eccezioni

Secondo il capoverso 3, l'obbligo di informare e sentire la persona interessata non si applica se la decisione individuale automatizzata è prevista da una legge. Per gli organi federali è necessaria una legge ai sensi dell'articolo 27 AP-LPD.

La violazione dell'obbligo di informare è punita (cfr. art. 50 cpv. 1 lett. a e b n. 1 e 2 AP-LPD).

8.1.3.4 Art. 16 Valutazione d'impatto sulla protezione dei dati

Il nuovo articolo 16 AP-LPD introduce l'obbligo di effettuare una valutazione d'impatto. La disposizione soddisfa le condizioni dell'articolo 8bis paragrafo 2 P-STE 108 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 dal capoverso 2 dell'articolo 16. La valutazione d'impatto sulla protezione dei dati è 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.

La valutazione d'impatto sulla protezione dei dati non costituisce una novità, in particolare per gli organi federali, e da questo punto di vista non ha quasi nessuna conseguenza pratica. Infatti gli organi federali sono già tenuti ad annunciare al responsabile della protezione dei dati o 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.

Capoverso 1 Motivi per la valutazione d'impatto sulla protezione dei dati

Secondo il capoverso 1 il titolare del trattamento (o il responsabile 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. 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 del singolo sia la sua dignità e identità[97]. In relazione ai 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 ed esaustiva 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 disporre, 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, ad esempio 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, l'autodeterminazione informativa e il diritto alla sfera privata vanno messi in relazione con il trattamento di dati in questione. 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. Ciò è il caso quando dati che riguardano da vicino la personalità sono trattati in modo tale da rendere possibile l'identificazione della persona interessata e delle sue caratteristiche specifiche. Il rischio elevato può risultare ad esempio dal tipo di dati trattati o dal loro contenuto (p. es. dati degni di

[97] Cfr. DIGGELMANN OLIVER, in: Waldmann/Belser/Epiney (a c. di), Basler Kommentar, Bundesverfassung, Basilea 2015, Art. 13 Cost. N 7.

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 ai dati può accedere una quantità elevata o addirittura illimitata di persone. Il fatto che nel caso di abusi i dati raccolti potrebbero pregiudicare la personalità, la dignità e lo sviluppo della persona interessata è un altro indizio per un rischio elevato. Anche una sorveglianza sistematica di una persona e del suo comportamento (p. es. della sua posta elettronica) oppure di uno spazio pubblico (p. es. una piazza affollata) può implicare un rischio elevato. Se è prevedibile che il trattamento di dati comporti un rischio elevato deve essere effettuata una valutazione d'impatto sulla protezione dei dati.

Capoverso 2 Contenuto della valutazione d'impatto

Secondo il capoverso 2 la valutazione d'impatto deve innanzitutto descrivere il trattamento previsto. Occorre ad esempio indicare i vari processi di trattamento, 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 della 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 4 AP-LPD, ma possono essere di rilievo anche gli obblighi della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 18 AP-LPD). Nel decidere le misure si possono eventualmente ponderare gli interessi della persona interessata e quelli del titolare o del responsabile del trattamento. Tale ponderazione va anch'essa illustrata e giustificata nella valutazione d'impatto.

Capoverso 3 Comunicazione all'Incaricato

Secondo il capoverso 3, il titolare (o il responsabile) del trattamento deve comunicare all'Incaricato il risultato della valutazione d'impatto nonché le misure previste per ridurre il rischio di ledere la personalità o i diritti fondamentali della persona interessata. Anche se il P-STE 108 non prescrive tale comunicazione, essa è prevista dalle regole europee (art. 28 della direttiva [UE] 2016/680 e art. 36 del regolamento [UE] 2016/679). La disposizione è inserita nell'AP-LPD in particolare 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.

Capoverso 4 Obiezioni dell'Incaricato

Secondo il capoverso 4*,* se ha obiezioni in merito alle misure previste, l'Incaricato ne informa il titolare del trattamento entro tre mesi dalla ricezione di tutte le informazioni necessarie. Dopo essere stato informato della valutazione d'impatto sul trattamento dei dati, l'Incaricato si limita a verificare che le misure proposte siano sufficienti per tutelare la personalità e i diritti fondamentali della persona interessata. Non procede invece a un esame esaustivo dell'intera procedura di trattamento, poiché tale esame è già oggetto della valutazione d'impatto. Se entro tre mesi non riceve alcuna informazione, il titolare del trattamento può presumere che l'Incaricato non abbia obiezioni contro le misure proposte a tutela dei diritti fondamentali. L'Incaricato è tuttavia libero di avviare un'inchiesta in una fase successiva se sussistono le condizioni di cui all'articolo 41 AP-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.

La violazione dell'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati e di comunicarne il risultato è punita (cfr. art. 50 cpv. 1 lett. c, 51 cpv. 1 lett. d AP-LPD).

8.1.3.5 Art. 17 Notificazione di violazioni della protezione dei dati

L'articolo 17 AP-LPD introduce l'obbligo di notificare violazioni della protezione dei dati. La disposizione costituisce un adeguamento ai requisiti dell'articolo 7 paragrafo 2 del P STE 108 e all'articolo 30 della direttiva (UE) 2016/680. L'articolo 33 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

Capoverso 1 Definizione e principio

Secondo il capoverso 1, il titolare del trattamento deve notificare all'Incaricato qualsiasi trattamento non autorizzato o perdita di dati, a meno che la violazione non presenti verosimilmente alcun rischio per la personalità e i diritti fondamentali della persona interessata. In tale contesto occorre basarsi sulla definizione di trattamento di cui all'articolo 3 lettera d AP-LPD. È pertanto considerato una violazione della protezione dei dati qualsiasi tipo di trattamento non autorizzato, compresa ad esempio la cancellazione non autorizzata. La violazione può essere commessa da terzi, ma anche da collaboratori del titolare del trattamento che usano in modo abusivo le loro competenze. In seguito a un trattamento non autorizzato, la persona interessata può perdere il controllo sui suoi dati o i suoi dati possono essere usati in modo abusivo. Inoltre, il trattamento non autorizzato può portare anche a una lesione della personalità dell'interessato, ad esempio rendendo note informazioni segrete. Secondo l'articolo 23 capoverso 2 lettera a si è ad esempio in presenza di una lesione della personalità se è violata la sicurezza dei dati.

Ai suddetti rischi la persona interessata può reagire soltanto se è a conoscenza della violazione, ragion per cui il titolare del trattamento deve in linea di principio notificare un trattamento non autorizzato innanzitutto all'Incaricato e, se sono soddisfatte le condizioni di cui al capoverso 2, anche alla persona interessata. Il trattamento non autorizzato deve essere notificato senza indugio. 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 tale rischio è elevato e quanto più elevato è il numero di persone interessate, tanto più rapidamente dovrà reagire il titolare del trattamento.

Il titolare del trattamento può rinunciare alla notificazione soltanto se la violazione della protezione dei dati non rischia di ledere la personalità e i diritti fondamentali della persona interessata. Questa regola intende evitare la notificazione di violazioni insignificanti. L'eccezione va tuttavia interpretata in senso stretto: il titolare del trattamento deve valutare le possibili ripercussioni della violazione per la persona interessata e può rinunciare alla notificazione soltanto se il trattamento non autorizzato dei dati non implica verosimilmente alcun rischio.

Capoverso 2 Informazione della persona interessata

Anche se in linea di massima la persona interessata non deve essere informata, secondo il capoverso 2 il titolare del trattamento le comunica la violazione della protezione dei dati qualora sia necessario per proteggerla o l'Incaricato lo esiga. Il titolare ha a disposizione un certo margine di apprezzamento 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, quali la modifica dei suoi dati d'accesso o delle sue parole chiave.

Capoversi 3 e 4

Secondo il capoverso 3 il titolare del trattamento può limitare o differire la notificazione alla persona interessata oppure rinunciarvi in presenza di uno dei motivi di cui all'articolo 14 capoversi 3 e 4 AP-LPD (cfr. n. 8.1.3.2).

Un trattamento non autorizzato può verificarsi anche presso il responsabile del trattamento. Per questo motivo il capoverso 4 prevede l'obbligo del responsabile di informare il titolare di qualsiasi trattamento non autorizzato. Spetta successivamente al titolare valutare i rischi e decidere se sussista un obbligo di notificazione all'Incaricato e alla persona interessata.

La violazione dell'obbligo di notificazione di un trattamento non autorizzato è punita (cfr. art. 50 cpv. 2 lett. d AP-LPD).

8.1.3.6 Art. 18 Protezione dei dati fin dalla progettazione e per impostazione predefinita

L'articolo 18 AP-LPD introduce l'obbligo della protezione dei dati fin dalla progettazione e per impostazione predefinita. La disposizione attua i requisiti dell'articolo 8 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.

Capoverso 1 Protezione dei dati fin dalla progettazione

Secondo il capoverso 1 il titolare e il responsabile del trattamento sono tenuti ad adottare, fin dalla progettazione del trattamento, le misure appropriate per prevenire e ridurre al minimo il rischio di ledere la personalità e i diritti fondamentali delle persone interessate. L'AP-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 raccomandazioni di buona prassi), nella misura in cui 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 della 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 4 AP-LPD. 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 ridurre al minimo indispensabile i dati da raccogliere, il che si evince anche dai principi generali di cui all'articolo 4 AP-LPD: sin dall'inizio il trattamento deve essere progettato in modo tale da raccogliere e trattare il minor numero possibile di dati o perlomeno da doverli conservare meno tempo possibile.

L'obbligo della protezione dei dati fin dalla progettazione del trattamento dovrebbe avere poche ripercussioni per gli organi federali, poiché anche il diritto vigente prevede che essi 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 cpv. 2 OLPD).

Capoverso 2 Protezione dei dati per impostazione predefinita

Secondo il capoverso 2, il titolare e il responsabile del trattamento sono tenuti ad adottare le misure appropriate per garantire che, per impostazione predefinita, siano trattati soltanto i dati necessari per lo scopo del trattamento. 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 procede a impostazioni diverse. Le impostazioni predefinite possono essere previste dal prodotto oppure programmate, ad esempio quando una determinata stampante è definita come stampante standard. Nel contesto del trattamento dei dati questo significa che il pertinente sistema è impostato in modo da favorire la protezione dei dati, a meno che la persona interessata modifichi tali 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 favorevo-

li alla protezione dei dati è costituita dalla possibilità della persona interessata di intervenire. Anche se non può modificare il sistema in sé, la persona interessata ha la possibilità di modificare le impostazioni predefinite. Queste ultime sono pertanto strettamente connesse al consenso della persona interessata (cfr. art. 4 cpv. 6 AP-LPD). Le impostazioni predefinite che favoriscono la protezione dei dati permettono pertanto alla persona interessata di acconsentire a un determinato trattamento dei dati.

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

Il titolare e il responsabile del trattamento possono dimostrare, in particolare attraverso la certificazione o la valutazione d'impatto sulla protezione dei dati, di rispettare gli obblighi di cui ai capoversi 1 e 2 del presente articolo.

La violazione degli obblighi di cui all'articolo 18 è punita (cfr. art. 51 cpv. 1 lett. e AP-LPD).

8.1.3.7 Art. 19 Altri obblighi

L'articolo 19 AP-LPD prevede vari altri obblighi del titolare o del responsabile del trattamento.

Lettera a Obbligo di documentazione

La lettera a obbliga il titolare e il responsabile del trattamento a documentare il trattamento dei dati. L'obbligo di documentazione è conforme all'articolo 8bis paragrafo 1 del P-STE 108 e all'articolo 25 della direttiva (UE) 2016/680. L'articolo 30 del regolamento (UE) 2016/679 prevede un disciplinamento analogo. Il nuovo obbligo sostituisce quello vigente secondo cui i privati sono tenuti a registrare le raccolte di dati presso l'Incaricato (secondo l'articolo 36 AP-LPD gli organi federali devono invece continuare a tenere un registro). La notifica per il registro è un ostacolo burocratico che causa un notevole onere amministrativo al titolare del trattamento e la sua utilità pratica è minima. Infatti, già il diritto vigente prevede in tale ambito diverse eccezioni per le persone private, mentre l'obbligo di documentazione vale in modo uniforme per tutte le attività di trattamento dei dati. Ciò permette di ottenere, con un onere amministrativo minore, una documentazione più uniforme di tutte le attività private di trattamento dei dati. La legge non definisce le informazioni che devono essere documentate e spetterà quindi all'ordinanza precisarle. La documentazione deve tuttavia essere disciplinata in modo tale che il titolare e il responsabile del trattamento possano adempiere i loro obblighi di informazione e notificazione. Devono ad esempio essere documentate anche le violazioni della protezione dei dati secondo l'articolo 17. L'obbligo di documentazione è pertanto anche un elemento fondamentale per garantire la trasparenza del trattamento di dati. Una violazione di tale obbligo è punita (cfr. art. 51 cpv. 1 lett. f AP-LPD).

Lettera b Altri obblighi d'informazione

Secondo la lettera b, il titolare e il responsabile del trattamento sono tenuti a informare i destinatari dei dati di qualsiasi rettifica, cancellazione, distruzione o violazione della protezione dei dati nonché di qualsiasi limitazione del trattamento secondo l'articolo 25 capoverso 3 o 34 capoverso 2. Tale obbligo completa varie regole per la protezione dei dati in caso di comunicazione di dati a terzi ed è previsto dall'articolo 16 paragrafo 5 della direttiva (UE) 2016/680 e dall'articolo 19 del regolamento (UE) 2016/679. Il trattamento di dati inesatti è in linea di principio lesivo della personalità, ragion per cui chiunque tratta dati deve accertarsi che questi siano esatti (art. 4 cpv. 5 AP-LPD). Anche la cancellazione o la distruzione dei dati e la limitazione del loro trattamento implica in linea di massima che il trattamento non è più lecito. Il presente obbligo d'informazione impedisce che, non essendo a conoscenza dei fatti, i terzi a cui sono stati trasmessi i dati continuino a trattarli.

Il titolare o il responsabile del trattamento può rinunciare all'informazione se ciò è impossibile o esige mezzi sproporzionati. Questa eccezione va interpretata in senso stretto. Il titolare o il responsabile del trattamento non può limitarsi a presumere che l'informazione sia impossibile o esiga mezzi sproporzionati. Deve perlomeno aver tentato di informare il destinatario ed essersi trovato di fronte a difficoltà concrete sormontabili soltanto con un onere straordinario. Quanto alla proporzionalità dei mezzi va anche considerato il contenuto della comunicazio-

ne: i mezzi devono essere messi in relazione con l'importanza che la rettifica, cancellazione o distruzione dei dati o la limitazione del loro trattamento ha per la persona interessata oppure con la gravità della violazione della protezione dei dati.

La violazione di questi obblighi è punita (art. 50 cpv. 3 lett. a AP-LPD).

8.1.4 Diritti della persona interessata

La sezione 4 disciplina i diritti della persona interessata. I diritti nei confronti dei titolari privati sono disciplinati nella sezione 5, quelli nei confronti degli organi federali nella sezione 6.

8.1.4.1 Art. 20 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 minorenni o interdette. Il carattere prettamente personale del diritto implica anche che nessuno può rinunciare preventivamente al diritto d'accesso (art. 20 cpv. 6 AP-LPD).

Capoverso 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.

Capoverso 2 Informazioni da comunicare

Secondo il capoverso 2, la persona interessata riceve innanzitutto le informazioni che devono esserle comunicate in base all'obbligo di informare (cfr. art. 13 cpv. 2-4 AP-LPD). Si tratta in linea di massima delle informazioni necessarie affinché la persona interessata possa far valere i diritti previsti dalla legge e sia quindi garantito un trattamento trasparente dei dati. In ogni caso devono esserle comunicate le informazioni di cui alle lettere a-c: l'identità e i dati di contatto del titolare del trattamento (lett. a), i dati personali trattati (lett. b) e lo scopo del trattamento (lett. c). Alla persona interessata devono inoltre essere comunicati la durata di conservazione dei dati o, qualora ciò non sia possibile, i criteri per stabilire la durata (lett. d). Tale informazione le permette in particolare di verificare che il titolare del trattamento conservi i dati conformemente ai principi di cui all'articolo 4 AP-LPD. Dato che la durata della conservazione dei dati non deve essere necessariamente comunicata nell'ambito dell'obbligo di informare, la persona interessata deve ottenere questa informazione nell'ambito del diritto d'accesso. Alla persona interessata è altresì comunicata un'eventuale decisione individuale automatizzata (lett. e) e, se del caso, le informazioni di cui al capoverso 3. Infine, la persona interessata deve ricevere le informazioni disponibili sull'origine dei dati (lett. f). Tale obbligo è previsto anche dal diritto vigente.

Capoverso 3 Comunicazione in caso di decisione basata sul trattamento dei dati

In caso di decisione basata sul trattamento dei dati, la persona interessata riceve le informazioni sul risultato di tale decisione, sul processo che vi ha condotto nonché sulle sue conseguenze e la sua portata. Ciò vale in particolare in caso di decisione individuale automatizzata, quale ad esempio la concessione di un credito o la conclusione di un assicurazione basata esclusivamente sull'analisi dei dati finanziari e sanitari della persona interessata (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Si tratta di informazioni maggiori rispetto a quelle previste dall'articolo 15 AP-LPD. Grazie al diritto d'accesso la persona interessata riceve informazioni più ampie sulla decisione in questione, di modo che possa ricostruire come si sia giunti a tale decisione e valutarne le conseguenze. Occorre pertanto comunicarle i dati presi in considerazione e la loro importanza per la decisione.

In virtù dell'articolo 21 il titolare del trattamento può rifiutare, limitare o differire la comunicazione delle informazioni. A tal fine i titolari privati possono far valere anche interessi propri, come ad esempio la tutela del segreto d'affari, ma è necessaria una ponderazione accurata degli interessi. Il titolare del trattamento può ad esempio far valere il segreto d'affari e non

rendere noti tutti i particolari di un'eventuale algoritmo che ha condotto alla decisione. Deve tuttavia motivare il risultato della decisione in modo tale che la persona interessata possa capire come si sia giunti al risultato in questione. Inoltre, la persona interessata deve essere informata sulle conseguenze e sull'importanza della decisione per la sua situazione giuridica e fattuale. Infine, se viene a conoscenza della decisione individuale automatizzata soltanto grazie al diritto d'accesso, la persona interessata deve avere la possibilità di esprimersi in merito (cfr. art. 15 cpv. 2 AP-LPD).

Capoversi 4 e 5

Il capoverso 4 è stato ripreso dal diritto vigente e ha subito soltanto una modifica redazionale. Il titolare del trattamento può comunicare alla persona interessata dati concernenti la salute per il tramite di un medico da essa designato.

Salvo alcuni adeguamenti redazionali, rimane invariato anche il capoverso 5. 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.

La violazione degli obblighi previsti dall'articolo 20 AP-LPD è punita (cfr. art. 50 cpv. 1 lett. a AP-LPD).

8.1.4.2 Art. 21 Restrizione del diritto d'accesso

Secondo il capoverso 1 il titolare del trattamento può rifiutare, limitare o differire la comunicazione delle informazioni per i motivi previsti all'articolo 14 capoversi 3 e 4 AP-LPD. Per le spiegazioni si rinvia al commento dell'articolo 14 AP-LPD (cfr. n. 8.1.3.2). Rispetto al diritto vigente i motivi per la restrizione del diritto d'accesso sono rimasti gli stessi, ma nell'AP-LPD sono enumerati in relazione all'obbligo di informare.

Il titolare del trattamento che rifiuta, limita o differisce la comunicazione delle informazioni deve indicarne il motivo (*cpv. 2*). In linea di principio i possibili motivi sono quelli previsti dall'articolo 14 capoversi 3 e 4. Gli organi federali devono emanare una decisione impugnabile, mentre i titolari privati non sottostanno ad alcun obbligo formale, ma per motivi probatori è raccomandabile comunicare la motivazione per scritto alla persona interessata. Il nuovo secondo periodo del capoverso 2 stabilisce che l'organo federale non è tenuto a indicare il motivo se ciò può pregiudicare gli interessi di cui all'articolo 14 capoverso 4 lettera b AP-LPD. Questa disposizione impedisce che fornendo il motivo della restrizione l'organo federale debba rivelare proprio quello che intendeva nascondere rifiutando l'informazione.

L'indicazione dei motivi deve permettere alla persona interessata di verificare se l'informazione sia stata giustamente rifiutata, limitata o differita. I requisiti posti alla motivazione non possono tuttavia essere troppo elevati, per evitare che entrino in conflitto con i motivi della restrizione dell'informazione.

8.1.4.3 Art. 22 Restrizioni a favore dei mezzi di comunicazione di massa

L'articolo 22 AP-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 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[98]. Deve inoltre trattarsi di un mezzo di comunicazione a carattere periodico. 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[99].

Salvo alcuni adeguamenti redazionali, le restrizioni del diritto d'accesso a favore dei mezzi di comunicazione di massa sono riprese senza modifiche.

[98] BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2ª ed., Berna 2011, N 1769.

[99] BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2ª ed., Berna 2011, N 1420.

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

La sezione 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 ad 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 23 AP-LPD precisa le lesioni della personalità nell'ambito della protezione dei dati, l'articolo 24 AP-LPD definisce i motivi giustificativi di una lesione e l'articolo 25 AP-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, l'AP-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[100]. Il presente avamprogetto intende ovviarvi adeguando il disciplinamento delle spese nel procedimento civile (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

8.1.5.1 Art. 23 Lesioni della personalità

L'articolo 28 CC non definisce il termine «lesioni della personalità». Pertanto, l'articolo 23 AP-LPD lo precisa per quanto riguarda le lesioni in seguito al trattamento di dati.

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

Capoverso 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 in quattro casi. Secondo la lettera a vi è lesione della personalità se sono trattati dati in violazione dei principi di cui agli articoli 4, 5, 6 e 11 AP-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. Secondo la lettera c vi è una lesione della personalità se sono comunicati a terzi dati degni di particolare protezione. Infine, secondo la lettera d, si presume una violazione della personalità nel caso di una profilazione senza l'espresso consenso della persona interessata.

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[101]. L'AP-LPD disciplina i motivi giustificativi esclusivamente nell'articolo 24.

---

[100] 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).

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

Capoverso 3 Nessuna 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 esplicitamente a un loro trattamento. Questa regola, ripresa senza modifiche dal diritto vigente, è coerente, poiché in questo caso la libertà individuale di disporre dei propri dati personali non è lesa. Tuttavia la disposizione si applica soltanto se i dati sono trattati in modo lecito ovvero se sono rispettati in particolare i principi di cui agli articoli 4, 5, 6 e 11.

8.1.5.2 Art. 24 Motivi giustificativi

L'articolo 24 precisa i motivi giustificativi del trattamento di dati lesivo della personalità. Fatte salve piccole modifiche, la norma resta invariata rispetto al diritto vigente.

Capoverso 1 Principi

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. La ponderazione 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'interessa a trattare i dati. Una lesione della personalità è giustificata soltanto se l'interesse al trattamento prevale sugli interessi della persona interessata.

Capoverso 2 Possibili interessi preponderanti della persona che tratta i dati

Il capoverso 2 precisa i casi in cui può sussistere un interesse preponderante della persona che tratta i dati. La formulazione chiarisce che non si tratta di motivi giustificativi assoluti. È infatti determinante la ponderazione degli interessi nel singolo caso.

L'elenco resta in gran parte invariato rispetto al diritto vigente e non è esaustivo. 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 l'indicazione delle finalità 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.

Capoverso 2 lettera c Verifica del credito

La lettera c numero 3 sancisce la nuova condizione secondo cui la persona interessata deve essere maggiorenne. Si tratta di una modifica tesa a migliorare la protezione dei minori, uno degli obiettivi della revisione. La portata di questa modifica dovrebbe in linea di massima essere molto circoscritta a causa della limitata capacità di agire dei minorenni. Tuttavia, l'esperienza insegna che nella prassi vi possono essere abusi, come evidenzia ad esempio il procedimento che l'Incaricato ha avviato contro l'impresa Moneyhouse[102].

Capoverso 2 lettera e Trattamento a scopi di ricerca

Le condizioni della lettera e relative al motivo giustificativo del trattamento di dati per scopi impersonali, in particolare nei settori della ricerca, pianificazione e statistica, sono state rese leggermente più severe. L'utilizzazione di dati per tali scopi è ammesso 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

[102] Cfr. https://www.edoeb.admin.ch/datenschutz/00626/00747/01022/index.html?lang=it. Il procedimento non è ancora chiuso.

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. In linea di principio lo si evince già dall'articolo 4 capoverso 4 AP-LPD. Secondo l'articolo 23 capoverso 2 lettera a, la violazione di tale disposizione costituisce una lesione della personalità che può essere giustificata da uno dei motivi di cui all'articolo 24. Grazie alla disposizione dell'articolo 24 capoverso 2 lettera e numero 1 non sarà più possibile giustificare una violazione dell'articolo 4 capoverso 4 con il trattamento a scopi di ricerca, pianificazione o statistica.

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 23 capoverso 2 lettera c, 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 24. Grazie all'articolo 24 capoverso 2 lettera e 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).

8.1.5.3 Art. 25 Pretese giuridiche

L'articolo 25 disciplina le pretese giuridiche che le persone interessate possono far valere nei confronti di persone private.

Capoverso 1 Azioni

Il capoverso 1 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 singoli diritti specifici che la persona interessata può far valere. Per maggiore chiarezza l'AP-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° capoverso 1 numeri 1 e 2 CC. Secondo la lettera a, la persona interessata può chiedere di proibire il trattamento dei dati. 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, nell'AP-LPD il diritto alla cancellazione è stato formulato esplicitamente. Ciò corrisponde ai 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[103]. Pertanto anche in Svizzera sarebbe possibile una decisione analoga a quella della Corte di giustizia europea nei confronti di Google[104]. Siffatto diritto all'oblio non vale tuttavia in modo assoluto[105]. La giurisprudenza, 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 modificarli.

Capoverso 2 Menzione del carattere contestato

Il capoverso 2 prevede la menzione del carattere contestato dei dati, ripresa senza modifiche dal diritto vigente. Se non può essere dimostrata né l'esattezza né l'inesattezza dei dati per-

[103] Cfr. in particolare DTF **109** II 353; DTF **111** II 209 e DTF **122** II 449.

[104] 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.

[105] DTF **111** II 209 consid. 3c.

sonali, la persona interessata può chiedere di aggiungere una menzione che ne rilevi il carattere contestato. Può inoltre chiedere di limitare il trattamento dei dati contestati. Il diritto a limitare il trattamento è conforme all'articolo 16 paragrafo 3 della direttiva (UE) 2016/680; una regola analoga è prevista dall'articolo 18 del regolamento (UE) 2016/679, mentre nel P-STE 108 non vi è alcuna regola simile. La limitazione del trattamento significa contrassegnare i dati contestati in modo tale che il loro futuro trattamento si limiti ad accertarne l'esattezza o l'inesattezza. I dati devono essere contrassegnati in modo chiaro. In pratica ciò può significare trasferire temporaneamente i dati in un altro sistema di trattamento, impedire agli utenti l'accesso ai dati o togliere temporaneamente i dati dalla pagina Internet sulla quale erano stati pubblicati. 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.

Capoverso 3 Comunicazione a terzi o pubblicazione

Alla stregua del diritto vigente, il capoverso 3 prevede il diritto di chiedere che la rettifica, la distruzione, il divieto di trattamento o della comunicazione a terzi nonché la menzione del carattere contestato dei dati siano comunicati a terzi o pubblicati. Questa regola concretizza l'articolo 28°capoverso 2 CC nell'ambito della protezione dei dati.

È invece abrogata la disposizione riguardante la procedura semplificata, poiché è divenuta obsoleta in seguito all'introduzione del Codice di procedura civile[106].

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

8.1.6.1 Art. 26 Organo responsabile e controlli

Rispetto all'articolo 16 LPD, l'articolo 26 subisce poche modifiche. Al capoverso 1, per motivi redazionali è cancellata l'espressione «nell'adempimento dei suoi compiti».

Per gli stessi motivi, nel capoverso 2 si è rinunciato all'espressione «regolare in modo specifico». Inoltre, secondo l'AP-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 (UE) 2016/680. L'articolo 26 del regolamento(UE) 2016/679 prevede una regola analoga.

8.1.6.2 Art. 27 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 27 capoverso 2 disciplina le basi legali per il trattamento di dati personali degni di particolare protezione, la profilazione e l'emanazione di decisioni individuali automatizzate. Il capoverso 3 fissa le deroghe ai requisiti posti alla base legale.

Capoverso 1 Basi legali

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.

Capoverso 2 Base in una legge in senso formale

Il capoverso 2 precisa che per il trattamento di dati personali degni di particolare protezione, la profilazione o l'emanazione di una decisione individuale automatizzata ai sensi dell'articolo 15 capoverso 1 è necessaria una base in una legge formale. Tuttavia è sufficiente una base in una legge in senso materiale se sono soddisfatte due condizioni. Secondo la lettera a il trattamento deve essere indispensabile per l'adempimento di un compito definito in una legge in senso formale. Affinché questa condizione sia soddisfatta, la natura dei compiti che richiedono il trattamento dei dati deve essere sufficientemente precisa. La seconda condizione (lett. b) è nuova ed ha il vantaggio di circoscrivere la portata del secondo periodo del capoverso 2 in modo più preciso rispetto al disciplinamento vigente dell'articolo 17 capo-

[106] Codice di procedura civile del 19 dic. 2008; RS **272**.

verso 2 lettera a LPD. Quest'ultimo è applicabile eccezionalmente, il che può anche portare a sfruttare il margine d'apprezzamento per supporre un caso eccezionale anche quando non sussiste.

Capoverso 3 Deroghe

Il capoverso 3 enumera le deroghe alla base legale secondo i capoversi 1 e 2. In un caso specifico un organo federale può trattare eccezionalmente dati personali in assenza di una pertinente base legale se sussiste una delle condizioni di cui alle lettere a-c. La lettera a prevede una decisione, impugnabile, del Consiglio federale di autorizzare eccezionalmente un organo federale a trattare dati personali senza una base legale. Secondo la lettera b gli organi federali possono trattare dati personali senza una pertinente base legale se la persona interessata vi ha acconsentito conformemente all'articolo 4 capoverso 6 AP-LPD o ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento. 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. Il trattamento è consentito se è necessario per proteggere la vita o l'incolumità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole.

8.1.6.3 Art. 28 Trattamento dei 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 «profilo della personalità» è sostituito da «profilazione». 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 alcune modifiche redazionali.

8.1.6.4 Art. 29 Comunicazione di dati personali

L'articolo 29 AP-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 27 capoverso 1 e 2 AP-LPD. Da questa precisazione si evince che l'articolo 29 non rinvia alle eccezioni previste dall'articolo 27 capoverso 3 AP-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 29 capoverso 2 lettere a-e AP-LPD.

I «dati personali» del capoverso 1 comprendono anche i dati degni di particolare protezione. Le deroghe previste dal capoverso 2 lettere a-e sono pertanto 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 27 capoverso 3 lettera c AP-LPD (cfr. n. 8.1.6.2).

L'articolo 29 capoverso 3 AP-LPD corrisponde all'articolo 19 capoverso 1bis LPD, salvo una piccola modifica. L'adeguamento del tenore dell'articolo 29 capoverso 3 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 AP-LPD) va chiarito che tale condizione si applica non solo addizionalmente (alternativamente), ma anche indipendentemente dall'articolo 29 capoversi 1 e 2. Si propone di sostituire, nella frase introduttiva dell'articolo 29 capoverso 3 AP-LPD, l'espressione «anche» (nella versione tedesca «auch», assente nella versione francese) con «inoltre / zudem / en outre», ponendola all'inizio della frase per evidenziare che il capoverso 3 costituisce una base legale supplementare a quelle previste dal capoverso 1.

L'articolo 29 capoverso 4 AP-LPD non subisce modifiche rispetto all'articolo 19 capoverso 2 LPD.

Per contro, il vigente articolo 19 capoverso 3 LPD sulle «procedure di richiamo» presso gli organi federali può essere abrogato poiché è contrario al carattere tecnologicamente neutro della legge sulla protezione dei dati e nell'era digitale appare ormai obsoleto.

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

8.1.6.5 Art. 30 Opposizione alla comunicazione di dati

Questa disposizione resta invariata rispetto al diritto vigente, fatti salvi alcuni adeguamenti redazionali.

8.1.6.6 Art. 31 Offerta di documenti all'Archivio federale

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

8.1.6.7 Art. 32 Trattamento dei dati per scopi di ricerca, pianificazione e statistica

La disposizione corrisponde all'articolo 22 LPD, eccetto due modifiche nel capoverso 2 riguardanti i rinvii agli articoli 4 capoverso 3, 27 capoverso 1 e 2 e 29 capoverso 1 AP-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.

8.1.6.8 Art. 33 Attività di diritto privato di organi federali

La disposizione corrisponde senza modifiche all'articolo 23 LPD e non subisce modifiche materiali.

8.1.6.9 Art. 34 Pretese e procedura

L'articolo 34 corrisponde ampiamente al vigente articolo 25 LPD, eccetto alcune piccole modifiche illustrate qui appresso.

Capoverso 2 Menzione del carattere contestato

Il capoverso 2 prevede la menzione del carattere contestato dei dati, riprendendo senza modifiche la disposizione dal diritto vigente. Se non può essere provata né l'esattezza né l'inesattezza dei dati personali, l'organo federale deve aggiungere ai dati una menzione che ne rilevi il carattere contestato. Inoltre, in questo caso la persona interessate può chiedere di limitare il trattamento dei dati in questione. Tale diritto corrisponde ai requisiti dell'articolo 16 paragrafo 3 della direttiva (UE) 2016/680; un disciplinamento analogo è previsto dall'articolo 18 del regolamento (UE) 2016/680, mentre nel P-STE 108 non contiene alcuna siffatta regola. Limitare il trattamento significa contrassegnare i dati contestati in modo tale che il loro futuro trattamento si limiti ad accertarne l'esattezza o l'inesattezza. I dati devono essere contrassegnati in modo chiaro. In pratica ciò può significare trasferire temporaneamente i dati in un altro sistema di trattamento, impedire agli utenti l'accesso ai dati o togliere temporaneamente i dati dalla pagina Internet su cui erano stati pubblicati. Nei sistemi di trattamento automatico dei dati la limitazione del trattamento dovrebbe essere in linea di mas-

sima garantita da mezzi tecnici, affinché i dati non possano essere trattati ulteriormente e modificati.

Capoverso 3 Richieste

Il capoverso 3 prevede altre richieste che la persona interessata può rivolgere all'organo federale.

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 34 capoverso 3 lettere a e b. L'articolo 17 del regolamento (UE) 2016/679 prevede anch'esso, a determinate condizioni, il diritto della persona interessata di richiedere la cancellazione dei propri dati («diritto all'oblio»). Lo stesso diritto è previsto dall'articolo 25 AP-LPD, al fine di applicare le stesse regole ai titolari del trattamento privati e pubblici (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**). La situazione giuridica concreta resta tuttavia immutata. È fatto salvo il capoverso 4.

Nella lettera a della disposizione 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 30 AP-LPD[107]. A differenza dei diritti di cui all'articolo 34, l'opposizione di cui all'articolo 30 AP-LPD non è connessa al trattamento illecito. La cancellazione non ha conseguenze pratiche, poiché la persona interessata che fa valere i diritti di cui all'articolo 34 può nel contempo opporsi alla comunicazione di dati a terzi in virtù dell'articolo 30.

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 30. Anche se l'articolo 30 non lo prevede, appare ragionevole che la persona interessata lo possa esigere almeno nel caso di una comunicazione illecita.

Capoverso 4 Fondi di istituzioni pubbliche della memoria collettiva

Secondo il capoverso 4 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. La disposizione si riferisce pertanto 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. Infatti, i documenti di questi fondi intendono rispecchiare il passato, il che è possibile soltanto se essi sono conservati nella loro forma originale. 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 4 permette alle persone interessate di chiedere che tali istituzioni limitino l'accesso ai dati controversi. A tal fine la persona interessata deve tuttavia dimostrare un interesse preponderante. Questa limitazione va considerata soprattutto in riferimento alla crescente tendenza di rendere grandi archivi pubblici accessibili a tutti su Internet. Ciò riduce il tempo necessario per ricerche mirate e nel contempo aumenta la cerchia di persone che hanno accesso all'archivio in questione. Per questi casi la legge deve permettere una ponderazione accurata degli interessi: da una parte, l'interesse del pubblico a un accesso non falsificato e illimitato ai documenti e, dall'altra, quello delle persone interessate di non rendere accessibili a tutti informazioni inesatte o che ledono la loro personalità. Come si evince dal primo periodo, nel caso di archivi o altre istituzioni simili prevale in linea di massimo l'interesse pubblico a un accesso libero e non falsificato. 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 prepon-

[107] 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.

derante 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.

8.1.6.10 Art. 35 Procedura in caso di comunicazione di documenti ufficiali che contengono dati

La disposizione corrisponde esattamente all'articolo 25bis LPD.

8.1.6.11 Art. 36 Registro delle attività di trattamento

Come illustrato nel commento all'articolo 19 AP-LPD, l'articolo 11*a* capoverso 3 LPD, che prevede l'obbligo per i privati di notificare all'Incaricato determinate collezioni di dati, è abrogato e sostituito dall'obbligo di documentare i trattamenti. Per contro, l'obbligo degli organi federali di notificare le loro collezioni è mantenuto con qualche modifica.

L'articolo 36 capoverso 1 prevede infatti che l'Incaricato tenga un registro delle attività di trattamento previamente notificategli dagli organi federali. Analogamente a quanto previsto dal diritto vigente, il registro è accessibile al pubblico su Internet (cpv. 2). L'obbligo dell'organo federale di notificare le attività di trattamento corrisponde sostanzialmente all'obbligo di notificare le collezioni di dati. Si tratta di un adeguamento terminologico, poiché la presente revisione abolisce l'espressione «collezione di dati» (art. 3 lett. g LPD). La nuova terminologia corrisponde a quella dell'articolo 24 della direttiva (UE) 2016/680 e dell'articolo 30 del regolamento (UE) 2016/679.

Anche se si distingue lievemente dalla normativa europea, l'articolo 36 AP-LPD ha in sostanza lo stesso effetto. La disposizione permette infatti al pubblico e all'Incaricato di usufruire di una panoramica delle attività di trattamento degli organi federali. Il contenuto della notifica corrisponde in gran parte a quello definito all'articolo 16 OLPD e andrà, se necessario, completato con altre informazioni quali quelle elencate all'articolo 24 della direttiva (UE) 2016/680.

L'onere amministrativo degli organi federali resta invariato.

8.1.7 Incaricato federale della protezione dei dati e della trasparenza

8.1.7.1 Art. 37 Nomina e statuto

La procedura di nomina di cui al capoverso 1 resta invariata, poiché è conforme alla direttiva (UE) 2016/680 e al P-STE 108. L'articolo 53 del regolamento (UE) 2016/679 ha lo stesso tenore dell'articolo 43 della direttiva (UE) 2016/680.

Anche i capoversi 2, 4 e 5 rimangono invariati rispetto al diritto vigente (art. 26 cpv. 2, 4 e 5 LPD). 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.

8.1.7.2 Art. 38 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. L'articolo 54 paragrafo 1 lettera e del regolamento (UE) 2016/679 contiene un disciplinamento analogo.

Il mandato dell'Incaricato potrà pertanto essere rinnovato soltanto due volte ed egli potrà rimanere in carica al massimo per 12 anni. Questa regola permette di rafforzare

l'indipendenza dell'Incaricato in quanto autorità. Il timore dell'Incaricato di non essere rinominato non deve costituire un freno all'adempimento dei suoi compiti. Il rapporto di lavoro si estingue automaticamente quando l'Incaricato raggiunge l'età di cui all'articolo 21 della legge federale del 20 dicembre 1946[108] sull'assicurazione per la vecchiaia e per i superstiti (LAVS; art. 10 cpv. 1 in combinato disposto con l'art. 14 cpv. 1 LPers).

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

8.1.7.3 Art. 39 Attività accessorie

L'articolo 39 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 38 capoverso 1 primo periodo AP-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, dell'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 Consiglio federale può autorizzare l'Incaricato a esercitare un'attività accessoria.

8.1.7.4 Art. 40 Sorveglianza

Il capoverso 1 stabilisce il principio secondo cui l'Incaricato è l'autorità cui compete la sorveglianza del rispetto delle disposizioni federali sulla protezione dei dati. L'Incaricato esercita la sua sorveglianza in modo indipendente e imparziale nei confronti sia dei privati sia degli organi federali. Determinate autorità federali sorvegliano privati o 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 e l'Ufficio federale delle comunicazione (UFCOM) sorveglia la Commissione federale delle comunicazioni (ComCom). L'espressione «organizzazioni esterne all'Amministrazione federale» corrisponde a quella dell'articolo 1 capoverso 2 lettera e della 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 2 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 41 AP-LPD contro la medesima parte, questi e l'autorità di sorveglianza devono coordinarsi a due livelli: 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. Il coordinamento deve essere 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.

8.1.7.5 Art. 41 Inchiesta

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 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 (lett. a), quando devono essere registrate collezioni

[108] RS **831.10**

di dati in virtù dell'art. 11*a* LPD (lett. b) o quando vi è l'obbligo d'informare secondo l'articolo 6 capoverso 3 LPD (lett. c). 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. È quindi necessario sopprimere i casi elencati all'articolo 29 capoverso 1 LPD.

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 confermi la decisione di adeguatezza nei confronti della Svizzera.

Capoverso 1 Apertura dell'inchiesta

Secondo l'articolo 41 capoverso 1 AP-LPD l'Incaricato può avviare 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. 44 capoverso 2 AP-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).

L'articolo 41 lascia un certo margine d'apprezzamento all'Incaricato, poiché la disposizione non lo obbliga ad avviare un'inchiesta appena constata degli indizi, bensì gli conferisce la facoltà di farlo. Spetta pertanto all'Incaricato decidere sull'opportunità di aprire un'inchiesta. Può ad esempio rinunciarvi se ritiene che si possa rimediare a una situazione problematica fornendo consigli al titolare del trattamento. L'Incaricato può invece essere indotto ad avviare un'inchiesta quando determinati trattamenti riguardano un numero elevato di persone e presentano pertanto un interesse per la società in generale. In altre parole, l'Incaricato interviene quando reputa che vi sia un interesse pubblico sufficiente per un'inchiesta e in linea di massima non interviene in un caso che riguarda la sfera privata di un singolo individuo. Nel secondo caso la persona interessata deve agire contro una persona privata per via civile o ricorrere contro l'organo federale d'innanzi all'autorità di ricorso competente, come d'altronde previsto anche dal diritto vigente.

Capoverso 2 Obblighi di collaborare

Il capoverso 2 disciplina l'obbligo di collaborare della persona privata o dell'organo federale. Secondo la disposizione, la parte del procedimento deve fornire all'Incaricato tutte le informazioni e i documenti necessari per l'inchiesta. Poiché l'Incaricato sottostà al segreto d'ufficio di cui all'articolo 22 LPers, la confidenzialità è garantita (art. 37 cpv. 2 AP-LPD)[109]. Il presente capoverso corrisponde agli articoli 27 capoverso 3 e 29 capoverso 2 LPD. L'articolo 50 capoverso 2 lettera c AP-LPD prevede una sanzione penale per la persona privata che viola il suo obbligo di collaborare; tale sanzione non è prevista dal diritto vigente.

Capoverso 3 Misure investigative

Nell'ambito dell'inchiesta, l'Incaricato può ordinare misure investigative nei confronti della persona privata o dell'organo federale. La disposizione corrisponde all'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.

Affinché le misure investigative siano proporzionali allo scopo, devono essere soddisfatte le condizioni di cui al capoverso 3. L'Incaricato può pertanto adottare le misure soltanto se l'organo federale o la persona privata non ottempera all'obbligo di collaborare e se i tentativi dell'autorità competente di ottenere le informazioni o i documenti necessari sono stati vani.

[109] TF 1C_41/2016 del 22 mar. 2016.

Ha il diritto di ispezionare senza preavviso i locali della persona privata o dell'organo federale oggetto della sorveglianza (lett. a) e di esigere l'accesso a tutti i dati e le informazioni necessari (lett. b). Per l'esecuzione delle misure investigative, l'Incaricato può chiedere assistenza amministrativa alle autorità federali e cantonali menzionate all'articolo 46 AP-LPD. Le misure previste al capoverso 3 possono essere adottate soltanto se è stata aperta un'inchiesta.

Capoverso 4 Accertamenti al di fuori di un'inchiesta

Il capoverso 4 precisa che l'Incaricato può verificare anche al di fuori di un'inchiesta se le persone private o gli organi federale rispettano le disposizioni federali sulla protezione dei dati. Può ad esempio ottenere dal titolare del trattamento determinate informazioni per accertare una situazione di cui è a conoscenza. Nell'ambito della verifica, l'Incaricato può consigliare il titolare del trattamento. Se dalle verifiche affiorano indizi di violazione della protezione dei dati, l'Incaricato avvia un'inchiesta conformemente al capoverso 1.

8.1.7.6 Art. 42 Provvedimenti cautelari

Secondo l'articolo 33 capoverso 2 LPD, qualora nell'ambito dell'accertamento dei fatti nei confronti di una persona 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 43 AP-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.

Secondo il capoverso 1, l'Incaricato stesso può ordinare provvedimenti cautelari per mantenere lo stato esistente, salvaguardare interessi giuridici minacciati o preservare mezzi di prova. Rispetto al diritto vigente, i casi in cui l'Incaricato può ordinare provvedimenti cautelari sono stati estesi. Il criterio determinante non è più soltanto il rischio per la persona interessata di subire un danno irreparabile; provvedimenti cautelari potranno infatti essere ordinati anche quando l'inchiesta è messa a repentaglio, ad esempio in presenza del rischio di collusione o della scomparsa di determinati elementi probatori.

L'Incaricato può ad esempio imporre alla persona privata o all'organo federale di sospendere il trattamento di dati per la durata dell'inchiesta o ordinare il sequestro di materiale.

Per l'esecuzione delle misure cautelari, l'Incaricato può far capo ad altre autorità federali e cantonali (cpv. 2).

Secondo l'articolo 44 capoverso 3, il ricorso contro i provvedimenti cautelari dell'Incaricato non ha effetto sospensivo.

8.1.7.7 Art. 43 Provvedimenti amministrativi

L'articolo 43 attua l'articolo 47 paragrafo 2 della direttiva (UE) 6016/680 e dà seguito alle raccomandazione 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 par. 2 lett. i) e ordinare la sospensione dei flussi di dati verso un destinatario in un Paese terzo o un'organizzazione internazionale (art. 58 par. 2 lett. j).

L'articolo 43 capoverso 1 è ampiamente conforme all'articolo 12^{bis} paragrafo 2 lettera c P-STE 108, secondo cui ciascuno Stato contraente è tenuto a conferire all'autorità di controllo la competenza di rendere decisioni e di infliggere sanzioni amministrative. Tuttavia, il Consiglio federale non intende conferire all'Incaricato la competenza di infliggere sanzioni amministrative, proponendo invece di attribuirgli maggiori poteri decisionali e di inasprire le disposizioni penali dell'AP-LPD (n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

In virtù dell'articolo 43 capoverso 1, l'Incaricato può ordinare di sospendere, modificare o cessare del tutto o in parte un trattamento contrario alle disposizioni sulla protezione dei dati, nonché di distruggere i dati. L'articolo 43 AP-LPD lascia tuttavia un certo margine

d'apprezzamento all'Incaricato, poiché la disposizione non lo obbliga a prendere provvedimenti amministrativi, bensì gli conferisce la facoltà di farlo. Prima di pronunciare tali provvedimenti può ad esempio consigliare il titolare del trattamento affinché ponga rimedio alla situazione. Se pronuncia un provvedimento, l'Incaricato è tenuto a rispettare il principio della proporzionalità. Se del caso, ordina di modificare o cessare il trattamento limitando il provvedimento alla parte problematica del trattamento.

Il capoverso 2 è conforme all'articolo 12 paragrafo 6 P-STE 108, secondo cui l'autorità di controllo può proibire o sospendere la comunicazione di dati personali verso un altro Paese.

L'Incaricato notifica la sua decisione soltanto alle parti oggetto dell'inchiesta. Se del caso, informa il pubblico conformemente all'articolo 48 AP-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 della procedura d'inchiesta possono presentare ricorso conformemente alle disposizioni generali sull'organizzazione giudiziaria federale (cfr. art. 44).

Secondo l'articolo 50 capoverso 2 lettera e AP-LPD, chi non ottempera a una decisione notificatagli dall'Incaricato è punito con una multa.

8.1.7.8 Art. 44 Procedura

Secondo il capoverso 1, la procedura d'inchiesta e le decisioni di cui all'articolo 42 e 43 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). La persona interessata non ha qualità di parte, neppure nel caso in cui l'Incaricato ha avviato un'inchiesta su sua denuncia. Se la persona interessata intende far valere le sue pretese nei confronti della persona privata deve agire in giudizio conformemente all'articolo 25 AP-LPD, ossia dinnanzi al giudice civile competente. Nel settore pubblico, la persona interessata deve agire contro l'organo federale responsabile (art. 34 AP-LPD), se del caso impugnando la decisione di quest'ultimo dinnanzi alla competente autorità di ricorso. La procedura è invariata rispetto al diritto vigente.

Secondo il capoverso 3, i ricorsi contro i provvedimenti cautelari di cui all'articolo 42 non hanno effetto sospensivo.

Secondo il capoverso 4, l'Incaricato può impugnare le decisioni del Tribunale amministrativo federale relative ai ricorsi.

8.1.7.9 Art. 45 Obbligo di denuncia

L'AP-LPD prevede l'obbligo dell'Incaricato di denunciare alle autorità di perseguimento penale i reati di cui è venuto a conoscenza nell'esercizio della sua funzione. Se ad esempio constata che una persona privata ha commesso una violazione ai sensi degli articoli 50 e seguenti AP-LPD, l'Incaricato deve denunciarlo alle competenti autorità cantonali di perseguimento penale (art. 3 e 104 CP). Rispetto all'articolo 22*a* LPers, questa disposizione ha il vantaggio di estendere l'obbligo di denuncia alle contravvenzioni. Per il resto si applica l'articolo 22*a* LPers.

L'articolo 45 AP-LPD è conforme all'articolo 47 paragrafo 5 della direttiva (UE) 2016/680 e all'articolo 12bis paragrafo 1 lettera d P-STE 108, secondo cui l'autorità di controllo deve avere il potere di sottoporre all'attenzione di autorità giudiziarie le violazioni delle disposizioni sulla protezione dei dati. L'articolo 58 paragrafo 5 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

8.1.7.10 Art. 46 Assistenza amministrativa in Svizzera

Questa disposizione disciplina l'assistenza amministrativa tra l'Incaricato, da una parte, e le autorità federali e cantonali, dall'altra. Si tratta di un articolo nuovo. L'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'esecuzione della legge. 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 45 AP-LPD (lett. b) e alle autorità federali nonché alle autorità cantonali e comunali di polizia per l'esecuzione dei provvedimenti di cui agli articoli 41 capoverso 3, 42 e 43 AP-LPD (lett. c).

Le comunicazioni di cui ai capoversi 1 e 2 possono essere effettuate spontaneamente o su domanda.

8.1.7.11 Art. 47 Assistenza amministrativa tra autorità svizzere ed estere

Questa nuova disposizione disciplina l'assistenza amministrativa tra l'Incaricato e le autorità incaricate della protezione dei dati all'estero. L'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 inoltre conforme agli articoli 15 e 16 P-STE 108. L'articolo 61 del regolamento (UE) 2016/679 prevede un disciplinamento analogo.

Capoverso 1 Domanda di assistenza amministrativa alle autorità estere

In virtù del capoverso 1 l'Incaricato può chiedere assistenza amministrativa a un'autorità estera anche senza aver aperto un'inchiesta ai sensi dell'articolo 41 capoverso 1 AP-LPD. L'incaricato deve rivolgere la richiesta al suo omologo all'estero, ossia all'autorità incaricata della protezione dei dati. Per poter comunicare le informazioni di cui al capoverso 1 l'Incaricato deve assicurarsi che siano rispettate le condizioni di cui all'articolo 5 AP-LPD.

Il capoverso 1 lettere a-g elenca le informazioni che l'Incaricato può fornire per ottenere assistenza amministrativa. Per poter comunicare l'identità delle persone interessate (lett. c), l'Incaricato deve ottenere il consenso di ciascuna di loro conformemente alle condizioni di cui all'articolo 4 capoverso 6 AP-LPD (cpv. 1, lett. c, n. 1). In mancanza del consenso, i dati possono essere comunicati soltanto se ciò è indispensabile all'adempimento dei compiti legali dell'Incaricato o dell'autorità estera (cpv. 1 lett. c n. 2). Queste condizioni corrispondono a quelle previste dall'articolo 29 capoverso 2 lettere a e b AP-LPD.

Capoverso 2 Assistenza amministrativa alle autorità estere

Il capoverso 2 disciplina l'assistenza amministrativa concessa dalla Svizzera a un'autorità estera. La prima condizione si trova nella frase introduttiva: l'autorità richiedente deve essere, nel proprio Paese, un'autorità competente in materia di protezione dei dati. Le lettere a-e elencano cinque ulteriori condizioni. Conformemente al principio della finalità, l'autorità richiedente deve impegnarsi a non utilizzare le informazioni e i dati personali per finalità che non siano quelle indicate nella domanda di assistenza amministrativa (lett. a). Lo Stato estero deve inoltre garantire il principio della reciprocità (lett. b). L'autorità richiedente deve altresì impegnarsi a rispettare il segreto d'ufficio e quello professionale e a non trasmettere a terzi, senza l'autorizzazione esplicita dell'Incaricato, le informazioni ricevute (lett. c e d). Infine, l'autorità richiedente deve rispettare le limitazioni di trattamento richieste dall'Incaricato (lett. e).

L'Incaricato può rifiutare la domanda di assistenza se ad esempio non sono rispettate le condizioni di cui all'articolo 5 AP-LPD o se uno dei motivi previsti dall'articolo 29 capoverso 6 AP-LPD si oppone alla comunicazione dei dati personali.

La comunicazione si svolge caso per caso e di regola è rapida e gratuita.

Le informazioni possono essere comunicate spontaneamente o su domanda dell'autorità estera (art. 5 o 25*a* PA).

8.1.7.12 Art. 48 Informazione

Il capoverso 1 corrisponde all'articolo 30 capoverso 1 LPD.

Il capoverso 2 estende l'informazione attiva 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 il contenuto dell'informazione da fornire al pubblico. I dati devono essere resi anonimi, salvo se sussiste un interesse pubblico preponderante alla loro pubblicazione (art. 29 cpv. 3 e 5 AP-LPD). Si applicano inoltre le condizioni di cui all'articolo 29 capoverso 6 AP-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.

8.1.7.13 Art. 49 Altri compiti

Rispetto al diritto in vigore (art. 31 LPD), l'elenco dei compiti conferiti all'Incaricato è completato allo scopo 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 lett. e P-STE 108.

L'Incaricato ha in particolare il compito di informare e offrire consulenza agli organi della Confederazione e dei Cantoni in merito alle questioni inerenti alla protezione dei dati. Ne fanno parte 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.

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, poiché l'AP-LPD conferisce all'Incaricato la competenza di adottare misure di controllo (art. 40) e provvedimenti cautelari (art. 41). Non è pertanto più necessario che egli si rivolga al Tribunale amministrativo federale per chiedere provvedimenti cautelari.

8.1.8 Disposizioni penali

Il Consiglio federale ha scelto di non conferire all'Incaricato la competenza di infliggere sanzioni amministrative. Infatti se così fosse, per assicurare la legalità e la disponibilità ad accettare tali decisioni e garantire la tutela dei diritti procedurali, la struttura organizzativa dell'Incaricato dovrebbe essere modificata, adeguandola ad esempio a quella della Commissione svizzera della concorrenza. È stato tuttavia deciso di rinunciarvi soprattutto per motivi legati ai costi. È inoltre preferibile punire i rei nell'ambito di procedimenti penali e fornire così tutte le garanzie del Codice di procedura penale. Questa opzione, che è controcorrente rispetto alla grande maggioranza della autorità di controllo estere[110], implica un rafforzamento notevole della parte penale della legge. Le sanzioni devono essere dissuasive, come lo esigono il P-STE 108 (art. 10)[111] e la direttiva (UE) 2016/680 (art. 57). Con un sistema penale

[110] Di regola, le autorità degli Stati membri dell'UE possono infliggere multe. Lo stesso vale per le autorità di Argentina, Singapore, Colombia e Turchia.

[111] Cfr. i nn. 95 e 96 del progetto di rapporto esplicativo di CAHDATA del 2 giu. 2016.

troppo debole, la Svizzera potrebbe vedersi rifiutare il rinnovo della decisione di adeguatezza da parte dell'Unione europea (art. 45 del regolamento [UE] 2016/679). Il regolamento (UE) 2016/679 prevede infatti la possibilità di infliggere, a complemento o in sostituzione dei provvedimenti amministrativi (art. 58), multe amministrative assai elevate per numerose violazioni degli obblighi, anche in caso di negligenza (art. 83). L'AP-LPD prevede pertanto di aumentare la multa a un massimo di 500 000 franchi. Tuttavia se la disposizione penale si rivolge soprattutto a persone fisiche, l'importo della multa rimane entro limiti ragionevoli; non sarebbe in particolare ragionevole determinarne l'ammontare in base alla cifra d'affari, come previsto per le sanzioni amministrative per le imprese. In virtù dell'articolo 53 AP-LPD le persone giuridiche possono direttamente essere perseguite penalmente (cfr. il commento all'art. 53 AP-LPD).

8.1.8.1 Art. 50 Violazione degli obblighi di informare, notificare e collaborare

L'articolo 50 AP-LPD riprende fondamentalmente l'articolo 34 LPD, completandolo in modo da tenere conto dei nuovi obblighi del titolare e del responsabile del trattamento.

Ammontare della multa

La disposizione prevede di aumentare l'importo massimo della multa – attualmente di 10 000 franchi in virtù dell'articolo 106 capoverso 1 CP – a 500 000 franchi. Il Consiglio federale ritiene infatti che, in considerazione dell'assenza di controllo da parte delle persone interessate sui propri dati, della mancante trasparenza dei trattamenti e del crescente potere degli operatori economici, sia necessario infliggere multe efficaci. Multe simili si trovano anche in altre leggi federali, quali la legge federale del 18 dicembre 1998[112] sulle case da gioco (LCG; art. 56) o la legge dell'8 novembre 1934[113] sulle banche (LBCR; art. 49). Va inoltre osservato che il regolamento (UE) 2016/679 (art. 83) prevede la possibilità di infliggere sanzioni amministrative fino a 10 milioni di euro o, nel caso di un'impresa, pari al 2 per cento della cifra d'affari annuale, o addirittura fino a 20 milioni di euro o al 4 per cento della cifra d'affari annuale. Anche questo è un argomento a favore dell'aumento della multa, che sarà certamente un criterio determinante per valutare se la legislazione svizzera garantisce una protezione adeguata ai sensi dell'articolo 45 del regolamento (UE) 2016/679. Si potrebbe anche pensare di trasformare le contravvenzioni in delitti, il che permetterebbe di punirli con una pena pecuniaria o con una pena detentiva di almeno tre anni. Il Consiglio federale intende tuttavia rinunciarvi in considerazione della minore gravità di questi comportamenti rispetto a quelli contemplati dall'articolo 52 AP-LPD (cfr. il commento all'art. 52).

È pertanto giustificato continuare a considerare come contravvenzioni le violazioni degli obblighi di informare, notificare e collaborare, aumentando tuttavia notevolmente le sanzioni. Va osservato che l'ammontare previsto costituisce un valore massimo e che spetta al giudice fissare la multa concreta tenendo conto della situazione economica dell'autore della contravvenzione (art. 106 cpv. 3 in combinazione con l'art. 47 CP). Inoltre, conformemente all'articolo 52 CP, occorre prescindere dal perseguimento penale o dalla punizione in casi di lieve entità.

Capoverso 1

Il capoverso 1 contempla le violazioni dell'obbligo di informare. La lettera a punisce le persone private che forniscono intenzionalmente informazioni inesatte o incomplete nell'ambito del loro obbligo d'informare (art. 13 e 15 AP-LPD) e del diritto d'accesso (art. 20 AP-LPD). La disposizione riprende sostanzialmente il contenuto del diritto vigente (art. 34 cpv. 1 lett. a LPD) adeguando i rinvii alle nuove disposizioni.

Il capoverso 1 lettera b punisce le persone private che omettono intenzionalmente, da una parte, di informare la persona interessata conformemente agli articoli 13 capoversi 1 e 5, 15 e 17 capoverso 2 AP-LPD, o, dall'altra, di fornirle le informazioni di cui all'articolo 13 capoversi 2-4 AP-LPD. L'AP-LPD riprende in linea di massima il diritto vigente (art. 34 cpv. 1 lett. b LPD), adeguandolo al nuovo contenuto dell'obbligo di informare.

[112] RS **935.52**

[113] RS **952.0**

Il capoverso 1 lettera c punisce le persone private che omettono intenzionalmente di comunicare all'Incaricato il risultato della valutazione d'impatto sulla protezione dei dati conformemente all'articolo 16 capoverso 3. La valutazione d'impatto è uno strumento importante che permette all'Incaricato di esercitare la sua funzione di sorveglianza. È pertanto giustificato sanzionare la violazione di tale obbligo. Anche il regolamento (UE) 2016/679 prevede sanzioni (art. 83 cpv. 4 lett. a).

Capoverso 2

L'articolo 49 capoverso 2 lettera a punisce le persone private che omettono di comunicare all'Incaricato le garanzie specifiche, segnatamente contrattuali (art. 5 cpv. 3 lett. b AP-LPD), o le norme vincolanti d'impresa (art. 5 cpv. 3 lett. c n. 2 e cpv. 6 AP-LPD) oppure non gli comunicano che intendono ricorrere a garanzie standardizzate (art. 5 cpv. 3 lettera d n. 2 e cpv. 6 AP-LPD). La disposizione corrisponde in parte al vigente articolo 34 capoverso 2 LPD adeguandolo ai nuovi obblighi in caso di comunicazione transfrontaliera.

Il capoverso 2 lettera b punisce le persone private che omettono di comunicare all'Incaricato, per approvazione, le garanzie standardizzate (art. 5 cpv. 3 lett. c numero 1) o le regole vincolanti d'impresa (art. 5 cpv. 3 lett. d n. 1). Si tratta di una novità, poiché tali obblighi non sono previsti dal diritto vigente. Il regolamento (UE) 2016/679 prevede in questi casi la possibilità di infliggere una multa fino a 10 milioni di euro o, se si tratta di un'impresa, fino al 2 per cento della cifra d'affari dell'anno d'esercizio precedente (art. 83 par. 5 lett. c).

La lettera c corrisponde al vigente articolo 34 capoverso 2 lettera b LPD. L'espressione «accertamento dei fatti» è tuttavia sostituita da «inchiesta».

La lettera d punisce la violazione del nuovo obbligo di comunicare all'Incaricato le violazioni della protezione dei dati (art. 17 cpv. 1 AP-LPD). Il Consiglio federale ritiene che si tratti di informazioni indispensabili all'Incaricato per esercitare la sorveglianza e che pertanto l'omissione debba essere punita. Anche il regolamento (UE) 2016/679 prevede la punizione della violazione di tali obblighi (art.83 par. 4 lett. a).

La lettera e punisce le persone private che non ottemperano a una decisione dell'Incaricato. La disposizione intende garantire che i provvedimenti presi dall'Incaricato esplichino effetto. Secondo il Consiglio federale non è sufficiente rinviare all'articolo 292 CP in quanto la multa prevista da tale disposizione è troppo esigua. Il regolamento (UE) 2016/679 prevede anch'esso la punizione di questo comportamento (art. 83 par. 4 lett. e).

Capoverso 3

Il capoverso 3 lettera a punisce la violazione dell'obbligo di informare i destinatari a cui sono stati comunicati dati di qualsiasi rettifica, cancellazione o distruzione di dati o di qualsiasi violazione della protezione dei dati nonché limitazione di trattamento (art. 19 lett. b AP-LPD). Secondo la lettera b è punibile anche la violazione dell'obbligo di informare il titolare del trattamento di qualsiasi trattamento non autorizzato di dati (art. 17 cpv. 4 AP-LPD). Il regolamento (UE) 2016/679 prevede la possibilità di infliggere una multa fino a 10 milioni di euro o, nel caso di un'impresa, fino al 2 per cento della cifra d'affari dell'anno d'esercizio precedente (art. 83 par. 4 lett. a).

I suddetti comportamenti sono punibili anche se l'autore agisce per negligenza. In tal caso la multa è di al massimo 250 000 franchi. Anche il regolamento (UE) 2016/679 prevede questa figura di reato (art. 83 cpv. 2 lett. b).

8.1.8.2 Art. 51 Violazione degli obblighi di diligenza

Questa disposizione è nuova poiché l'AP-LPD prevede una serie di obblighi che non sono contemplati dalle disposizioni penali vigenti. Il Consiglio federale ritiene 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. Di conseguenza, e per incitare questi ultimi a rispettare globalmente la legge, il Consiglio federale propone di completare l'elenco delle violazioni penali della legge. Occorre inoltre sottolineare che il regolamento (UE) 2016/679 prevede la possibilità di punire questi comportamenti (art. 83 par. 4

lett. a e 5 lett. c) anche in caso di negligenza. La disposizione non si applica agli organi federali, visto che per loro sono già previsti provvedimenti disciplinari.

Secondo l'articolo 51 capoverso 1 sono punite con la multa fino a 500 000 franchi le persone private che intenzionalmente violano determinati obblighi. I motivi per tale pena sono quelli illustrati nel commento all'articolo 50.

La lettera a punisce la comunicazione di dati all'estero in violazione dell'articolo 5 capoversi 1 e 2 senza che siano soddisfatte le condizioni di cui all'articolo 6 AP-LPD.

La lettera b punisce il conferimento del trattamento di dati a un responsabile in violazione dell'articolo 7 capoversi 1 e 2 AP-LPD.

La lettera c punisce chi non prende i provvedimenti necessari per proteggere i dati contro il trattamento non autorizzato e la perdita (art. 11 AP-LPD).

La lettera d punisce chi non effettua la valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 16 AP-LPD.

La lettera e punisce chi non prende le misure appropriate ai sensi dell'articolo 18 AP-LPD.

Infine, la lettera f punisce la mancata documentazione del trattamento di dati conformemente all'articolo 19 lettera a AP-LPD.

8.1.8.3 Art. 52 Violazione dell'obbligo di discrezione

Questa disposizione intende completare la tutela del segreto professionale prevista dall'articolo 321 CP. Quest'ultimo è ormai lacunoso a causa della crescente specializzazione delle attività professionali e dei metodi sempre più sofisticati del trattamento di informazioni. L'articolo 52 AP-LPD applica pertanto l'obbligo di discrezione a determinate professioni, non contemplate dall'articolo 321 CP nonostante il loro esercizio renda indispensabile la tutela della confidenzialità. Si è preferita questa soluzione all'estensione del campo d'applicazione dell'articolo 321 CP, ritenendo inopportuno estendere anche il diritto di rifiutare di testimoniare in giudizio generalmente previsto dalle leggi procedurali per le professioni contemplate dall'articolo 321 CP[114].

Dall'entrata in vigore della LPD, le tecnologie dell'informazione e della comunicazione hanno registrato immensi progressi e una crescita senza precedenti. La comunicazione elettronica è ormai generalizzata e costituisce il modo più importante, se non l'unico, di trasmettere e conservare informazioni. I mezzi tecnici sono tali e il loro costo così esiguo da permettere ormai a un numero sempre crescente di persone di trattare quantità titaniche di dati. Mentre gli schedari di una volta imponevano limiti fisici concreti alle possibilità di archiviazione, è oggi sempre meno necessario distruggere dati elettronici vecchi per fare posto a quelli più recenti. La perennità delle informazioni è ormai garantita. Infine, l'evoluzione tecnologica è incessante e progredisce in maniera folgorante; pertanto in futuro queste possibilità non possono che amplificarsi. Ne consegue un pericolo per la tutela della sfera privata e una maggiore necessità di proteggerla.

Vista 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 all'articolo 321 CP, poiché anche per quest'ultimo il criterio determinante è che l'informazione in questione sia segreta, a prescindere dal suo contenuto. Ciò permette inoltre di impedire che la tutela penale venga indebolita a causa dell'abrogazione del termine «profilo della personalità».

È inoltre necessario adeguare il contenuto della disposizione penale per tenere meglio conto delle realtà descritte sopra. Le possibilità odierne agevolano il trattamento di dati per meri fini lucrativi. Si pensi in particolare ai commercianti e alle reti sociali attivi su Internet, che vendono e acquistano tali informazioni a scopi pubblicitari. Rispetto alle attività professionali per le quali è necessaria la conoscenza di tali dati, nell'ambito di attività commerciali vi è un peri-

[114] Messaggio LPD, FF **1988** II 353, 425; NIGGLI Marcel Alexander/MAEDER Stefan, Kommentar zu Art. 35 DSG in: Maurer-Lambrou/Blechta (a c. di), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 3ª ed., Basilea 2014, art. 35 LPD N 1.

colo maggiore di ingerenza nel bene giuridico tutelato. La pena prevista dal capoverso 1 lettera b intende pertanto impedire tali ingerenze.

Inoltre, una multa non corrisponde più in alcun modo alla gravità delle possibili ingerenze, soprattutto in riferimento all'articolo 321 CP. È quindi opportuno eliminare questa sproporzione e considerare la violazione dell'obbligo di diligenza un delitto passibile di una pena detentiva fino a tre anni o una pena pecuniaria.

8.1.8.4 Art. 53 Infrazioni commesse nell'azienda

Questa disposizione riprende il disciplinamento previsto dall'articolo 7 della legge federale del 22 marzo 1974[115] sul diritto penale amministrativo (DPA), aumentando però a 100 000 franchi l'importo massimo della multa a partire dal quale non è più possibile perseguire l'azienda invece della persona fisica. L'articolo 102 CP non è infatti applicabile alle contravvenzioni e, per le ragioni illustrate sopra, le violazioni della presente legge devono per lo più essere considerate contravvenzioni. Poiché vi è da temere che le contravvenzioni siano principalmente commesse in un'azienda, è giustificato applicare il regime dell'articolo 7 DPA per evitare di nuocere all'efficacia delle nuove disposizioni. È necessario un rinvio esplicito, poiché altrimenti la DPA non è applicabile nel caso specifico. Per i delitti dell'articolo 52 resta invece applicabile l'articolo 102 CP.

8.1.8.5 Art. 54 Diritto applicabile e procedura

Analogamente a quanto previsto dal diritto vigente, il perseguimento e il giudizio dei reati competono ai Cantoni, che applicano il CPP. L'articolo 54 contiene un rinvio specifico che non ha alcun influsso sulla questione della legge di procedura applicabile.

8.1.8.6 Art. 55 Prescrizione dell'azione penale per le contravvenzioni

L'esperienza insegna che le inchieste in materia di protezione dei dati sono spesso complesse e onerose. Per le contravvenzioni, l'azione penale si prescrive in tre anni (art. 109 CP). Per evitare che nella maggior parte dei casi i procedimenti penali siano sin dall'inizio votati all'insuccesso, l'AP-LPD propone di prolungare a cinque anni il termine di prescrizione dell'azione penale.

Non è invece necessario prevedere una deroga al termine di prescrizione dell'azione penale, pari a 10 anni, per i delitti di cui all'articolo 52 (art. 97 cpv. 1 lett. c CP).

8.1.9 Conclusione di trattati internazionali

Art. 56 Conclusione di trattati internazionali

L'articolo 56 AP-LPD 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 Consiglio federale può concludere trattati internazionali con uno o più soggetti di diritto internazionale (Stati, organizzazioni internazionali) in due casi. Secondo la lettera a, il Consiglio federale può concludere trattati internazionali concernenti la cooperazione internazionale tra le autorità incaricate della protezione dei dati. Si tratta di accordi di cooperazione sul modello dell'Accordo tra la Confederazione Svizzera e l'Unione europea del 17 maggio 2013[116] concernente la cooperazione in merito all'applicazione dei rispettivi diritti della concorrenza. Secondo la lettera b, il Consiglio federale può inoltre concludere trattati internazionali sul riconoscimento reciproco della protezione adeguata in caso di comunicazione internazionale di dati. Si pensi in particolare a un eventuale futuro accordo con gli Stati Uniti che sostituisca l'attuale «U.S-Swiss safe harbor framework».

Gli altri capoversi dell'articolo 36 LPD sono abrogati: i capoversi 1 e 4 sono superflui poiché la prassi di prescrivere esplicitamente che il Consiglio federale debba emanare le disposizioni d'esecuzione è stata abbandonata. Può essere abrogato anche il capoverso 3, secondo

[115] RS **313.0**

[116] RS **0.251.268.1**. Va osservato che in questo caso la competenza per la conclusione non era stata conferita al Consiglio federale.

cui il Consiglio federale 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 inutile, poiché il Consiglio federale 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.

8.1.10 Disposizioni finali e transitorie

8.1.10.4 Art. 57 Esecuzione da parte dei Cantoni

Questa disposizione corrisponde all'articolo 37 LPD. Sono adeguati soltanto i rimandi alle nuove disposizioni dell'AP-LPD. Per il resto si rinvia alle spiegazioni del messaggio del Consiglio federale 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[117].

8.1.10.5 Art. 58 Abrogazione e modifica di altri atti normativi

L'abrogazione e la modifica di altri atti normativi sono commentate al numero 8.2.

8.1.10.6 Art. 59 Disposizione transitoria

Secondo il capoverso 1, il titolare e il responsabile del trattamento dispongono di un termine di due anni dall'entrata in vigore della nuova LPD per mettere in atto l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (art. 16 AP-LPD) e adottare le misure di cui agli articoli 18 e 19 lettera a per i trattamenti in corso al momento dell'entrata in vigore della legge.

8.2 Commento alle modifiche degli altri atti normativi

L'abrogazione e la modifica di altre leggi federali sono necessarie in seguito all'AP-LPD e sono disciplinate nel suo allegato[118].

8.2.1 Abrogazione della legge federale del 19 giugno 1992 sulla protezione dei dati

Trattandosi di una revisione totale, la LPD vigente va abrogata.

8.2.2 Modifica terminologica in determinate leggi federali

In seguito alla soppressione dell'espressione «collezione di dati» nell'AP-LPD devono essere adeguate anche le leggi settoriali in cui essa appare. È sostituita pure l'espressione «titolare della collezione di dati».

L'AP-LPD prevede inoltre di sostituire l'espressione «profilo della personalità» con «profilazione», che è più precisa e definisce un'azione (cfr. il commento all'art. 3 lett. f AP-LPD). Per ragioni di coerenza, l'espressione «profili della personalità» va sostituita anche in buona parte delle leggi settoriali. Nella maggior parte delle leggi è sufficiente eliminarla. Questa soppressione non ha ripercussioni pratiche: in effetti, l'AP-LPD esige una base legale formale soltanto se il trattamento consiste nell'analizzare o prevedere caratteristiche essenziali quali il rendimento sul lavoro, la situazione economica, la salute, la vita sessuale o gli spostamenti, ossia se si effettua una profilazione. L'introduzione dell'espressione «profilazione» è pertanto giustificata unicamente nei casi in cui l'autorità effettua questo tipo di analisi o previsioni. Nelle norme sulla protezione dei dati specifiche a un settore, la base legale per il trattamento di dati degni di particolare protezione non viene per contro modificata. L'introduzione della nuova espressione «profilazione» nell'articolo 3 lettera f AP-LPD esige tuttavia la soppressione dell'espressione «profilo della personalità» in un certo numero di norme specifiche a un settore, commentate qui di seguito.

---

[117] FF **2003** 1885, hier 1927-1928

[118] Alcune di queste leggi federali sono attualmente oggetto di revisioni separate: la legge del 29 set. 1952 sulla cittadinanza (RS **141.0**; FF **2014** 4461), la legge del 4 ott. 1991 sui PF (RS **414.110**; FF **2016** 2977), e la legge militare del 3 feb. 1995 (RS **510.10**; FF **2016** 1731). Gli art. 27 e 27*d* LPers saranno modificati dal progetto di legge sui fondi di compensazione (FF **2016** 255).

8.2.3 Legge federale del 16 dicembre 2015[119] sugli stranieri

Art. 101

L'espressione «profilo della personalità» è soppressa. Si veda il commento nel capitolo 8.2.1.

Art. 111d cpv. 2 lett. a e b

Attualmente, la lettera a dispone che la persona interessata debba aver senza ombra di dubbio dato il suo consenso e che, se si tratta di dati personali degni di particolare protezione, tale consenso deve essere esplicito. Il «consenso» della persona interessata deve essere definito in maniera uniforme nel diritto federale. La lettera a va dunque modificata rinviando all'articolo 4 capoverso 6 AP-LPD. La lettera b è modificata per tenere conto della nuova prescrizione di cui all'articolo 6 capoverso 1 lettera d AP-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 20 capoverso 2 lettera f AP-LPD.

8.2.4 Legge del 26 giugno 1998[120] sull'asilo

Art. 96 cpv. 1, art. 99a cpv. 2 lett. a, art. 100 cpv. 2 e art. 102 cpv. 1 e 2

L'espressione «profilo della personalità» è soppressa. Si veda il commento nel capitolo 8.2.2.

Art. 99 cpv. 6 primo periodo

L'espressione «titolare della collezione di dati» è sostituita con «titolare del trattamenti». Si veda il commento nel capitolo 8.2.2.

Art. 102c, frase introduttiva, cpv. 2 lett. a

Si veda il commento all'articolo 111*d* capoverso 2 lettere a e b AP-LStr.

Art. 102e secondo periodo

Si veda il commento all'articolo 111*f* secondo periodo AP-LStr.

8.2.5 Legge del 7 dicembre 2004[121] sulla trasparenza (LTras)

Art. 7 cpv. 2 e 3

Il capoverso 2 limita il diritto di accesso a documenti ufficiali se l'accesso può ledere la sfera privata di terzi, a meno che non prevalga eccezionalmente l'interesse pubblico all'accesso.

La modifica degli articoli 11 capoverso 1, 12 capoverso 3 e 15 capoverso 2 della LTras esige l'adeguamento della sistematica dell'articolo 7 capoverso 2 LTras. L'AP-LTras prevede dunque la limitazione del diritto d'accesso nell'articolo 7 capoverso 2 e la relativa eccezione al capoverso 3. Per il resto, le disposizioni del diritto vigente rimangono immutate.

Art. 11 cpv. 1

119 RS **142.20**

120 RS **142.31**

121 RS **152.3**

Secondo l'articolo 11 LTras l'autorità consulta la persona interessata e le dà la possibilità di presentare le proprie osservazioni se una domanda d'accesso concerne documenti ufficiali che contengono dati personali.

A causa del nuovo campo d'applicazione dell'AP-LPD è necessario garantire alle persone giuridiche il diritto di essere sentite nel caso in cui l'autorità intende accordare un diritto d'accesso ai sensi dell'articolo 7 capoverso 3 AP-LTras. Conformemente agli adeguamenti del capoverso 1, in futuro l'autorità dovrà consultare le persone interessate se intende consentire l'accesso a un documento che contiene dati personali che le riguardano o se intende applicare l'articolo capoverso 3 AP-LTras.

Art. 12 cpv. 3

L'adeguamento degli articoli 7 capoverso 3 e 11 capoverso 1 LTras richiede la modifica dell'articolo 12 capoverso 3, secondo cui il diritto d'accesso a un documento che contiene dati personali o l'accesso in virtù dell'articolo 7 capoverso 3 AP-LTras va sospeso fino a quando la situazione giuridica sia chiarita.

Art. 15 cpv. 2 lett. c (nuova)

Per i motivi suesposti è necessario integrare l'articolo 15 capoverso 2 con una nuova lettera c secondo cui l'autorità deve pronunciare una decisione se, diversamente da quanto raccomandato dall'Incaricato, intende accordare il diritto d'accesso a un documento ufficiale conformemente all'articolo 7 capoverso 3 AP-LTras.

8.2.6 Legge federale del 20 marzo 1968[122] sulla procedura amministrativa

Art. 71a

Il capoverso 1 introduce nella legge un principio sviluppato dal Tribunale federale[123], secondo cui le questioni relative alla protezione dei dati in una procedura che ha per oggetto pretese diverse da quelle specifiche fondate sulla LPD sono trattate nel quadro della procedura di ricorso principale e sottostanno ai medesimi rimedi di diritto.

Da questo principio (cpv. 1) consegue che l'Incaricato non ha la competenza di sorvegliare i trattamenti di dati effettuati nel quadro di una procedura di ricorso o di revisione (cpv. 2).

8.2.7 Codice civile

L'abrogazione dell'eccezione prevista all'articolo 2 capoverso 2 lettera d LPD per i registri pubblici relativi ai rapporti di diritto privato comporta la necessità di modificare determinate disposizioni federali del Codice civile inerenti allo stato civile. Ciò al fine di tenere conto, da un lato, del principio sancito all'articolo 9 CC – secondo cui i registri pubblici fanno piena prova dei fatti che attestano finché non sia dimostrata l'inesattezza del loro contenuto – e, dall'altro, dell'interesse pubblico alla tenuta di tali registri (cfr. consid. 73 del regolamento [UE] 2016/679).

Art. 45a cpv. 3 n. 3 e cpv. 4

L'articolo 45*a* capoverso 3 numero 3 AP-CC[124] incarica il Consiglio federale di disciplinare, con la partecipazione dei Cantoni, la vigilanza sulla banca dati centrale «Infostar». Si tratta in particolare di modificare l'articolo 83 dell'ordinanza del 28 aprile 2004 sullo stato civile (OSC), ispirandosi ad esempio alla soluzione prevista all'articolo 55 capoverso 1 dell'ordinanza N-SIS dell'8 marzo 2013[125]. Quest'ultima dispone che le autorità cantonali di protezione dei dati e l'Incaricato collaborino attivamente nel quadro delle loro rispettive com-

122 RS **172.021**

123 DTF **128** II 311 consid. 8.4

124 L'articolo 45*a* CC è attualmente oggetto di una revisione (cfr. il messaggio concernente la modifica del Codice civile svizzero [Atti dello stato civile e registro fondiario], FF **2014** 3059).

125 RS **362.0**

petenze ed esercitino una vigilanza coordinata sul trattamento dei dati personali. Per quanto riguarda la vigilanza su Infostar, l'Incaricato e le autorità cantonali di protezione dei dati non devono invadere la competenza del giudice di modificare i dati litigiosi (art. 42 CC).

In virtù dell'articolo 45*a* capoverso 4 AP-CC, il Consiglio federale può inoltre disciplinare i diritti delle persone interessate adottando una regolamentazione speciale che deroga del tutto o in parte all'articolo 32 capoversi 1-3 AP-LPD. Si tratta di una delega legislativa facoltativa. Il Consiglio federale può ricorrervi se ritiene che l'adozione di disposizioni speciali sia necessaria in considerazione dell'obiettivo perseguito dal registro centrale e tenendo conto delle esigenze della futura Convenzione STE 108, premesso che la Svizzera accetti il pertinente protocollo aggiuntivo.

8.2.8 Legge federale del 24 marzo 2000[126] sul trattamento di dati personali in seno al Dipartimento federale degli affari esteri

Art. 1, primo periodo, e art. 2 cpv. 2, primo periodo

Allo scopo di valutare le possibilità di impiegare all'estero una persona accompagnata dai familiari e di stimare i rischi legati alla situazione personale, l'articolo 3 abilita i servizi del personale del DFAE a trattare dati relativi ai familiari. È dunque necessario riformulare queste disposizioni al fine di autorizzare il trattamento di dati personali degni di particolare protezione e la profilazione.

8.2.9 Codice di procedura civile[127] (CPC)

8.2.9.1 Foro

Art. 20 lett. d

L'articolo 20 lett. d AP-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 12 AP-LPD, le azioni in esecuzione del diritto d'accesso secondo l'articolo 20 AP-LPD e le azioni secondo l'articolo 25 AP-LPD.

8.2.9.2 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[128]. Questa situazione, dovuta ai costi che devono assumere le persone interessate, riduce notevolmente l'efficacia della LPD. Di 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 sulla parità dei sessi [LPar] o controversie secondo il diritto del lavoro fino a un valore litigioso di 30 000 CHF o controversie derivanti dalla legge del 17 dicembre 1993 sulla partecipazione). In tal modo si riduce notevolmente il rischio economico per le persone interessate. In base al numero di casi finora trattati è però improbabile che la modifica faccia aumentare repentinamente il numero di casi portati in giudizio. 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

---

126 RS **235.2**

127 RS **272**

128 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)

Per le procedure secondo la LPD, l'AP propone di eliminare l'obbligo – di cui all'articolo 99 capoverso 1 – 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 concerne procedure ordinarie concernenti azioni di diritto civile secondo l'articolo 25 AP-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, così come è già il caso ad esempio nelle controversie 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.

Il nuovo disciplinamento riduce il rischio economico per la persona interessata. Le spese ripetibili sono invece assegnate conformemente ai principi usuali (art. 104 segg. CPC).

8.2.9.3 Procedura applicabile

Art. 243 cpv. 2 lett. d

Analogamente al diritto d'accesso, i diritti secondo l'articolo 12 AP-LPD possono essere fatti valere con procedura semplificata. Questa modifica è necessaria in quanto l'articolo 12 AP-LPD è nuovo.

8.2.10 Legge federale del 18 dicembre 1987[129] sul diritto internazionale privato (LDIP)

Art. 130 cpv. 3
L'adeguamento dell'articolo è necessario poiché l'AP-LPD non utilizza più l'espressione «collezione di dati».
L'articolo 130 AP-LDIP dispone 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 oppure i tribunali svizzeri del luogo nel quale i dati sono gestiti o utilizzati. Un diritto d'informazione riferito a una determinata attività deve essere fatto valere nel luogo in cui tale attività ha luogo e non in un altro luogo in cui i dati sono trattati anche da qualcun altro.

8.2.11 Codice penale

*Art. 179^novies^*

[129] RS **291**

Questa disposizione punisce la sottrazione di dati personali non liberamente accessibili. In base agli svariati sviluppi tecnici è giustificato estenderla a tutti i tipi di dati personali, così come è già il caso per quanto riguarda la violazione dell'obbligo di discrezione di dell'articolo 52 AP-LPD (cfr. cap. 8.1.8.3). Va in particolare sottolineato che proprio per la profilazione di cui all'articolo 3 lettera f AP-LPD, che comporta un pericolo particolare per la persona interessata, possono essere utilizzati sia dati personali che dati privi di una relazione personale diretta, che però con la profilazione diventano a loro volta dati personali. È pertanto opportuno che la protezione dell'articolo 179^{novies} contempli tutti i tipi di dati personali.

L'espressione «non liberamente accessibili» è inoltre sostituita con «non […] accessibili a chiunque».

Art.179^{decies}

La mozione Comte (14.3288), accolta dal Parlamento, incarica il Consiglio federale 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 in un contesto giuridico 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. La disposizione va collocata sotto il titolo dei delitti contro l'onore e la sfera personale riservata[130]. S'intende però rinunciare a sanzionare l'usurpazione dell'identità altrui fine a sé stessa, 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. L'usurpazione d'identità per pura spacconeria o per celia non rientra dunque nel campo d'applicazione della norma e neppure l'utilizzo di una nuova identità fittizia.

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 merci o una presa di contatto personale e orale per preparare la cosiddetta truffa del falso nipote.

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[131].

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

[130] Art. 173 segg. CP.

[131] Cfr. la medesima figura di reato nel caso dell'abuso di autorità: HEIMGARTNER STEFAN, in: Niggli/Wiprächtiger (Ed.), Basler Kommentar, Strafrecht II, 3ª ed., Basilea 2013, Art. 312 StGB N 23.

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[132] 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, in caso contrario 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.

8.2.12 Legge federale del 22 marzo 1974[133] 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 2 lettera c AP-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

Questa disposizione disciplina la trasparenza della raccolta di dati personali. Si tratta di una disposizione speciale che prevale sugli articoli 13 e 14 AP-LPD. Corrisponde alla regolamentazione prevista dall'articolo 95 CPP.

Art. 18b

Si veda per analogia il commento all'articolo 349*g* capoverso 3 AP-CP (n. 8.2.10.7).

Art. 18c

Questa disposizione disciplina la comunicazione e l'utilizzazione di dati in procedimenti pendenti e corrisponde alla regolamentazione prevista all'articolo 96 CPP.

Art. 18d

Questa disposizione disciplina i diritti d'informazione in procedimenti pendenti. Si tratta di una disposizione speciale che prevale sugli articoli 19 e 20 AP-LPD. Corrisponde alla regolamentazione prevista all'articolo 97 CPP.

Art. 18e

Questa disposizione disciplina il requisito dell'esattezza dei dati. Corrisponde alla regolamentazione prevista all'articolo 98 CPP. Si tratta di una disposizione speciale che prevale sugli articoli 4 capoverso 5 e 34 capoverso 2 AP-LPD. Per quanto concerne il capoverso 2 si rinvia al commento all'articolo 98 capoverso 2 AP-CPP (n. 8.3.2).

Art. 18f

---

132 Art. 179^{novies} CP.

133 RS **313.0**

Il capoverso 1 recepisce un principio sviluppato dal Tribunale federale[134], secondo cui allorquando una questione relativa alla protezione dei dati si presenta nell'ambito di un procedimento che ha per oggetto pretese diverse da quelle che risultano specificamente dalla LPD, tale questione deve essere trattata nel quadro del procedimento principale e sottostare ai medesimi rimedi giuridici.

Dal principio sancito al capoverso 1 risulta che l'Incaricato non è competente per sorvegliare i trattamenti di dati effettuati dall'autorità amministrativa federale nel quadro di un procedimento penale amministrativo pendente (cpv. 2). Questa precisazione è necessaria poiché di norma le autorità amministrative federali non sono autorità giudiziarie indipendenti ai sensi dell'articolo 2 capoverso 2 lettera c AP-LPD. La sorveglianza del rispetto dei principi della protezione dei dati nel quadro di un procedimento pendente è garantita dal controllo indipendente esercitato dall'autorità giudiziaria di ricorso. Ciò costituisce un sistema di sorveglianza equivalente a quello dell'Incaricato.

8.2.13 Procedura penale militare del 23 marzo 1979[135] (PPM)

La giustizia militare è un'autorità giudiziaria indipendente (art. 1 PPM) e rientra nelle eccezioni di cui all'articolo 2 capoverso 2 lettera c AP-LPD. Diversamente dal CPP, la PPM non prevede però alcuna disposizione a sé stante sulla protezione dei dati. Il Consiglio federale ritiene pertanto opportuno adeguare la legge riprendendo in buona parte il disciplinamento previsto nel CPP tenendo conto delle modifiche apportate dal presente progetto.

Art. 25a

Questa disposizione disciplina la trasparenza della raccolta di dati personali. Si tratta di una disposizione speciale che prevale sugli articoli 13 e 14 AP-LPD. Corrisponde alla regolamentazione prevista all'articolo 95 CPP.

Art. 25b

Si veda per analogia il commento all'articolo 349*g* capoverso 3 AP-CP (n. 8.2.10.7).

Art. 25c

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

Questa disposizione disciplina il diritto d'accesso nel quadro di un procedimento pendente. Si tratta di una disposizione speciale che prevale sugli articoli 20 e 21 AP-LPD. Corrisponde all'articolo 97 CPP.

Art. 25e

Questa disposizione disciplina il requisito dell'esattezza dei dati e corrisponde all'articolo 98 CPP. Si tratta di una disposizione speciale che prevale sugli articoli 4 capoverso 5 e 34 capoverso 2 AP-LPD. Per il rimanente si rinvia al commento all'articolo 349*g* capoverso 2 AP-CP (n. 8.2.107).

8.2.14 Legge federale del 13 giugno 2008[136] sui sistemi d'informazione di polizia della Confederazione

Art. 5, titolo e cpv. 2

Il Consiglio federale ritiene che il capoverso 2 possa essere abrogato. L'affidamento del trattamento a un responsabile, anche se finalizzato al controllo e alla manutenzione informatica,

[134] DTF 128 II 311, consid 8.4

[135] RS **321.0**

[136] RS **361**

è retto esclusivamente dall'articolo 7 AP-LPD. L'articolo 5 capoverso 2 risulta dunque superfluo e pertanto occorre adeguare anche il titolo.

8.2.15 Legge federale del 9 ottobre 1992[137] sulla statistica federale

Art. 14a cpv. 1 primo e secondo periodo

L'articolo 14*a* disciplina i collegamenti di dati, tra cui anche la profilazione. Il capoverso 1 va dunque integrato autorizzando l'Ufficio federale a effettuare profilazioni per adempiere i suoi compiti statistici. Il secondo periodo del capoverso 1 dispone che se si tratta di dati che richiedono una particolare protezione o se dal collegamento emergono profili della personalità, i dati collegati vanno eliminati al termine delle elaborazioni statistiche. Questa disposizione va modificata nel senso che i dati vanno eliminati al termine delle elaborazioni statistiche.

8.2.16 Legge militare del 3 febbraio 1995[138]

Art. 31 cpv. 2

In ragione della natura dei compiti del servizio informazioni dell'esercito occorre riformulare la disposizione introducendo la competenza alla profilazione.

Art. 99 cpv. 2

In ragione della natura dei compiti del servizio informazioni dell'esercito occorre riformulare la disposizione introducendo la competenza alla profilazione.

Art. 100 cpv. 2

In ragione della natura dei compiti del servizio di sicurezza militare occorre riformulare la disposizione introducendo la competenza alla profilazione.

8.2.17 Legge federale del 3 ottobre 2008[139] sui sistemi d'informazione militari

Art. 1 cpv. 1, frase introduttiva, e art. 11 cpv. 2, frase introduttiva

In ragione della natura dei compiti dell'esercito e dell'amministrazione militare, occorre riformulare le disposizioni per rendere possibile la profilazione e definire la scadenza entro cui devono essere cancellati i dati utilizzati a tal fine.

8.2.18 Legge federale del 20 giugno 1997[140] sulle armi

Art. 32e cpv. 2 lett. a e b

Si veda il commento all'articolo 111*d* capoverso 2 lettere a e b AP-LStr.

Art. 32g secondo periodo

Si veda il commento all'articolo 111*f* secondo periodo AP-LStr.

8.2.19 Legge federale del 4 ottobre 2002[141] sulla protezione della popolazione e sulla protezione civile

Art. 72 cpv. 1 e 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 protezio-

137 RS **431.01**
138 RS **510.10**
139 RS **510.91**
140 RS **514.54**
141 RS **520.1**

ne civile e dei partecipanti ai corsi[142]. Queste disposizioni vanno dunque modificate stabilendo che la suddetta autorità può effettuare profilazioni ai sensi dell'articolo 3 lettera f AP-LPD.

8.2.20 Legge federale del 21 dicembre 1948[143] sulla navigazione aerea

Art. 107a cpv. 2, frase introduttiva, 4 e 5

Il diritto in vigore dispone che l'autorità federale competente può valutare le capacità delle persone attive nell'aviazione civile. La disposizione va dunque riformulata introducendo la competenza di effettuare profilazioni.

Al capoverso 5, invece, i profili della personalità sono cancellati senza essere sostituiti. I dati risultanti da una profilazione, infatti, sono considerati dati personali, per la cui diffusione occorre una base legale.

8.2.21 Legge del 3 ottobre 1951[144] sugli stupefacenti

Art. 3f cpv. 1

L'espressione «profili della personalità» è soppressa. Si veda il commento al numero 8.2.12.

Art. 18c secondo periodo

Si veda il commento all'articolo 111*f* secondo periodo AP-LStr.

8.3 Commenti 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; in seguito si rinvia a tale commento.

8.3.1 Codice penale

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.

8.3.1.1 Art. 349*a*

Questa disposizione sancisce il principio secondo cui i trattamenti di dati effettuati nell'ambito della cooperazione di polizia sono retti dalle disposizioni federali e cantonali di protezione dei dati, fatte salve le disposizioni speciali previste dagli articoli 349*b* e seguenti AP-CP. Queste ultime sono quindi applicabili anche alle autorità cantonali, a meno che contemplino esplicitamente soltanto gli organi federali. 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 che devono applicare il diritto federale.

8.3.1.2 Art. 349*b*

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. Al fine di attuare le esigenze della direttiva (UE) 2016/680, l'articolo 349*b* prevede una deroga all'articolo 29 AP-LPD. In assenza di una base legale, le autorità federali hanno quindi il diritto di comunicare dati unicamente nei casi previsti dall'articolo 349*b* lettere a e b. Queste disposizioni corrispondono all'articolo 29 capoverso 2 lettere b e c AP-LPD. Per contro, le autorità federali competenti non possono basarsi sull'articolo 29 capoverso 3

[142] L'art. 72 è oggetto di una revisione, la cui entrata in vigore è prevista il 1° gen. 2017 (FF 2014 5939).

[143] RS **748.0**

[144] RS **812.121**

lett. a, b ed e AP-LPD per comunicare dei dati poiché tale disposizione non è compatibile con le esigenze di cui agli articoli 8 e 10 della direttiva (UE) 2016/680.

8.3.1.3 Art. 349*c*

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*c* 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 quella a un'autorità nazionale. L'adozione di nuove restrizioni legali rimane possibile a condizione che il principio della parità di trattamento sia rispettato.

8.3.1.4 Art.349*d*

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*d* s'ispira alla sistematica e al contenuto degli articoli 5 e 6 AP-LPD, fatte salve certe modifiche legate alle esigenze degli articoli 35-38 della direttiva (UE) 2016/680.

Capoverso 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.

Capoverso 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 per comunicare 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 la Commissione europea l'ha constatato tramite decisione conformemente all'articolo 36 della direttiva (UE) 2016/680. Il capoverso 2 lettera a si distingue dall'articolo 5 capoverso 2 lettera a AP-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 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 sull'adeguatezza.

Il capoverso 2 lettera 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 5 capoverso 3 lettera a AP-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, ad esempio la Convenzione STE 108 e il suo protocollo aggiuntivo[145]. Il capoverso 2 lettera c corrisponde all'articolo 5 capoverso 3 lettera b AP-LPD. In virtù di questa di-

[145] Cfr. consid. 73 della direttiva (UE) 2016/680.

sposizione, 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.

Capoverso 3

Secondo il capoverso 3, la competente autorità federale 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, le comunicazioni vanno documentate, il che permette all'Incaricato di effettuare gli accertamenti necessari e se del caso pronunciare un divieto ai sensi dell'articolo 43 capoverso 2 AP-LPD.

Capoversi 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.

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. In questo caso l'autorità deve dunque 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. La competente autorità deve comunicare all'Incaricato la comunicazione di dati secondo il capoverso 4 (cpv. 5).

Capoverso 6

Nel capoverso 6 sono fatte salve le disposizioni relative all'autorizzazione per lo scambio nell'ambito della cooperazione internazionale in materia penale. In effetti, garantire la protezione adeguata prescritta al capoverso 1 non è l'unica condizione da soddisfare per poter comunicare lecitamente dati personali a uno Stato terzo, occorre inoltre rispettare le disposizioni legali in materia di cooperazione internazionale. Dati possono pertanto essere trasmessi a uno Stato terzo unicamente se l'autorità destinataria è competente per prevenire, accertare o perseguire un reato e se la comunicazione è necessaria per adempiere questi compiti legali. Qualsiasi ulteriore trattamento dei dati da parte dell'autorità destinataria deve rispettare le regole del principio della specialità. Per trasmettere i dati a un altro Stato terzo, l'autorità destinataria deve ottenere il consenso preliminare dell'autorità competente che glieli ha comunicati.

8.3.1.5 Art. 349*e*

Questa disposizione attua le esigenze 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*e* 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*d* (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).

8.3.1.6 Art. 349*f*

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[146].

Secondo la definizione dell'articolo 3 paragrafo 8 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. All'articolo 349*f*, il concetto di «destinatario» è espresso con il termine «terzo».

Capoverso 1

In virtù del capoverso 1, dati personali possono essere comunicati a un terzo stabilitosi in uno Stato terzo soltanto se sono soddisfatte quattro condizioni cumulative. Le comunicazioni di dati in virtù dell'articolo 349*f* 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.

La seconda condizione (cpv. 1 lett. a) è che la possibilità di cui alla frase introduttiva deve essere prevista da una legislazione speciale o da un trattato internazionale. In effetti, l'articolo 349*f* in sé non costituisce una base legale per comunicare dati personali. Devono essere rispettate anche le disposizioni legali in materia di cooperazione internazionale.

Il capoverso 1 lettera b dispone che 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*f* 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. c). L'autorità deve dunque ponderare gli interessi per determinare se prevalga l'interesse pubblico minacciato o l'interesse della persona interessata.

Capoverso 2

[146] Consid. 73 della direttiva (UE) 2016/680

Il capoverso 2 dispone che l'autorità competente comunichi i dati personali al terzo con l'espresso divieto di utilizzarli per scopi altri da quelli fissati dall'autorità. Si tratta di una concretizzazione del principio del vincolo alla finalità.

Capoverso 3

In virtù del 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).

Capoverso 4

Secondo il capoverso 4 l'autorità competente deve informare senza indugio l'Incaricato sulle comunicazioni di dati effettuate in virtù dell'articolo 349*f*. Contrariamente all'obbligo previsto all'articolo 349*d* 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. 4), il che permette all'Incaricato di effettuare le verifiche necessarie e se del caso di pronunciare un divieto di comunicazione in virtù dell'articolo 43 capoverso 2 AP-LPD.

8.3.1.7 Art. 349*g*

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 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 3 lascia un certo margine di manovra all'autorità competente. Quest'ultima deve adottare, per quanto possibile, i provvedimenti necessari per evitare la confusione tra le diverse categorie di persone interessate prima di comunicare i dati che le concernono a un destinatario. In certi casi questa distinzione potrebbe non essere possibile, ad esempio se lo stato di fatto non consente 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, che dispone che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali. Secondo la considerazione 30 della suddetta direttiva, questa disposizione è motivata dal fatto che la seconda categoria comprende dati basati sulla percezione soggettiva delle persone fisiche non sempre verificabili, per cui il requisito dell'esattezza non dovrebbe riferirsi all'esattezza di un'affermazione ma al semplice fatto che è stata fatta[147].

[147] Consid. 30 della direttiva (UE) 2016/680

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.

8.3.1.8 Art. 349*h*

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*h* s'ispira alla soluzione prevista all'articolo 8 della legge federale del 13 giugno 2008[148] sui sistemi d'informazione di polizia della Confederazione (LSIP) tenendo conto delle modifiche apportate dal presente avamprogetto (cfr. il n. 8.3.6).

Il capoverso 1 dispone che nei casi previsti alle lettere a-d la persona interessata possa chiedere all'Incaricato di verificare che gli eventuali dati che la concernono siano trattati conformemente al diritto. In ragione della sistematica del titolo quarto del libro terzo CP, la persona interessata può avvalersi dell'articolo 349*h* 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, 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. 44 cpv. 2 AP-LPD) e non può dunque ricorrere a rimedi giuridici contro le eventuali misure amministrative pronunciate dall'Incaricato (art. 43 AP-LPD).

8.3.1.9 Art. 349*i*

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 41 capoverso 1 AP-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 AP-LPD a contrario). Dato che la Svizzera è tenuta a riprendere e mettere in atto le esigenze 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*i* capoverso 1, la persona interessata che rende verosimile che uno scambio di dati personali che la concernono potrebbe violare le disposizioni di protezione dei dati (p.es. in relazione alle esigenze applicabili alla comunicazione di dati a uno Stato terzo o a un organo internazionale [art. 349*d* AP-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*h* cpv. 2 AP-CP). Se del caso, l'Incaricato può ordinare provvedimenti cautelari o amministrativi

[148] RS **361**

nei confronti dell'autorità federale in questione (art. 42 e 43 AP-LPD). L'Incaricato deve notificare la sua decisione all'autorità federale in questione e alla persona interessata, indicando loro i mezzi di ricorso.

8.3.1.10 Art. 355*a* cpv. 1 e 4

Visto che viene soppressa nell'AP-LPD, l'espressione «profilo della personalità» deve essere soppressa pure nel capoverso 1 del presente articolo (cfr. il commento al n. 8.2.1).

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*c*). 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.

8.3.1.11 Art. 355*f* e art. 355*g*

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. Per ragioni di sistematica, questa categoria di comunicazioni è disciplinata nell'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.

8.3.2 Codice di procedura penale[149]

Art. 95a

Questa disposizione attua le esigenze di cui agli articoli 6 e 7 paragrafo 1 della direttiva (UE) 2016/680. La lettera a tiene conto del fatto che con l'avanzare della procedura le persone interessate possono cambiare categoria. Le autorità giudicanti distinguono tra dati personali fondati su fatti e quelli fondati su valutazioni personali nelle considerazioni della sentenza debitamente motivata. Per il rimanente si rinvia per analogia al commento all'articolo 349*g* capoverso 3 AP-CP (n. 8.2.10).

Art. 98 cpv. 2

L'articolo 98 disciplina il requisito dell'esattezza. Si tratta di una disposizione speciale che prevale sugli articoli 4 capoverso 5 e 34 capoverso 2 AP-LPD. Per quanto concerne la modifica apportata al capoverso 2 si rinvia al commento all'articolo 349*g* capoverso 2 AP-CP (n. 8.2.10).

8.3.3 Assistenza internazionale in materia penale del 20 marzo 1981[150] (AIMP)

Il presente avamprogetto introduce nell'AIMP un nuovo capitolo 1*b* concernente la protezione dei dati e ispirato alla soluzione proposta dal legislatore federale negli articoli 95 e seguenti CPP. Le nuove disposizioni attuano inoltre determinate esigenze della direttiva (UE) 2016/680. Si tratta di disposizioni speciali sulla protezione dei dati che prevalgono sui principi generali dell'AP-LPD fintantoché è pendente una procedura di ricorso.

149 RS **312.0**

150 RS **351.1**

8.3.3.1 Art. 11*b*

L'articolo 11*b* disciplina l'obbligo d'informazione dell'autorità in caso di trattamento di dati nel quadro di un procedimento di assistenza giudiziaria avviato su richiesta di uno Stato estero. Si tratta di una disposizione speciale sulla protezione dei dati che prevale sugli articoli 13 e 14 AP-LDP. L'articolo 11*b* si applica anche alle autorità cantonali che collaborano a un procedimento di assistenza giudiziaria o che sono incaricate di eseguire una domanda di assistenza, ad esempio una domanda di estradizione. Dato che la cooperazione internazionale in materia penale è retta dal diritto federale, la Confederazione fa uso della sua competenza legislativa.

In virtù del capoverso 1, l'autorità competente, ossia l'autorità chiamata a decidere sulla domanda estera di assistenza giudiziaria (art. 1 cpv. 1 AIMP), è tenuta a informare la persona oggetto di una domanda di cooperazione in materia penale in merito a tutti i trattamenti di dati che la concernono. La disposizione è applicabile a qualsiasi persona penalmente perseguita o condannata nei confronti della quale lo Stato estero richiede la cooperazione svizzera per ottenerne l'estradizione o delegare il perseguimento e la repressione di un reato commesso da tale persona oppure eseguire la decisione penale straniera pronunciata nei suoi confronti (art. 1 cpv. 1 lett. a, c e d AIMP). L'autorità deve inoltre informare gli aventi diritto, di cui all'articolo 80*b* AIMP, in un procedimento volto a fornire assistenza giudiziaria per un procedimento penale estero.

L'obbligo d'informazione dell'autorità non è tuttavia assoluto. Essa ne è per esempio esonerata se un interesse pubblico o privato preponderante vi si oppone. L'autorità deve dunque ponderare se prevalga l'interesse pubblico minacciato o quello della persona interessata. Deve rinunciare a informare la persona interessata se giunge alla conclusione che un interesse privato o pubblico prevale sull'interesse della persona a essere informata.

Il capoverso 2 elenca i casi in cui l'interesse pubblico prevale. Secondo questa disposizione, l'interesse pubblico è preponderante segnatamente se l'informazione della persona interessata rischia di compromettere una procedura investigativa, un'istruzione, una procedura giudiziaria o una procedura di cooperazione internazionale in materia penale, ad esempio l'arresto di una persona ai fini dell'estradizione. L'elenco non è esaustivo. L'autorità può dunque fondarsi su altri elementi specifici al caso in questione.

Per il rimanente sono applicabili gli articoli 52 e 80*b* AIMP.

8.3.3.2 Art. 11*c*

Questa disposizione disciplina il diritto d'informazione durante una procedura pendente. Corrisponde all'articolo 97 CPP. Si tratta di una disposizione speciale che prevale sugli articoli 20 e 21 AP-LPD. Solo la persona oggetto di una domanda di assistenza giudiziaria internazionale in materia penale, può, nel quadro dei suoi diritti, consultare gli atti e ottenere dati personali che la concernono.

Per il rimanente sono applicabili gli articoli 52 e 80*b* AIMP.

8.3.3.3 Art. 11*d*

Questa disposizione introduce una restrizione del diritto d'accesso applicabile alle 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 avamprogetto (cfr. n. 8.3.6). L'articolo 11*d* tiene pure conto dell'articolo 7 della direttiva (UE) 2016/680, che obbliga gli Stati Schengen a prevedere un diritto per la 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.

Capoverso 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 domanda 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.

Capoversi 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 è quindi in grado di 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 è effettivamente oggetto di una domanda d'arresto ai fini dell'estradizione. Con l'introduzione di un diritto d'accesso indiretto l'AP 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*d* è inoltre di durata limitata. In effetti, se è arrestata in Svizzera la persona interessata può avvalersi dell'insieme dei diritti conferitigli dall'AIMP nel quadro della procedura d'estradizione.

Come indicato più 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. 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, 4, 5 e 6 sono identici alle corrispondenti disposizioni dell'articolo 349*h* AP-CP.

Capoverso 7

Il capoverso 7 dispone che in deroga al capoverso 2 l'UFG può, d'accordo con lo Stato richiedente, fornire alla persona interessata le informazioni richieste.

8.3.3.4 Art. 11*e*

Questa disposizione disciplina la parità di trattamento delle autorità Schengen e delle autorità nazionali in materia di protezione dei dati. Per il rimanente si rinvia al commento all'articolo 349*c* AP-CP (n. 8.2.10).

8.3.3.5 Art. 11*f*

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*d* AP-CP. Contrariamente al capoverso 3 di quest'ultimo, tuttavia, l'articolo 11*f* non prevede per l'autorità competente un obbligo di comunicare all'Incaricato le categorie di comunicazioni di dati personali effettuate conformemente all'articolo 11*f* capoverso 2 lettera c. Questa differenza è giustificata dalla necessità di introdurre nell'articolo 11*i* capoverso 2 la regola secondo cui all'Incaricato non compete sorvegliare i trattamenti di dati effettuati nel quadro di una procedura di assistenza giudiziaria in corso (cfr. il commento all'art. 11*i* AP-AIMP). Per il rimanente si rinvia al commento all'articolo 349*d* AP-CP (n. 8.2.10).

8.3.3.6 Art. 11*g*

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*e* AP-CP. Contrariamente al capoverso 1 lettera a di quest'ultimo, tuttavia, l'articolo 11*g* capoverso 1 lettera a contempla pure 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 al commento relativo all'articolo 349*e* AP-CP (n. 8.2.10).

8.3.3.7 Art. 11*h*

Questa disposizione disciplina il requisito dell'esattezza dei dati. Si tratta di una disposizione speciale che prevale sugli articoli 4 capoverso 5 e 34 capoverso 2 AP-LPD. Corrisponde all'articolo 349*g* AP-CP (cfr. il relativo commento al n. 8.2.10).

8.3.3.8 Art. 11*i*

Questa disposizione disciplina le pretese in materia di protezione dei dati delle persone oggetto di una domanda di cooperazione in materia penale nel quadro di un procedimento d'assistenza giudiziaria pendente. Corrisponde alla soluzione prevista dall'articolo 18*g* salvo che il capoverso 2 esclude esplicitamente l'applicazione degli articoli 20 e 21 AP-LPD concernenti il diritto d'accesso della persona interessata, dell'articolo 30 AP-LPD concernente l'opposizione alla comunicazione dei dati e dell'articolo 34 AP-LPD concernente le pretese in caso di trattamento illecito di dati da parte di un organo federale. Per il rimanente si rinvia al commento all'articolo 18*g* AP-DPA (n. 8.2.12).

8.3.4 Legge federale del 3 ottobre 1975[151] relativa al Trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale

Al fine di trasporre le esigenze della direttiva (UE) 2016/680 è necessario introdurre nella legge relativa al Trattato un rinvio agli articoli 11*b*-11*d* e 11*g*-11*i* AP-AIMP (art. 9*a*). L'articolo 11*e* AP-AIMP non è applicabile poiché instaura la parità di trattamento soltanto per le autorità Schengen e le autorità penali svizzere in materia di protezione dei dati. Come l'articolo 7 capoverso 3 della legge relativa al Trattato, l'articolo 9*a* fa salve le disposizioni del trattato del 25 maggio 1973[152] fra la Confederazione Svizzera e gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale.

8.3.5 Legge federale del 7 ottobre 1994[153] sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati (LUC)

Art. 13 cpv. 2

Al fine di attuare le esigenze della direttiva (UE) 2016/680 è necessario adeguare l'articolo 13 capoverso 2 introducendovi un rinvio agli articoli 349*a*-349*i* AP-CPP.

8.3.6 Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione (LSIP)

Art. 7 cpv. 2

Il capoverso 2 fa salvo pure il nuovo articolo 8bis.

Art. 8 cpv. 2-6 e 8

Questo articolo deve essere modificato poiché in virtù dell'AP-LPD l'Incaricato non emana più raccomandazioni può aprire un'inchiesta ai sensi dell'articolo 41 AP-LPD e se del caso ordinare misure amministrative in virtù degli articoli 42 e 43.

Il capoverso 2 è modificato dal punto di vista redazionale.

La seconda alternativa del primo periodo del capoverso 3 è modificata in quanto il sintagma «che ha inviato a fedpol una raccomandazione ai sensi dell'articolo 27 LPD affinché tali errori

151 RS **361.93**

152 RS **0.351.933.6**

153 RS **360**

vengano corretti» è sostituito da «che ha aperto un'inchiesta conformemente all'articolo 41 LPD». Visto che gli articoli 42 e 43 AP-LPD conferiscono all'Incaricato competenze decisionali, l'intervento del Tribunale amministrativo federale previsto dall'ultimo periodo del capoverso 3 e al capoverso 5 della LSIP vigente può essere soppresso.

Il capoverso 4 può essere abrogato. Il rinvio all'articolo 41 AP-LPD è sufficiente.

L'inchiesta dell'Incaricato può sfociare in una decisione (art. 43 AP-LPD) che fedpol può impugnare (cpv. 5).

Il capoverso 6 è modificato dal punto di vista redazionale.

Il capoverso 8 è modificato in quanto, se le condizioni sono soddisfatte, l'Incaricato può ordinare, e non più solo raccomandare, a fedpol di fornire alla persona interessata le informazioni richieste.

Art. 8a

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. Corrisponde all'articolo 11*e* AP-AIMP, per cui si rinvia al relativo commento (n. 8.3.3).

8.3.7 Legge del 12 giugno 2009 sullo scambio di informazioni con gli Stati Schengen (LSIS)

Art. 2 cpv. 3

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 Consiglio federale propone di abrogare questa disposizione e introdurre un rinvio agli articoli 349*a*-349*i* AP-CPP.

9 Ripercussioni

Le ripercussioni dell'avamprogetto e del recepimento della direttiva sono strettamente connesse e non sono pertanto illustrate separatamente.

9.1 Ripercussioni finanziarie e sull'effettivo del personale della Confederazione

Al presente stadio dei lavori è difficile valutare le ripercussioni finanziari dell'avamprogetto sull'effettivo del personale della Confederazione e in particolare sulle risorse dell'Incaricato.

Come risulta dalle risposte del Consiglio federale alle interpellanze Derder 15.4253 «Proteggere i dati per condividerli meglio. Un'opportunità urgente» e Aebischer 16.3011 «Adeguare le risorse e non soltanto la legge sulla protezione dei dati», il Consiglio federale intende esaminare la questione dell'aumento delle risorse dell'Incaricato nel messaggio, una volta fissati definitivamente i nuovi compiti di quest'ultimo. Se l'avamprogetto sarà mantenuto in questa forma, i compiti di cui agli articoli 5, 8, 16 e 17 AP-LPD e la competenza decisionale di cui agli articoli 41 e seguenti AP-LPD comporteranno presumibilmente un considerevole aumento del fabbisogno finanziario dell'Incaricato. In considerazione della crescente digitalizzazione dell'economia e dell'amministrazione, è inoltre prevedibile un aumento del numero di progetti pubblici e privati nonché di progetti legislativi in merito ai quali l'Incaricato sarà chiamato a esprimersi, da cui risulterà un bisogno di risorse supplementari. Per contro, già oggi l'Incaricato ha il compito di controllare, nel quadro della cooperazione Schengen e Dublino, il trattamento di dati personali da parte di organi federali. Secondo le sue indicazioni, attualmente l'Incaricato effettua da tre a quattro controlli all'anno. Questa cifra potrebbe crescere leggermente. Anche se in futuro l'Incaricato avrà nuove competenze in base alla direttiva UE, ciò non dovrebbe richiedere risorse supplementari, dato che già oggi può pronunciare raccomandazioni all'attenzione degli organi federali e, se la sua raccomandazione non è attuata, trasmettere per decisione una questione all'autorità superiore nonché impugnare la decisione di tale autorità. Non è tuttavia possibile escludere un aumento delle domande di

accertamenti da parte di persone interessate e delle domande di cooperazione delle autorità preposte alla protezione dei dati di altri Stati Schengen. Il fatto che in futuro le persone interessate avranno il diritto di chiedere all'Incaricato di avviare un'inchiesta potrebbe inoltre comportare un aumento dei casi. Questi nuovi compiti potrebbero dunque rendere necessaria l'attribuzione di due o tre posti supplementari al massimo.

Le ripercussioni finanziarie dell'avamprogetto sull'Amministrazione federale dovrebbero essere limitate. Sarà tuttavia opportuno esaminare la questione parallelamente a quella relativa alle risorse dell'Incaricato.

9.2 Ripercussioni per i Cantoni e i Comuni

L'accettazione del protocollo aggiuntivo 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.

9.3 Ripercussioni informatiche

L'avamprogetto 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 dell'impatto sulla protezione dei dati e comunicare all'Incaricato i rischi e le misure prese in considerazione. Inoltre, il titolare del trattamento deve di norma adottare le misure adeguate per attuare il principio della protezione fin dalla progettazione e documentare i suoi trattamenti. Deve infine notificare all'Incaricato e, se del caso, anche alla persona interessata determinati casi di violazione della protezione dei dati.

Le ripercussioni informatiche per gli organi federali sono più limitate sotto diversi aspetti. L'obbligo d'informare la persona interessata, ad esempio, non si applicherà nei casi in cui la decisione automatizzata è prevista dalla legge. Gli obblighi di allestire una valutazione d'impatto e di rispettare di norma il principio della protezione dei dati fin dalla progettazione hanno poche ripercussioni 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). La trasposizione dell'articolo 25 della direttiva (UE) 2016/680, che obbliga gli Stati Schengen a disporre che determinati trattamenti siano registrati in sistemi di trattamento automatizzato, ha ripercussioni sui sistemi di trattamento automatizzato di dati tenuti dagli organi federali. L'obbligo di verbalizzazione previsto dall'articolo 10 OLPD deve dunque essere adeguato poiché nel suo tenore attuale si applica unicamente ai trattamenti di dati degni di particolare protezione o di profili della personalità se le misure preventive non sono sufficienti a garantire la protezione dei dati. Al riguardo occorre prevedere una disposizione transitoria, come del resto autorizzato dall'articolo 63 paragrafo 2 della direttiva (UE) 2016/680. L'obbligo per gli organi federali di annunciare le loro attività di trattamento all'Incaricato 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.

9.4 Ripercussioni per l'economia

L'avamprogetto 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 svi-

luppo di nuove tecnologie è in effetti sempre più difficile sapere chi raccoglie dati su una persona, a quale scopo e chi ne è il destinatario. L'avamprogetto 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.

L'avamprogetto 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[154], 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. L'avamprogetto ha dunque anche l'obiettivo di adeguare il diritto federale alle esigenze europee 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 riveduta 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) –

Innalzando la protezione dei dati agli standard europei, l'avamprogetto ha inoltre l'effetto indiretto di rafforzare 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 l'avamprogetto può generare ripercussioni positive non solo per i consumatori ma anche per le imprese, che in tal modo resteranno attrattive e potrebbero approfittare di nuove possibilità commerciali soprattutto nel settore del commercio elettronico. I costi necessari per la realizzazione dei nuovi obblighi per i titolari del trattamento dovrebbero essere ampiamente compensati da queste ripercussioni positive.

L'intervento dello Stato è limitato allo stretto necessario con l'idea di responsabilizzare i titolari del trattamento incoraggiandoli ad esempio a rispettare le raccomandazioni di buona prassi emanate dall'Incaricato o da altri organi 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 garanzie o di regole d'impresa vincolanti precedentemente approvate dall'Incaricato, possono assicurarsi dell'esistenza di una protezione adeguata dei dati nel quadro dei flussi transfrontalieri.

9.5 Ripercussioni per la società e la sanità pubblica

Al fine di reagire alle sfide sociali rappresentate dalle nuove tecnologie, l'avamprogetto prevede in particolare di rafforzare i poteri di sorveglianza dell'Incaricato. Quest'ultimo potrà infatti aprire un'inchiesta e, se necessario, adottare misure amministrative, ad esempio nel caso di trattamenti che, riguardando un gran numero di persone, presentano un interesse per la società in generale. L'avamprogetto prevede pure di attribuire all'Incaricato 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.

9.6 Ripercussioni per la parità tra i sessi

L'avamprogetto non ha alcuna ripercussione per la parità trai sessi.

[154] GU L 215 del 25.8.2000, pag. 1

9.7 Ripercussioni per l'ambiente

L'avamprogetto non ha alcuna ripercussione diretta per l'ambiente.

10 Rapporto con il programma di legislatura e le strategie nazionali del Consiglio federale

10.1 Rapporto con il programma di legislatura

Il progetto è annunciato nel messaggio del 27 gennaio 2016[155] sul programma di legislatura 2015-2019.

10.2 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 (OGD). L'avamprogetto fa d'altronde parte del catalogo di misure adottato per l'attuazione della Strategia Svizzera digitale (cfr. n. 0).

11 Aspetti giuridici

11.1 Costituzionalità

11.1.1 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. Non si tratta neppure di un trattato di portata limitata. Di conseguenza è l'Assemblea generale a essere competente per l'approvazione dello scambio di note tra la Svizzera e l'Unione europea concernente il recepimento della direttiva (UE) 2016/680.

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).

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.

[155] FF **2016** 981, 1097

11.1.2 Competenza per l'approvazione del progetto di revisione della Convenzione STE 108

L'articolo 4 del progetto di protocollo d'emendamento della Convenzione 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.

L'AP-LPD è conforme al progetto di revisione della Convenzione STE 108. Non appena il suo protocollo di emendamento sarà aperto alla firma, il Consiglio federale potrà firmarlo e sottoporlo al Parlamento per approvazione. Per i motivi di cui al numero 11.1.1, il decreto federale concernente l'approvazione del protocollo di emendamento della Convenzione STE 108 sottostà a referendum in virtù dell'articolo 141 capoverso 1 lettera d numero 3 Cost.

11.1.3 Competenza legislativa della Confederazione

Come rilevato dal Consiglio federale 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[156], 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 provvedono affinché, per quanto vi si prestino, siano realizzati anche nelle relazioni tra privati. In questo senso l'avamprogetto contribuisce ad attuare l'articolo 13 capoverso 2 Cost., sia nelle relazioni tra Stato e privati che in quelle orizzontali tra privati.

Per quanto riguarda l'adozione delle disposizioni di protezione dei dati applicabili al diritto privato, il legislatore può basarsi sulla competenza di legiferare in materia di diritto civile (art. 122 Cost.), nonché in merito all'esercizio dell'attività economica privata (art. 95 Cost.) e alla protezione dei consumatori (art. 97 Cost.).

Nel settore del diritto pubblico, il legislatore federale si è fondato sul potere d'organizzazione conferitogli 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 nel loro settore. 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. L'avamprogetto 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.

11.2 Compatibilità con gli impegni internazionali della Svizzera

L'avamprogetto è compatibile con gli impegni internazionali della Svizzera. Le permette di aderire non appena possibile al protocollo d'emendamento della Convenzione STE 108 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.

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 alla sua entrata in vigore e conformi al diritto dell'Unione applica-

[156] FF **2003** 1885, 1932

bile anteriormente a tale data, restano in vigore fino alla loro modifica, sostituzione o revoca[157].

11.3 Forma dell'atto

In aggiunta al decreto federale che approva lo scambio di note tra la Svizzera e l'UE concernente il recepimento della direttiva (UE) 2016/680, il presente progetto comprende un avamprogetto di legge federale concernente la revisione totale della legge sulla protezione dei dati e la modifica di altri atti relativi alla protezione dei dati personali. Si tratta di un atto modificatore unico che sottostà a referendum. Tale atto mantello è costituito dalla cifra I contenente la revisione totale della LPD (AP-LPD) e in allegato le necessarie modifiche di altre leggi federali. La cifra II dell'atto mantello comprende invece le modifiche di leggi federali necessarie per l'attuazione della direttiva (UE) 2016/680 nel quadro degli obblighi Schengen.

11.4 Subordinazione al freno delle spese

L'avamprogetto non implica spese che sottostanno al freno delle spese (art. 159 cpv. 3 lett. b Cost.).

11.5 Conformità alla legge sui sussidi

L'avamprogetto non prevede sussidi.

11.6 Delega di competenze legislative

L'avamprogetto prevede principalmente le deleghe legislative seguenti.

- Il Consiglio federale rimane competente per emanare disposizioni sul riconoscimento delle procedure di certificazione e sull'introduzione di un marchio di qualità inerente alla protezione dei dati (art. 10 cpv. 2 AP-LPD).
- Se un organo federale tratta dati congiuntamente ad altre autorità, il Consiglio federale è incaricato di disciplinare in modo specifico i controlli e la responsabilità in materia di protezione dei dati (art. 26 AP-LPD).
- Il Consiglio federale conserva la sua competenza di autorizzare, a determinate condizioni, il trattamento automatizzato di dati degni di particolare protezione nel quadro di progetti pilota (art. 28 AP-LPD)
- Il Consiglio federale può inoltre disciplinare i diritti delle persone interessate adottando nella legislazione sullo stato civile disposizioni speciali che derogano del tutto o in parte all'articolo 34 AP-LPD (art. 45*a* cpv. 4 AP-CC).

[157] Consid. 95.