Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Ufficio federale di giustizia UFG
Ambito direzionale Diritto pubblico
Ambito specialistico Progetti legislativi I

Ottobre 2022

Revisione totale della legge sulla protezione dei dati (LPD)

Elaborazione di basi legali per il trattamento dei dati da parte di organi federali: sinossi delle modifiche principali

La revisione totale della legge sulla protezione dei dati (di seguito «nLPD») mira ad adeguare la protezione dei dati ai progressi tecnologici e ad allineare agli standard europei il livello di protezione dei dati imposto dalla Svizzera. La nLPD continua a rimanere una legge quadro valida per tutti gli ambiti. Nei principi relativi alla protezione dei dati fissa i requisiti del trattamento dei dati e prevede misure istituzionali, organizzative e procedurali che mirano a garantirne il rispetto. Tuttavia, il trattamento dei dati nel settore pubblico a livello federale continuerà a essere disciplinato principalmente nei pertinenti atti materiali. La nLPD si limita a fornire prescrizioni generiche al riguardo. Sebbene molti dei principi cardine rimangano immutati, la revisione totale della LPD prevede anche diverse novità che dovranno essere considerate nei futuri progetti legislativi (p. es. la cosiddetta «profilazione» o le «decisioni individuali automatizzate»).

Il presente documento illustra in dettaglio le principali modifiche che incidono sull'elaborazione di basi legali vertenti sul trattamento dei dati da parte di organi federali, integrando le spiegazioni di base contenute nella Guida di legislazione (cap. 14; n. marg. 813 segg.) e nella Guida di legislazione – Protezione dei dati. È rivolto soprattutto ai responsabili dell'elaborazione delle basi legali che desiderano conoscere in dettaglio la revisione della LPD per i loro progetti legislativi.

Di seguito questo documento presenta una breve panoramica dei punti chiave e dei lavori preliminari della revisione totale della LPD (► n. 1), per poi illustrare i principi legistici e normativi che restano immutati (► n. 2.1). Nella sezione principale vengono presentate le novità più importanti introdotte per quanto riguarda il livello e la densità normativi delle basi legali speciali per il trattamento dei dati personali da parte degli organi federali (► n. 2.2). Un capitolo separato è poi dedicato alla gestione dei dati delle persone giuridiche, da ora in poi escluse dal campo di applicazione della nLPD (► n. 3). L'ultimo capitolo contiene una panoramica di varie altre novità che possono risultare rilevanti anche per i progetti legislativi (► n. 4).

BJ-D-12643401/222

Indice

1 Punti chiave della revisione totale della LPD

Il Parlamento ha scisso il Progetto del Consiglio federale del 15 settembre 2017 concernente la revisione totale della LPD (D-LPD) in due tappe.

- Nella **prima tappa** è stata attuata soltanto la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, rilevante per Schengen (di seguito: direttiva [UE] 2016/680 sulla protezione dei dati in materia penale, rilevante per Schengen). A tal fine è stata creata, in via transitoria, una nuova legge sulla protezione dei dati in ambito Schengen (LPDS; RS 235.3), che è entrata in vigore il 1° marzo 2019[1] e che contiene le condizioni quadro in materia di protezione dei dati per la cooperazione di Schengen nel settore penale nella misura in cui la precedente LPD non soddisfaceva i requisiti della direttiva (UE) 2016/680. Oltre alla LPDS sono state adeguate o integrate anche le disposizioni sulla protezione dei dati rilevanti per la collaborazione giudiziaria e di polizia contenute in altre leggi federali (soprattutto nel Codice penale [CP; RS 311.0] e nella legge sull'assistenza in materia penale [AIMP; RS 351.1]). Con l'entrata in vigore della revisione totale della LPD, la LPDS sarà di nuovo abrogata, dato che lo standard di protezione richiesto dalla direttiva (UE) 2016/680 sarà garantito essenzialmente dalla nLPD. Le modifiche apportate agli atti normativi settoriali rimarranno invece in vigore.

- Nella **seconda tappa** è stata invece discussa la vera e propria revisione totale della LPD, che attua, tra le altre cose, i requisiti della Convenzione sulla protezione dei dati 108+ del Consiglio d'Europa[2]. Inoltre allinea il diritto svizzero in materia di protezione dei dati al regolamento generale (UE) 2016/679 sulla protezione dei dati, in modo che l'UE possa attestare anche in futuro che la Svizzera dispone di un adeguato livello di protezione dei dati (mediante una cosiddetta «decisione di adeguatezza»). Il Parlamento ha adottato la revisione totale della LPD il 25 settembre 2020, dopo che il termine per il referendum è scaduto inutilizzato il 14 gennaio 2021.

1.1 Documentazione relativa alla revisione totale della LPD

- **Testo della votazione finale** relativa alla nLPD del 25 settembre 2020: FF **2020** 6695
- **Bollettino Ufficiale**https://www.parlament.ch/de/ratsbetrieb/suche-amtliches-bulletin -k=PdAffairId:20170059
- **Curia Vista:** la documentazione dei Consigli, i paragrammi e la cronologia sono consultabili sotto l'affare 17.095
- **Messaggio e disegno del Consiglio federale** del 15 settembre 2017: FF **2017** 5939 e **2017** 6173

[1] Cfr. in merito anche il rapporto esplicativo dell'ottobre 2018 dell'UFG relativo alla legge federale che attua la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (consultabile all'indirizzo: https://www.bj.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html).

[2] La Svizzera non ha ancora ratificato la Convenzione del Consiglio d'Europa sulla protezione dei dati 108+, ma il Consiglio federale ha firmato il Protocollo di emendamento il 21 novembre 2019. Il 19 giugno 2020 il Parlamento ha approvato a larga maggioranza il decreto federale che approva la Convenzione 108+ (affare n. 19.068). La revisione totale della LPD attua le disposizioni della Convenzione 108+ a livello federale. La ratifica, ovvero l'adesione della Svizzera alla Convenzione 108+, sarà possibile solo all'entrata in vigore del nuovo diritto sulla protezione dei dati.

- **Ulteriore documentazione**: i documenti relativi alle prime fasi del progetto, come ad esempio l'avamprogetto, i risultati della consultazione o i rapporti degli esperti, si trovano sul sito dell'UFG sotto «Rafforzamento della protezione dei dati».

1.2 Adeguamento di ordinanze ed entrata in vigore del nuovo diritto in materia di protezione dei dati

- A causa della revisione totale della LPD dovranno essere adeguate l'ordinanza relativa alla legge federale sulla protezione dei dati (**OLPD**; in futuro: ordinanza sulla protezione dei dati, **OPDa**) e l'ordinanza sulle certificazioni in materia di protezione dei dati (**OCPD**). Inoltre, nell'allegato dell'OPDa vanno modificate numerose disposizioni a protezione dei dati previste in leggi speciali. Le **modifiche di altre ordinanze** si limitano ad adeguamenti che derivano direttamente dalla nLPD o dalle revisioni dell'OPDa o dell'OCPD (p. es. l'abrogazione dei «profili della personalità» [► n. 2.2.1 lett. b)] o l'adeguamento del concetto di «raccolta di dati» [► n. 4.4.2]).

- **Principali contenuti della revisione dell'OLPD**: requisiti minimi per la sicurezza dei dati; svolgimento del compito; comunicazione di dati personali all'estero (incluso l'elenco degli Stati con un livello di protezione adeguato); modalità di vari obblighi dei titolari del trattamento dei dati (segnatamente l'obbligo di informare, la valutazione d'impatto sulla protezione dei dati e la notifica di violazioni della sicurezza dei dati); modalità del diritto di accesso e del diritto di farsi consegnare e trasmettere dati (portabilità dei dati); nomina, compiti e posizione dei consulenti per la protezione dei dati; notifica all'IFPDT dei progetti degli organi federali che prevedono il trattamento automatizzato di dati personali; obblighi d'informare; progetti pilota; organizzazione e compiti dell'IFPDT.

- **Entrata in vigore del nuovo diritto in materia di protezione dei dati**: secondo l'articolo 74 capoverso 2 nLPD, il Consiglio federale determina l'entrata in vigore della revisione totale della LPD (e delle ordinanze riviste). Il nuovo diritto entrerà in vigore il 1° settembre 2023.

2 Requisiti delle basi legali per il trattamento di dati personali da parte di organi federali secondo la nuova LPD

2.1 Cosa *non cambia* con la revisione totale della LPD

- **Principi del diritto in materia di protezione dei dati**: nel trattamento di dati di persone fisiche (= dati personali; per i dati delle persone giuridiche cfr. ► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**) da parte di organi federali devono essere considerati i principi generali del diritto in materia di protezione dei dati stabiliti dagli articoli 6–8 nLPD. I principi cardine della legalità (art. 6 cpv. 1 nLPD), della proporzionalità (incluso quello dell'economicità dei dati) e della buona fede (art. 6 cpv. 2 e 4 nLPD), dello scopo vincolante[3] e della riconoscibilità di tale scopo[4] (art. 6 cpv. 3 nLPD), dell'esattezza dei dati (art. 6 cpv. 5 nLPD)[5] nonché della sicurezza dei dati (art. 8 nLPD) corrispondono essenzialmente al diritto attualmente in vigore. L'articolo 7 nLPD menziona ora anche i principi della protezione dei dati sin dalla progettazione e per impostazione predefinita («*privacy by design and by default*»). Il primo esige che fin dalla progettazione il trattamento dei dati sia predisposto, sotto il profilo organizzativo e tecnico, in modo da rispettare le prescrizioni in materia di protezione dei dati (art. 7 cpv. 1 nLPD). Il secondo richiede invece appropriate impostazioni predefinite che circoscrivano il trattamento dei dati al minimo indispensabile per le finalità perseguite, sempreché la persona interessata non disponga altrimenti (art. 7 cpv. 3 nLPD). Questi due principi si evincono in parte già dagli attuali principi delle proporzionalità e della sicurezza dei dati. Per quanto concerne, invece, la comunicazione di dati all'estero vanno poi osservati gli articoli 16 e 17 nLPD (► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

- **Principio dell'autorizzazione speciale**: fatte salve alcune deroghe, la nLPD non conferisce agli organi federali carta bianca per trattare dati, bensì esige basi legali settoriali specifiche a tal fine. Quando gli organi federali trattano dati personali, occorre pertanto creare le basi legali negli atti materiali pertinenti. La nLPD stabilisce diversi requisiti per queste basi legali.

- **Requisito della base legale**: gli organi federali possono trattare dati personali soltanto se sussiste una pertinente base legale (art. 34 cpv. 1 nLPD). Questo vale per tutte le forme e fasi del *trattamento dei dati* (art. 5 lett. d nLPD) come, ad esempio, la raccolta, l'utilizzazione, la conservazione e la cancellazione dei dati («*lifecycle*» dei dati personali). La *comunicazione dei dati* (art. lett. e nLPD), che costituisce una forma particolarmente sensibile del trattamento di dati, è disciplinata nell'articolo 36 nLPD. Per la comunicazione dei dati gli organi federali necessitano di una base legale autonoma (vale a dire che non è sufficiente

[3] Nell'art. 6 cpv. 3 nLPD il principio dello scopo determinato del trattamento è formulato in modo leggermente diverso dal passato (art. 4 cpv. 3 LPD). In particolare si stabilisce espressamente che i dati possono essere trattati soltanto **in modo compatibile** con lo scopo per cui sono stati inizialmente raccolti. Secondo il messaggio del Consiglio federale del 15 settembre 2017 (► FF **2017** 5939, 6016), questa nuova formulazione non implica cambiamenti notevoli: come nel diritto vigente, un ulteriore trattamento non è ammissibile se la persona interessata può legittimamente considerarlo inatteso, inappropriato o contestabile. Una modifica dello scopo iniziale del trattamento dei dati da parte degli organi federali deve quindi essenzialmente essere prevista per legge. Il principio dello scopo determinato va rispettato anche nei progetti dall'Amministrazione federale che prevedono un uso molteplice dei dati (principio «*once-only*»).

[4] Sebbene il principio della riconoscibilità dello scopo di cui all'art. 6 cpv. 3 nLPD si discosti leggermente dalla formulazione del diritto in vigore (art. 4 cpv. 4 LPD), secondo il messaggio del Consiglio federale del 15 settembre 2017 (► FF **2017** 5939, 6016) – e contrariamente a quanto affermato da certi esponenti della dottrina (segnatamente DAVID ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter del 16 novembre 2020, n. marg. 35) –, questo non comporterà modifiche materiali.

[5] Secondo l'art. 6 cpv. 5 *primo e secondo periodo* nLPD, chi tratta dati personali deve accertarsi della loro esattezza e prendere tutte le misure adeguate per rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto allo scopo per il quale sono stati raccolti o trattati. Questo corrisponde all'attuale art. 5 cpv. 1 LPD. Nell'art. 6 cpv. 5 *terzo periodo* nLPD il Parlamento ha precisato che l'adeguatezza delle misure dipende segnatamente dal tipo e dall'entità del trattamento dei dati come pure dai rischi derivanti dal trattamento per la personalità o i diritti fondamentali della persona interessata. Con questa integrazione la dottrina e la prassi (soprattutto quella del Tribunale amministrativo federale) in materia di correttezza dei dati vengono trasposte esplicitamente nella legge. Non si intende però apportare alcuna modifica materiale.

una competenza generale a trattare dati). I requisiti di questa base legale sono però perlopiù uguali a quelli previsti per altre forme di trattamento dei dati (l'art. 36 cpv. 1 nLPD rinvia all'art. 34 cpv. 1–3 nLPD).

- **Requisiti relativi al livello normativo**: essenzialmente, più è grave l'ingerenza nel diritto all'autodeterminazione informativa (art. 13 cpv. 2 della Costituzione federale [Cost.; RS 101])[6], più è richiesta una base legale sotto forma di legge in senso formale per il trattamento dei dati. Come in passato, il legislatore stesso indica i casi in cui è necessaria un'autorizzazione legale (art. 34 cpv.2 e 36 cpv. 1 nLPD). In questo contesto vi sono alcune modifiche da considerare rispetto al diritto attualmente in vigore (► n. 2.2.1).

- **Requisiti relativi alla densità normativa**: la base legale per il trattamento dei dati deve essere sufficientemente determinata. Né l'attuale LPD né la nLPD prevedono regole particolari in merito. I requisiti relativi alla densità normativa si orientano pertanto ai principi generali della legalità e del potenziale di rischio del trattamento dei dati. Quanto più è grave l'ingerenza nel diritto all'autodeterminazione informativa, tanto più dettagliata deve essere la base legale. Determinanti sono soprattutto i seguenti criteri: il tipo di dati, il tipo di trattamento dei dati, lo scopo del trattamento, il numero e la cerchia degli interessati, l'eventuale coinvolgimento di altri servizi nel trattamento dei dati (organi federali, organi cantonali o servizi privati) o l'impiego di nuove tecnologie.

  Come regola generale vale: la base legale deve rendere trasparente il trattamento dei dati da parte degli organi federali. Nei casi previsti dall'articolo 34 capoverso 2 nLPD (in combinato disposto con l'art. 36 cpv. 1 nLPD), la legge in senso formale deve consentire agli interessati di riconoscere essenzialmente *chi* (► n. 4.1) tratta *quali dati per quale scopo*, incluso *a chi* li comunica per *quale scopo* e *in che modo* avviene il trattamento. Per quanto riguarda il tipo di trattamento dei dati si tratta, ad esempio, di metodi di trattamento come il collegamento e il confronto dei dati (inclusa la profilazione; v. ► n. 2.2.1 lett. b)), l'impiego di nuove tecnologie (p. es. procedure biometriche o intelligenza artificiale; v. ► n. 2.2.1 lett. c)/cc) nonché, in caso di ingerenza grave nei diritti fondamentali, la durata di conservazione dei dati. Per quanto riguarda le modalità di comunicazione dei dati si rimanda al ► n. 2.2.2.

  Negli ultimi anni è spesso sorto l'interrogativo se e, in caso affermativo, quanto dettagliatamente le basi legali debbano descrivere l'*architettura di un sistema* con cui vengono trattati dati personali. Questo riguarda in particolare le unità amministrative che non impiegano sistemi informatici «monolitici», bensì architetture più moderne come microservizi, in cui i dati trattati non possono più essere attribuiti a «compartimenti» separati. Ai fini della regolamentazione legale conta meno l'architettura informatica (tecnica) quanto più l'«architettura di trattamento dei dati» (segnatamente gli scopi e la logica del trattamento nonché i flussi di dati e gli accessi). L'importante è che, anche in caso di scomparsa delle tradizionali strutture di sistema, sia sempre possibile riconoscere quali dati sono trattati da chi per quali compiti o scopi. Il «riferimento al compito» alla base del trattamento dei dati deve quindi essere garantito anche nel caso di un'architettura orizzontale.

[6] Il diritto fondamentale all'autodeterminazione informativa secondo l'art. 13 cpv. 2 Cost. in sostanza garantisce che, a prescindere da quanto sensibili effettivamente siano le informazioni in questione, ogni persona debba poter decidere se e per quale finalità le informazioni che la riguardano possano essere trattate da terzi di natura statale o privata (DTF **146** I 11 consid. 3.1.1).

Riassumendo, i requisiti di densità normativa non sono di norma soddisfatti se una disposizione si limita all'indicazione sommaria che il trattamento dei dati è inteso a consentire all'organo federale competente di adempiere ai suoi compiti legali[7]. Valgono tuttavia requisiti meno severi nei casi in cui i compiti di un organo federale siano già descritti in modo preciso e l'organo non effettui trattamenti di dati delicati o complessi.

- **Deroghe al requisito della base legale**: poiché è praticamente impossibile creare le disposizioni necessarie per tutte le costellazioni, come in passato sono previste deroghe al requisito della base legale per il trattamento dei dati (art. 34 cpv. 4[8] e 36 cpv. 2[9] nLPD). In queste situazioni (elencate in modo esaustivo) e in singoli casi, è ammissibile trattare i dati *senza una base legale*, a prescindere che si tratti di un trattamento «ordinario» secondo l'articolo 34 capoverso 1 nLPD o di uno particolarmente delicato secondo l'articolo 34 capoverso 2 nLPD. Le fattispecie eccezionali previste dalla nLPD corrispondono perlopiù al diritto vigente. Per le novità si rimanda al messaggio del Consiglio federale del 15 settembre 2017 (► FF **2017** 5939, 6067 seg.). Anche se nel testo di legge – diversamente da oggi (cfr. art. 17 cpv. 2 LPD) – non compare più l'espressione «eccezionalmente», questo non comporta modifiche materiali. Come in passato, un trattamento dei dati di una certa regolarità e durata deve fondarsi su una base legale.

- **«Casi speciali»**: come finora, la nLPD prevede diverse disposizioni speciali che allentano i requisiti della base legale (nel caso di progetti pilota secondo l'art. 35 nLPD e del trattamento per scopi impersonali come la ricerca, la pianificazione o la statistica secondo l'art. 39 nLPD) o che autorizzano direttamente gli organi federali a comunicare dati (comunicazione agevolata dei dati di base secondo l'art. 36 cpv. 4 nLPD). Un'ulteriore regola speciale riguarda la comunicazione dei dati personali nell'ambito dell'informazione ufficiale del pubblico (art. 36 cpv. 3 e 5 nLPD). Queste disposizioni speciali della nLPD corrispondono perlopiù al diritto vigente. Per le novità si rimanda al messaggio del Consiglio federale del 15 settembre 2017 (► FF **2017** 5939, 6067 seg.).

- **Rapporto LPD – leggi speciali**: considerata la parità di rango delle norme dello stesso livello normativo, non è escluso che un'altra disposizione di una legge formale prevalga, in quanto legge speciale, sulla LPD[10]. Nelle basi legali settoriali il legislatore può pertanto derogare a determinati principi della nLPD se i valori tutelati da un'altra legge lo esigono. Vanno comunque rispettati i limiti imposti dalla Costituzione e dal diritto internazionale:

  – la nLPD attua diversi principi di protezione del *diritto fondamentale all'autodeterminazione informativa secondo l'articolo 13 capoverso 2 Cost. e l'articolo 8 CEDU* (p. es. il

[7] Per quanto concerne i requisiti del Tribunale federale in merito alla densità normativa cfr. due esempi che riguardano il trattamento dei dati da parte della polizia nei Cantoni di Turgovia (DTF **146** I 11) e Zurigo (DTF **136** I 87).

[8] Secondo l'art. 34 cpv. 4 nLPD, gli organi federali possono trattare dati personali senza base legale se: (a) il Consiglio federale ha autorizzato il trattamento poiché non ritiene pregiudicati i diritti delle persone interessate; (b) la persona interessata ha dato, nel caso specifico dell'art. 6 cpv. 6 e 7 nLPD, il suo consenso al trattamento oppure ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento; o *(nuovo)* (c) il trattamento è necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole. *A differenza* dell'attuale art. 17 cpv. 2 lett. a LPD non è più prevista una deroga al requisito della base legale quando il trattamento dei dati è indispensabile per l'adempimento di un compito chiaramente definito in una legge in senso formale. In questo caso valgono comunque requisiti più severi per la densità normativa (v. art. 34 cpv. 3 nLPD; ► n. 2.2.1 lett. a)/cc e b)/ee).

[9] Secondo l'art. 36 cpv. 2 nLPD, gli organi federali possono, nel caso specifico, comunicare dati personali senza base legale se: (a) la comunicazione è indispensabile all'adempimento dei compiti legali *(nuovo)* del titolare del trattamento o del destinatario; (b) la persona interessata ha dato il suo consenso alla comunicazione secondo l'art. 6 cpv. 6 e 7 nLPD; (c) la comunicazione è necessaria per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole *(nuovo)*; (d) la persona interessata ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente alla comunicazione; o (e) il destinatario rende verosimile che la persona interessata rifiuta di dare il proprio consenso, oppure si oppone alla comunicazione, al solo scopo di impedirgli l'attuazione di pretese giuridiche o la difesa di altri interessi degni di protezione; la persona interessata deve previamente essere invitata a pronunciarsi, salvo che ciò sia impossibile o richieda un onere sproporzionato.

[10] Cfr. p. es. DTF **142** II 268 consid. 6.3 nonché la sentenza del Tribunale amministrativo federale B-6547/2014 del 25 aprile 2017, consid. 5.2.

diritto d'accesso, di rettifica e di cancellazione dei dati). Per limitare tali garanzie concretizzate dalla legislazione in materia di protezione dei dati si applicano le prescrizioni dell'articolo 36 Cost.

Secondo la giurisprudenza del Tribunale federale, il **diritto fondamentale all'autodeterminazione informativa** in sostanza garantisce che, a prescindere da quanto sensibili effettivamente siano le informazioni in questione, ogni persona debba poter decidere se e per quale finalità le informazioni che la riguardano possano essere trattate da terzi di natura statale o privata[11]. La dottrina e la giurisprudenza fanno derivare da questa decisione diverse pretese specifiche, tra cui il diritto di consultare i propri dati, il diritto di far rettificare dati personali errati e il diritto di far cancellare dati personali trattati illecitamente[12].

- Va inoltre tenuto presente che la nLPD riprende disposizioni del diritto internazionale ed europeo vincolanti per la Svizzera: ad esempio, la *Convenzione sulla protezione dei dati 108+* del Consiglio d'Europa e la *direttiva (UE) 2016/680* sulla protezione dei dati in materia penale, rilevante per Schengen, pongono limiti alle deroghe che le leggi speciali possono prevedere alla nLPD.

- Al di fuori del campo d'applicazione della direttiva (UE) 2016/680 sulla protezione dei dati in materia penale, l'UE considera la Svizzera come uno Stato terzo. Nel 2000 la Commissione europea ha attestato che la Svizzera dispone di un livello adeguato di protezione dei dati. Questa *decisione di adeguatezza* fa sì che gli Stati membri dell'UE possano comunicare alla Svizzera dati personali senza ulteriori ostacoli. Attualmente la Commissione europea sta verificando la decisione di adeguatezza della Svizzera. Sono previste verifiche periodiche del diritto svizzero in materia di protezione dei dati anche in futuro. La Svizzera può mantenere la decisione di adeguatezza solo se garantisce un livello di protezione dei dati *adeguato* al regolamento generale (UE) 2016/679 sulla protezione dei dati. In questo contesto la Commissione europea valuta non solo la protezione dei dati generale, ma anche quella settoriale. In particolare si concentra sugli accessi ai dati da parte delle autorità nei settori della sicurezza nazionale e del diritto penale[13]. Va pertanto garantito un adeguato livello di protezione dei dati anche negli atti normativi settoriali. Una revoca (parziale o totale) della decisione di adeguatezza pregiudicherebbe notevolmente il traffico transfrontaliero di dati. Cfr. in merito l'articolo 45 e seguenti del regolamento generale (UE) 2016/679 sulla protezione dei dati.

Conclusione: le leggi speciali possono derogare alla nLPD (in quanto «standard minimo» del diritto in materia di protezione dei dati) solo per motivi validi e le deroghe vanno debitamente motivate.

---

[11] A titolo esemplificativo DTF **146** I 11 consid. 3.1.1. Cfr. in merito anche PASCAL MAHON, Le droit à l'intégrité numérique: réelle innovation ou simple évolution du droit? Le point de vue du droit constitutionnel, in: Le droit à l'intégrité numérique, 2021, pag. 44–63 (soprattutto pag. 47 seg.).

[12] Cfr. in merito ALEXANDRE FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP 2013 pag. 837 segg. (soprattutto pag. 852) con ulteriori rimandi. FLÜCKIGER fa derivare dal diritto fondamentale all'autodeterminazione informativa ulteriori pretese di diritto costituzionale, segnatamente «*le droit de spécifier le but de l'utilisation des données récoltées, le droit de s'opposer à leur traitement, le droit à la transparence de la collecte (caractère reconnaissable de celle-ci et devoir d'information), le droit de ne pas exporter ses données vers des pays moins protecteurs, le droit à la sécurité des données (protection en cas d'atteinte à l'intégrité des données suite à un traitement illicite ou contraire à sa volonté ainsi qu'en cas de brèche de sécurité [vol ou perte des données], comprenant en plus le droit d'être avisé en pareil cas), le droit à l'anonymat, en particulier celui d'aller et venir anonymement, le droit à l'oubli, le droit d'exiger un cadre et des moyens techniques permettant à chacun d'exercer effectivement des choix éclairés: architecture informatique conçue pour améliorer le pouvoir de contrôle (privacy enhancing technologies), protection intégrée de la vie privée (privacy by design), dépôts de données personnelles (personal data store), de même que le droit de disposer librement de ses données à sa mort (droit successoral numérique)*».

[13] Cfr. in merito il documento del 28 novembre 2017 e 6 febbraio 2018 «Criteri di riferimento per l'adeguatezza» pubblicato dall'ex Gruppo di lavoro articolo 29 (scaricabile in italiano all'indirizzo: ARTICLE29 - Working document on Adequacy Referential (wp254rev.01) (europa.eu)).

2.2 Cosa *cambia* con la revisione totale della LPD

2.2.1 Requisiti di livello normativo (occorre una legge in senso formale)

L'articolo 34 capoversi 2 e 3 nLPD impone diverse condizioni riguardo al livello normativo affinché gli organi federali possano effettuare trattamenti di dati comportanti rischi particolarmente elevati. Le stesse condizioni si applicano anche alla comunicazione dei dati (art. 36 cpv. 1 nLPD).

a) Trattamento di dati personali degni di particolare protezione (art. 34 cpv. 2 lett. a nLPD)

aa) Come in passato: principio della base legale in una legge in senso formale

Secondo l'articolo 34 capoverso 2 lettera a nLPD, per il trattamento di dati personali degni di particolare protezione è essenzialmente necessaria un'autorizzazione contenuta in una legge in senso formale. Per garantire la trasparenza nei confronti degli interessati, nella disposizione di legge vanno menzionate le *categorie* dei dati degni di particolare protezione trattati *secondo l'articolo 5 lettera c numeri 1–6 nLPD*. Il principio della proporzionalità impone che l'autorizzazione comprenda solo alle categorie necessarie affinché l'organo federale possa adempiere i suoi compiti. Laddove possibile e necessario, vanno create delle sottocategorie (es.: non possono essere trattati tutti, ma solo determinati dati sanitari, come i dati sulle patologie cancerogene). Queste norme corrispondono al diritto vigente. Vanno però considerate due novità:

- viene ampliato l'elenco dei dati personali degni di particolare protezione previsto dall'articolo 5 lettera c nLPD (► di seguito lett. bb);
- a determinate condizioni, è ammesso disciplinare il trattamento di dati personali degni di particolare protezione prevalentemente in un'ordinanza (► di seguito lett. cc).

bb) Nuovo: più dati personali degni di particolare protezione

Il concetto di dati personali degni di particolare protezione è definito in modo esaustivo nell'articolo 5 lettera c nLPD. Come *finora*, si tratta di dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali (n. 1), dati concernenti la salute, la sfera intima o l'appartenenza a una razza o a un'etnia (n. 2), dati concernenti perseguimenti e sanzioni amministrativi e penali (n. 5) e dati concernenti le misure d'assistenza sociale (n. 6). *Ora* si aggiungono le seguenti categorie:

- **dati concernenti l'appartenenza a un'etnia** (art. 5 lett. c n. 2 nDSG): sulla base della giurisprudenza del Tribunale federale in merito all'art. 261bis CP, un'etnia è un segmento della popolazione che si ritiene un gruppo distinto e viene visto come tale anche dal resto della popolazione. Deve avere una storia comune e un sistema comune di idee e norme comportamentali (tradizioni, usi, costumi, lingua ecc.) e usare tali caratteristiche per distinguersi[14];

  Esempi: albanesi kosovari, arabi, palestinesi o zingari[15].

- **dati genetici** (art. 5 lett. c n. 3 nLPD): secondo il messaggio del 15 settembre 2017 del Consiglio federale, si tratta di «informazioni sul patrimonio genetico di una persona ottenute

[14] DTF **143** IV 193 consid. 2.3.

[15] FABIENNE ZANNOL, L'applicazione della norma penale contro la discriminazione razziale (studio commissionato dalla CFR), Berna 2007.

attraverso un esame genetico» (► FF **2017** 5939, 6012)[16]. Questa definizione corrisponde all'articolo 3 lettera l della legge federale sugli esami genetici sull'essere umano;

Esempio: profilo del DNA.

- **dati biometrici che identificano in modo univoco una persona fisica** (art. 5 lett. c n. 4 nLPD): informazioni relative a *caratteristiche fisiche, fisiologiche o comportamentali* di una persona fisica, ottenuti grazie a un *processo tecnico specifico* e che permettono di *identificare univocamente* una persona o di confermarne l'identificazione (► FF **2017** 5939, 6012). A differenza dei dati genetici, nel caso dei dati biometrici il processo tecnico che permette l'*identificazione univoca* dell'interessato è un elemento essenziale per qualificarli come dati degni di particolare protezione. Senza questa limitazione, anche semplici fotografie o registrazioni audio risulterebbero degne di particolare protezione.

  Esempi: immagini del viso elaborate con un software per il riconoscimento facciale, scansione delle impronte digitali, dell'iride e della retina.

I concetti di «dati genetici» e «dati biometrici che identificano in modo univoco una persona fisica» sono molto ampi, per cui nella legge in senso formale va precisato *quali* dati genetici o biometrici sono trattati. Eventuali norme di delega vanno usate con parsimonia.

Cfr. come esempio di norma di delega l'articolo 2*b* capoverso 4 del disegno del 4 dicembre 2020 della legge sui profili del DNA[17] concernente la fenotipizzazione: «Il Consiglio federale può definire caratteristiche fisiche visibili supplementari in funzione del progresso tecnico e se l'affidabilità pratica dei nuovi metodi volti a evincere tali caratteristiche è assicurata».

Ampliando l'elenco dei dati degni di particolare protezione, la legge riveduta attua i requisiti dell'articolo 6 paragrafo 1 della Convenzione sulla protezione dei dati 108+ del Consiglio d'Europa e degli articoli 3 numeri 12 e 13 e 10 della direttiva (UE) 2016/680 sulla protezione dei dati in materia penale, rilevante per Schengen. Inoltre allinea il diritto svizzero in materia al regolamento generale (UE) 2016/679 sulla protezione dei dati (art. 4 n. 13 e 14 e art. 9). Queste disposizioni europee vanno quindi considerate nell'interpretare l'articolo 5 lettera c nLPD.

cc) Nuovo: allentamento dei requisiti relativi al livello normativo a determinate condizioni

L'articolo 34 capoverso 3 nLPD prevede [18] che, per trattare dati personali degni di particolare protezione, è sufficiente una base legale figurante in una legge in senso materiale se sono adempiute (cumulativamente) due condizioni:

- **il trattamento è indispensabile per adempire un compito stabilito in una legge in senso formale**: si presuppone che il compito per cui vengono trattati i dati personali sia previsto espressamente in una legge formale e che la sua portata sia chiaramente riconoscibile. Solo così è garantita la necessaria trasparenza per l'interessato. Non è sufficiente che il compito possa essere desunto implicitamente. Inoltre il trattamento dei dati deve es-

[16] La richiesta di limitare il concetto di dati genetici nell'art. 15 lett. c n. 3 nLPD per considerarli degni di particolare protezione soltanto quando «identificano univocamente una persona fisica», come chiesto dal Consiglio nazionale, è stata rigettata dal Consiglio degli Stati (= versione del Consiglio federale). Nell'appianamento delle differenze si è imposto il Consiglio degli Stati. Per evitare eventuali malintesi, il capo del DFGP ha spiegato al Consiglio nazionale che l'art. 5 lett. c n. 3 non comprende tutti i dati genetici, ma solo i dati genetici *personali* (= dati che si riferiscono a una persona determinata o determinabile; art. 5 lett. a nLPD). Ciò significa che i dati genetici sono da considerarsi dati personali degni di particolare protezione soltanto quando contengono informazioni che permettono di identificare un interessato con un onere proporzionato. Se questo non è il caso (p. es. nel caso di dati anonimizzati), i dati genetici non rientrano nel campo di applicazione della nLPD (cfr. Boll. Uff. **2019** N 1787).

[17] FF **2021** 45

[18] Secondo l'attuale art. 17 cpv. 2 lett. a LPD, i dati personali degni di particolare protezione possono essere trattati senza base legale se, eccezionalmente, ciò è indispensabile per l'adempimento di un compito chiaramente definito in una legge in senso formale. Tuttavia, un trattamento dei dati si può basare su questa disposizione derogatoria solo nel caso specifico (v. CLAUDIA MUND, Stämpflis Handkommentar zum Datenschutzgesetz, Berna 2015 [«SHK DSG»], art. 17 LPD n. 16).

sere indispensabile per adempire il compito, vale a dire che sarebbe praticamente impossibile portarlo a termine senza trattare i dati in questione. Per contro, il semplice migliorare o rendere più efficiente l'adempimento del compito non è sufficiente[19];

- **lo scopo del trattamento non comporta rischi particolari per i diritti fondamentali della persona interessata**: si pensi qui in particolare alla protezione della sfera privata secondo l'articolo 13 Cost. Contrariamente al tenore (troppo) restrittivo della disposizione, secondo la dottrina prevalente e la giurisprudenza del Tribunale federale, l'articolo 13 capoverso 2 Cost. non solo protegge dall'uso illecito dei dati personali, ma conferisce anche un diritto generale all'autodeterminazione informativa. Significa che essenzialmente ogni persona deve poter decidere autonomamente se e per quale scopo vengono trattate informazioni che la riguardano (► cfr. n. 2.1)[20]. Inoltre, la personalità beneficia di una tutela costituzionale di base, concretizzata nel diritto alla libertà personale di cui all'articolo 10 capoverso 2 Cost. (soprattutto la protezione delle manifestazioni elementari dell'espressione della personalità). Vanno però considerati anche altri diritti fondamentali come, ad esempio, la libertà economica (art. 27 Cost.). Per le costellazioni in cui lo scopo del trattamento comporta un'ingerenza grave nei diritti fondamentali dell'interessato, si rimanda a ► n. 2.2.1 lett. c)/lett. bb. Va inoltre considerato che non solo lo scopo ma anche il tipo di trattamento può mettere a rischio i diritti fondamentali dell'interessato; cfr. in merito l'articolo 34 capoverso 2 lettera c nLPD e il ► n. 2.2.1 lett. c)/cc.

b) Profilazione (art. 34 cpv. 2 lett. b nLPD)

aa) Situazione di partenza: dal profilo della personalità alla profilazione

Il progresso tecnico ha portato a nuovi metodi di trattamento dei dati, tra cui la possibilità di salvare, collegare e analizzare grandi quantità di dati (parola chiave «*big data*»). In questo modo, da quantità enormi di dati, che di per sé sono probabilmente poco significativi, è possibile generare, grazie a procedure statistico-matematiche, nuove informazioni sulle persone. Nella revisione totale della LPD si tiene conto di questi sviluppi tra l'altro sostituendo il concetto di «profilo della personalità» (art. 3 lett. d LPD) con quello di «profilazione» (art. 5 lett. f e g nLPD). Sebbene, a una prima occhiata, i due concetti possano sembrare molto simili, non indicano la stessa cosa. Mentre un **profilo della personalità** è il *risultato di un processo di trattamento* (= combinazione di dati da cui emerge un quadro di aspetti [parziali] essenziali di una persona fisica), la **profilazione** descrive un *tipo ovvero un metodo di trattamento* (= valutazione automatizzata di determinati aspetti di una persona fisica).

Come avviene oggi per il trattamento dei profili della personalità, la nLPD prevede effetti giuridici qualificati anche per la profilazione (nel caso di trattamenti di dati da parte di privati: per la profilazione a rischio elevato). Pertanto, di massima, è obbligatoria una legge in senso formale che autorizzi la profilazione da parte degli organi federali s (► v. lett. dd di seguito). La profilazione può comportare rischi particolari per i diritti fondamentali degli interessati: le procedure sono spesso poco trasparenti, soprattutto quando la profilazione si basa sull'uso di algoritmi. Le persone non sanno secondo quale logica sono trattati i loro dati e quali conseguenze può avere per loro un tale trattamento. La profilazione consente di analizzare persone, classificarle e giudicarle, rischiando non solo di consolidare cliché già esistenti, ma anche di giungere a false previsioni e di compiere discriminazioni.

bb) Concetto di «profilazione» (art. 5 lett. f nLPD)

[19] Cfr. in merito anche la sentenza del Tribunale federale DTF **147** II 227, secondo cui «indispensabile» significa che un compito legale può essere adempiuto solo grazie ai dati in questione e questi costituiscono quindi l'unica possibilità di adempiere il compito (consid. 5.4).

[20] DTF **140** I 2 consid. 9.1.

Nella definizione legale di «profilazione» il Parlamento si è discostato dal disegno del Consiglio federale ispirandosi al **tenore delle disposizioni in materia di protezione dei dati dell'UE** (art. 3 n. 4 della direttiva [UE] 2016/680 sulla protezione dei dati in materia penale e art. 4 n. 4 del regolamento generale [UE] 2016/679 sulla protezione dei dati)[21]. Originariamente il Consiglio federale aveva scelto una propria definizione di profilazione, sebbene non volesse creare alcuna differenza materiale rispetto al diritto europeo (► FF **2017** 5939, 6013 seg.). Questa genesi dimostra che le norme europee giocano un ruolo importante nell'interpretare il concetto di profilazione.

Secondo l'articolo 5 lettera f nLPD, per **profilazione** si intende qualsiasi «trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona». In dettaglio:

- il **trattamento dei dati**, soprattutto il processo di valutazione[22] è **automatizzato**. Diversamente dalla decisione individuale automatizzata (► cfr. in merito il n. 2.2.1 lett. c)/cc), nella profilazione il trattamento dei dati *non* deve essere *completamente automatizzato*. L'intervento di un umano non esclude un'attività dalla definizione di profilazione se i dati sono trattati *essenzialmente in modo automatizzato*[23];

- lo **scopo del trattamento dei dati** consiste nel **valutare** determinati aspetti personali di una persona fisica. La valutazione può consistere nell'*analisi* di caratteristiche della personalità, ma può anche essere usata per *predire* determinati comportamenti o caratteristiche di una persona. La definizione legale nell'articolo 5 lettera f nLPD menziona alcuni esempi a titolo illustrativo (analisi o previsione del rendimento lavorativo, situazione economica, salute, preferenze, luogo di permanenza e spostamenti).

  Il concetto di «valutazione» mostra che la profilazione implica una specie di valutazione o giudizio su una persona. La profilazione permette di analizzare, ad esempio, determinate caratteristiche di una persona per capire se è idonea o meno a svolgere determinate attività. A tal fine la profilazione si basa sull'assunto che in futuro un individuo si comporterà in modo uguale o simile al passato o che una persona con un determinato profilo si comporta come altre persone con un profilo uguale o simile. Con la profilazione si fanno dunque affermazioni sulla probabilità, che non corrispondono però per forza alla realtà[24]. Nessuna profilazione è quindi una constatazione oggettiva dei fatti. D'altro canto, la semplice classificazione delle persone in base a caratteristiche conosciute come l'età, il sesso o l'altezza non implica necessariamente una profilazione. Dipende tutto dal motivo della classificazione. Un titolare del trattamento dei dati può, ad esempio, suddividere i propri clienti in base all'età o al sesso a fini statistici, in modo da ottenere una panoramica riassuntiva senza emettere previsioni o trarre conclusioni sulle singole persone. In questo caso il motivo della classificazione non consiste nel valutare caratteristiche individuali, per cui non

[21] Cfr. in merito l'intervento del relatore CIP-N MATTHIAS JAUSLIN nel Consiglio nazionale il 24 settembre 2019: Boll. Uff. **2019** N 1790.

[22] Cfr. in merito l'esempio fatto da SIMON ROTH, Das Profiling im neuen Datenschutzrecht, in: SWZ 2021 34–39, pag. 35: se un detective privato utilizza una fotocamera o videocamera per osservare una persona che afferma di avere problemi di salute rilevanti ai fini delle assicurazioni sociali, non si tratta di profilazione; infatti, per determinare se la persona osservata presenta o meno le infermità asserite si procede a un'analisi manuale delle immagini e non a una procedura automatizzata. La fotocamera o videocamera non rilascia alcuna affermazione automatizzata sullo stato di salute della persona interessata.

[23] V. in merito le «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679» dell'ex Gruppo di lavoro articolo 29 del 6 febbraio 2018, pag. 7. Queste linee guida sono state nel frattempo riprese dal Comitato europeo per la protezione dei dati (EDPB). Cfr. inoltre DAVID VASELLA, Profiling nach der DSGVO und dem E-DSG bei Banken, in: SUSAN EMMENEGGER (editore), Banken und Datenschutz, Basilea 2019, pag. 197. Nel messaggio del Consiglio federale del 15 settembre 2017 si afferma che sussiste una profilazione soltanto se il processo di valutazione è interamente automatico. Questa affermazione risulta troppo assoluta considerati l'adeguamento della definizione legale da parte del Parlamento (allineamento al diritto europeo in materia di protezione dei dati) e l'interpretazione del concetto di profilazione negli atti normativi europei.

[24] OLIVIER HEUBERGER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, tesi, Lucerna, 2020, n. marg. 59.

si tratta di una profilazione[25]. Nemmeno la semplice raccolta di dati di riferimento – come nome, data di nascita e sesso a fini identificativi – costituisce una profilazione, poiché non vengono valutate caratteristiche personali[26].

Esempi[27] (senza distinzione tra profilazione «ordinaria» o «a rischio elevato»; ► cfr. in merito la lett. cc di seguito)

- *Analisi della situazione economica o del merito creditizio:* il *credit scoring* è un metodo statistico per valutare il merito creditizio (solvibilità e affidabilità nei pagamenti) di una persona; prende ad esempio in considerazione informazioni riguardanti esecuzioni, attestati carenza beni, carte bancarie o di credito bloccate per morosità, domande di credito, procedure di pagamento e d'incasso o esperienze fatte nelle relazioni d'affari precedenti. Alla persona valutata è assegnata un punteggio, utilizzato ad esempio per decidere sulla concessione di un prestito o le modalità di pagamento (acquisto dietro fattura). Il *credit scoring* automatizzato (e non manuale) costituisce profilazione.
- *Analisi dello stato di salute*: se un tracker di attività si limita a contare i passi, in linea di massima non si ha ancora un'analisi dello stato di salute di una persona e quindi non si tratta di profilazione. Se però ai passi contati vanno ad aggiungersi altri dati, come ad esempio altezza, peso, sesso, comportamento alimentare, ritmo del sonno o dati GPS, è possibile trarre conclusioni sullo stato della salute. Una tale analisi (automatizzata) dello stato di salute costituisce profilazione.
- *Analisi delle preferenze*: si deve supporre una profilazione se gli interessati sono classificati in base ai loro schemi comportamentali (p. es. «fa molto sport», «punta sul lavoro», «è introverso/estroverso») grazie ai diversi metodi di monitoraggio degli utenti in Internet, come ad esempio cookies che indicano i siti visitati, ai like sulle piattaforme social media o alle app usate su uno smartphone. Tali profili vengono poi usati, tra le altre cose, per pubblicità personalizzate.
- *Analisi del comportamento:* nel settore pubblico potrebbe sussistere una profilazione qualora un'autorità di polizia valutasse dati personali in modo automatico per giudicare il grado di pericolosità di una persona.
- *Analisi del comportamento:* nel quadro della sua attività di vigilanza sui mercati finanziari, la FINMA riceve grandi quantità di dati, dai quali desume, mediante profilazione, un'eventuale condotta scorretta in materia di vigilanza. In particolare nell'ambito della vigilanza sul mercato (p. es. al fine di accertare un possibile insider trading o una manipolazione del mercato), la FINMA è confrontata con una gran quantità di dati relativi agli scambi commerciali e alle transazioni, che analizza e valuta in maniera automatizzata in relazione alle persone interessate (► cfr. in merito il messaggio del 15 settembre 2017, FF **2017** 5939, 6134 seg. in merito al nuovo art. 23 cpv. 3 LFINMA).

cc) Concetto di «profilazione a rischio elevato» (art. 5 lett. g nLPD)

Il concetto di «profilazione a rischio elevato» è stato introdotto durante i **dibattimenti parlamentari**. Secondo il Parlamento, il disegno del Consiglio federale era troppo restrittivo per quanto riguardava la profilazione, soprattutto per i titolari privati del trattamento dei dati. Il Consiglio federale aveva infatti classificato la profilazione come rischiosa di per sé, senza considerare che può comprendere anche attività innocue. Il Parlamento si è quindi espresso a favore di un approccio basato sul rischio, non prevedendo effetti giuridici qualificati per i titolari *privati* del trattamento nel caso di profilazioni in generale, bensì solo in caso di «profilazione a rischio elevato». Per gli *organi federali*, invece, la differenziazione tra i due tipi di profilazione ha una portata più limitata (► cfr. in merito la lett. dd di seguito).

---

[25] Cfr. in merito le «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679» dell'ex Gruppo di lavoro articolo 29 del 6 febbraio 2018, pag. 7; David ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter del 16 novembre 2020, n. marg. 24; David VASELLA, op. cit., pag. 193 seg.

[26] OLIVIER HEUBERGER, op. cit., n. marg. 147.

[27] I primi tre esempi sono tratti da OLIVIER HEUBERGER, op. cit., n. marg. 157 segg.

Il Consiglio nazionale e il Consiglio degli Stati sono riusciti a trovare un'intesa sulla **definizione legale di «profilazione a rischio elevato»** solo su proposta della conferenza di conciliazione[28]. Secondo l'articolo 5 lettera g nLPD, per profilazione a rischio elevato si intende una profilazione «che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica». Per chiarire:

- la definizione di rischio elevato nell'articolo 5 lettera g nLPD corrisponde all'**attuale concetto di «profilo della personalità»** di cui all'articolo 3 lettera d LPD. L'espressione «compilazione di dati», usata finora, è però sostituita con «collegamento di dati» per tenere meglio conto, dal punto di vista linguistico, delle nuove possibilità tecniche. In tal modo rimane determinante anche la giurisprudenza in materia di profilo della personalità (soprattutto la sentenza di principio del Tribunale amministrativo federale nella causa Moneyhouse[29]);

- in termini semplici, si è in presenza di una profilazione a rischio elevato ai sensi dell'articolo 5 lettera g nLPD quando la profilazione ha come **risultato** un profilo della personalità secondo la vigente LPD. Vengono quindi combinati il metodo del trattamento dei dati (profilazione) e il risultato del trattamento dei dati (profilo della personalità);

- questa definizione legale tiene conto del fatto che la profilazione permette di collegare una molteplicità di dati (anche non degni di particolare protezione) per formare un'**immagine della persona interessata**, implicante come tale un rischio elevato per i diritti della personalità e i diritti fondamentali. La persona interessata spesso non ha alcun influsso su questa immagine e non può controllarne né la correttezza né l'utilizzo. Pertanto viene limitata nella sua libertà di rappresentarsi come ritiene giusto. Se dati personali sono raccolti per un periodo di tempo prolungato, portano con più probabilità a un profilo della personalità ossia a una profilazione a rischio elevato rispetto a quelli che rappresentano una semplice istantanea[30].

Esempi

– Il GPS integrato consente in linea di massima di localizzare ogni smartphone con una precisione di pochi metri. È poi possibile analizzare in automatico questi *dati sugli spostamenti* traendo conclusioni in merito al detentore. Se l'analisi si limita a un periodo circoscritto e a un luogo determinato (p. es. breve sosta in una stazione ferroviaria), si ha di norma e regola soltanto una *profilazione «ordinaria»*. Se invece i dati sugli spostamenti sono analizzati per periodi prolungati e uno spazio geografico più ampio, è possibile dedurre informazioni in merito a svariati ambiti della vita di una persona, come ad esempio il luogo di lavoro, la situazione abitativa, le abitudini alimentari, le relazioni personali, eventuali visite mediche e le abitudini di consumo. Ne risulta un'immagine individuale che richiede particolare protezione. Si tratta verosimilmente di una profilazione a rischio elevato.

– Una profilazione per *verificare il merito creditizio* che non considera soltanto la situazione economica o la solvibilità di una persona, ma anche altri aspetti (come la situazione abitativa o personale) è da considerarsi *a rischio elevato*[31].

Nella prassi, una profilazione da parte degli organi federali può comportare ingerenze gravi nei diritti fondamentali delle persone interessate anche per altri motivi (ossia senza che ne risulti un profilo della personalità). Si pensi, ad esempio, alla profilazione vertente su minori e altre persone vulnerabili o a quella che potrebbe portare al rifiuto di una prestazione importante. Questi rischi vanno considerati nell'elaborare le basi legali secondo l'articolo 34 e seguenti nLPD o nel

[28] Sedute del Consiglio nazionale (Boll. Uff. **2020** N 1816 segg.) e del Consiglio degli Stati del 24 settembre 2020 (Boll. Uff. **2020** S 1024 segg.).

[29] Sentenza del 18 aprile 2017 del Tribunale amministrativo federale A-4232/2015 nella causa IFPDT contro Moneyhouse AG.

[30] V. SIMON ROTH, op. cit., pag. 36 con relativi rimandi.

[31] Per valutare questa situazione in base al diritto vigente ovvero per il concetto di profilo della personalità cfr. la sentenza del 18 aprile 2017 del Tribunale amministrativo federale A-4232/2015 nella causa IFPDT contro Moneyhouse AG.

valutare l'impatto sulla protezione dei dati secondo l'articolo 22 nLPD (► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**), tanto più che le pertinenti disposizioni non contemplano la presenza di una profilazione a rischio elevato secondo l'articolo 5 lettera g nLPD.

dd) Principio: base legale in una legge in senso formale

L'articolo 34 capoverso 2 lettera b nLPD stabilisce che, di norma, gli organi federali hanno il diritto di effettuare una profilazione solo se lo prevede una **base legale figurante in una legge in senso formale**. Questa disposizione sostituisce l'attuale articolo 17 capoverso 2 LPD, secondo cui gli organi federali possono trattare profili della personalità soltanto se una legge in senso formale lo prevede espressamente. Il requisito della legge formale non vale solo per la profilazione a rischio elevato, bensì anche per la profilazione «ordinaria». Una disposizione a livello di ordinanza può essere considerata solo alle condizioni di cui all'articolo 34 capoverso 3 nLPD (► lett. ee di seguito).

La base legale per la profilazione, figurante in una legge in senso formale, deve essere **sufficientemente determinata**, ossia deve prevedere espressamente la profilazione ai sensi dell'articolo 5 lettera f nLPD o descriverla in modo adeguato. Lo stesso vale per la profilazione a rischio elevato secondo l'articolo 5 lettera g nLPD. Il principio della proporzionalità impone che gli organi federali vengano autorizzati a effettuare una profilazione (anche a rischio elevato) soltanto se è necessario per espletare i loro compiti. Vanno sempre considerati anche altri metodi di trattamento di dati. Nell'esaminare la proporzionalità occorre, tra le altre cose, chiedersi se opzioni alternative ma con la stessa efficacia non tutelerebbero meglio la personalità degli interessati. Inoltre, la base legale deve menzionare perlomeno lo scopo della profilazione e le categorie di dati degni di particolare protezione secondo l'articolo 5 lettera c numeri 1–6 nLPD che confluiscono nella profilazione. Per di più, l'interessato deve poter riconoscere quali sono le sue caratteristiche personali analizzate nella profilazione. Vanno chiariti nel singolo caso gli ulteriori punti da definire eventualmente nella base legale (p. es. quali dati personali «ordinari» confluiscono nella profilazione). Vanno indicati i parametri della profilazione particolarmente determinanti per l'ingerenza nell'autodeterminazione informativa. Infine è importante che gli organi federali utilizzino procedure matematiche e statistiche adeguate e adottino provvedimenti tecnici e organizzativi per ridurre il rischio di errori e discriminazioni.

Da ultimo si pone la questione se creare basi legali speciali anche per gestire i **dati risultanti dalla profilazione**, non sempre degni di particolare protezione; si può trattare anche di dati personali «ordinari» (come p. es. l'informazione che una persona è considerata non meritevole di credito). La questione dovrebbe essere analizzata nei singoli progetti legislativi e giudicata tenendo conto del contesto.

ee) Allentamento dei requisiti relativi al livello normativo a determinate condizioni

Come per il trattamento di dati personali degni di particolare protezione, secondo l'articolo 34 capoverso 3 nLPD anche per la profilazione è sufficiente una base legale figurante in una legge in senso materiale quando sono soddisfatte (cumulativamente) due condizioni:

- la profilazione è **indispensabile per l'adempimento di un compito stabilito in una legge in senso formale**;
- lo **scopo della profilazione non comporta rischi particolari** per i diritti fondamentali della persona interessata.

Cfr. in merito le spiegazioni del ► n. 2.2.1 lett. a)/cc.

c) Grave ingerenza nei diritti fondamentali della persona interessata (art. 34 cpv. 2 lett. c nLPD)

aa) Requisito della base legale in una legge in senso formale

Il nuovo articolo 34 capoverso 2 lettera c nLPD esplicita quanto vale già in base all'articolo 36 capoverso 1 Cost.: a prescindere dal fatto che si trattino dati degni di particolare protezione o che si esegua una profilazione, occorre una base legale in una legge in senso formale, quando lo **scopo** (► lett. bb di seguito) o il **tipo di trattamento** (► lett. cc di seguito) può comportare una **grave ingerenza nei diritti fondamentali** della persona interessata (► per i diritti fondamentali rilevanti cfr. n. 2.2.1 lett. a)/cc). In questi casi non è possibile allentare i requisiti relativi al livello normativo secondo l'articolo 34 capoverso 3 nLPD. Oltre al grado di ingerenza nei diritti fondamentali dell'interessato vanno considerati anche altri criteri generali come il numero di destinatari, la rilevanza politica, l'accettazione da parte della popolazione, la discrepanza dalle regole in vigore o la dimensione temporale delle ripercussioni del trattamento dei dati.

bb) Grave ingerenza nei diritti fondamentali derivante dallo scopo del trattamento dei dati (primo caso di applicazione dell'art. 34 cpv. 2 lett. c nLPD)

Un'ingerenza grave nei diritti fondamentali dell'interessato può risultare dallo **scopo del trattamento dei dati**. Il messaggio del 15 settembre 2017 porta come esempio il caso in cui, in certi ambiti, gli organi federali trattano dati personali per giudicare la pericolosità di una persona, il suo potenziale per esercitare una funzione o l'idoneità ad adempiere un obbligo legale o il suo modo di vivere. A seconda delle finalità perseguite dall'organo federale e a prescindere dal tipo di dati trattati, tale trattamento può costituire una grave ingerenza nei diritti fondamentali della persona interessata, per cui deve essere previsto in una legge in senso formale (► FF **2017** 5929, 6066 seg.). Va tuttavia considerato che in questo esempio, che consiste nel giudicare determinate caratteristiche di una persona, potrebbe anche sussistere una profilazione ai sensi dell'articolo 5 lettera f nLPD se il trattamento presenta un elevato grado di automazione (► n. 2.2.1 lett. b)).

cc) Grave ingerenza nei diritti fondamentali derivante dal tipo di trattamento dei dati (secondo caso di applicazione dell'art. 34 cpv. 2 lett. c nLPD)

Una grave ingerenza nei diritti fondamentali della persona interessata può risultare anche dal **tipo di trattamento dei dati**, ad esempio nel caso in cui la forma di raccolta dei dati (soprattutto la raccolta segreta o la sorveglianza per mezzo di videocamera) raggiunge un grado di ingerenza tale da rendere necessaria una base legale in una legge in senso formale. Anche per le nuove tecnologie (p. es. procedure biometriche come il riconoscimento facciale) sono di norma necessarie chiare basi legali in una legge in senso formale[32].

Di seguito analizzeremo in particolare l'**impiego dell'intelligenza artificiale[33] nell'amministrazione**. L'amministrazione può usare l'intelligenza artificiale in diversi ambiti e con diversa intensità per espletare i propri compiti. Le possibilità spaziano dal semplice *supporto interno*

[32] Cfr. DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zurigo 2008 («Handkommentar DSG»), art. 17 LPD n. 26 segg.; CLAUDIA MUND, SHK DSG, art. 17 LPD n. 9.

[33] Non esiste ancora una definizione valida a livello generale del concetto di intelligenza artificiale. Per dettagli sulla terminologia e le modalità di funzionamento si rimanda a BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 10 (disponibile solo in tedesco). Nel rapporto «Défis de l'intelligence artificielle» (disponibile in francese e tedesco) del gruppo di lavoro interdipartimentale della Confederazione «Intelligenza artificiale» del 13 dicembre 2019, il concetto di intelligenza artificiale (IA) è definito non in astratto, bensì caratterizzato da diversi elementi strutturali. Secondo questa caratterizzazione, i sistemi IA sono in grado di (1) analizzare dati in una forma non possibile con altre tecnologie allo stato attuale in termini di complessità e volume, soprattutto quando gli algoritmi imparano autonomamente trovando nei dati caratteristiche statistiche rilevanti; (2) effettuare previsioni come base essenziale per decisioni (automatizzate); (3) riprodurre quindi capacità assimilabili a capacità cognitive e all'intelligenza umane; (4) agire in modo ampiamente autonomo su tale base.

senza ripercussioni esterne o con poche ripercussioni esterne (p. es. applicazioni che attribuiscono automaticamente incarichi ai collaboratori, traducono documenti o redigono verbali di colloqui) a *sistemi che supportano l'amministrazione nell'adottare decisioni* (automazione parziale) fino a *sistemi che adottano la decisione autonomamente* (automazione totale). Di seguito saranno approfondite le ultime due casistiche: la nLPD contiene diverse disposizioni riguardanti le decisioni individuali automatizzate (automazione totale; casistica 1), ma per il momento nella prassi riveste maggiore importanza l'intelligenza artificiale impiegata a sostegno del processo decisionale (automazione parziale; casistica 2). Presenta un potenziale particolare per l'intelligenza artificiale l'amministrazione di massa, in cui l'amministrazione è chiamata a decidere in un gran numero di casi simili (p. es. procedure fiscali o assicurative)[34].

Nota: un gruppo di lavoro interdipartimentale della Confederazione sotto la guida della SEFRI si è occupato dell'impiego dell'intelligenza artificiale. Da questi lavori sono risultate le linee guida «Intelligenza artificiale» per l'Amministrazione federale, approvate dal Consiglio federale il 25 novembre 2020[35]. Una discussione dettagliata delle sfide giuridiche ed etiche poste dall'intelligenza artificiale figura inoltre nello studio del 28 febbraio 2021 commissionato dal Cantone di Zurigo «*Einsatz Künstlicher Intelligenz in der Verwaltung*» (disponibile solo in tedesco). Da questo studio sono tratti anche gli esempi presentati qui di seguito sull'impiego dell'intelligenza artificiale nell'amministrazione (perlopiù cantonale).

Esempi[36]

- *Procedure fiscali*: attualmente diversi Cantoni stanno considerando l'impiego dell'intelligenza artificiale nelle procedure fiscali. Nella maggior parte dei Cantoni le dichiarazioni d'imposta presentate per via digitale sono trattate da programmi di tassazione automatici e quindi risultano automatizzate, in parte almeno. In futuro s'intende potenziare il supporto alle amministrazioni fiscali grazie all'intelligenza artificiale. A tal fine si sta incentivando soprattutto la tassazione totalmente automatica. L'intelligenza artificiale potrebbe però essere usata anche a sostegno del processo decisionale, ad esempio per segnalare elementi contenenti errori agli esperti competenti per la tassazione o confrontare in automatico la dichiarazione d'imposta e i giustificativi presentati.
- *Procedure delle assicurazioni sociali*: nel diritto svizzero delle assicurazioni sociali l'uso di tecnologie dell'intelligenza artificiale non è ancora molto diffuso. Soprattutto il Cantone di Ginevra desidera impiegare l'intelligenza artificiale nella lotta alle frodi a danno delle assicurazioni sociali per individuare, tra l'altro, le prestazioni sociali percepite in modo ingiustificato (p. es. sviluppando algoritmi per sistemi di allerta e allarme, per effettuare controlli di coerenza e analisi incrociate delle oscillazioni di reddito e patrimonio).
- *«Predictive policing» riferito a luoghi*: le polizie cantonali di Argovia e Basilea Campagna e la polizia comunale di Zurigo impiegano il software tedesco PRECOBS per combattere i furti con scasso negli appartamenti e ne stanno valutando l'applicazione per altri tipi di reati. PRECOBS si basa sulla teoria che i furti (professionali) spesso avvengono in serie e si concentrano in precisi punti geografici e temporali. Il software effettua previsioni sull'aumentata probabilità di scassi in determinate aree e in determinati orari.
- *«Predictive policing» riferito a persone*: alcuni Cantoni (tra cui Lucerna e San Gallo) impiegano lo strumento di analisi DyRiAS-Intimpartner, che analizza il rischio potenziale che una persona di sesso maschile commetta reati violenti ai danni dell'attuale partner o dell'ex. Tuttavia è emerso che DyRiAS stima il rischio per eccesso.
- *Riconoscimento automatico dei veicoli* e nella *sorveglianza del traffico*[37]*:* una telecamera registra le targhe dei veicoli, permettendo di accertare l'identità del proprietario nonché il momento, il luogo, il senso di marcia e la presenza di altri viaggiatori. Questi dati sono poi confrontati automaticamente con altre banche dati, ad esempio

[34] In generale si rimanda a JESSICA WULF/CATHERINE EGLI, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 23 seg. (disponibile solo in tedesco).

[35] Cfr. in merito il sito Internet della SEFRI; consultabile sotto <Intelligenza artificiale (admin.ch)>.

[36] Gli esempi sono tratti da NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 23 seg. (disponibile solo in tedesco).

[37] Per quanto riguarda la ricerca automatica di veicoli e la sorveglianza del traffico cfr. DTF **146** I 11.

per trovare veicoli rubati o perseguire criminali. La maggior parte di queste videocamere è attualmente impiegata dal Corpo delle guardie di confine della Confederazione per la lotta contro la criminalità transfrontaliera.

– *Esecuzione penale*: in Svizzera non viene (ancora) usata l'intelligenza artificiale per decidere la sentenza da pronunciare. Nel l'esecuzione delle pene, invece, il programma ROS (*Risikoorientierter Sanktionenvollzug,* ossia esecuzione delle sanzioni basata sul rischio, in usa in tutta la Svizzera tedesca) esamina la possibilità di allentare il regime detentivo. A tal fine i dati figuranti nell'estratto del casellario giudiziario di una persona (p. es. età, reati violenti commessi prima dei 18 anni, numero di precedenti penali o entità della pena) vengono immessi nello strumento di screening dei casi (*Fall-Screening-Tool* o FaST), che in automatico suddivide gli interessati in tre categorie di rischio secondo il loro pericolo di fuga e di recidiva. In base a questa classificazione si decide se, nel caso specifico, occorre un'approfondita analisi basata sul rischio.

- **Casistica 1: decisioni individuali automatizzate**

  Secondo l'articolo 21 capoverso 1 nLPD una decisione individuale automatizzata è una «decisione basata esclusivamente su un trattamento di dati personali automatizzato che abbia per [la persona interessata] effetti giuridici o conseguenze significative».

  Definizione

  – **La decisione si basa esclusivamente su un trattamento di dati automatizzato**: significa che sia la valutazione materiale dei fatti sia la decisione che ne deriva sono opera di una macchina ovvero da un algoritmo senza l'intervento di una persona fisica. Per contro è irrilevante se l'algoritmo è stato programmato da un umano. La decisione individuale automatizzata può essere effettuata grazie a un algoritmo semplice basato su regole oppure grazie a un'applicazione in grado di sviluppare e impiegare regole in piena autonomia partendo da grandi quantità di dati e dalle correlazioni tra di essi (apprendimento automatico)[38]. È considerata automatizzata anche la decisione individuale comunicata da una persona fisica che non l'abbia adottata [39].

    In tale contesto va notato che un'interpretazione alla lettera dell'articolo 21 capoverso 1 nLPD amplierebbe molto il campo di applicazione delle norme in materia di decisioni individuali automatizzate. Nel messaggio del 15 settembre 2017 il Consiglio federale ha pertanto chiarito che solo una decisione che presenta un «**determinato grado di complessità**» rientra nella definizione (► FF **2017** 5939, 6045). Il messaggio non definisce però il grado di complessità che la decisione individuale automatizzata deve presentare. Ciononostante, lo scopo tutelare delle pertinenti disposizioni (segnatamente art. 21, 25 cpv. 2 lett. f nonché 34 cpv. 2 lett. c LPD) sembra porre l'accento sui processi decisionali che risultano incomprensibili agli interessati[40]. Ecco perché, a titolo di riduzione teleologica dell'articolo 21 capoverso 1 nLPD, non dovrebbero rientrare nel concetto di decisione individuale automatizzata né le banali decisioni conseguenziali del tipo se/allora né le semplici domande cui rispondere sì/no in base a criteri oggettivi evidenti per l'interessato. Ne sono un esempio il prelievo di denaro a un bancomat o il controllo degli accessi tramite badge ed elenchi predefiniti di persone autorizzate[41]. Nemmeno le banali operazioni matematiche (come p. es. una semplice addizione) dovrebbero di norma

[38] Cfr. NADJA BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 19 (disponibile solo in tedesco).

[39] Cfr. DAVID RECHSTEINER, Der Algorithmus verfugt. Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, in: Jusletter del 26 novembre 2018, n. marg. 1 e 5 seg.

[40] P. es. per quanto concerne lo scopo protettivo dell'art. 22 del regolamento generale (UE) 2016/679 sulla protezione dei dati cfr. tra l'altro MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (ed.), Künstliche Intelligenz und Robotik, Monaco di Baviera 2020, § 11 n. marg. 41 seg.

[41] Cfr. per quanto concerne l'art. 22 del regolamento generale (UE) 2016/679 sulla protezione dei dati SEBASTIAN SCHULZ, in: PETER GOLA (ed.), Kommentar zur DS-GVO, 2. A., Monaco di Baviera 2018, Art. 22 DS-GVO n. marg. 20; GISELHER RÜPKE/KAI VON LEWINSKI/JENS ECKHARDT, Datenschutzrecht, Monaco di Baviera 2018 § 16 n. marg. 11; MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (Hrsg.), op. cit., § 11 n. marg. 41 seg.

raggiungere il grado di complessità richiesto per una decisione individuale automatizzata ai sensi dell'articolo 21 capoverso 1 nLPD.

– **Effetto della decisione**: inoltre, il concetto di decisione individuale automatizzata secondo l'articolo 21 capoverso 1 nLPD comprende solo decisioni che hanno effetti giuridici o conseguenze significative per la persona interessata.

  La decisione ha effetti giuridici quando comporta conseguenze dirette, previste dalla legge, per la persona interessata. Nel diritto privato gli effetti giuridici sono legati alla conclusione o alla risoluzione di un contratto. La mancata conclusione di un contratto non espleta invece di regola alcun effetto giuridico, dato che la posizione giuridica dell'interessato non viene modificata (una situazione particolare si ha invece nel caso dell'obbligo di contrarre). Ciononostante, un contratto non concluso può comportare conseguenze significative (seconda eventualità; v. qui di seguito). Nel settore pubblico si hanno effetti giuridici soprattutto quando una decisione è emanata in una procedura totalmente automatizzata (► FF **2017** 5939, 6045). Non è ancora chiaro se nella definizione rientrino anche effetti giuridici positivi. La dottrina europea e quella svizzera respingono in parte l'idea a causa dello scopo tutelare della norma, dato che la persona interessata non deve essere protetta da una decisione totalmente a suo favore. Il rimando all'articolo 30 capoverso 2 della legge sulla procedura amministrativa (PA), contenuto nell'articolo 21 capoverso 4 nLPD, potrebbe far pensare che, nel caso di una decisione individuale automatizzata che soddisfa pienamente la richiesta dell'interessato, gli organi federali possano solo rinunciare a sentirlo e a far riesaminare la decisione da una persona fisica secondo l'articolo 21 capoverso 2 nLPD, ma non possono negargli il diritto di informarlo secondo l'articolo 21 capoversi 1 e 4 nLPD.

  Si possono presumere **conseguenze significative** per la persona interessata se questa subisce durevolmente pregiudizi economici o personali. Un semplice inconveniente non è sufficiente. Tutto dipende dalle circostanze concrete del caso. Occorre in particolare tenere conto dell'importanza del bene in questione per la persona interessata, della durata degli effetti della decisione e delle eventuali alternative a disposizione. Ripercussioni notevoli possono risultare, ad esempio, in caso di prestazioni mediche effettuate sulla base di una decisione individuale automatizzata (► FF **2017** 5939, 6045 seg.).

– **Rapporto con la profilazione (► n. 2.2.1 lett. b))**: la decisione individuale automatizzata va distinta dalla profilazione, anche se le due operazioni possono sovrapporsi. Il trattamento dei dati alla base di una decisione individuale automatizzata può costituire profilazione, ma non lo è per forza[42]. Inversamente, una profilazione può portare a una decisione individuale automatizzata, ma non per forza (p. es. se si tratta soltanto di un esame preliminare per una decisione poi presa da una persona fisica)[43].

– Con le disposizioni sulle decisioni individuali automatizzate nella nLPD attua, tra l'altro, i requisiti dell'articolo 9 paragrafo 1 lettera a della Convenzione sulla protezione dei dati 108+ del Consiglio d'Europa e dell'articolo 11 della direttiva (UE) 2016/680 sulla protezione dei dati in materia penale. Inoltre in tal modo allinea il diritto svizzero in materia di protezione dei dati al regolamento generale (UE) 2016/679 sulla protezione dei dati

[42] Nel disegno del Consiglio federale, l'articolo 19 capoverso 1 D-LPD (dopo la votazione finale: art. 21 cpv. 1 nLPD) aveva il tenore seguente: «Il titolare del trattamento informa la persona interessata di qualsiasi decisione basata esclusivamente su un trattamento di dati personali automatizzato, *compresa la profilazione*, che abbia per lei effetti giuridici o ripercussioni significative». In Parlamento l'inciso «compresa la profilazione» è stato eliminato. Come spiegato dal capo del DFGP nel Consiglio degli Stati il 18 dicembre 2019, l'eliminazione non comporta alcuna modifica materiale (cfr. Boll. Uff. **2019** S 1241). La profilazione non ha in questa disposizione alcun valore autonomo e ricade, con o senza menzione espressa, nel campo d'applicazione dell'art. 19 cpv. 1 D-LPD ovvero art. 21 cpv. 1 nLPD qualora porti a una decisione individuale automatizzata. Questo vale sia per la profilazione «ordinaria» che per la profilazione a rischio elevato secondo l'art. 5 lett. g nLPD.

[43] V. in merito le «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679» dell'ex Gruppo di lavoro articolo 29 del 6 febbraio 2018, pag. 8 seg. con esempi.

(art. 14 par. 2 lett. g e art. 22). Queste **disposizioni europee** vanno quindi considerate nell'interpretare il concetto di decisione individuale automatizzata.

Requisiti relativi alla base legale

- **Livello normativo**: in determinate condizioni, le decisioni individuali automatizzate possono comportare un'ingerenza grave nei diritti fondamentali della persona interessata secondo l'articolo 34 capoverso 2 lettera c nLPD, per cui è necessaria un'autorizzazione in una legge in senso formale (cfr. in merito il messaggio del 15 settembre 2017: ►FF **2017** 5939, 6067). Questo soprattutto quando la decisione individuale automatizzata si basa su una profilazione o sul trattamento di dati personali degni di particolare protezione. Inoltre vanno considerati il grado e la durata dell'ingerenza nei diritti della persona interessata o delle conseguenze significative causate. Per di più vale quanto segue: quanto più complessa è una decisione individuale automatizzata, vale a dire quanto più difficile è da comprendere per l'interessato, tanto più occorre una base legale in una legge in senso formale. Le decisioni individuali automatizzate possono inoltre essere considerate importanti anche per motivi di diritto procedurale o organizzativo, richiedendo quindi una base legale in una legge formale secondo l'articolo 164 capoverso 1 lettera g Cost. È ad esempio il caso quando una procedura amministrativa viene condotta esclusivamente in modo elettronico.

- **Densità normativa**: la base legale deve prevedere espressamente la decisione individuale automatizzata e definirla in modo adeguato. Inoltre deve specificare i tipi di decisioni emessi in maniera completamente automatizzata (p. es. decisioni di tassazione) e i dati che confluiscono nella decisione. Infine, l'interessato dovrebbe poter riconoscere, almeno a grandi linee, su quale logica si basa la decisione individuale automatizzata (p. es. tipo di dati e loro ponderazione). Va poi chiarito nel caso concreto se nella base legale vadano menzionati ulteriori aspetti.

Ulteriori effetti giuridici delle decisioni individuali automatizzate

Secondo l'articolo 21 capoversi 1 e 4 nLPD, nel caso delle decisioni individuali automatizzate sussiste un **obbligo di informare** la persona interessata. Gli organi federali devono designare come tali le decisioni emesse con procedure completamente automatizzate. L'articolo 21 capoverso 2 nLPD conferisce alla persona interessata il **diritto** di **esprimere**, su sua richiesta, **il proprio punto di vista** e di esigere che la decisione sia **riesaminata da una persona fisica**. L'articolo 21 capoverso 2 nLPD non è applicabile agli organi federali se, in virtù dell'articolo 30 capoverso 2 PA o di un'altra legge federale, la persona interessata non deve essere sentita prima di prendere la decisione (p. es. quando la decisione individuale automatizzata può essere riesaminata in una procedura di opposizione non automatizzata). Infine, secondo l'articolo 25 capoverso 2 lettera f nLPD, alla persona interessata devono essere fornite, nell'ambito del suo **diritto d'accesso**, informazioni sull'esistenza di una decisione individuale automatizzata e la logica su cui si fonda. Nel caso di un organo federale autorizzato a emanare decisioni individuali automatizzate, va **verificato se sia possibile rispettare tutte queste norme**.

Compatibilità con il diritto costituzionale e procedurale

In caso di ricorso a decisioni individuali automatizzate nell'Amministrazione federale – a prescindere dalle normative in materia di protezione dei dati –, sorge la domanda se e a quali condizioni l'emanazione totalmente automatizzata di decisioni sia compatibile con i principi del diritto costituzionale e amministrativo. Ulteriori restrizioni potrebbero inoltre risultare soprattutto dalle garanzie procedurali (art. 29 segg. Cost.; PA).

Seguono alcune questioni di principio sollevate dalla dottrina, che vanno approfondite:

- **principio inquisitorio e obbligo di cooperazione** (art. 12 segg. PA): nelle decisioni individuali automatizzate è possibile rispettare le disposizioni procedurali relative all'accertamento dei fatti?[44] È imprescindibile che i dati utilizzati per la decisione individuale automatizzata siano completi, corretti e presenti nella quantità necessaria. Questo vale anche per i dati impiegati per consentire l'apprendimento automatico[45];
- **divieto di discriminazione**: grandi sfide si prospettano inoltre per quanto riguarda il divieto di discriminazione. Come l'intelligenza artificiale in generale, anche le decisioni individuali automatizzate celano il rischio che i dati usati per sviluppare e nutrire il sistema riflettano pregiudizi storici, rafforzando determinate discriminazioni (inconsapevoli). È quindi essenziale garantire la qualità dei dati. Ulteriori misure potrebbero essere algoritmi di controllo per analizzare la ponderazione dei fattori che concorrono alla decisione o verifiche regolari da parte di altre istituzioni statali o organizzazioni terze[46];
- **diritto a una motivazione**: come garantirlo nel caso di una decisione individuale automatizzata? Non dovrebbe essere particolarmente difficile con un algoritmo basato su una regola che, come l'approccio mentale giuridico di una persona, verifica la presenza di determinate condizioni. È invece dubbio se sia possibile motivare con sufficiente rigore giuridico una decisione individuale automatizzata basata sull'intelligenza artificiale, poiché il funzionamento dei processi di apprendimento meccanico spesso sono difficilissimi da capire[47]. Secondo lo studio commissionato dal Catone di Zurigo, una decisione emessa con l'aiuto dell'intelligenza artificiale deve, tra le altre cose, illustrare sia la logica decisionale dell'algoritmo indicando tipo, quantità, periodo di rilevamento e ponderazione dei dati, sia la sua applicazione nello specifico. Inoltre possono essere necessarie informazioni sul gruppo di confronto in cui l'algoritmo inquadra la persona e sulle peculiarità individuali determinanti nel singolo caso. In via eccezionale e in circostanze particolari è presa in considerazione anche la divulgazione del codice sorgente dell'algoritmo[48];
- **margine di discrezionalità e di apprezzamento**: infine non è chiaro se debbano essere possibili decisioni individuali automatizzate qualora le autorità dispongano di un margine di discrezionalità e di apprezzamento. Parte della dottrina respinge l'idea, in quanto ritiene giuridicamente errato che un organo federale rinunci all'esercizio del proprio margine di discrezionalità o di apprezzamento emanando una decisione automatizzata. Per fare giustizia nel singolo caso è necessario poter derogare alle regole. Gli algoritmi basati su regole non ne sono in grado; quelli basati sull'apprendimento meccanico non seguono rigidamente le regole, tuttavia il loro processo decisionale si basa esclusivamente su decisioni già prese in passato, il che pregiudica la corretta valutazione di un caso ancora sconosciuto[49].

---

[44] NADJA BRAUN BINDER, Automatisierte Entscheidungen: Perspektive Datenschutzrecht und öffentliche Verwaltung, in SZW / RSDA 2020 pag. 27 segg.

[45] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 38 seg.

[46] Cfr. NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 39 segg.

[47] DAVID RECHSTEINER, op. cit., n. marg. 24 segg.

[48] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 38.

[49] DAVID RECHSTEINER, op. cit., n. marg. 28 segg. Cfr. anche NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 46 segg., che giungono a loro volta alla conclusione che l'intelligenza artificiale non andrebbe utilizzata nell'amministrazione laddove sussiste un margine di discrezionalità e di apprezzamento.

- **Casistica 2: impiego ausiliario dell'intelligenza artificiale**

  Una decisione solo *preparata in modo automatizzato*, ma poi presa da una persona fisica non è una decisione invidiale automatizzata secondo l'articolo 21 capoverso 1 nLPD. In futuro si ricorrerà sempre più spesso a sistemi basati sull'intelligenza artificiale anche per ***assistere*** **in automatico il processo decisionale**. Le sfide giuridiche illustrate per le decisioni individuali automatizzate si pongono in modo simile per l'impiego – anche solo ausiliario – dell'intelligenza artificiale, sebbene in parte esistano altre soluzioni possibili. Per evitare decisioni discriminatorie si può ad esempio fare in modo che gli specialisti dispongano delle conoscenze e competenze necessarie a riconoscere le proposte discriminatorie presentate dall'intelligenza artificiale per poter poi decidere diversamente[50].

  Se l'impiego ausiliario dell'intelligenza artificiale comporta un trattamento di dati personali, occorre garantire che esista una **base legale sufficiente** sia per livello normativo che per densità normativa e conforme ai requisiti dell'articolo 34 nLPD. Se il tipo di trattamento o l'impiego dell'intelligenza artificiale implica ingerenze gravi nei diritti fondamentali della persona interessata, è richiesta una base legale in una legge in senso formale secondo l'articolo 34 capoverso 2 lettera c nLPD. Per la densità normativa vanno contemplati gli stessi requisiti previsti per le decisioni individuali automatizzate (► casistica 1) e la profilazione (► n. 2.2.1 lett. b)/dd): nella base legale vanno indicati soprattutto lo scopo dell'impiego dell'intelligenza artificiale, i dati che confluiscono nell'apposita applicazione e la logica alla base dell'applicazione (p. es. tipo di dati e loro ponderazione) nonché (se applicabile) le caratteristiche valutate della personalità. Va poi chiarito nel caso concreto se nella base legale vadano menzionati ulteriori aspetti.

2.2.2 Modalità di comunicazione dei dati: abrogazione dei requisiti supplementari per la base legale della procedura di richiamo

La procedura di richiamo («accesso online») è una forma particolare di comunicazione dei dati. Si tratta di una procedura automatizzata, in cui il destinatario può ottenere dati personali senza che l'organo federale in loro possesso debba cooperare o possa addirittura notare la cosa (principio del «self-service»). Secondo l'attuale articolo 19 capoverso 3 LPD, gli organi federali possono permettere l'accesso a dati personali mediante una procedura di richiamo soltanto qualora la base legale lo preveda esplicitamente. Nel caso di dati personali degni di particolare protezione (e profili della personalità), occorre addirittura una base legale esplicita in una legge in senso formale.

La revisione totale della LPD abroga questi requisiti supplementari poiché, secondo il messaggio del 15 settembre 2017, appaiono obsoleti nell'era digitale (► FF **2017** 6941, 6069). In altre parole: la forma della procedura di richiamo non andrà più indicata espressamente nella base legale. Ovviamente la comunicazione dei dati in sé continuerà però a richiedere una base legale. Inoltre, in molti casi – soprattutto di grave ingerenza nei diritti fondamentali – si imporrà comunque, per ragioni di trasparenza, la scelta di specificare nel testo di legge o di ordinanza che si tratta di un «accesso» ai dati in cui il titolare dei dati rimane passivo (sostituendo eventualmente il termine «procedura di richiamo» con «accesso ai dati / ai sistemi d'informazione / ecc.»). Occorre poi anche distinguere tra un «accesso completo» o un mero «accesso indicizzato». Per il resto, anche in futuro l'accesso ai dati va concesso con parsimonia, soprattutto se lo scopo del sistema d'informazione a cui si accede si discosta fortemente dalle finalità perseguite dal destinatario dei dati. Vanno pertanto sempre presi in considerazione anche altri tipi di comunicazione dei dati rispetto all'accesso mediante procedura di richiamo.

[50] Cfr. NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Cancelleria di Stato del Cantone di Zurigo (ed.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 febbraio 2021, pag. 42.

Oltre alla procedura di richiamo, si distinguono altre tre forme di comunicazione dei dati: l'obbligo di comunicazione (d'ufficio o su richiesta), la comunicazione spontanea e la comunicazione dei dati su richiesta e a discrezione dell'autorità interpellata ► cfr. in merito soprattutto la Guida di legislazione (cap. 14; n. marg. 834 segg.). Queste forme di comunicazione dei dati dovranno essere indicate nelle basi legali anche in futuro – non solo per ragioni legate al diritto in materia di protezione dei dati.

3 Dati concernenti persone giuridiche

3.1 Situazione di partenza: abrogazione della protezione per i dati concernenti persone giuridiche

Con la revisione totale, il trattamento di dati concernenti persone giuridiche viene escluso dal campo d'applicazione materiale della LPD. Secondo l'articolo 2 capoverso 1 nLPD, questa legge si applica solo al trattamento di dati personali di persone fisiche, definiti come «informazioni concernenti una persona *fisica* identificata o identificabile» (art. 5 lett. a nLPD). Le persone giuridiche continuano a rimanere tutelate da altre disposizioni dell'ordinamento giuridico svizzero, segnatamente quelle a protezione della personalità previste nel Codice civile (art. 28 segg. CC), quelle della legge contro la concorrenza sleale e della legge sul diritto d'autore o quelle relative alla protezione dei segreti professionali, d'affari e di fabbricazione.

L'abrogazione della protezione per i dati concernenti persone giuridiche nella nLPD e la limitazione del concetto di dati personali alle informazioni relative alle persone fisiche hanno diverse ripercussioni sul trattamento dei dati da parte degli organi federali. Questa novità implica in particolare che, in futuro, le basi legali di diritto federale che autorizzano gli organi federali a trattare e comunicare dati *personali* non saranno più applicabili al trattamento e alla comunicazione dei *dati concernenti persone giuridiche*. Tuttavia, in virtù del principio della legalità secondo l'articolo 5 capoverso 1 Cost. e del requisito della base legale per la restrizione dei diritti fondamentali secondo l'articolo 36 capoverso 1 Cost., il trattamento e la comunicazione dei dati concernenti persone giuridiche da parte di organi statali richiede una base legale. Infatti, anche le persone giuridiche godono della protezione della sfera privata secondo l'articolo 13 Cost., pur non beneficiando completamente di questo diritto fondamentale[51].

Con la revisione totale della LPD, nella legge sull'organizzazione del Governo e dell'Amministrazione (nLOGA; n. 13 dell'Allegato 1/II della nLPD) viene pertanto introdotta una serie di nuove disposizioni per la gestione dei dati concernenti persone giuridiche da parte di organi federali (art. 57*r* segg. nLOGA; ► n. 3.2). Inoltre, la disposizione transitoria dell'articolo 71 nLPD mira a impedire lacune giuridiche nei prossimi cinque anni (► n. 3.3).

3.2 Nuove disposizioni per la gestione dei dati concernenti persone giuridiche

3.2.1 Concetti

Di seguito sono illustrati i concetti più importanti per il trattamento dei dati concernenti persone giuridiche da parte di organi federali[52]. A tal fine si fa riferimento soprattutto alle disposizioni della LPD, ovvero della nLPD, applicandole per analogia. Negli articoli 57*r* e seguenti nLOGA è definito solo il concetto di «dati concernenti persone giuridiche degni di particolare protezione».

- **Dati (concernenti persone giuridiche)**: analogamente al concetto di dati personali (art. 5 lett. a nLPD), si intendono tutte le informazioni concernenti una persona giuridica identificata o identificabile. Se la persona giuridica non è nemmeno identificabile (p. es. perché i suoi dati sono stati anonimizzati), le disposizioni degli articoli 57*r* e seguenti nLOGA non sono applicabili.

[51] DTF **137** II 371 consid. 6.

[52] Secondo il messaggio del 15 settembre 2017 del Consiglio federale (► FF **2017** 5939, 6103), il concetto di «organi federali» nell'articolo 57*r* segg. nLOGA s'ispira alla definizione legale nell'art. 5 lett. i nLPD («autorità o servizio della Confederazione, oppure persona cui sono affidati compiti federali»).

- **Persone giuridiche**: principalmente tutti i gruppi di persone organizzati in società, nonché gli istituti autonomi dotati di personalità giuridica e dedicati a uno scopo particolare, segnatamente associazioni, fondazioni, società per azioni, società in accomandita per azioni, società a responsabilità limitata, cooperative nonché enti di diritto privato previste dal diritto cantonale, istituti di diritto pubblico ed enti dei Cantoni e della Confederazione. La dottrina relativa all'attuale LPD interpreta tuttavia in senso più ampio il concetto di persona giuridica, estendendolo oltre il tenore della legge anche alle società di persone che, pur non essendo dotate di una propria personalità in senso giuridico, possono essere parte e stare in giudizio (come le società collettive, le società in accomandita semplice e le proprietà per piani). Su questa interpretazione ampia del concetto di persona giuridica si basano anche i nuovi articoli 57*r* e seguenti nLOGA. Non vi rientrano, invece, i gruppi di persone che, secondo il diritto svizzero, non presentano alcun elemento di una personalità giuridica come, ad esempio, le società semplici o le comunioni ereditarie[53].

- **Dati degni di particolare protezione concernenti persone giuridiche**: secondo l'elenco esaustivo all'articolo 57*r* capoverso 2 nLOGA si tratta di

  – dati relativi a perseguimenti e sanzioni di natura amministrativa e penale (lett a; v. in merito anche l'art. 5 lett. c n. 5 nLPD);

  – dati relativi a segreti professionali, d'affari o di fabbricazione (lett. b)[54].

  L'elenco dei dati degni di particolare protezione delle persone giuridiche è quindi meno esteso rispetto a quello delle persone fisiche, sebbene con l'espressione «dati relativi a segreti professionali, d'affari o di fabbricazione» si introduca una nuova categoria di dati. In questo contesto le persone giuridiche hanno esigenze di protezione meno estese rispetto alle persone fisiche.

3.2.2 Trattamento di dati concernenti persone giuridiche (art. 57*r* LOGA)

L'articolo 57*r* capoverso 1 LOGA istituisce una base legale generale e direttamente applicabile per il *trattamento* di dati concernenti persone giuridiche, compresi quelli degni di particolare protezione: gli organi federali possono trattarli

- se è **necessario per l'adempimento dei loro compiti** e

- il **compito è descritto in una legge in senso formale**. Una disposizione d'ordinanza o un compito soltanto implicito non sono sufficienti. Il compito deve essere chiaramente riconoscibile e sufficientemente determinato.

Se le prescrizioni dell'articolo 57*r* capoverso 1 LOGA sono soddisfatte, non è necessaria un'autorizzazione in una legge speciale. Questo vale per il trattamento sia dei dati «ordinari» sia di quelli degni di particolare protezione. L'articolo 57*r* LOGA comprende quindi essenzialmente tutti i possibili tipi di trattamento, inclusa la profilazione. Diversa è invece la situazione quando lo scopo e le modalità di trattamento implicano un'ingerenza così grave nei diritti fondamentali della persona giuridica interessata che l'articolo 57*r* LOGA non soddisfa più i requisiti del principio della legalità secondo gli articoli 5 capoverso 1 e 36 capoverso 1 Cost. per la densità normativa: in tal caso è necessaria una norma esplicita nel pertinente atto materiale.

Occorre valutare per ogni singolo progetto legislativo se il trattamento dei dati concernenti persone giuridiche può fondarsi sull'articolo 57*r* LOGA oppure se è necessaria una norma in

[53] In relazione al tutto cfr. DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar DSG, art. 2 LPD n. 6 segg., BEAT RUDIN, SHK DSG, art. 2 LPD n. 12. Già nel messaggio del 23 marzo 1988 del Consiglio federale relativo alla legge federale sulla protezione dei dati, il concetto di persone giuridiche era stato interpretato nel senso ampio sopra esposto (FF **1988** II 413, 378).

[54] L'art. 57*r* LOGA non implica modifiche alle esistenti disposizioni di diritto penale, amministrativo e procedurale a protezione dei segreti professionali, d'affari e di fabbricazione, bensì può essere applicato soltanto nella misura in cui tali dati possono essere ottenuti dagli organi federali.

una legge speciale. Va prestata particolare attenzione affinché il compito legale che richiede il trattamento di dati sia definito con sufficiente chiarezza. Va inoltre verificato se eventualmente occorre disciplinare anche altre modalità di trattamento (come termini di conservazione o provvedimenti tecnici e organizzativi per garantire la sicurezza dei dati).

3.2.3 Comunicazione di dati concernenti persone giuridiche (art. 57*s* LOGA)

L'articolo 57*s* capoverso 1 LOGA stabilisce che la *comunicazione* di dati concernenti persone giuridiche deve essere prevista da una base legale in una legge speciale. Contrariamente all'articolo 57*r* LOGA (trattamento di dati concernenti persone giuridiche), l'articolo 57*s* LOGA non costituisce quindi una base legale che permetta agli organi federali di comunicare dati specifici. In questa sede vale invece il **principio dell'autorizzazione speciale**.

Analogamente all'articolo 36 nLPD (comunicazione di dati personali), l'articolo 57*s* LOGA disciplina la base legale richiesta affinché un organo federale possa comunicare dati concernenti una persona giuridica, e stabilisce le condizioni in cui, in via eccezionale, non occorre base legale.

- **Requisito della base legale**: essenzialmente gli organi federali possono comunicare i dati concernenti persone giuridiche soltanto se lo prevede una base legale (art. 57*s* cpv. 1 LOGA). La base legale può essere costituita da un trattato internazionale, una legge in senso formale o un'ordinanza. Mentre per la comunicazione dei dati «ordinari» concernenti persone giuridiche di norma è sufficiente una **disposizione in un'ordinanza**, per i dati degni di particolare protezione è richiesta una **base legale in una legge in senso formale** (art. 57*s* cpv. 2 LOGA). A differenza dell'articolo 36 capoverso 1 in combinato disposto con l'articolo 34 capoverso 3 nLPD, l'articolo 57*s* LOGA non prevede espressamente che è sufficiente una disposizione d'ordinanza quando la comunicazione è indispensabile per adempire un compito previsto in una legge formale e lo scopo del trattamento non implica rischi particolari per i diritti fondamentali della persona interessata. Questa lacuna può tuttavia essere colmata per analogia, dato che la LOGA vuole essere più generosa (e non più severa) della nLPD per quanto riguarda la gestione dei dati concernenti persone giuridiche.

- **Eccezioni al requisito della base legale**: l'articolo 57*s* capoverso 3 LOGA elenca in modo esaustivo i casi in cui è ammissibile la comunicazione di dati «ordinari» o degni di particolare protezione concernenti persone giuridiche, nello specifico anche *senza una base legale*. Si tratta delle stesse eccezioni previste dall'articolo 36 capoverso 2 lettere a, b ed e nLPD per la comunicazione dei dati personali (► n. 2.1).

- **«Casi speciali»**: l'articolo 57*s* capoversi 4 e 5 LOGA contiene la stessa regola speciale dell'articolo 36 capoversi 3 e 5 nLPD per la comunicazione dei dati concernenti persone giuridiche nel quadro dell'informazione del pubblico da parte delle autorità (► n. 2.1).

3.2.4 Diritti delle persone giuridiche (art. 57*t* LOGA)

L'abrogazione della protezione per i dati concernenti persone giuridiche nella nLPD implica che le persone giuridiche non possono più rivendicare i diritti particolari previsti dal diritto in materia. Questo riguarda in particolare il diritto d'accesso di cui all'articolo 25 e seguente nLPD. L'articolo 57*t* LOGA rimanda pertanto al diritto procedurale applicabile. Nel quadro di una procedura amministrativa di prima istanza, ad esempio, le persone giuridiche possono esaminare gli atti ai sensi degli articoli 26 e seguenti PA, esercitare il diritto di essere sentite ai sensi degli articoli 29 e seguenti PA e, se del caso, impugnare la decisione pronunciata dall'autorità competente. Le persone giuridiche possono anche invocare l'articolo 25*a* PA, secondo cui chiunque abbia un interesse degno di protezione può esigere una decisione impu-

gnabile dall'autorità competente per atti materiali che si fondano sul diritto pubblico federale e che tangono diritti od obblighi. In tal modo le persone giuridiche possono far rettificare o distruggere i loro dati.

Infine, in virtù della legge sulla trasparenza (LTras), le persone giuridiche possono chiedere di consultare i documenti ufficiali. Nella LTras vale il principio dello stesso accesso per ogni persona: quello che viene reso noto a una persona deve essere accessibile a tutti («*acces to one, access to all*»). Quando però si tratta dell'accesso ai propri dati, nei confronti di una persona giuridica non è possibile far valere l'eccezione riguardante i segreti professionali, d'affari o di fabbricazione di cui all'articolo 7 capoverso 1 lettera g LTras. Questa eccezione vale solo per terzi e non per la persona giuridica richiedente, che è titolare di tali segreti.

3.3 Disposizione transitoria per i dati concernenti persone giuridiche (art. 71 nLPD)

La nuova normativa a protezione dei dati concernenti persone giuridiche implica la modifica di numerose basi legali contenute in leggi speciali. Non è stato possibile effettuarle tutte nel contesto della revisione totale della LPD[55]. Dopo l'entrata in vigore del nuovo diritto in materia di protezione dei dati, tutte le disposizioni delle leggi speciali saranno verificate e conformate quanto più possibile alle nuove prescrizioni dell'articolo 57*r* e seguenti LOGA nel quadro di un progetto coordinato dall'UFG.

Per evitare lacune giuridiche fino ad allora, nell'articolo 71 nLPD è stata introdotta una disposizione transitoria per gli organi federali: le attuali disposizioni di protezione dei dati contenute nelle leggi speciali[56] – inserite sia in leggi in senso formale che in leggi in senso materiale – continueranno ad applicarsi ai dati concernenti persone giuridiche per cinque anni dall'entrata in vigore della nLPD. Durante questo periodo gli organi federali potranno in particolare fondarsi, per la comunicazione di dati concernenti persone giuridiche, sulle basi legali applicabili finora alla comunicazione di dati personali. L'articolo 71 nLPD vale anche per le disposizioni relative alla protezione dei dati contenute in leggi speciali che entreranno in vigore dopo l'approvazione o l'entrata in vigore della nLPD.

L'applicazione della disposizione transitoria dell'articolo 71 nLPD non è obbligatoria: se un'unità amministrativa desidera disciplinare espressamente la gestione dei dati concernenti persone giuridiche già durante il periodo transitorio di cinque anni, è libera di farlo.

[55] Per motivi di certezza del diritto e praticità, nell'Allegato 1/II della nLPD alcune leggi federali sono già state verificate e adeguate per quanto riguarda la gestione dei dati concernenti persone giuridiche. Questo vale soprattutto per la LOGA, la LTras, la legge sulla statistica federale (LStat) e la legge sui revisori (LSR). Una panoramica dettagliata si trova nel messaggio del 15 settembre 2017 del Consiglio federale (► FF **2017** 5939, 6092 seg.). Anche le relative ordinanze sono state adeguate nell'Allegato 2 della nLPD. Un elenco delle ordinanze si trova nel rapporto esplicativo relativo alla OPDa del 31 agosto 2022 (► Rapporto esplicativo OPDa, n. 7.2).

[56] Al contrario, il regime transitorio dell'art. 71 nLPD non è applicabile alle disposizioni della nLPD.

4 Ulteriori novità della revisione totale della LPD

4.1 Attori del trattamento dei dati: titolare e responsabile

La legislazione in materia di protezione dei dati conosce diversi attori, i cui ruoli implicano diversi diritti e obblighi. Per allinearsi al diritto europeo in materia (cfr. art. 2 lett. d ed f della Convenzione sulla protezione dei dati 108+ del Consiglio d'Europa; art. 3 n. 8 e 9 della direttiva [UE] 2016/680 sulla protezione dei dati in materia penale nonché art. 4 n. 8 e 9 del regolamento generale [UE] 2016/679), in futuro la nLPD userà principalmente i concetti di «titolare del trattamento» e «responsabile del trattamento». Il precedente «detentore di una collezione di dati» (art. 3 lett. i LPD) viene eliminato. Tuttavia, le sue funzioni saranno in gran parte riprese dal «responsabile del trattamento». Per quanto ravvisabile attualmente, le nuove designazioni dei ruoli implicheranno modifiche materiali di pochissimo conto.

Nelle disposizioni in materia di protezione dei dati figuranti in leggi speciali vanno chiariti i vari attori che partecipano al trattamento dei dati. Le disposizioni devono indicare il servizio responsabile per il trattamento. Inoltre, gli interessati devono poter riconoscere eventuali altre persone coinvolte nel trattamento e i loro ruoli. In tale contesto fa sempre stato solo ed esclusivamente il *rapporto rilevante in termini di protezione dei dati*, che può essere diverso dal «rapporto apparente». In un mandato retto dal Codice delle obbligazioni, ad esempio, il mandante non è per forza anche titolare del trattamento e il mandatario non è per forza il responsabile del trattamento.

- **Titolare del trattamento** (art. 5 lett. j nLPD): persona fisica o giuridica che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento dei dati. Decidere i mezzi del trattamento significa stabilire i parametri essenziali del trattamento. Con ciò non si intendono tanto i mezzi tecnici e organizzativi, quanto i fattori rilevanti per l'ammissibilità o i rischi in termini di protezione dei dati (p. es. quali dati sono trattati da quale fonte per quanto tempo e in che modo)[57]. Il titolare del trattamento deve garantire che siano rispettate le disposizioni del diritto in materia. Inoltre è suo compito tutelare i diritti degli interessati e soprattutto il loro diritto d'accesso (art. 25*f* nLPD).

- **Responsabile del trattamento** (art. 5 lett. k nLPD): chi tratta dati per conto del titolare è considerato – come in passato – responsabile del trattamento. È quanto accade, ad esempio, utilizzando un servizio cloud. Se in questo contesto i dati vengono comunicati all'estero, devono essere rispettate cumulativamente anche le prescrizioni dell'articolo 16 e seguenti nLPD. Essenzialmente il responsabile effettua il trattamento seguendo le istruzioni del titolare. Anche gli organi federali possono affidare, per contratto o per legge, il trattamento di dati personali a un responsabile (art. 9 cpv. 1 nLPD), il che però non li libera dall'obbligo di assumersi la responsabilità per la protezione dei dati. Devono garantire attivamente – mediante una selezione accurata, istruzioni e controlli – che il responsabile si attenga al diritto in materia di protezione dei dati (soprattutto la sicurezza dei dati) come dovrebbero fare loro stessi. La delega del trattamento dei dati non deve peggiorare la situazione giuridica degli interessati.

  Se sono adempiute le condizioni per affidare il trattamento a un responsabile, questi è considerato alla stregua del titolare in termini di protezione dei dati e quindi non è più un terzo (v. sotto). Nella revisione totale della LPD le condizioni per il deferimento del trattamento a un responsabile sono essenzialmente rimaste invariate (cfr. in merito l'art. 9 nLPD). Nuova

[57] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter del 17 giugno 2019, n. marg. 33.

è, invece, la norma dell'articolo 9 capoverso 3 nLPD, secondo cui questa specie di «subappalto della responsabilità» (vale a dire il ricorso a ulteriori responsabili da parte del responsabile primario) è ammessa soltanto previa autorizzazione del titolare. Questa autorizzazione può essere di natura specifica o generale (art. 7 cpv. 1 e 2 OPDa).

- **Trattamento congiunto dei dati personali** (art. 33 nLPD): se un organo federale tratta dati insieme ad altri organi federali, a organi cantonali o a privati, può risultare difficile attribuire le responsabilità[58]. Per evitare queste difficoltà, l'articolo 33 nLPD impone al Consiglio federale di disciplinare le procedure di controllo e la responsabilità. Questa disposizione corrisponde in larga parte all'attuale articolo 16 capoverso 2 LPD, con la differenza, però, che il Consiglio federale è obbligato, e non solo autorizzato, a prevedere regole speciali in materia. La LPD non specifica ulteriormente tale obbligo; spetta agli organi federali adempiervi negli atti normativi settoriali. In questo contesto vanno chiarite anche altre questioni, come i diritti di accesso ai dati, la sicurezza dei dati e l'attuazione dei diritti delle persone interessate dal trattamento.

- **Terzi**: il concetto di «terzi» non è definito esplicitamente nella nLPD. Ispirato al regolamento generale (UE) 2016/679 sulla protezione dei dati (art. 4 n. 10), comprende privati, organi federali o organi cantonali che non sono né titolari né responsabili del trattamento dei dati. Per questo motivo il responsabile non viene più definito «terzo» nella nLPD, a differenza di quanto avviene nell'attuale articolo 10*a* LPD, dato che, dal momento in cui inizia la sua attività per il titolare, non è più un terzo (► FF **2017** 5939, 6014).

- **Destinatario**: è un privato, un organo federale o un organo cantonale a cui vengono comunicati dati personali, a prescindere che si tratti di un terzo o meno (cfr. art. 2 lett. d della Convenzione sulla protezione dei dati 108+ del Consiglio d'Europa; art. 3 n. 10 della direttiva [UE] 2016/680 sulla protezione dei dati in materia penale nonché art. 4 n. 9 del regolamento generale [UE] 2016/679 [entrambi con eccezioni per le autorità che ricevono dati personali nell'ambito di un determinato mandato d'indagine preliminare]). Pertanto, anche i responsabili del trattamento (o i co-responsabili) sono considerati destinatari.

4.2 Comunicazione dei dati all'estero

Come il diritto vigente (art. 6 LPD), anche la legge riveduta contempla requisiti particolari per la comunicazione di dati personali all'estero (art. 16 seg. nLPD). Tuttavia, con la revisione totale della LPD la comunicazione transfrontaliera dei dati subisce alcune modifiche sistematiche e materiali.

- **Livello adeguato di protezione dei dati**: secondo l'articolo 16 capoverso 1 nLPD, essenzialmente i dati personali possono essere comunicati all'estero soltanto se la legislazione dello Stato interessato o l'organismo internazionale garantisce una protezione adeguata dei dati. *In futuro* il Consiglio federale dovrà stabilire un elenco vincolante dei Paesi o organismi internazionali che dispongono di un tale livello di protezione. I criteri in base ai quali il Consiglio federale dovrà verificare la legislazione straniera sono precisati nell'ordinanza (art. 8 OPDa). Gli Stati con un livello adeguato di protezione dei dati sono elencati nell'Allegato 1 dell'OPDa.

- **Garanzie appropriate a protezione dei dati**: secondo l'articolo 16 capoverso 2 nLPD, i dati personali possono essere comunicati a uno Stato che non compare nell'elenco del Consiglio

[58] In merito alla problematica nel diritto europeo in materia di protezione dei dati cfr. le «Guidelines 07/2020 on the concepts of controller and processor in the GDPR» del Comitato europeo per la protezione dei dati (EDPB) (documento disponibile solo in inglese).

federale soltanto se tale Stato garantisce una protezione dei dati appropriata[59] con altri strumenti, ossia: trattati internazionali (lett. a), clausole contrattuali di protezione dei dati (lett. b), garanzie specifiche stabilite da organi federali (lett. c), clausole tipo di protezione dei dati (lett. d) e norme interne vincolanti stabilite dall'impresa per la protezione dei dati («*binding corporate rules*»; lett. e). I contenuti minimi di queste garanzie sono concretizzati nell'OPDa (art. 9–11 OPDa). Inoltre, l'OPDa prevede altre due garanzie: codici di condotta e certificazioni (art. 12 OPDa e art. 16 cpv. 3 nLPD). Alcune di queste vanno preventivamente comunicate o approvate dall'IFPDT (risp. art. 16 cpv. 2 lett. b e c nLPD e art. 16 cpv. 2 lett. d ed e nLPD nonché art. 12 cpv. 2 OPDa). Le garanzie appropriate di cui all'articolo 16 capoverso 2 nLPD corrispondono in gran parte al diritto attualmente in vigore (art. 6 cpv. 2 lett. a e g e cpv. 3 LPD). Subiscono tuttavia alcune modifiche materiali. Per le novità si rimanda soprattutto al messaggio del 15 settembre 2017 (► FF **2017** 5939, 6029 segg.).

In considerazione di quanto esposto, **quando si concludono trattati internazionali** occorre prestare particolare attenzione che all'estero sia garantito un livello adeguato di protezione dei dati. A tale proposito sono fondamentali il rispetto dei principi in materia, i diritti degli interessati (come il diritto d'accesso, di opposizione, di cancellazione e di rettifica con corrispondenti possibilità di tutela giurisdizionale), le condizioni per eventuali ulteriori comunicazioni di dati all'estero e l'esistenza di un organo di vigilanza indipendente in materia.

- **Eccezioni**: come il diritto vigente (art. 6 cpv. 2 lett. b–f LPD), anche l'articolo 17 nLPD contempla varie eccezioni che consentono di comunicare i dati all'estero anche in assenza di una protezione adeguata secondo l'articolo 16 capoverso 1 nLPD e di garanzie appropriate secondo l'articolo 16 capoversi 2 e 3 nLPD. Le eccezioni di cui all'articolo 17 capoverso 1 lettere a–e nLPD sono state riprese nel diritto vigente con modifiche minime, spiegate nel messaggio del 15 settembre 2017 (► FF **2017** 5939, 6032 seg.). È invece nuova la lettera f dell'articolo 17 capoverso 1 nLPD. Questa disposizione permette di comunicare dati personali anche in mancanza di adeguata protezione nel caso in cui i dati provengano da un registro pubblico previsto dalla legge e siano adempiute le condizioni legali.

4.3 Valutazione d'impatto sulla protezione dei dati

Con la **valutazione d'impatto sulla protezione dei dati**, i titolari del trattamento (organi federali e privati) dovranno individuare per tempo eventuali rischi e, se necessario, adottare provvedimenti di protezione adeguati. Il titolare valuta l'impatto sulla protezione dei dati quando il trattamento dei dati in programma può comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata (art. 22 cpv. 1 nLPD). A titolo di esempio, la nLPD menziona il trattamento su grande scala di dati personali degni di particolare protezione (art. 22 cpv. 2 nLPD). Nella valutazione d'impatto vanno descritti il trattamento previsto, i rischi per la personalità o per i diritti fondamentali della persona interessata nonché i provvedimenti a loro tutela già adottati o da adottare (art. 22 cpv. 3 nLPD). Se, nonostante i provvedimenti adottati o previsti, rimane un «rischio residuo» elevato per la personalità o i diritti fondamentali della persona interessata, occorre **consultare l'IFPDT** (art. 23 cpv. 1 nLPD), che comunica le sue eventuali obiezioni e può suggerire provvedimenti di protezione adeguati. Per gli organi federali la valutazione d'impatto sulla protezione dei dati costituisce solo in parte una novità. L'attuale articolo 20 capoverso 2 OLDP impone loro infatti di annunciare al responsabile della protezione dei dati o all'IFPDT ogni progetto di trattamento automatizzato di dati personali, affinché siano prese in considerazione le esigenze della protezione dei dati. Gli organi federali

[59] Nella sentenza del 16 luglio 2020 nella causa C-311/18 («Schrems II»), la Corte europea ha stabilito che le garanzie appropriate devono essere tali da assicurare un livello di protezione equivalente (vale a dire: adeguato) a quello garantito nell'UE (n. mag. 96).

dovranno coordinare le regola da seguire nel valutare l'impatto sulla protezione dei dati con i processi esistenti, segnatamente con quello del metodo di gestione dei progetti Hermes.

In futuro si intende **coordinare** la valutazione d'impatto **con la procedura legislativa**: se il trattamento di dati da parte di un organo federale richiede l'emanazione o la modifica di una base legale e vi sono le condizioni per una valutazione d'impatto sulla protezione dei dati, quest'ultima va allegata alla proposta per il Consiglio federale insieme al disegno di legge (ed eventualmente al parere dell'IFPDT). L'esito della valutazione d'impatto (e un eventuale parere dell'IFPDT) vanno inoltre pubblicati nel messaggio del Consiglio federale.

4.4 Adeguamenti terminologici

4.4.1 Incaricato federale della protezione dei dati e della trasparenza

Per la denominazione «Incaricato federale della protezione dei dati e della trasparenza», la revisione totale della nLPD introduce nuove abbreviazioni, usate anche nelle pertinenti disposizioni delle leggi speciali:

- l'**autorità** «Incaricato federale della protezione dei dati e della trasparenza» viene abbreviata in «IFPDT» (cfr. art. 4 cpv. 1 nLPD); mentre
- la **persona fisica**, ossia il «capo dell'IFPDT», è designata con il termine «Incaricato» (cfr. art. 43 cpv. 1 nLPD).

Esempio: modifica della legge sul Parlamento al numero 12 dell'allegato 1/II della nLPD (nLParl)

Art. 40*a* cpv. 1 lett. d nLParl: «La Commissione giudiziaria è competente per la preparazione dell'elezione e della destituzione: *del capo dell'Incaricato federale della protezione dei dati e della trasparenza (Incaricato)*».

Art. 142 cpv. 2 nLParl: «[Il Consiglio federale] riprende nel suo disegno di preventivo e nel consuntivo della Confederazione, senza modificarli, i progetti di preventivo e i consuntivi dell'Assemblea federale, dei tribunali della Confederazione, del Controllo federale delle finanze, del Ministero pubblico della Confederazione, dell'autorità di vigilanza sul Ministero pubblico della Confederazione e dell'*Incaricato federale della protezione dei dati e della trasparenza (IFPDT)*».

4.4.2 Detentore di una collezione di dati / collezione di dati

- Il concetto di «**detentore di una collezione di dati**» viene sostituito con «**titolare del trattamento**»: cfr. in merito n. 4.1.
- Inoltre la nLPD rinuncia al concetto di «**collezione di dati**». La legge attuale, nella quale è la collezione di dati a determinare svariati diritti e obblighi (p. es. il diritto d'accesso secondo l'art. 8 LPD), definisce il concetto come «ogni complesso di dati personali la cui struttura permette di ricercare i dati secondo le persone interessate» (art. 3 lett. g LPD). Questa definizione risale a un tempo in cui le collezioni di dati erano costituite prevalentemente da sistemi di schede e archivi di raccoglitori. Considerate le odierne possibilità tecnologiche (di ricerca), si parte dall'idea che praticamente ogni archivio elettronico costituisca una raccolta di dati ai sensi della LPD. Pertanto il concetto di «collezione di dati» risulta obsoleto. In futuro la responsabilità in materia di protezione dei dati sarà quindi vincolata al trattamento dei dati personali. Nell'allegato 1/II della nLPD, il concetto «raccolta di dati» è stato eliminato in modo sistematico dalle disposizioni settoriali a protezione dei dati e sostituito da espressioni adeguate al contesto.

  Esempi: trattare (...) dati personali, (attività di) trattamento, banca dati, infrastruttura elettronica, sistema d'informazione.

Il concetto di collezione di dati va assolutamente evitato anche nelle nuove disposizioni sulla protezione dei dati e in quelle da rivedere.

4.4.3 Dati relativi a perseguimenti o sanzioni amministrativi e penali

La modernizzazione della terminologia nell'articolo 5 lettera c numero 5 nLPD (definizione di «dati degni di particolare protezione») riguarda solo la versione tedesca. Invece di «*Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen*» (art. 3 lett. c n. 4 LPD) si parlerà ora di «*Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen*». Questo adeguamento va considerato anche nelle disposizioni a protezione dei dati nelle leggi speciali.

Esempi: art. 65 cpv. 2, art. 101 cpv. 1 e art. 110 della legge riveduta sui giochi in denaro (n. 90 dell'Allegato 1/II della nLPD).

4.5 Panoramica degli ulteriori contenuti della revisione totale della LPD

Oltre alle modifiche sopra esposte, particolarmente rilevanti per i progetti legislativi dell'Amministrazione federale, la revisione totale della LPD contiene numerose altre novità per la protezione dei dati (panoramica sommaria, non esaustiva).

- **Campo d'applicazione della nLPD**
  - *Campo d'applicazione materiale*
    - Con la revisione totale, il **trattamento dei dati concernenti persone giuridiche** non rientra più nel campo d'applicazione materiale della LPD: ► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**.
    - Per i procedimenti (pendenti) retti dal diritto civile, penale, pubblico e amministrativo nonché le procedure di assistenza giudiziaria internazionale non è più prevista alcuna eccezione relativa al campo d'applicazione della nLPD. L'articolo 2 capoverso 3 nLPD disciplina invece il **rapporto tra diritto processuale e LPD**: il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali sono retti dal diritto processuale applicabile. Le disposizioni della nLPD si applicano (come finora) alle procedure amministrative di primo grado. Cfr. in merito le spiegazioni contenute nel messaggio del 15 settembre 2017 ► FF **2017** 5939, 6005 e seguenti. Per le eccezioni alla vigilanza dell'IFPDT cfr. l'articolo 4 capoverso 2 lettere c–e nLPD.
    - Anche per i **registri pubblici relativi ai rapporti di diritto privato**, la nLPD non prevede più eccezioni al campo d'applicazione della nLPD. L'articolo 2 capoverso 4 nLPD prevede, però, che questi registri (in particolare l'accesso a tali registri e i diritti delle persone interessate) sono retti dalle disposizioni speciali del diritto federale applicabile. In assenza di disposizioni speciali si applica la nLPD. Cfr. in merito le spiegazioni contenute nel messaggio del 15 settembre 2017 del Consiglio federale ► FF **2017** 5939, 6007 e seguente. I registri pubblici relativi a rapporti di diritto privato gestiti da organi federali sono ora soggetti alla vigilanza dell'IFPDT (art. 4 cpv. 1 nLPD).
  - *Campo d'applicazione territoriale*: nell'articolo 3 nLPD il Parlamento ha specificato il **campo d'applicazione territoriale** della nLPD. Questa disposizione non dovrebbe però comportare modifiche materiali. Per le *disposizioni a protezione dei dati nel diritto privato e penale*, l'articolo 3 capoverso 2 nLPD rimanda a titolo dichiaratorio alle norme di conflitto attualmente contemplate nella legge sul diritto internazionale privato (art. 139

LDIP) e nel Codice penale (art. 3 segg. CP). Per le *disposizioni a protezione dei dati nel diritto pubblico* (inclusa la vigilanza da parte dell'IFPDT), l'articolo 3 capoverso 1 nLPD stabilisce che la nLPD si applica alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero. Anche questa disposizione non è nuova di per sé, ma codifica soltanto la prassi giudiziaria in merito al principio della territorialità e degli effetti nel diritto pubblico[60].

– *Campo d'applicazione personale*: nessuna modifica.

  Come in passato, la nLPD si applica al trattamento di dati personali da parte di *privati e organi federali* (art. 2 cpv. 1 lett. a e b nLPD). Per organi federali si intendono autorità o servizi della Confederazione, oppure persone cui sono affidati compiti federali (art. 5 lett. i nLPD). Il trattamento dei dati da parte di autorità comunali e cantonali sottostà al diritto cantonale in materia, a prescindere che le autorità si siano procurate i dati direttamente o accedendo online a una banca dati della Confederazione. Anche il trattamento di dati da parte di organi cantonali nell'esecuzione del diritto federale è essenzialmente retto dal diritto cantonale[61]. Alcuni settori di competenza della Confederazione – ad esempio le assicurazioni sociali – conoscono una normativa particolare a tutela dei dati, applicabile sia alle autorità federali competenti che alle autorità cantonali incaricate di eseguire il diritto federale. La Confederazione deve tuttavia tenere conto del diritto organizzativo cantonale[62].

- **Registro delle attività di trattamento anziché collezioni di dati**: in futuro i responsabili privati e gli organi federali dovranno tenere un registro delle proprie attività di trattamento. Gli organi federali dovranno inoltre notificare questi registri all'IFPDT (art. 12 cpv. 1 e 4 nLPD), che dovrà tenere un registro pubblico in merito (art. 56 nLPD).

  Il registro delle attività di trattamento sostituisce la vecchia notifica all'IFPDT delle collezioni di dati (art. 11*a* LPD). Il contenuto minimo del registro è stabilito nell'articolo 12 capoversi 2 e 3 nLPD (risp. titolari e responsabili del trattamento). Le informazioni che devono essere inserite nel registro delle attività di trattamento dei titolari sono leggermente maggiori rispetto a quanto avviene oggi per la notifica delle raccolte di dati. Devono ad esempio essere indicati non solo lo scopo del trattamento e le categorie di dati personali trattati e di destinatari, bensì – se possibile – anche la durata di conservazione, i provvedimenti tesi a garantire la sicurezza dei dati ed eventuali garanzie in caso di comunicazione dei dati all'estero.

  Diversamente da quanto vale per i responsabili privati (art. 12 cpv. 5 nLPD e art. 24 OPDa), per gli organi federali la nLPD non prevede eccezioni all'obbligo di tenere un registro. Per esentare un organo federale dall'obbligo di tenere un registro delle attività di trattamento o di notificarlo all'IFPDT occorre una disposizione nella pertinente legge speciale.

  Esempi: art. 11 cpv. 2 della legge sulla geoinformazione (n. 41 dell'Allegato 1/II della nLPD) nonché art. 99 cpv. 3 lett. d e 100 cpv. 4 lett. c n. 2 della legge militare (n. 40 dell'Allegato 1/II della nLPD).

- **Ampliamento degli obblighi dei titolari del trattamento**

  – *Obbligo d'informare sulla raccolta di dati personali*: con la revisione totale della LPD l'obbligo di informare viene esteso alla raccolta *di tutti i tipi di dati personali* (art. 19 cpv. 1 nLPD). Per gli organi federali questa non è una novità (cfr. art. 18*a* LPD). La modifica riguarda soprattutto i responsabili privati, che attualmente devono informare solo sulla raccolta di dati degni di particolare protezione o profili della personalità. Come

[60] Cfr. per il diritto in materia di protezione dei dati DTF **138** II 346 nella causa «Google Street View».

[61] Con la revisione totale della LPD viene abrogato il vecchio art. 37 cpv. 1 LPD, secondo cui il trattamento di dati personali da parte di organi cantonali che agiscono in applicazione del diritto federale è disciplinato dagli articoli 1–11*a*, 16, 17, 18–22 e 25 capoversi 1–3 LPD, nella misura in cui non esistono prescrizioni cantonali sulla protezione dei dati che garantiscano una protezione adeguata.

[62] Cfr. il rapporto del 22 dicembre 2010 del Consiglio federale «Scambio di dati personali tra autorità federali e cantonali» stilato in adempimento del postulato Lustenberger 07.3682 (FF **2011** 593, 601 seg.).

finora, l'obbligo di informare sussiste anche se i dati sono raccolti non presso l'interessato ma presso terzi. Secondo l'articolo 19 capoverso 2 periodo introduttivo nLPD, alla persona interessata devono essere fornite tutte le informazioni necessarie affinché questa possa far valere i propri diritti secondo la nLPD e sia garantito un trattamento trasparente dei dati. L'articolo 19 capoverso 2 lettere a–c, capoversi 3 e 4 nLPD concretizza tale principio indicando diverse informazioni che vanno fornite, permettendo di gestire l'obbligo d'informare in modo flessibile e in base al rischio. L'articolo 20 nLPD prevede poi *eccezioni all'obbligo di informare e limitazioni*. Per gli organi federali è importante soprattutto l'articolo 20 capoverso 1 lettera b nLPD, secondo cui l'obbligo di informare non sussiste se il trattamento dei dati personali è previsto dalla legge. È quindi essenziale che la persona interessata possa evincere dalle basi legali le grandi linee del trattamento (► n. 2).

- *Valutazione d'impatto sulla protezione dei dati:* ► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**.

- *Obbligo di notificare violazioni della sicurezza dei dati*: secondo l'articolo 24 capoverso 1 nLPD, ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata deve essere notificata quanto prima all'IFPDT. In determinate circostanze vanno informate direttamente anche le persone interessate (art. 24 cpv. 4 nLPD). La violazione della sicurezza dei dati è definita nell'articolo 5 lettera h nLPD come una «violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate».

- *Obblighi particolari per le decisioni individuali automatizzate*: ► n. 2.2.1 lett. c).

- **Diritti delle persone interessate**

  - *Diritto d'accesso*: previsto all'articolo 25 e seguenti nLPD, corrisponde in larga misura all'attuale articolo 8 e seguenti LPD. Viene tuttavia ampliato l'*elenco delle informazioni da fornire* (art. 25 cpv. 2 nLPD). In futuro andranno fornite informazioni anche sulla durata di conservazione dei dati personali o, se ciò non è possibile, sui criteri per stabilire tale durata (lett. d), nonché sull'eventuale presenza di una decisione individuale automatizzata (► n. 2.2.1 lett. c)/cc) e sulla logica su cui si basa tale decisione (lett. f). Nuova è anche l'*eccezione al diritto d'accesso* di cui all'articolo 26 capoverso 1 lettera c nLPD, secondo cui il diritto d'accesso può essere rifiutato, limitato o differito se la domanda d'accesso è manifestamente infondata, segnatamente se persegue uno *un obiettivo estraneo alla protezione dei dati*, o se è querulosa. Secondo la giurisprudenza del Tribunale federale persegue un obiettivo estraneo alla protezione dei dati, ad esempio, chi abusa del diritto per procurarsi informazioni su una possibile controparte o per risparmiarsi i costi della raccolta di prove[63].

  - *Portabilità dei dati*: il Parlamento ha introdotto nell'articolo 28 e seguente nLPD il diritto di farsi consegnare dati o di esigerne la trasmissione a terzi (cosiddetta portabilità dei dati). Secondo l'articolo 28 capoverso 1 nLPD, la persona interessata può esigere che i dati personali che la concernono e che ha comunicato al titolare del trattamento le siano consegnati in un formato elettronico usuale. Se non richiede un onere sproporzionato, la persona interessata può inoltre esigere che il titolare trasmetta a un altro titolare i dati personali che la concernono. Poiché entrambe le pretese sussistono sol-

[63] Cfr. DTF **138** III 425 consid. 5.4 seg.

tanto nel caso di dati il cui trattamento è effettuato con il consenso della persona interessata oppure in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare e la persona interessata, si presume che il diritto alla portabilità troverà applicazione soprattutto nel settore del diritto privato. Le restrizioni del diritto di farsi consegnare i dati o di esigerne la trasmissione a terzi sono disciplinate nell'articolo 29 nLPD.

  - *Ulteriori pretese* sono contenute negli articoli 37 (opposizione alla comunicazione di dati personali) e 41 nLPD (p. es. diritto alla cancellazione e alla distruzione di dati personali trattati in modo illecito). Queste pretese corrispondono in larga parte al diritto vigente (art. 20 e 25 nLPD). Nuovo è invece il diritto a limitare il trattamento di dati (art. 41 cpv. 3 nLPD). Cfr. per le ulteriori modifiche il messaggio del 15 settembre 2017: ► FF **2017** 5939, 6070 e seguenti.

- **Vigilanza sulla protezione dei dati (IFPDT)**
  - **Elezione del capo dell'IFPDT**: secondo il diritto vigente, il capo dell'IFPDT (► n. **Fehler! Verweisquelle konnte nicht gefunden werden.**) deve essere nominato dal Consiglio federale e la sua nomina deve essere approvata dall'Assemblea federale (art. 26 cpv. 1 LPD); in futuro, invece, l'elezione competerà esclusivamente all'Assemblea federale (art. 43 cpv. 1 nLPD). Questo implica diversi adeguamenti in termini di diritto organizzativo e del personale, ad esempio per quanto riguarda il preventivo dell'IFPDT (art. 45 nLPD). Inoltre l'Assemblea federale ha emanato un'ordinanza concernente il rapporto di lavoro del capo dell'Incaricato federale della protezione dei dati e della trasparenza (► FF **2022** 348; cfr. in merito l'iniziativa parlamentare 21.443 della CIP-N). L'IFPDT continuerà però a essere un'unità amministrativa decentralizzata (priva di personalità giuridica), aggregata amministrativamente alla Cancelleria federale (art. 43 cpv. 4 nLPD, art. 2 cpv. 3 LOGA nonché art. 7*a* cpv. 1 lett. b e allegato 1 lett. A n. 2.1.1 dell'ordinanza sull'organizzazione del Governo e dell'Amministrazione).
  - **Inchiesta per violazione delle disposizioni sulla protezione dei dati**: la revisione totale della LPD rafforza le competenze di vigilanza dell'IFPDT, che in futuro dovrà aprire, d'ufficio o su denuncia, un'inchiesta nei confronti di un organo federale o di un privato, se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati (art. 49 cpv. 1 nLPD). Rispetto a oggi, questo comporta una maggiore facoltà di intervenire, soprattutto nei confronti di responsabili privati (cfr. art. 29 cpv. 1 LPD, che presuppone per gli accertamenti da parte dell'IFPDT nel settore privato tra l'altro un errore di sistema). Tuttavia l'IFPDT può rinunciare ad aprire un'inchiesta se la violazione è di poca importanza (art. 29 cpv. 2 nLPD). L'articolo 50 nLPD amplia gli strumenti a disposizione dell'IFPDT per l'accertamento dei fatti nel caso in cui il responsabile del trattamento (organo federale o privato) non ottemperi al proprio obbligo di cooperare. Secondo l'articolo 51 nLPD, se sono state violate le disposizioni sulla protezione dei dati, in futuro l'IFPDT potrà **ordinare** provvedimenti amministrativi (e non semplicemente formulare una raccomandazione). Questo vale sia per i responsabili privati che per gli organi federali. La procedura d'inchiesta e le decisioni dell'IFPDT sono rette dalla PA (art. 52 cpv. 1 nLPD).
  - **Attività legislativa**: come finora, l'IFPDT continuerà a rivestire grande importanza anche in sede legislativa. Secondo l'articolo 58 capoverso 1 lettera e nLPD, l'IFPDT si pronuncia sui progetti di atti normativi e sui provvedimenti della Confederazione implicanti il trattamento di dati.
- **Ampliamento delle disposizioni penali**: l'articolo 60 e seguenti nLPD amplia le fattispecie penali rilevanti per il diritto in materia di protezione dei dati e aumenta il tetto massimo delle multe per violazioni, portandolo da 10 000 franchi a 250 000 franchi. Da rilevare in particolare il nuovo articolo 63 nLPD, che punisce l'inosservanza intenzionale di decisioni

dell'IFPDT, conferendogli quindi una specie di potere di sanzione «indiretto». L'IFPDT può inoltre sporgere denuncia presso l'autorità di perseguimento penale competente e avvalersi nel procedimento dei diritti dell'accusatore privato (art. 65 cpv. 2 nLPD). Queste misure non sono però rilevanti per gli organi federali, poiché le disposizioni penali della nLPD si applicano soltanto ai responsabili privati (come in precedenza con la LPD).