GUIDA DI LEGISLAZIONE – PROTEZIONE DEI DATI

La nuova legge sulla protezione dei dati e i suoi effetti sui lavori legislativi

Berna, agosto 2022

Ultimo aggiornamento: marzo 2024

Indice

Introduzione ... 3
A) Contesto ... 3
B) Rimandi alla Guida di legislazione, al metodo di gestione dei progetti HERMES e alla valutazione d'impatto sulla protezione dei dati ... 3
I Quadro costituzionale ... 4
1.1 Diritto all'autodeterminazione informativa ai sensi dell'articolo 13 capoverso 2 Cost. e dell'articolo 8 CEDU ... 4
1.2 Ripartizione costituzionale delle competenze ... 5
II Quadro legale, concetti, principi ... 5
2.1 Osservazioni preliminari ... 5
2.2 Campo di applicazione personale e materiale ... 7
2.3 Concetti ... 7
2.3.1 Dati personali ... 8
2.3.2 Dati personali degni di particolare protezione ... 8
2.3.3 Profilazione ... 8
2.3.4 Decisione individuale automatizzata ... 9
2.3.5 Processo decisionale individuale assistito da intelligenza artificiale ... 9
2.3.6 Trattamento di dati ... 10
2.3.7 Titolare del trattamento ... 10
2.3.8 Responsabile del trattamento ... 11
2.3.9 Terzi ... 11
2.3.10 Attività di trattamento ... 11
2.4 Principi ... 11
III Domande da porsi nella fase concettuale di un progetto normativo ... 13
3.1 Osservazioni preliminari e requisiti del principio della legalità ... 13
3.1.1 Requisiti imposti dal principio della legalità ... 13
3.1.2 Comunicazione dei dati e principio della legalità ... 14
3.1.3 Architettura informatica e principio della legalità ... 14
3.1.4 Obbligo di informare e principio della legalità ... 15
3.1.5 Sistemi di gestione degli affari ... 16
3.1.6 Progetti pilota ... 17
3.2 Livello normativo (legge in senso formale / ordinanza) e densità normativa ... 17
3.2.1 Trattamento di dati degni di particolare protezione ... 17
3.2.2 Profilazione (art. 34 cpv. 2 lett. b LPD) ... 18
3.2.3 Rischio di una grave ingerenza nei diritti fondamentali a causa dello scopo o del tipo di trattamento previsto (art. 34 cpv. 2 lett. c LPD) ... 19
3.2.4 Comunicazione e consultazione di dati personali ... 20
3.2.5 Comunicazione all'estero ... 22
3.3 Delega di competenze legislative ... 24
IV Lista di controllo ... 26

Introduzione

A) Contesto

Questo documento, che subentra alla ormai obsoleta Guida del 16 dicembre 2010 per l'elaborazione delle basi legali necessarie per l'esercizio di un sistema di trattamento automatizzato dei dati personali, fornisce una risposta sintetica alle seguenti domande: come elaborare le basi legali indispensabili agli organi federali per trattare i dati delle persone fisiche nel rispetto della nuova legge federale sulla protezione dei dati (LPD; cfr. n. 2.1 *infra*)[1], così come risulta dalla revisione totale della legge precedente? Quali sono i principi, rimasti invariati, in materia di protezione dei dati? Si tratta del riepilogo di una nota esaustiva dell'Ufficio federale di giustizia (UFG) intitolata *Revisione totale della legge sulla protezione dei dati. Elaborazione di basi legali per il trattamento dei dati da parte di organi federali: sinossi delle modifiche principali* (*«Nota UFG/LPD»*), cui fa riferimento.

Come quella precedente, anche la presente guida è un ausilio tra tanti destinato ai giuristi incaricati di redigere le basi legali indispensabili agli organi federali per trattare i dati delle persone fisiche. Illustra gli elementi di cui tener conto nello stilare le normative del caso, ma non copre tutti gli aspetti inerenti alla protezione dei dati. Non approfondisce in particolare alcuni punti molto importanti come la sicurezza dei dati, che non comporta per forza disposizioni specifiche, pur richiedendo, in particolare, provvedimenti tecnici e organizzativi secondo l'articolo 3 dell'ordinanza del 31 agosto 2022[2] sulla protezione dei dati (OPDa).

B) Rimandi alla Guida di legislazione, al metodo di gestione dei progetti HERMES e alla valutazione d'impatto sulla protezione dei dati

Le esigenze in materia di protezione dei dati vanno analizzate già nella fase iniziale di un progetto di legge. Non di rado occorre modificare le basi legali o crearne nuove. La presente Guida illustra gli aspetti principali in materia, andando quindi a integrare la procedura proposta nella Guida di legislazione[3].

Inoltre il metodo HERMES[4], seguito alla Confederazione soprattutto in ambito informatico, prevede l'allestimento di un piano SIPD (sicurezza dell'informazione e protezione dei dati)[5]. La presente Guida può rivelarsi utile nel definire i requisiti in materia di protezione dei dati, valutare i rischi e stabilire le misure per allestire il piano SIPD.

Valutare l'impatto sulla protezione dei dati è necessario quando il trattamento dei dati personali può comportare un rischio elevato per la personalità o i diritti fondamentali della

---

1 Il nuovo testo è entrato in vigore il 1° settembre 2023.

2 Ordinanza sulla protezione dei dati, OPDa; RS **235.11**.

3 La versione elettronica del capitolo 14 della Guida di legislazione consacrato alla protezione dei dati è stata aggiornata nell'ottobre 2023: UFG, Guida di legislazione, 1a ed. italiana, 2019 Strumenti di legistica (admin.ch).

4 https://www.hermes.admin.ch/it/, Panoramica del metodo (admin.ch)

5 Elaborare il piano SIPD (admin.ch)

persona (art. 22 LPD). Il 28 giugno 2023[6] il Consiglio federale ha emanato le direttive per l'esame preliminare dei rischi e la valutazione d'impatto sulla protezione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale (direttive VIPD). Sul sito dell'UFG sono disponibili altri documenti utili, come lo strumento per l'esame preliminare dei rischi[7], la guida VIPD[8] e le FAQ sul diritto in materia di protezione dei dati[9].

I Quadro costituzionale

1.1 Diritto all'autodeterminazione informativa ai sensi dell'articolo 13 capoverso 2 Cost. e dell'articolo 8 CEDU

Il diritto all'autodeterminazione informativa, sancito nell'articolo 13 capoverso 2 della Costituzione federale (Cost.)[10] e nell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)[11], conferisce all'individuo una specie di padronanza sui propri dati personali[12]. Pertanto l'articolo 13 capoverso 2 Cost. non si limita a tutelare la persona dall'*«impiego abusivo»* dei suoi dati, come lascia supporre il testo costituzionale, ma comprende ogni attività statale volta a trattare dati personali, ad esempio a rilevarli, conservarli o comunicarli[13]. In materia di protezione dei dati, il diritto costituzionale all'autodeterminazione informativa (art. 13 cpv. 2 Cost. e 8 n. 1 CEDU) garantisce al singolo di rimanere padrone dei propri dati, indipendentemente dal grado di sensibilità delle informazioni in questione[14]. Si tratta di un diritto fondamentale, la cui restrizione deve adempire i requisiti costituzionali della base legale, dell'interesse pubblico, della proporzionalità e dell'intangibilità dell'essenza dei diritti fondamentali (art. 36 Cost.)[15]. Le restrizioni gravi dei diritti fondamentali devono essere previste da una legge in senso formale (art. 36 cpv. 1 secondo periodo Cost.). Chi redige un atto normativo che comporta o disciplina il trattamento di dati personali è tenuto a provvedere al rispetto di tali requisiti costituzionali e di quelli convenzionali imposti

---

6 Direttive del Consiglio federale (FF **2023** 1882)

7 Strumento per l'esame preliminare dei rischi

8 Guida VIPD

9 FAQ sul diritto in materia di protezione dei dati, UFG, settembre 2023

10 RS **101**

11 RS **0.101**

12 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, Helbing Lichtenhahn, 2021, pag. 44–63 [47–48] e la giurisprudenza citata.

13 DTF **128** II 259 consid. 3.2.

14 DTF **138** II 346 consid. 8.2 (ted.) o DTF **140** I 381 consid. 4.1 (fra.); cfr. anche la nota UFG/LPD, n. 2.1.

15 Riguardo alla restrizione dei diritti fondamentali, cfr. Guida di legislazione, n. marg. 688.

dall'articolo 8 CEDU[16] (anche quando la LPD non si applica, come nei casi in cui i dati sono trattati da organi pubblici cantonali)[17].

1.2 Ripartizione costituzionale delle competenze

La Costituzione federale non autorizza esplicitamente la Confederazione a legiferare in materia di protezione dei dati. La Confederazione può emanare norme a protezione dei dati soltanto fondandosi su disposizioni costituzionali che le conferiscono competenze legislative in un determinato ambito, ad esempio in materia di assicurazioni sociali (assicurazioni per la vecchiaia, i superstiti e l'invalidità, contro la disoccupazione, contro le malattie e gli infortuni). Tuttavia, laddove la Costituzione federale attribuisce alla Confederazione competenze legislative in un determinato ambito, può sorgere l'obbligo, per il legislatore federale, di emanare disposizioni specifiche in materia di protezione dei dati, applicabili anche alle autorità cantonali incaricate di eseguire il diritto federale, ad esempio nel settore delle assicurazioni sociali.

Incombe ai Cantoni legiferare sulla protezione dei dati nei settori di loro competenza[18]. Fatte salve eventuali disposizioni di leggi federali speciali, il trattamento di dati da parte di organi cantonali (e comunali) è retto dal diritto cantonale, anche quando tali organi eseguono il diritto federale o hanno ottenuto i dati accedendo online a una banca dati della Confederazione[19].

II Quadro legale, concetti, principi

2.1 Osservazioni preliminari

La legge federale del 25 settembre 2020 sulla protezione dei dati (LPD) subentra alla legge federale del 19 giugno 1992 sulla protezione dei dati (vLPD o legge del 1992)[20]. La revisione intende perfezionare gli strumenti per affrontare le sfide poste dalle nuove tecnologie, migliorando la trasparenza del trattamento di dati[21] e rafforzando il diritto costituzionale

---

16 In merito alla durata di conservazione dei dati personali, cfr. sentenza Corte EDU del 24 gennaio 2019 *Catt contro il Regno Unito*, n. 43514/15.

17 Cfr. la nota UFG/LPD, n. 2.1, e i rimandi alla dottrina e alla giurisprudenza riguardanti i diritti costituzionali risultanti dall'art. 13 cpv. 2 Cost., in particolare il diritto di sapere che esistono dati personali, di consultarli e di farli rettificare se inesatti.

18 Scambio di dati personali tra autorità federali e cantonali. Rapporto del 5 ottobre 2007 del Consiglio federale in adempimento del postulato Lustenberger 07.3682 *«Agevolazione dello scambio di dati tra autorità federali e cantonali»*, FF **2011** 593.

19 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939 pag. 5951 (Messaggio sulla revisione totale della LPD); cfr. anche la nota UFG/LPD, n. 4.5, e il citato rapporto del Consiglio federale in adempimento del postulato Lustenberger, n. 2.1, FF **2011** 593.

20 Subentra anche alla legge del 28 settembre 2018 sulla protezione dei dati in ambito Schengen, RS **235.3**, cfr. nota a piè di pagina n. 22.

21 Messaggio sulla revisione totale della LPD, FF **2017** 5941, cfr. Tuttavia Bertil COTTIER, *Transparence des traitements de données personnelles opérés par les organes fédéraux : un pas en avant, deux en arrière* (RSDA 2021 pag. 65 segg., 65) in cui si afferma: *« Le présent projet de loi vise à renforcer la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs*

all'autodeterminazione informativa. La LPD riprende i concetti e i principi consolidati; non conferisce nuove competenze alla Confederazione, preservando quindi la sovranità cantonale fatte salve le citate disposizioni federali materiali settoriali (cfr. n. 1.2).

Il diritto svizzero deve adempire i requisiti per lo sviluppo dell'acquis di Schengen, e in particolare la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali in ambito Schengen[22].

Le basi legali settoriali in materia di protezione dei dati devono comunque adempire i requisiti della versione aggiornata della Convenzione 108+ del Consiglio d'Europa sulla protezione dei dati[23], che la Svizzera ha ratificato il 7 settembre 2023 e che entrerà in vigore se sarà ratificata da almeno 38 Stati[24].

La Svizzera beneficia inoltre di una decisione di adeguatezza dell'Unione europea, che la riconosce come Stato terzo dotato di un livello adeguato di protezione dei dati, consentendo quindi il trasferimento agevolato dei dati[25]. Ecco perché è indispensabile che la legislazione svizzera in materia di protezione dei dati, compreso il diritto settoriale, rispetti lo standard previsto dal Regolamento generale dell'Unione europea sulla protezione dei dati (Regolamento [UE] 2016/679, GDPR). Nel suo rapporto del 15 gennaio 2024 la Commissione europea ha stabilito che il diritto svizzero in materia di protezione dei dati continua a soddisfare gli standard europei[26].

---

données.› Autant dire qu'à l'entame de son message à la révision totale de la loi sur la protection des données, le Conseil fédéral exprime sans détours ses intentions : une des priorités de la nouvelle loi sera d'accroitre la visibilité des traitements de données personnelles. La révision de la loi fédérale sur la protection des données enfin sous toit, il y a lieu de se demander si cet objectif fondamental a réellement été atteint. C'est sans ambages que l'on répondra oui s'agissant des traitements opérés par des personnes privées ; et ce, en raison avant tout de l'ampleur du devoir d'information désormais à la charge du responsable du traitement. Pour ce qui concerne les traitements opérés par des organes fédéraux, la réponse est en revanche mitigée. Certes, des coups de projecteurs bienvenus ont été apportés ici ou là : intelligibilité des décisions automatisées, extension du droit d'accès et annonce des violations de la sécurité des données notamment. Ces avancées ponctuelles ne sauraient toutefois masquer un recul majeur : la révision a affaibli le devoir d'information des autorités fédérales ».

22 Il Parlamento ha suddiviso in due tappe la proposta iniziale del Consiglio federale per la revisione della LPD. In un primo tempo è stata attuata soltanto la direttiva (UE) 2016/680 sulla protezione dei dati in materia penale (cfr. p. es. il rapporto esplicativo alla legge federale che attua la direttiva [UE] 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali [Sviluppo dell'acquis di Schengen]). La legge federale sulla protezione dei dati personali nell'ambito dell'applicazione dell'acquis di Schengen in materia penale (Legge sulla protezione dei dati in ambito Schengen, LPDS) è entrata in vigore il 1° marzo 2019, mentre il Parlamento continuava a deliberare sulla revisione totale della LPD. La LPD abroga la LPDS e ne riprende il contenuto.

23 Protocollo di emendamento della Convenzione del 10 ottobre 2018 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 223).

24 La Suisse ratifie le Protocole d'amendement à la Convention 108 - Protection des données (coe.int; non disponibile in italiano); il 6 febbraio 2024 il protocollo era ratificato da 31 Paesi.

25 Procedura in vista di una decisione di adeguatezza, cfr. art. 45 GDPR.

26 Il 15 gennaio 2024 la Commissione europea ha pubblicato un rapporto sull'adeguatezza del livello di protezione dei dati in diversi Paesi terzi, in cui riconosce che la Svizzera continua a garantire una protezione adeguata dei dati personali, cfr. L'UE conferma l'adeguatezza della protezione dei dati in Svizzera (admin.ch).

2.2 Campo di applicazione personale e materiale

Lo scopo della LPD è proteggere la personalità e i diritti fondamentali delle persone i cui dati personali sono oggetto di trattamento (art. 1 LPD).

Il campo d'applicazione è stato circoscritto ai dati delle persone fisiche, con le eccezioni elencate come finora nell'articolo 2 e comprendenti, ad esempio, il trattamento di dati personali nei procedimenti giudiziari.

Per contro non rientrano più nel campo d'applicazione della LPD i dati delle persone giuridiche, il cui trattamento è ormai disciplinato nella legge sull'organizzazione del Governo e dell'Amministrazione (LOGA)[27], così come modificata dall'allegato 1/II LPD. Le persone giuridiche possono di fatto appellarsi all'articolo 13 capoverso 2 Cost.; questo significa in particolare che gli organi federali possono trattare o comunicare i dati delle persone giuridiche soltanto se esiste una base legale sufficiente. Nel corso della revisione totale della LPD, sono state introdotte nuove disposizioni nella legge sull'organizzazione del Governo e dell'Amministrazione per disciplinare il trattamento dei dati di persone giuridiche da parte di organi federali (art. 57*r* segg. LOGA). Inoltre, la disposizione transitoria dell'articolo 71 LPD dovrebbe prevenire eventuali lacune giuridiche per cinque anni[28].

I requisiti della LPD non si applicano se un organo federale intende trattare dati che non contengono informazioni riferite a una persona fisica identificata o identificabile. Nella sua valutazione l'organo federale tiene conto del rischio che dati materiali vengano collegati ad altri dati o a processi tecnici permettendo di risalire a una persona specifica.

2.3 Concetti

In virtù dei requisiti per la restrizione dei diritti fondamentali e del principio della legalità (art. 5 Cost.), gli organi statali possono trattare dati personali soltanto in presenza di una base legale[29] – a prescindere dal fatto che i dati siano o no degni di particolare protezione.

Le basi legali vanno create negli atti normativi settoriali, con la LPD che ne definisce i requisiti (art. 34 e 36 LPD). La LPD modifica alcuni concetti rispetto alla legge del 1992 (p. es. dati degni di particolare protezione) e introduce concetti nuovi (p. es. profilazione)[30].

---

27 RS **172.010**

28 Cfr. la nota UFG/LPD, n. 3 (e in particolare il n. 3.2).

29 Cfr. in merito la nota UFG/LPD, n. 2 (e in particolare il n. 2.1).

30 Cfr. in particolare i commenti seguenti sulla LPD: Bruno BAERISWYL, Kurt PÄRLI, Dominika BLONSKI, Stämpflis *Handkommentar SHK, Datenschutzgesetz (DSG), Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)*, 2a ed., 2023; Philippe MEIER, Sylvain MÉTILLE, *Commentaire romand sur la loi fédérale sur la protection des données*, Helbing Lichtenhahn, 2023; Yaniv BENHAMOU, Bertil COTTIER, *Petit commentaire LPD, Loi sur la protection des données*, Helbing Lichtenhahn, 2023; Adrian BIERI, Julian POWELL, *Orell Füssli Kommentar (OFK) DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen*, 2023; Thomas STEINER, Anne-Sophie MORAND, Daniel HÜRLIMANN (ed.), *Onlinekommentar zum Bundesgesetz über den Datenschutz* – versione del 25.08.2023: https://onlinekommentar.ch/de/kommentare/dsg43 (ultima consultazione il 12 dicembre 2023), DOI: 10.17176/20230825-103609-0.

2.3.1 Dati personali

Il concetto di dati personali resta invariato (art. 5 lett. a LPD): comprende tutte le informazioni relative a una persona identificata o identificabile. Il concetto va inteso in senso lato anche in futuro; tanto per fare un esempio, a determinate condizioni può considerarsi dato personale anche un indirizzo IP (= Internet Protocol, ossia l'identificativo assegnato a ogni computer che accede a Internet)[31].

In linea di massima[32] un organo federale è autorizzato a trattare e comunicare dati personali soltanto in presenza di una base legale (art. 5 cpv. 1 Cost.; art. 34 cpv. 1 LPD).

2.3.2 Dati personali degni di particolare protezione

L'elenco dei dati personali degni di particolare protezione viene esteso (art. 5 lett. c LPD). Da un lato riprende tutte le categorie di dati considerati degni di particolare protezione ai sensi della vLPD, ossia dati personali riguardanti le opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, i procedimenti o le sanzioni di natura amministrativa e penale, nonché le misure d'assistenza sociale.

Dall'altro comprenderà anche le seguenti categorie di dati[33]:

– dati che rivelano l'appartenenza a un'etnia;

– dati genetici;

– dati biometrici che identificano in modo univoco una persona fisica.

In linea di massima il trattamento dei dati degni di particolare protezione dev'essere previsto in una legge in senso formale (art. 34 cpv. 2 lett. a LPD; cfr. n. 3.2.1 *infra*).

2.3.3 Profilazione

La profilazione ai sensi della LPD è una forma particolare di trattamento automatizzato dei dati personali consistente nell'utilizzarli per valutare determinati aspetti personali di una persona fisica (art. 5 lett. f LPD). Metodi statistici e matematici, in particolare gli algoritmi, permettono di generare nuove informazioni su individui partendo da grosse quantità di dati, in sé magari nemmeno particolarmente informativi. Il concetto di profilazione va a sostituire quello del profilo della personalità contemplato nella legge del 1992 e dal quale comunque differisce: un profilo della personalità è il risultato di un trattamento, la profilazione è invece un metodo di trattamento[34], ossia una valutazione automatizzata di determinati aspetti di una persona fisica[35].

---

31 DTF **136** II 508 consid. 3; Philippe MEIER / Nicolas TSCHUMY, *L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !*, in: Jusletter del 23 gennaio 2017, n. marg. 22 segg.

32 Cfr. in merito la nota UFG/LPD, n. 2.1 (e in part. *Deroghe al requisito della base legale*).

33 Cfr. in merito il rapporto dell'UFG sulla revisione totale della LPD, n. 2 (e in particolare i n. 2.2 e 2.2.1 lett. a).

34 Cfr. in merito la nota UFG/LPD, n. 2.2.1 lett. b.

35 La profilazione è quindi una tecnica per analizzare e prevedere il comportamento umano, interpretando dati a mezzo di modelli matematici, i cosiddetti algoritmi, fondati su statistiche, analisi dei dati e probabilità. Questi modelli mirano a creare una correlazione tra talune caratteristiche personali e fattuali (input), da un lato, e un determinato stato o comportamento

Il Parlamento ha inoltre introdotto il concetto di profilazione a rischio elevato (art. 5 lett. g LPD), ossia quella che comporta elevati rischi per la personalità in quanto collega svariati dati permettendo di valutare aspetti essenziali della personalità[36]. Per gli organi federali la distinzione è comunque di poco conto: una profilazione da parte loro (a rischio elevato o no) richiede per principio una base legale in una legge formale (art. 34 cpv. 2 lett. b LPD; cfr. n. 3.2.2 *infra*). Andrebbero applicati requisiti particolari anche al trattamento e alla trasmissione di dati derivanti da profilazione (cfr. n. 3.2.4 *infra*)[37].

2.3.4 Decisione individuale automatizzata

La decisione individuale automatizzata ai sensi della LPD è una decisione basata esclusivamente su un trattamento di dati personali automatizzato che abbia effetti giuridici o conseguenze significative per l'interessato (art. 21 LPD).

Significa che la valutazione di un fatto e la decisione individuale che ne risulta è opera di una macchina, ossia di un algoritmo, senza l'intervento di una persona fisica[38]. In questi casi la macchina non è un semplice strumento o ausilio per la decisione (cfr. n. 2.3.5 *infra*)[39].

Solo le decisioni individuali automatizzate di una certa complessità sono considerate tali (non rientrano p. es. nella categoria i controlli d'accesso a uno stabile tramite badge)[40].

Il ricorso a una decisione automatizzata può (ma non deve) rientrare nelle fattispecie descritte all'articolo 34 capoverso 2 lettera c LPD (ossia considerarsi una forma di trattamento suscettibile di ledere gravemente i diritti fondamentali dell'interessato). In tal caso occorre una legge in senso formale.

2.3.5 Processo decisionale individuale assistito da intelligenza artificiale

La LPD non disciplina di per sé il processo decisionale individuale assistito da sistemi algoritmici («*intelligenza artificiale*»[41]). Non costituisce decisione individuale automatizzata ai

---

che si desidera prevedere, influenzare o addirittura imporre (output), dall'altro; cfr. Michael MONTAVON, *Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyenne-s et des autorités de contrôle*, Ginevra – Zurigo – Basilea 2021, pag. 639.

36 Sylvain MÉTILLE, *Le traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données vom 25. September 2021*, edizione speciale della Semaine judiciaire 2021 II 1, pag. 26.

37 In merito alla problematica del trattamento di dati (non per forza degni di particolare protezione) derivanti da profilazione, cfr. la nota UFG/LPD, n. 2.2 (e in part. n. 2.2.1, lett. b/dd).

38 In merito alla problematica dell'ammissibilità di decisioni individuali automatizzate in presenza di un margine discrezionale per l'autorità, cfr. la nota UFG/LPD, n. 2.2 (e in part. n. 2.2.1, lett. c/cc [cfr. spec. *Categoria 1: decisioni individuali automatizzate*]).

39 *Ibid*.

40 *Ibid*.

41 Il diritto svizzero non fornisce una definizione dell'intelligenza artificiale. A livello internazionale la tendenza è quella di utilizzare il concetto di "sistemi di intelligenza artificiale". Secondo il progetto di convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale, i diritti umani, la democrazia e lo Stato di diritto del 14 marzo 2024, si tratta di "un sistema informatico che deduce, a partire dai dati che riceve e in base a degli obiettivi espliciti o impliciti, come generare risultati quali previsioni, contenuti, raccomandazioni o decisioni in grado di influenzare ambienti materiali o virtuali. I diversi sistemi di intelligenza artificiale variano nei loro livelli di autonomia e adattabilità una volta implementati". Questo testo si basa sulla definizione aggiornata di "sistema di intelligenza artificiale" adottata dall'OCSE in data 8 novembre 2023 (si veda la Raccomandazione del Consiglio sull'intelligenza artificiale). La definizione corrisponde sostanzialmente a quella della proposta di regolamento UE sull'intelligenza artificiale (COM [2021] 206 final). In assenza di una definizione specifica, queste descrizioni possono essere utilizzate a titolo orientativo.

sensi dell'articolo 21 LPD la decisione preparata da una macchina, ma presa da un umano[42]. I quesiti giuridici sollevati nel contesto delle decisioni individuali automatizzate possono però sorgere per analogia anche nel caso delle decisioni individuali assistite da intelligenza artificiale[43].

Alla stregua di quanto descritto in precedenza, il ricorso all'*intelligenza artificiale* può (ma non deve) rientrare nelle fattispecie descritte all'articolo 34 capoverso 2 lettera c LPD (ossia considerarsi una forma di trattamento suscettibile di ledere gravemente i diritti fondamentali dell'interessato). In tal caso occorre una legge in senso formale che lo preveda.

2.3.6 Trattamento di dati

La definizione ai sensi dell'articolo 5 lettera d LPD non subisce modifiche materiali sebbene ora comprenda esplicitamente anche la registrazione e la cancellazione di dati[44].

2.3.7 Titolare del trattamento

Il titolare del trattamento di cui all'articolo 5 lettera j LPD è il privato o l'organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento di dati personali, ossia i fattori e i rischi rilevanti ai sensi della LPD (p. es. categoria e fonte dei dati, durata e modalità del trattamento[45]).

Il concetto di titolare del trattamento va a sostituire quello di detentore di una collezione di dati. Come quest'ultimo fino ad ora, anche il titolare va designato con precisione nella legge settoriale; gli incombe infatti vegliare sul rispetto delle norme a protezione dei dati e garantire agli interessati il diritto d'accesso, elemento chiave della legislazione in materia di protezione dei dati[46].

Per fare un esempio, l'articolo 3 della legge federale sui sistemi d'informazione della Confederazione nel campo dello sport[47] recita:

> *«L'UFSPO è responsabile della sicurezza dei sistemi d'informazione e della legalità del trattamento dei dati.»*

Il Consiglio federale disciplina in un'ordinanza le procedure di controllo e la responsabilità in materia di protezione dei dati nei casi in cui un organo federale competente tratta dati personali congiuntamente ad altri organi federali, a organi cantonali o a privati (art. 33 LPD).

---

42 Cfr. in merito il rapporto dell'UFG sulla revisione totale della LPD, n. 2.2 (in particolare n. 2.2.1, lett. c/cc [cfr. spec.: *Categoria 2: decisioni assistite da intelligenza artificiale*]).

43 *Ibid*.

44 Messaggio sulla revisione totale della LPD, pag. 6012.

45 Cfr. in merito la nota UFG/LPD, n. 4 (e in part. il n. 4.1).

46 *« L'obligation d'information est complétée par le droit d'accès. Le droit d'accès est un élément clé du droit de la protection des données car il permet à la personne concernée de faire valoir les droits que lui octroie la loi »,* cfr. Sylvain MÉTILLE, *Le traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données*, edizione speciale della Semaine judiciaire 2021 II 1, pag. 30.

47 LSISpo; RS **415.1**

La LPD amplia determinati obblighi del titolare o gliene attribuisce nuovi (art. 19–24 LPD)[48], in particolare l'obbligo di valutare l'impatto quando il trattamento previsto dei dati rischia di ledere gravemente la personalità o i diritti fondamentali dell'interessato[49].

2.3.8 Responsabile del trattamento

Il responsabile del trattamento di cui all'articolo 5 lettera k LPD è il privato o l'organo federale che tratta dati personali per conto del titolare del trattamento.

Gli organi federali possono affidare per contratto o per legge il trattamento di dati personali a un responsabile del trattamento (art. 9 LPD), il che non li esime dall'obbligo di assumere la responsabilità in materia di protezione dei dati[50].

La responsabilità può d'altronde applicarsi anche ai servizi informatici che trattano dati nel cloud, il che comporta rischi particolari[51] e soprattutto richiede garanzie e misure tecniche e organizzative.

2.3.9 Terzi

Il concetto non è definito esplicitamente nella LPD. In pratica si tratta di un privato o di un organo federale o cantonale che non sia né titolare né responsabile del trattamento. Quest'ultimo non è più considerato un terzo, a differenza di quanto prevedeva la legge del 1992 (cfr. risp. art. 10*a* vLPD e 9 LPD *e contrario*)[52].

2.3.10 Attività di trattamento

Il concetto, introdotto all'articolo 12 LPD, va a sostituire quello di collezione di dati contemplato nella legge del 1992 (art. 11*a* vLPD). Gli organi federali devono tenere un registro delle loro attività di trattamento, da notificare all'IFPDT (art. 12 LPD).

2.4 Principi

La LPD riprende in sostanza i principi preesistenti, sancendo che ogni trattamento dei dati personali di una persona fisica deve rispettare i principi generali in materia di protezione dei dati (art. 6–8 LPD): liceità (art. 6 cpv. 1 LPD), buona fede (art. 6 cpv. 2 e 4 LPD),

---

48 Cfr. in merito la nota UFG/LPD, n. 1.2.

49 Cfr. in merito la nota UFG/LPD, n. 4.3, nonché il cap. Introduzione lett. B *supra* e le direttive del Consiglio federale del 28 giugno 2023 per l'esame preliminare dei rischi e la valutazione d'impatto sulla protezione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale (direttive VIPD), FF **2023** 1882.

50 Cfr. in merito la nota UFG/LPD, n. 4 (e in particolare il n. 4.1).

51 Cfr. Sylvain MÉTILLE, *Utilisation de l'informatique en nuage par l'administration publique*, AJP/PJA 6/2019, pag. 609 seg.; cfr. anche *Cloud Computing, Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Züri*ch, in: *Künstliche Intelligenz und Datenschutz*, Schulthess, 2021 pag. 65 segg.

52 Cfr. la nota UFG/LPD, n. 4 (e in particolare il n. 4.1).

proporzionalità (art. 6 cpv. 2 LPD), riconoscibilità (art. 6 cpv. 3 LPD), scopo (art. 6 cpv. 3 LPD), esattezza (art. 6 cpv. 5 LPD) e sicurezza dei dati (art. 8 LPD)[53].

La liceità verrà in genere verificata insieme al requisito della base legale che consente agli organi federali di trattare i dati personali.

La proporzionalità comprende il principio di minimizzazione dei dati, che impone al titolare di raccogliere e trattare soltanto i dati necessari allo scopo**.** I dati raccolti devono essere proporzionati alle esigenze del trattamento, in altre parole, *«le informazioni salvate devono essere pertinenti e indispensabili allo scopo della collezione di dati» [tradotto dal francese]*[54]. Il titolare deve tener conto di questo principio sin dalla pianificazione del trattamento.

Il principio della finalità non subisce modifiche materiali sostanziali[55], ma il tenore è conformato all'articolo 5 della versione aggiornata della Convenzione 108+ del Consiglio d'Europa sulla protezione dei dati (e del GDPR). L'articolo 6 capoverso 3 LPD prevede che i dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata e che possono essere trattati ulteriormente soltanto in modo compatibile con tale scopo. L'articolo 4 della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)[56], nella versione modificata dalla LPD[57], prevede ad esempio che determinate autorità specificate nella disposizione possono trattare soltanto i dati *«di cui necessitano per disporre, approvare e attuare la sorveglianza.»*

In particolare, la conservazione dei dati deve rispettare i principi della proporzionalità e della finalità. Il legislatore deve limitare la durata del trattamento a quanto necessario per l'adempimento di un determinato compito (e non a ciò che potrebbe essere utile), stabilendo una durata di conservazione[58].

Il messaggio del Consiglio federale parte dal principio che l'interessato è in linea di massima capace di riconoscere una determinata finalità prevista dalla legge[59]. Pertanto una legge può modificare in una certa misura la finalità originaria del trattamento dei dati, fermo restando il principio della buona fede.

L'articolo 96*d* della legge sull'assicurazione contro la disoccupazione[60] ad esempio recita:

---

53 Cfr. in merito la nota UFG/LPD, n. 2.1 (e in particolare *Requisiti in materia di densità normativa*).

54 Cfr. art. 5 lett. c GDPR; cfr. anche i cinque sommi principi della protezione dei dati secondo la Commission nationale de l'informatique et des libertés, Quels sont les grands principes des règles de protection des données personnelles = | Besoin d'aide | CNIL.

55 Messaggio sulla revisione totale della LPD, pag. 6016.

56 RS **780.1**

57 FF **2020** 6695, in particolare pag. 6765

58 Thomas HELD, Markus BRÖNIMANN, in: *Orell Füssli Kommentar (OFK) DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen*, 2023, ed. Adrian BIERI, Julian POWELL, ad art. 34 n. 9 -10 e la giurisprudenza citata.

59 Cfr. il messaggio sulla revisione totale della LPD, pag. 6016. *«Il trattamento ulteriore è ritenuto compatibile con le finalità iniziali anche nel caso in cui la modifica di tali finalità è prevista dalla legge, richiesta da una modifica legislativa o legittimata da un altro motivo giustificativo (p. es. il consenso della persona interessata).»*

60 LADI; RS **837.0**

«Sempre che vi siano autorizzati dal diritto cantonale, gli organi di esecuzione di cui all'articolo 76 capoverso 1 lettere a e c possono accedere mediante procedura di richiamo al registro degli abitanti per verificare il domicilio degli assicurati.»

La LPD introduce inoltre la protezione dei dati fin dalla progettazione[61] e per impostazione predefinita (art. 7 LPD). I due principi non sono del tutto nuovi (derivano in parte da quelli già applicabili, ossia proporzionalità e sicurezza dei dati).

III Domande da porsi nella fase concettuale di un progetto normativo

3.1 Osservazioni preliminari e requisiti del principio della legalità

Una volta inizializzato il progetto, le domande da porsi coincidono in parte con quelle che sorgevano già sotto la legge del 1992 al momento d'impostare una base legale per il trattamento di dati da parte di organi federali.

Il giurista deve in particolare chiedersi se è previsto trattare dati personali e/o dati degni di particolare protezione, analizzare la gravità della lesione dei diritti fondamentali ai danni degli interessati e determinare lo scopo del trattamento, considerando sempre i requisiti imposti dal principio della legalità (cfr. anche n. 2.3 *supra*).

Se non sono in discussione compiti statali nuovi, vale a dire se già esiste una base legale per trattare i dati necessari all'adempimento di tali compiti, va innanzi tutto analizzata la situazione *attuale* confrontandola con quella *auspicata* per appurare se la situazione specifica comporta nuovi trattamenti di dati e/o nuovi rischi per gli interessati. La risposta a tale domanda indica al giurista il livello normativo e la densità normativa delle basi legali da elaborare.

3.1.1 Requisiti imposti dal principio della legalità

Il principio della legalità esige che le norme giuridiche siano sufficientemente precise, ossia formulate con una precisione tale da permettere ai soggetti giuridici di conformarvisi e di riconoscere le conseguenze di un determinato comportamento con un grado di certezza adeguato alle circostanze[62].

La base legale per il trattamento di dati personali da parte di organi federali deve quindi consentire all'interessato di capire quale organo federale tratta quali categorie di dati a quale scopo (chi, cosa, perché) ed eventualmente anche in che forma i dati vengono trattati, in particolare nel caso di un accesso online.

La base legale deve infatti indicare la forma del trattamento, in particolare se vengono impiegati strumenti tecnologici non riconoscibili dal soggetto giuridico e se il ricorso a tali

---

61 Cfr. in merito Sylvain MÉTILLE, 9 novembre 2020, La notion de protection des données dès la conception.

62 DTF **146** I 11; **136** I 87 Jacques DUBEY, *Petit commentaire Constitution*, n. 79 ad art. 36.

strumenti può tangere i diritti fondamentali[63], comportando ad esempio un rischio di discriminazione in seguito al trattamento dei dati mediante algoritmo[64] o un rischio d'ingerenza nella libertà personale derivante dal ricorso a strumenti di sorveglianza sul suolo pubblico. Più l'ingerenza nei diritti fondamentali può essere grave, più dev'essere precisa la base legale. Per contro, se il trattamento dei dati è inerente al compito svolto dall'autorità e il rischio di una violazione dei diritti fondamentali è minimo, ad esempio nel caso di autorità chiamate a fornire sostegno finanziario, non è per forza necessaria una base legale esplicita per trattare i dati; potrà essere relativamente generica anche l'eventuale base legale specifica per comunicarli.

3.1.2 Comunicazione dei dati e principio della legalità

I dati personali possono essere comunicati soltanto se una base legale lo prevede espressamente (art. 36 LPD). La comunicazione dei dati richiede quindi una base legale specifica (cfr. n. 3.2.4 *infra*) che definisca le persone autorizzate ad accedere ai dati, i destinatari e lo scopo di un'eventuale comunicazione nonché le sue modalità e, a grandi linee, la portata del trattamento (chi, cosa, a chi, perché, come).

L'articolo 20*b* capoverso 1 della legge federale sui politecnici federali[65] prevede, ad esempio, quanto segue:

> *«Caso per caso e su precisa richiesta scritta, il Consiglio dei PF, i PF e gli istituti di ricerca possono comunicare agli organi di università, di istituzioni di ricerca o di promozione della ricerca, nazionali o estere, incaricati di individuare e sanzionare comportamenti scientifici scorretti:*
>
> > *a. se loro membri hanno violato le regole dell'integrità scientifica e della buona prassi scientifica o se sussiste il sospetto fondato di una tale violazione;*
> >
> > *b. quali sanzioni sono state inflitte alle rispettive persone.»*

L'articolo 20*c* della legge impone l'informazione scritta dell'interessato.

3.1.3 Architettura informatica e principio della legalità

In che misura la base legale deve specificare l'architettura di un sistema informativo? Sotto la legge del 1992 la domanda era rilevante in particolare per le unità amministrative dotate di un sistema di microservizi anziché di compartimentazione.

Si ha un accesso mediante procedura di richiamo quando più unità amministrative gestiscono il medesimo sistema informatico o terzi, considerati tali in relazione al titolare del trattamento, possono accedere liberamente ai dati di detto sistema (self service). La LPD non contempla più il concetto di procedura di richiamo ai sensi dell'articolo 19 capoverso 3

---

63 Monique COSSALI SAUVAIN, in: *Petit commentaire LPD, Loi sur la protection des données*, ed. Yaniv BENHAMOU, Bertil COTTIER, Helbing Lichtenhahn, 2023, ad art. 34 n. 13.

64 Frederik J. ZUIDERVEEN BORGESIUS, *Discrimination, artificial intelligence and algorithmic decision-making*, pag. 13 segg. e 36.

65 Legge sui PF; RS **414.110**

vLPD[66], il che però non indebolisce la protezione dei dati[67]. Questa modalità di comunicazione deve necessariamente essere prevista da una legge. L'accesso mediante procedura di richiamo in modalità self service può infatti violare gravemente i diritti fondamentali della persona interessata e deve pertanto essere sempre previsto in una legge in senso formale quando riguarda dati personali degni di particolare protezione o dati di profilazione. Può essere disciplinato in una legge in senso materiale se il titolare del trattamento consente l'accesso mediante procedura di richiamo a dati non considerati degni di particolare protezione e se la probabilità di una violazione grave dei diritti fondamentali è bassa. Nel rispetto del principio della finalità, l'accesso mediante procedura di richiamo deve essere strettamente connesso al compito dell'autorità per cui è richiesto. Ad esempio, l'autorità x ha accesso mediante procedura di richiamo alle categorie di dati y per eseguire il compito previsto all'art. z di una data legge, mentre un'altra autorità ha accesso mediante procedura di richiamo alle categorie di dati b per adempiere il compito c previsto all'art. d della legge. La precisione delle basi legali deve essere proporzionata al rischio di violazione dei diritti fondamentali. La gravità della violazione deve essere valutata considerando non solo la natura dei dati, ma anche e soprattutto lo scopo del trattamento.

Nell'elaborare le norme sul trattamento dei dati, l'accento è dunque posto meno sull'infrastruttura informatica (tecnica) che sull'*«architettura del trattamento dei dati»*, ossia lo scopo e la logica del trattamento, come pure il flusso dei dati e l'accesso online ai dati (chi ha accesso a quali dati)[68]. Se i dati sono trattati per svolgere più compiti legali, la relativa normativa va differenziata in funzione di questi compiti specificando chi è autorizzato a quale trattamento nell'adempimento di quale compito legale e quali sono le modalità di tale trattamento.

Nel caso di più compiti legali è indispensabile che la legge differenzi chiaramente quali dati personali possono essere trattati per quale compito e a chi è conferito tale diritto. È un dettame cruciale, dal momento che nei sistemi moderni le «*soluzioni compartimentate*» sono sostituite da soluzioni strutturate in altro modo (p. es. i citati «*microservizi*») e che la legge deve fare astrazione dalla tecnologia utilizzata. Ecco perché il trattamento dei dati va disciplinato in funzione dei compiti da svolgere.

L'articolo 9 capoverso 1 della legge federale sulla cartella informatizzata del paziente[69] prevede, ad esempio, quanto segue:

> *«I professionisti della salute possono accedere ai dati dei pazienti soltanto nella misura in cui questi abbiano accordato loro diritti d'accesso.»*

3.1.4 Obbligo di informare e principio della legalità

La LPD continua inoltre a prevedere un obbligo di informare che aumenta la trasparenza del trattamento. L'organo federale responsabile del trattamento dei dati è però esentato da tale

---

66 Esprime critiche in merito Michael MONTAVON, *L'abandon de la procédure d'appel en protection des données,* in: LeGes 31 (2020) 2 pag. 1–10.

67 Messaggio sulla revisione totale della LPD, pag. 6099.

68 Cfr. in merito la nota UFG/LPD, n. 2.1.

69 LCIP; RS **816.1**

obbligo se il trattamento è imposto dalla legge[70]. Questa deve pertanto prevedere le informazioni necessarie all'interessato per far valere i propri diritti e garantire la trasparenza del trattamento[71].

Prendiamo ad esempio l'articolo 7*a* capoverso 3 della legge federale sul sistema d'informazione per il settore degli stranieri e dell'asilo[72], che prevede quanto segue:

> *«Per adempiere i loro compiti legali, le autorità o i servizi seguenti possono trattare dati biometrici nel sistema d'informazione:*
>
> *[…]*
>
> *g. l'Ufficio SIRENE di fedpol».*

Una disposizione legale di questo tenore probabilmente non sarebbe più considerata come un'informazione sufficiente dell'interessato.

La cooperazione con gli informatici chiamati a implementare il trattamento dei dati resta pertanto decisiva per comprendere in una qualche misura il potenziale informatico di un progetto di questo tipo. Del resto il titolare deve, già nella fase pianificativa, adottare le misure tecniche e organizzative atte a garantire la conformità del trattamento con i principi della protezione dei dati e la tutela dei diritti dell'interessato[73].

Ne consegue che nella fase concettuale di una normativa per il trattamento dei dati da parte di organi federali vanno affrontate due domande in particolare: il livello normativo e la densità normativa delle disposizioni previste. La risposta a queste domande dipende dalle specificità della materia da disciplinare; non è né schematica né dovrebbe risultare in una normativa sproporzionata.

3.1.5 Sistemi di gestione degli affari

L'articolo 57*h* della legge sull'organizzazione del Governo e dell'Amministrazione (LOGA)[74], nella versione modificata dalla LPD[75], costituisce la base legale che permette alle unità dell'Amministrazione federale di gestire sistemi elettronici per lo svolgimento impeccabile dei loro processi operativi e per la gestione dei documenti. Se necessario per i processi operativi

---

70 Cfr. in merito Bertil COTTIER, *Transparence des traitements de données personnelles opérés par les organes fédéraux* : *un pas en avant, deux en arrière*, RSDA 2021 pag. 65 segg., 70, che confronta le deroghe restrittive all'obbligo d'informare secondo l'art. 18*a* vLPD con la deroga estensiva di cui all'art. 20 cpv. 1 lett. b nLPD per giungere alla conclusione seguente (pag. 72):

« Reste que cette regrettable exemption n'est en soi pas contraire au droit international supérieur : […], la convention 108 modernisée la prévoit déjà, au motif implicite que « Nul n'est censé ignorer la loi ». Cela dit, comme le souligne la doctrine, cet adage permet certes de considérer que les citoyens sont déjà informés, mais cela n'est valable qu'à la condition que la loi en question soit suffisamment précise et apporte les renseignements nécessaires pour assurer une information loyale de personnes concernées ».

71 Messaggio sulla revisione totale della LPD, pag. 6040 e 6042. cfr. Anche Claudius ETTLINGER, *Die Informationspflicht gemäss neuem Datenschutzgesetz*, in: Jusletter IT del 16 dicembre 2021.

72 LSISA; RS **142.51**

73 Art. 7 LPD, cfr. Sylvain MÉTILLE, *La notion de protection des données dès la conception*, 9 novembre 2020 in www.swissprivacy.law/26.

74 RS **172.010**

75 FF **2020** 6734

(p. es. nella consultazione degli uffici), possono concedere ad altre autorità federali e a servizi esterni (p. es. autorità cantonali) un accesso limitato ai propri sistemi di gestione degli affari.

L'ordinanza sulla gestione elettronica degli affari nell'Amministrazione federale (ordinanza GEVER)[76] concretizza lo scopo e il contenuto dei sistemi di gestione elettronica degli affari. Prevede in linea di massima l'utilizzo del sistema GEVER standardizzato pur ammettendo, a determinate condizioni, il ricorso a sistemi non standardizzati (art. 3).

In presenza di un sistema di gestione degli affari è possibile rinunciare a emanare nuove disposizioni se il trattamento dei dati può fondarsi sulla LOGA e l'ordinanza GEVER, purché il complesso di tale disposto generale, comprese eventuali norme settoriali, sia sufficiente affinché l'interessato possa riconoscere il trattamento dei suoi dati.

3.1.6 Progetti pilota

Per poter effettuare progetti pilota, la LPD contempla anche la possibilità di allentare i requisiti imposti dal principio della legalità[77].

3.2 Livello normativo (legge in senso formale / ordinanza) e densità normativa

Il rischio di un'ingerenza nei diritti fondamentali determina il livello normativo (legge in senso formale / ordinanza) e la densità normativa del futuro atto normativo. Per il trattamento di dati personali e la loro comunicazione, che costituisce una forma particolare di trattamento, vanno quindi considerati entrambi i punti.

3.2.1 Trattamento di dati degni di particolare protezione

L'articolo 34 capoverso 2 lettera a LPD impone che il trattamento di dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c numeri 1–6 LPD sia previsto in una legge in senso formale (cfr. n. 2.3.2 *supra*). Per garantire il principio della legalità e la trasparenza del trattamento nei confronti dell'interessato, la legge formale deve elencare le categorie di dati da trattare tra quelli personali degni di particolare protezione ai sensi dell'articolo 5 lettera c numeri 1–6 LPD. In virtù del principio di proporzionalità possono essere trattate soltanto le categorie di dati necessarie per adempire un compito legale. Per quanto possibile le categorie di cui all'articolo 5 lettera c numeri 1–6 LPD vanno quindi suddivise in sottocategorie; per i dati sanitari va ad esempio specificato che vengono trattati soltanto quelli sul cancro[78] (cfr. l'art. 3 della legge federale sulla registrazione delle malattie tumorali[79]).

---

76 Ordinanza GEVER; RS **172.010.441**

77 Art. 35 LPD, cfr. in merito la nota UFG/LPD, n. 2.1.

78 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.1 lett. a).

79 LRMT; RS **818.33**

Riguardo alla densità normativa: più è elevato il rischio di una lesione della personalità o di un'ingerenza nei diritti fondamentali, più la disposizione legale dev'essere precisa e lo scopo del trattamento definito in modo inequivocabile e riconoscibile per l'interessato.

Quanto illustrato finora corrisponde al diritto anteriore. L'articolo 34 capoverso 3 LPD invece autorizza il Consiglio federale a creare una base legale in senso materiale per trattare dati degni di particolare protezione, purché siano adempite due precise condizioni:

> – il trattamento è indispensabile per l'adempimento di un compito stabilito in una legge in senso formale; il compito dev'essere esplicitamente definito in una legge formale e l'interessato deve poterne riconoscere la portata[80].
>
> – Lo scopo del trattamento non comporta rischi particolari per i diritti fondamentali dell'interessato, in particolare per il rispetto della sua sfera privata (cfr. art. 13 e 36 cpv. 1 Cost.; cfr. n. 1.1 *supra*). Va inoltre verificato se il tipo di trattamento possa comportare una grave ingerenza nei diritti fondamentali (cfr. art. 34 cpv. 2 lett. c LPD).

Soltanto se sono adempite tutte queste condizioni, è possibile disciplinare il trattamento in un'ordinanza in applicazione dell'articolo 34 capoverso 3 LPD.

3.2.2 Profilazione (art. 34 cpv. 2 lett. b LPD)

Quanto illustrato in precedenza si applica anche alla profilazione. Il Consiglio federale riteneva che per la profilazione andasse prevista una base legale di livello equivalente a quella per il trattamento di dati particolarmente degni di protezione[81]. Pertanto la profilazione da parte di organi federali è lecita soltanto se una legge in senso formale la prevede. Soppesando la proporzionalità, il giurista dovrà in particolare interrogarsi se non entrano in linea di conto altre possibilità di trattamento che meglio tutelino la personalità degli interessati[82].

Quello della base legale formale non è un requisito assoluto; anche alla profilazione si applica l'articolo 34 capoverso 3 LPD, illustrato poc'anzi riguardo al trattamento di dati degni di particolare protezione (cfr. n. 3.2.1).

La base legale dev'essere sufficientemente precisa, ossia deve esplicitamente prevedere o adeguatamente descrivere la profilazione ai sensi dell'articolo 5 capoverso f LPD. Vanno perlomeno indicati lo scopo della profilazione e le categorie di dati. L'interessato dovrebbe anche poter riconoscere le proprie caratteristiche personali analizzate in sede di profilazione. Si applica il diritto all'autodeterminazione informativa; la persona oggetto di profilazione individuale deve poter esercitare il proprio diritto d'accesso e ottenere dagli organi federali le informazioni necessarie a comprendere la logica sottostante all'analisi sulla sua persona. Gli

---

80 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.1 lett. a).

81 Messaggio sulla revisione totale della LPD, pag. 6066 segg.

82 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.1 lett. b/dd).

organi federali sono inoltre tenuti ad adottare misure tecniche e organizzative al fine di ridurre al minimo il rischio di errori[83], di discriminazioni[84] o di arbitrio.

L'articolo 21*c* capoverso 1 lettera b e capoverso 1bis della legge federale sulla navigazione aerea[85], nella versione modificata dalla LPD[86], prevede ad esempio quanto segue:

> «*Nel sistema d'informazione sono trattati i seguenti dati relativi a eventi rilevanti per la sicurezza e a individui potenzialmente pericolosi che vi sono implicati:*
>
> *[…]*
>
> *b. dati personali che sono necessari per valutare il pericolo per il traffico aereo commerciale internazionale, compresi i dati personali degni di particolare protezione, come informazioni relative allo stato di salute, alle condanne o alle procedure penali o amministrative pendenti e all'appartenenza a gruppi criminali o terroristici».*

Il capoverso 1bis autorizza fedpol «*a effettuare profilazioni […] ai sensi della legge federale del 25 settembre 2020 sulla protezione dei dati»* per «*valutare la pericolosità degli individui di cui al capoverso 1*».

3.2.3 Rischio di una grave ingerenza nei diritti fondamentali a causa dello scopo o del tipo di trattamento previsto (art. 34 cpv. 2 lett. c LPD)

La LPD impone esplicitamente una legge formale se lo scopo del trattamento o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali dell'interessato (art. 36 cpv. 1 Cost.). Questo a prescindere che s'intenda trattare dati degni di particolare protezione o procedere a una profilazione. Il rischio di una grave ingerenza può risultare dallo scopo del trattamento previsto (p. es. valutare la pericolosità di una persona[87]). Può però anche derivare dal tipo di trattamento previsto, in particolare nel caso di decisioni individuali automatizzate o del ricorso all'*«intelligenza artificiale»* senza decisione individuale automatizzata. Per fare un esempio, una notifica di tassazione allestita in automatico sarebbe una decisione automatizzata. Se invece la notifica è opera di una persona fisica che si serve di un algoritmo per individuare possibili incongruenze nella dichiarazione d'imposta, avremmo un ricorso all'intelligenza artificiale senza decisione automatizzata.

In determinati casi le decisioni individuali automatizzate possono ledere gravemente i diritti fondamentali ai sensi dell'articolo 34 capoverso 2 lettera c LPD; ecco perché vanno previste in una legge formale. Possono anche considerarsi importanti questioni organizzative e

---

83 In applicazione del principio dell'esattezza dei dati (cfr. art. 6 cpv. 5 LPD del 2020), il titolare che procede alla profilazione deve garantire l'esattezza materiale dei dati utilizzati alla luce dello scopo perseguito, come pure la sufficiente affidabilità delle conclusioni tratte. Gli errori essendo inerenti all'attività di profilazione, il titolare deve adottare misure adeguate per escludere i fattori d'imprecisione sia nei dati utilizzati sia nelle previsioni allestite, cfr. Michael MONTAVON, *Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle*, Ginevra – Zurigo – Basilea 2021, pag. 647.

84 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.1 lett. b/dd).

85 LNA; RS **748.0**

86 FF **2020** 6765

87 Messaggio sulla revisione totale della LPD, pag. 6066 seg.

procedurali delle autorità federali, da sancire in una base legale formale secondo l'articolo 164 capoverso 1 lettera g Cost.[88] La base legale deve esplicitamente prevedere o adeguatamente descrivere la decisione individuale automatizzata, e l'interessato deve poter comprendere a grandi linee la logica sottostante alla decisione automatizzata[89].

Attualmente non esistono norme specifiche che disciplinano il ricorso all'intelligenza artificiale da parte dell'amministrazione pubblica per preparare le proprie decisioni[90]. Il 25 novembre 2020 il Consiglio federale ha emanato le linee guida *«Intelligenza artificiale»*[91], che in particolare pongono al centro l'essere umano e illustrano il quadro giuridico per il rispetto dei diritti fondamentali, senza tuttavia fornire criteri concretizzabili nella legislazione[92].

3.2.4 Comunicazione e consultazione di dati personali

La comunicazione di dati personali costituisce un trattamento ai sensi dell'articolo 5 lettera d LPD. Costituisce una forma particolarmente delicata di trattamento, consistente nel trasmettere o rendere accessibili dati (art. 5 lett. e LPD); è disciplinata all'articolo 36 LPD.

Tale disposizione precisa che gli organi federali continuano a necessitare di una base legale specifica che preveda la comunicazione dei dati (cfr. art. 19 vLPD e art. 36 LPD). Non sarebbe insomma sufficiente una norma di legge che autorizza in termini generali gli organi federali a trattare dati[93].

Prima di elaborare una base legale che abiliti un'autorità federale a comunicare dati degni di particolare protezione o una profilazione, il giurista determina la misura in cui la comunicazione lede la personalità dell'interessato, tenendo particolare conto del tipo di dati comunicati, dello scopo della comunicazione, dei destinatari e della forma di trasmissione, con particolare attenzione al rispetto del principio della proporzionalità (cfr. n. 2.4 *supra*).

3.2.4.1 Rischio di una lesione della personalità o di una violazione dei diritti fondamentali

I requisiti posti alla base legale in funzione della gravità del rischio di una lesione della personalità o di una violazione dei diritti fondamentali dell'interessato sono in sostanza identici a quelli applicabili ad altre forme di trattamento dei dati. In merito l'articolo 36 capoverso 1 LPD rimanda all'articolo 34 capoversi 1–3 LPD.

---

88 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.1 lett. c).

89 *Ibid.*

90 Cfr. in merito Nadja BRAUN BINDER / Thomas BURRI / Melinda Florina LOHMANN / Monika SIMMLER / Florent THOUVENIN / Kerstin Noëlle VOKINGER, *Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht*, in: Jusletter del 28 giugno 2021. Gli autori segnalano che il 21 aprile 2021 la Commissione ha presentato una proposta di regolamento per disciplinare l'intelligenza artificiale.

91 Consiglio federale, *«Intelligenza artificiale», Linee guida per la Confederazione, Quadro di riferimento in materia di intelligenza artificiale (IA) nell'Amministrazione federale*.

92 Il ricorso all'intelligenza artificiale da parte dell'amministrazione è invece stato analizzato in dettaglio nell'ottica delle sfide giuridiche ed etiche che solleva. L'analisi del 28 febbraio 2021, commissionata dal canton Zurigo, verte sulla questione del livello normativo e della densità normativa; Staatskanzlei Kanton Zürich, *Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen – Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4*, 28 febbraio 2021, consultabile all'indirizzo: https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2021/04/kuenstliche-intelligenz-in-der-verwaltung-braucht-klare-leitlini.html (ultimo accesso il 12.10.2021).

93 Cfr. in merito il rapporto dell'UFG sulla revisione totale della LPD, n. 2.1

La comunicazione di dati degni di particolare protezione va in linea di massima prevista in una legge formale; lo stesso vale per i dati derivanti da una profilazione. Si applica la deroga di cui all'articolo 34 capoverso 3 LPD (cfr. *supra* n. 3.2.1 in fine e n. 3.2.2 in fine).

3.2.4.2 Riconoscibilità e scopo della comunicazione

La comunicazione dei dati dev'essere riconoscibile per l'interessato, che deve poter capire a chi e perché i suoi dati possono essere comunicati. Lo scopo della comunicazione deve inoltre essere conforme allo scopo della raccolta dei dati (art. 6 cpv. 3 LPD). Una legge può prevedere uno scopo diverso per la comunicazione rispetto a quello definito in origine per la raccolta dati, fatto salvo il rispetto del principio della buona fede (cfr. n. 2.4 *supra*).

Se lo scopo della comunicazione differisce da quello per la raccolta dati, può essere importante modificare entrambe le leggi – quella sulla raccolta iniziale e quella sul successivo utilizzo dei dati per altri scopi – affinché l'interessato abbia la possibilità di sapere che i suoi dati potrebbero essere comunicati. L'articolo 50*a* capoverso 2 della legge federale sull'assicurazione per la vecchiaia e per i superstiti (LAVS)[94] prevede, ad esempio, quanto segue:

> «*Le autorità federali, cantonali e comunali interessate possono comunicare i dati necessari per la lotta contro il lavoro nero conformemente agli articoli 11 e 12 della legge del 17 giugno 2005 contro il lavoro nero.*»

La collaborazione delle autorità cantonali o federali e delle organizzazioni private incaricate di applicare la legislazione sulle assicurazioni sociali con gli organi cantonali di controllo ai sensi della legge contro il lavoro nero[95], nonché la comunicazione dei dati, in particolare ad opera delle casse di compensazione AVS, è disciplinata più nel dettaglio nella legge contro il lavoro nero.

3.2.4.3 Modalità di comunicazione

Si distinguono quattro modalità di comunicazione: l'obbligo di comunicazione (d'ufficio o su richiesta scritta), la comunicazione spontanea, la comunicazione su richiesta (a discrezione dell'autorità interpellata) e l'accesso online (con consultazione autonoma dei dati)[96].

La modalità scelta deve essere conforme al principio della proporzionalità: se, ad esempio, la comunicazione dei dati su richiesta è sufficiente per raggiungere gli obiettivi stabiliti dalla legge, non è necessario prevedere uno scambio di dati più ampio come l'accesso online.

La modalità di comunicazione si deve evincere dalla disposizione di legge, in altre parole, il giurista deve continuare a differenziarle formulando adeguatamente, per esempio come segue:

---

94 RS **831.10**

95 Legge federale del 17 giugno 2005 concernente i provvedimenti in materia di lotta contro il lavoro nero (LLN, RS **822.41**)

96 Cfr. in merito la Guida di legislazione, n. marg. 829 segg., e la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.2); cfr. anche Camille DUBOIS, (2012): *Recommandations pour la rédaction de dispositions légales réglant l'échange de données personnelles entre autorités*, in: LeGes 23 (2012) 3, pag. 389–396.

– *«l'autorità comunica d'ufficio [...]»;*

– *«l'autorità può avvertire di moto proprio [...]»;*

– *«l'autorità può, in casi particolari e su richiesta scritta e motivata, [...]».*

– *«l'autorità può concedere l'accesso in linea [oppure... può accedere in linea]»*

Non occorre più una base legale specifica[97] per la procedura di richiamo (come indicato al n. 3.1 *supra*); questo accesso automatizzato consente al destinatario di consultare i dati personali senza che l'organo federale responsabile del trattamento debba comunicarli o possa accorgersi che i dati sono stati consultati (self service). In termini materiali comunque la modifica di legge è minima in quanto il legislatore vuole mantenere la protezione ai livelli precedenti. Del resto l'accesso online continua a richiedere una base in una legge formale se comporta una grave ingerenza nei diritti fondamentali (art. 34 cpv. 2 lett. b LPD), vale a dire specialmente e per definizione nel caso di dati degni di particolare protezione o di una profilazione. Negli altri casi questa modalità di comunicazione va – alla stregua delle altre – almeno indicata nell'ordinanza per motivi di legalità di trasparenza. Si tratta, in altri termini, di specificare nella legge e nell'ordinanza che i dati sono consultati in modalità self service mentre il titolare del trattamento resta passivo; allo scopo vanno utilizzate formulazioni come *«permette l'accesso in linea»*. Nella legge va anche precisato se l'accesso ai dati è *«integrale»* o *«indicizzato»*[98].

Occorre inoltre rispettare il principio della proporzionalità: in altri termini, possono essere comunicati al destinatario unicamente i dati di cui questi necessita per adempire i compiti specificati nella legge.

3.2.4.4 Densità normativa e contenuto minimo della legge

Come per il trattamento dei dati, la densità normativa delle disposizioni dipenderà dal rischio che vadano a ledere la personalità e i diritti fondamentali dell'interessato. Ne consegue che la legge deve disciplinare quanto segue:

– la/le autorità cui compete la comunicazione dei dati;

– le finalità della comunicazione;

– le categorie di dati, profilazione compresa;

– le modalità della comunicazione;

– i destinatario / i destinatari[99].

3.2.5 Comunicazione all'estero

---

97 Cfr. in merito la nota UFG/LPD, n. 2.2 (e in particolare il n. 2.2.2).

98 *Ibid.*

99 Guida di legislazione, n. marg. 833.

Sono stati introdotti alcuni cambiamenti in materia di comunicazione transfrontaliera dei dati: in linea di massima, il Consiglio federale deve aver constatato che la legislazione e la sua applicazione nello Stato destinatario garantiscono un adeguato livello di protezione dei dati (art. 16 cpv. 1 LPD). In questo caso nessun ostacolo si oppone alla comunicazione dei dati. In assenza di una tale decisione del Consiglio federale, i dati possono essere comunicati all'estero soltanto in presenza di altre garanzie (art. 16 cpv. 2 e 3 LPD). L'articolo 17 LPD elenca le situazioni in cui è ammesso derogare all'articolo 16 capoversi 2 e 3 LPD e trasmettere dati senza altre garanzie a uno Stato sprovvisto di un adeguato livello di protezione.

L'articolo 16 capoverso 1 LPD autorizza la comunicazione all'estero di dati personali soltanto se il Consiglio federale ha constatato che la legislazione dello Stato destinatario o l'organismo internazionale garantisce una protezione adeguata dei dati.

Spetta al Consiglio federale determinare gli Stati e gli organismi internazionali che rientrano nella categoria. I criteri per giudicare l'adeguato livello di protezione dei dati personali da parte di uno Stato o un organismo internazionale sono definiti all'articolo 8 OPDa. L'elenco degli Stati rientranti nella categoria figura nell'allegato alla nuova ordinanza[100].

È possibile comunicare dati personali a uno Stato che non figura nell'elenco del Consiglio federale se l'adeguato livello di protezione è garantito da altri strumenti ai sensi dell'articolo 16 capoverso 2 LPD, quali in particolare trattati internazionali o clausole contrattuali a protezione dei dati (art. 16 cpv. 2 lett. a, b e d LPD).

Nel concludere trattati internazionali è pertanto indispensabile assicurarsi che sia garantito un adeguato livello di protezione dei dati all'estero. A tale proposito sono fondamentali il rispetto dei principi in materia di protezione dei dati, i diritti degli interessati (come p. es. il diritto d'accesso), la tutela giurisdizionale, le condizioni per eventuali ulteriori comunicazioni di dati all'estero nonché l'esistenza di un organo di vigilanza indipendente in materia.

L'articolo 9 del trattato di assistenza giudiziaria con l'Indonesia[101] prevede tra le altre cose (citazione incompleta):

1. I dati personali trasmessi sulla base di questo Trattato possono essere utilizzati esclusivamente per gli scopi per i quali sono stati trasmessi; il loro uso sottostà alle condizioni formulate dallo Stato che li trasmette.

2. Per la trasmissione e l'uso di dati personali trasmessi nell'ambito di una domanda di assistenza giudiziaria ai sensi del presente Trattato, valgono le condizioni seguenti:

> *a. all'autorità competente dello Stato richiedente sono trasmessi solamente i dati relativi alla domanda;*
>
> *b. su richiesta, la Parte che ha ricevuto i dati informa lo Stato che li ha trasmessi in merito all'uso di questi ultimi e ai risultati ottenuti;*

---

[100] Cfr. in merito la nota UFG/LPD, n. 4.2.

[101] Trattato di assistenza giudiziaria in materia penale tra la Confederazione Svizzera e la Repubblica di Indonesia, entrato in vigore il 14 settembre 2021; RS **0.351.942.7**.

c. se lo Stato che trasmette i dati constata che sono stati trasmessi dati inesatti o dati che non avrebbero dovuto essere trasmessi, avverte senza indugio lo Stato che li ha ricevuti. Quest'ultimo corregge senza indugio eventuali errori o distrugge i dati ricevuti;

d. le Parti registrano la trasmissione e il ricevimento dei dati in modo facilmente consultabile;

e. l'inoltro di dati personali è permesso esclusivamente in conformità con il diritto interno e con l'assenso preventivo dello Stato che li trasmette;

f. i dati trasmessi che non sono più necessari per gli scopi autorizzati dal presente Trattato vanno distrutti senza indugio; eventualmente vanno adottate altre misure autorizzate dal diritto interno che tutelino allo stesso modo i diritti dell'interessato.

3. Le Parti proteggono i dati personali da una perdita accidentale, da una distruzione o un'alterazione accidentali o non autorizzate, da un accesso, un utilizzo o una divulgazione non autorizzati nonché da altri abusi.

4. Le Parti garantiscono il diritto legittimo della persona interessata dalla trasmissione dei dati secondo il presente Trattato alle informazioni sui dati che la riguardano, alla loro rettifica o cancellazione oppure all'eventuale limitazione del loro trattamento nonché, su richiesta dell'interessato, a un rimedio giuridico efficace in relazione alla trasmissione o all'utilizzo delle informazioni.»

Occorre infine considerare che, a seconda delle circostanze, le clausole contrattuali a protezione dei dati (art. 16 cpv. 2 lett. a, b e d LPD) potrebbero non bastare a garantire una protezione adeguata[102].

3.3 Delega di competenze legislative

L'articolo 182 Cost. abilita il Consiglio federale a emanare norme di esecuzione e d'attuazione, ossia norme di rango secondario che esplicitano una disposizione di legge, ne definiscono le conseguenze giuridiche pratiche, concretizzano concetti giuridici poco chiari o disciplinano aspetti organizzativi[103]. In materia di protezione dei dati il Consiglio federale può, ad esempio, specificare le modalità del diritto d'accesso.

L'articolo 164 capoverso 2 Cost. consente al legislatore di delegare la competenza normativa primaria sempreché la Costituzione non lo escluda, come ad esempio nel caso di gravi restrizioni dei diritti fondamentali. La durata di conservazione di dati degni di particolare protezione deve ad esempio rispettare i principi della proporzionalità e della finalità (cfr. n. 2.4 *supra*) e va fissata in una legge formale. Può però essere oggetto di una disposizione che prevede la delega di competenze legislative, e la legge formale può incaricare il

---

[102] Cfr. in merito i commenti dell'IFPDT, https://www.edoeb.admin.ch/edoeb/it/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html..

[103] Guida di legislazione, n. marg. 721.

Consiglio federale di disciplinare la durata di conservazione (cfr. p. es. l'art. 38 cpv. 1 lett. b in fine della legge federale sulle prestazioni di sicurezza private fornite all'estero[104]).

La norma di delega deve definire l'oggetto, l'obiettivo (a meno che non sia evidente), la portata e – nella misura del possibile – le grandi linee della normativa delegata[105].

[104] LPSP; RS **935.41**

[105] Guida di legislazione, n. marg. 725.

IV Lista di controllo

Qui di seguito sono riassunte le domande esposte in precedenza cui va risposto nell'elaborare le basi legali per il trattamento di dati personali da parte di organi federali.

Domanda	**Procedura in base alla risposta**	**Rimandi**
È previsto il trattamento di dati personali di una o più persone fisiche?	Se sì: si applica la LPD.	cfr. n. 2.2 e 2.3.1 *supra* cfr. anche la nota UFG/LPD, n. 4.5
Vanno compiute altre procedure, prima di poter iniziare a elaborare le basi legali?	Sì. Prima ancora di elaborare le basi legali per il trattamento, va appurato se occorre verificare l'impatto sulla protezione dei dati (art. 22 LPD) e allestire un piano SIPD (sicurezza delle informazioni e protezione dati in conformità con il metodo Hermes). In tale contesto va verificata l'opportunità di adottare provvedimenti tecnici e organizzativi, definendoli all'occorrenza (protezione dei dati fin dalla progettazione e per impostazione predefinita, cfr. art. 7 cpv. 2 LPD). Consultare la documentazione specifica per la gestione di progetti in materia di digitalizzazione e i documenti generici in materia di legislazione	cfr. introduzione *supra* cfr. anche la nota UFG/LPD, n. 4.3 e 4.5
La base legale prevista consente all'interessato di riconoscere il trattamento dei suoi dati?	La base legale per il trattamento di dati personali da parte di organi federali deve specificare chi tratta quali dati per quale scopo (chi, cosa, perché) e, in determinati casi, anche come vengono trattati.	cfr. n. 2.4 e 3.1 *supra*
Il trattamento dei dati comporta rischi elevati per i diritti	Sì. Incide sul livello normativo (base legale formale ai sensi dell'art. 34	cfr. n. 1.1, 3.1 e 3.2 *supra* cfr. anche la nota UFG/LPD, n. 4.3

fondamentali dell'interessato?	cpv. 2 lett. c LPD) e sulla densità normativa.	
Verranno trattati dati degni di particolare protezione ai sensi dell'elenco ampliato all'art. 5 lett. c LPD?	Sì. Incide sulla base legale, che in linea di massima dovrà essere formale (art. 34 cpv. 2 lett. a LPD). Per garantire la trasparenza del trattamento nei confronti dell'interessato, la disposizione di legge deve specificare le categorie di cui all'art. 5 lett. c n. 1–6 LPD o le sottocategorie di dati degni di particolare protezione.	cfr. n. 2.3.2 e 3.2.1 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. a
È prevista una profilazione ai sensi dell'art. 5 lett. f LPD?	Sì. Incide sulla base legale, che in linea di massima dovrà essere formale (art. 34 cpv. 2 lett. b LPD). La disposizione di legge deve specificare almeno lo scopo della profilazione, le categorie di dati degni di particolare protezione utilizzate e gli aspetti personali analizzati.	cfr. n. 2.3.3 e 3.2.2 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. b
La finalità o la modalità del trattamento rischiano di pregiudicare gravemente i diritti fondamentali?	Sì. Potrebbe incidere sul livello normativo (base legale formale ai sensi dell'art. 34 cpv. 2 lett. c LPD) e sulla densità normativa.	cfr. n. 3.2.3 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. cc
Si ha una decisione individuale automatizzata ai sensi dell'art. 21 LPD?	Sì. Potrebbe incidere sul livello normativo (base legale perlopiù formale ai sensi dell'art. 34 cpv. 2 lett. c LPD). L'interessato deve poter comprendere a grandi linee la logica su cui si fonda la decisione automatizzata.	cfr. n. 2.3.4 e 3.2.3 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. cc
Si ha un processo decisionale assistito (preparazione della decisione a mezzo di un processo automatizzato o	Sì. Potrebbe incidere sul livello normativo (base legale perlopiù formale ai sensi dell'art. 34 cpv. 2 lett. c LPD).	cfr. n. 2.3.5 e 3.2.3 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. cc

addirittura dell'intelligenza artificiale)?		
Il titolare del trattamento ai sensi dell'art. 5 lett. j LPD è identificato?	Sì. Deve apparire come tale nelle disposizioni legali, alla stregua dell'attuale detentore della collezione di dati. È presso il titolare che si esercita il diritto d'accesso. Il titolare deve inoltre garantire che vengano rispettate le disposizioni in materia di protezione dei dati.	cfr. n. 2.3.7 *supra* cfr. anche la nota UFG/LPD, n. 4.1, 4.4.2 e 4.5
Un organo federale tratta dati congiuntamente ad altri organi federali o cantonali o a privati (art. 33 LPD)?	Sì. In tal caso spetta al Consiglio federale disciplinare le procedure di controllo e le responsabilità.	cfr. n. 2.3.7 *supra* cfr. anche la nota UFG/LPD, n. 4.1
Il trattamento dei dati è affidato a un responsabile?	Sì. Potrebbe incidere sulla legislazione, altrimenti prevedere per contratto l'affidamento a un responsabile del trattamento.	cfr. n. 2.3.8 *supra* cfr. anche la nota UFG/LPD, n. 4.1
Lo scopo del trattamento è esplicitato?	Sì. Dev'essere indicato chiaramente nella base legale.	cfr. n. 2.4 *supra* cfr. anche la nota UFG/LPD, n. 2.1
Sono rispettati gli altri principi in materia di protezione dei dati, in particolare quello della proporzionalità del trattamento e dell'esattezza dei dati?	Sì. Assicurarsi che siano rispettati sia i principi in materia di protezione dei dati garantiti dal diritto internazionale sia i limiti costituzionali imposti alla restrizione dei diritti fondamentali (art. 36 Cost.).	cfr. n. 1.1 *supra* cfr. anche la nota UFG/LPD, n. 2.1
La durata di conservazione dei dati è disciplinata?	Sì. Assicurarsi che siano rispettati i principi della proporzionalità e della finalità.	cfr. n. 2.4 in combinato disposto con n. 3.3 *supra*
È prevista una comunicazione (compreso l'accesso ai dati personali)?	Sì. Occorre una base legale specifica che deve disciplinare: l'autorità responsabile della comunicazione;	cfr. n. 3.2.4 *supra* cfr. anche la nota UFG/LPD, n. 2.1

	lo scopo della comunicazione o dell'accesso ai dati; le categorie di dati interessate; le modalità di comunicazione; i destinatari.	
Lo scopo o la modalità della comunicazione (compreso l'accesso ai dati) possono ledere gravemente i diritti fondamentali dell'interessato?	Sì. Incide sul livello normativo (base legale formale ai sensi dell'art. 34 cpv. 2 lett. c LPD, al quale rimanda l'art. 36 cpv. 2 LPD) e sulla densità normativa.	cfr. n. 3.2.3 *supra* cfr. anche la nota UFG/LPD, n. 2.1 e 2.2.2
La comunicazione (o l'accesso) verte su dati degni di particolare protezione?	Sì. Incide sulla base legale, che in linea di massima dovrà essere formale (art. 34 cpv. 2 lett. a LPD, al quale rimanda l'art. 36 cpv. 1 LPD).	cfr. n. 2.3.2 e 3.2.4.1 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. a
La comunicazione (o l'accesso) verte su una profilazione?	Sì. Incide sulla base legale, che in linea di massima dovrà essere formale (art 34 cpv. 2 lett. b LPD, al quale rimanda l'art. 36 cpv. 1 LPD).	cfr. n. 2.3.3 e 3.2.4.1 *supra* cfr. anche la nota UFG/LPD, n. 2.2.1, lett. b
I dati sono comunicati (o resi accessibili) all'estero?	Sì. Assicurarsi che la legislazione dello Stato destinatario garantisca un adeguato livello di protezione ai sensi dell'art. 16 cpv. 1 LPD o che siano adempite le condizioni di cui all'art. 16 cpv. 2 LPD.	cfr. n. 3.2.5 *supra* cfr. anche la nota UFG/LPD, n. 4 e 4.2
È prevista una delega di competenze legislative?	Sì. Assicurarsi che vengano rispettati i principi della delega legislativa.	cfr. n. 3.3 *supra*