



32° Rapporto d'attività 2024/2025

Incaricato federale della protezione
dei dati e della trasparenza



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapporto d'attività 2024/2025

dell’Incaricato federale della protezione dei dati e della trasparenza

L’IFPDT presenta annualmente all’Assemblea federale un rapporto d’attività. Lo trasmette contemporaneamente al Consiglio federale. Il rapporto è pubblicato (art. 57 LPD).

In materia di protezione dei dati il presente rapporto riguarda il periodo dal 1º aprile 2024 al 31 marzo 2025.
In materia di trasparenza copre il periodo dal 1º gennaio al 31 dicembre 2024.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Primato della politica e linguaggio

L'intelligenza artificiale, oggi ormai accessibile a tutti, può essere considerata l'ultimo straordinario traguardo della digitalizzazione, un autentico prodigo in grado di sorprenderci attraverso la produzione autonoma di testi, discorsi, canzoni e immagini.

Tuttavia, chi si limita semplicemente a osservare con meraviglia rischia di rimanere indietro. Per evitare ciò, è essenziale acquisire le competenze digitali, come ci viene ripetutamente esortato da più parti. Una tra queste è il settore della protezione dei dati, il quale, ci fornisce indicazioni, e a buon diritto, su come prevenire il «tracking», ovvero la divulgazione dei dati sulla propria posizione o l'integrazione dei dati nell'intelligenza artificiale.

È indubbiamente legittimo aspettarsi che i politici, così come tutti i cittadini, acquisiscano familiarità con il mondo digitale. Al di là degli obiettivi, vi è chi chiede che i candidati dimostrino competenze digitali per poter assumere una carica politica. I rappresentanti del Popolo sono in grado di valutare le opportunità e i rischi sociali legati alle tecnologie digitali. Per farlo, tuttavia, devono poter contare sul fatto che chi possiede una visione approfondita di queste tecnologie e dei loro complessi ambienti applicativi sia disposto e in grado di trasmettere le proprie conoscenze in un linguaggio chiaro e accessibile.

In tal senso, anche nell'attuale periodo in rassegna, la vigilanza della Confederazione sulla protezione dei dati ha ribadito l'importanza che l'Amministrazione adotti un linguaggio comprensibile nelle proposte al Consiglio federale e nei messaggi destinati al Parlamento affinché siano chiaramente evidenziati i rischi significativi per la protezione dei dati derivanti dai progetti di digitalizzazione.

Adrian Lobsiger

Incaricato federale della protezione dei dati e della trasparenza



Berna, 31 marzo 2025

Sfide attuali	8
----------------------------	----------

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali ...	15
– Consulenza: Progetto CEBA della Cancelleria federale ..	15
– Amministrazione digitale Svizzera (ADS): Questioni giuridiche correlate ai nuovi compiti.....	16
– Frode elettorale: Pratiche irregolari in relazione alla raccolta di firme.....	16
– Voto elettronico: Definizione chiara delle competenze ..	17
– ID-E: Partecipazione dell'IFPDT al progetto di legge sull'identità elettronica	17
– Scambio elettronico di atti giuridici: Progetto Justitia 4.0 della Confederazione e dei Cantoni	18
– Cibercriminalità: Ciberattacco a OneLog.....	18
– Ciberattacco: Chiusura degli accertamenti preliminari informali nei confronti di Concevis AG e dell'Ufficio federale di statistica (UST).....	19
Tema prioritario.....	20
Nuove prassi e attività di vigilanza	
1.2 Giustizia, polizia, sicurezza	29
– Cibercriminalità: Le inchieste nei confronti della ditta Xplain e degli uffici federali fedpol e UDSC si sono concluse con l'adozione delle raccomandazioni	29
– Legisiazione: Revisione della legge sulle attività informative.....	30
1.3 Economia e società	32
– Tracciamento trasversale alla piattaforma: Presa di posizione di Ricardo e TX Group riguardo alle raccomandazioni	32
– Account utenti: L'IFPDT segue l'attuazione delle raccomandazioni accolte dalla piattaforma di e-commerce ..	33
– Campagna online: Inchiesta sull'associazione Bürgerforum Schweiz.....	34
– Mercato immobiliare: Domande inammissibili nei moduli d'iscrizione per la locazione di un alloggio	36
1.4 Salute	39
– Doping: Trasmissione di dati medici di atleti svizzeri....	39
– Moduli dei pazienti: Tra obbligo di informare e consenso.....	40
– Cartella informatizzata del paziente: Revisione completa della legge e finanziamento transitorio	41

1.5 Lavoro	42
– Diritto in materia di personale federale: Piattaforma di segnalazione	42
– Diritto in materia di personale federale: Profilazione nel contesto di valutazioni e ricerca attiva di personale ..	43
– Sorveglianza del personale: Rispetto dei principi di protezione dei dati nell'ambito della sorveglianza del personale	44
1.6 Trasporti	47
– Progetto Swisscom Broadcast: L'IFPDT chiede delle risposte in merito alla rete di droni di Swisscom	47
– Biometria: Riconoscimento facciale presso l'aeroporto di Zurigo	47
– Passenger Name Record: Legge sui dati dei passeggeri aerei.....	48
– Piattaforma per i TP NOVA: Controlli sulle FFS	48
1.7 Internazionale	50
– Estrazione di dati (Data Scraping)	50
– Swiss-US DPF (Data Privacy Framework)	51
– Schengen	54
– Consiglio d'Europa	57
– Spring Conference	59
– European Case Handling Workshop (ECHW)	59
– OCSE	59
– Privacy Symposium	61
– AMVP	61
– AFAPDP	62
– Incontri bilaterali	63

Principio di trasparenza

2.1 In generale	66
2.2 Domande di accesso: forte incremento nel 2024	68
2.3 Procedure di mediazione: notevole aumento delle domande di mediazione	72
– Percentuale di soluzioni consensuali	72
– Durata delle procedure di mediazione.....	73
– Numero di casi pendenti	75
2.4 Procedura legislativa	76
– Rapporto della CdG-S: Il Consiglio federale rinuncia a esaminare in modo più approfondito se sia possibile riconoscere all'IFPDT il diritto di pronunciare decisioni .	76
– Diritto in materia di personale federale: Limitazione del principio di trasparenza in caso di «whistleblowing» ..	78
– Aviazione: Limitazione del principio di trasparenza nella vigilanza sull'aviazione civile	79
– Aviazione: Modifica dell'ordinanza concernente le inchieste sulla sicurezza in caso di eventi imprevisti nei trasporti (OJET).....	80
– Vigilanza finanziaria: Nuova legge federale sulla trasparenza delle persone giuridiche	81
– Ricorso al diritto di necessità: Rapporto del Consiglio federale.....	82
2.5 Riserve di disposizioni speciali ai sensi dell'articolo 4 LTras	84

L'IFPDT

3.1 Compiti e risorse	90
– Prestazioni e risorse nell'ambito della protezione dei dati	90
– Prestazioni e risorse nell'ambito della legge sulla trasparenza	92
– Visita di servizio della Sottocommissione DFGP/CaF della Commissione della gestione del Consiglio nazionale ..	94
– Il consulente per la protezione dei dati dell'IFPDT	94
3.2 Comunicazione	96
– Comunicati stampa	96
– Comunicazioni «in breve»	96
– Informazione e sensibilizzazione.....	96
– Sito Internet	97
– Attività mediatica	97
3.3 Statistiche	98
– Statistiche sulle attività dell'IFPDT dal 1° aprile 2024 al 31 marzo 2025.....	98
– Panoramica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2024	100
– Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2024	101
– Numero di domande di mediazione secondo la categoria di richiedenti	104
– Domande d'accesso dell'intera amministrazione federale dal 1° gennaio al 31 dicembre 2024	105
3.4 Organizzazione dell'IFPDT	106
– Organigramma	106
– Personale dell'IFPDT.....	107
Abbreviazioni	108
Elenco delle illustrazioni	109
Impressum	110
Nella copertina	
– Cifre chiave	

Sfide attuali

I Protezione dei dati

Le società democratiche occidentali dispongono oggi di tecnologie digitali, risorse finanziarie e forza lavoro sufficienti per poter ampliare le proprie infrastrutture di controllo in misura tale da erodere le garanzie costituzionali liberali in materia di tutela della vita privata e di autodeterminazione dei cittadini. Sensori e droni a basso prezzo possono essere prodotti in quantità praticamente illimitate e utilizzati per una sorveglianza di massa, incluso il riconoscimento dei movimenti e dei volti nei luoghi pubblici. In combinazione con una rete che collega tutti i sistemi d'informazione delle autorità e con una sorveglianza del mondo virtuale gestita dallo Stato e dall'economia digitale, ciò può portare all'introduzione di sistemi di controllo sociale basati sull'intelligenza artificiale o incentrati sul principio del «punteggio sociale». In tal modo anche nei Paesi

occidentali sarebbe possibile esercitare una sorveglianza pressoché totale sulla vita quotidiana dei cittadini.

La legge federale sulla protezione dei dati (LPD), formulata in modo tecnologicamente neutrale, vieta l'applicazione capillare del riconoscimento facciale e di sistemi di «punteggio sociale», seppure l'Incaricato possa dedurre tale divieto soltanto mediante interpretazione della legge, dato che la stessa, contrariamente al regolamento dell'Unione europea sull'intelligenza artificiale, non contiene un divieto esplicito (cfr. comunicazione del 9.11.2023). Il diritto in materia di protezione dei dati e le autorità quali l'IFPDT contribuiscono così a impedire che le democrazie occidentali cedano troppo facilmente alle tentazioni tanto lusinghiere quanto ambigue della tecnologia. La protezione dei dati si fonda infatti sulle garanzie costituzionali in materia di libertà e su una concezione garantista dell'ordinamento giuridico che affida a istituzioni statali democratiche indipendenti il compito di vigilare sull'attuazione di tali diritti.

In numerosi Stati occidentali con cui la Svizzera ha stretti legami si assiste nondimeno a una crescente divergenza tra i sostenitori dello Stato di diritto e cerchie che ritengono di non avere nulla da nascondere e si oppongono alla pro-

tezione dei diritti fondamentali e dei dati, respingendola per sé stessi in quanto forma di paternalismo e considerandola invece, quando applicata ad altri, un eccesso di zelo burocratico finalizzato a proteggere più i «colpevoli» che non i cittadini. Tali cerchie, spesso mosse da un risentimento contro le cosiddette «élite», si mostrano particolarmente insofferenti nei confronti del controllo sul potere esecutivo da parte di tribunali e autorità di vigilanza.

Le ripetute critiche allo Stato di diritto e il crescente divario tra i due punti di vista portano nelle società occidentali all'affermarsi di una mentalità mossa da una perpetua ricerca di sicurezza: uno schema cognitivo che esige il potenziamento delle infrastrutture di controllo al ritmo dello sviluppo tecnologico e che accetta di buon grado le limitazioni conseguenti al controllo sociale digitale quando si applicano a «criminali», «stranieri» e dissidenti, mentre ne minimizza la gravità quando concernono la propria persona e le cerchie ideologicamente affini. Laddove in Occidente tale pensiero diventerà prevalente, il cittadino si trasformerà, verosimilmente in un futuro più prossimo che lontano, in un soggetto controllato da poteri informazionali esterni fin negli aspetti più intimi della sua esistenza.

«La LPD proibisce il riconoscimento facciale su larga scala e il controllo sociale digitale.»

II Principio di trasparenza

Tempo necessario per il trattamento delle domande di accesso e le procedure di mediazione

Il crescente interesse nei confronti del principio di trasparenza si traduce in un aumento significativo delle domande di accesso ai documenti ufficiali.

Una situazione analoga si verifica nelle procedure di mediazione dell'IFPDT: nel 2024 si è registrato un numero record di domande, con ripercussioni negative sui tempi delle procedure di mediazione. Nell'anno in rassegna, l'Incaricato è riuscito a rispettare il termine di 30 giorni previsto dalla legge per il trattamento delle domande soltanto in un buon quarto dei casi (v. n. 2.3). Oltre all'aumento numerico, si è registrata una crescente complessità delle questioni giuridiche sollevate, contribuendo ulteriormente a un allungamento dei tempi delle procedure. Ad esempio, la delimitazione dell'applicabilità della

LTras può richiedere verifiche complesse prima di giungere a una valutazione nel merito. Inoltre, l'intervento di una rappresentanza legale nella procedura di mediazione, sia da parte dei richiedenti o di terzi sia da parte dell'Amministrazione, comporta nella maggior parte dei casi procedure più lunghe.

Poiché è ragionevole attendersi anche nei prossimi anni un crescente interesse ad accedere ai documenti ufficiali, con un conseguente incremento del numero di domande, l'evasione tempestiva delle procedure di mediazione continuerà a rappresentare una sfida.

Aumento delle deroghe alla LTras fondate su leggi speciali

Nell'anno in rassegna si sono registrati ulteriori tentativi da parte dell'Amministrazione di escludere settori della sua attività o determinate categorie di documenti dalla LTras. Nelle relative consultazioni degli uffici, l'IFPDT si è espresso in modo critico a riguardo: l'introduzione di simili riserve indebolisce infatti il principio di trasparenza e la trasparenza dell'Amministrazione a cui è finalizzato. Il primato di una norma giuridica ai sensi di una disposizione speciale secondo l'articolo 4 LTras deve essere stabilito caso per caso interpretando le norme interessate.

Alla luce dell'aumento delle deroghe alla LTras fondate su leggi speciali, l'IFPDT pubblica, come nell'ultima edizione del rapporto d'attività, una tabella che riepiloga le deroghe attuali (v. n. 2.5), disponibile anche sul suo sito Internet.

«Nel 2024 sono state inoltrate più domande di mediazione che mai.»

III Cooperazione nazionale ed internazionale

Cooperazione nazionale

Le autorità di protezione dei dati della Confederazione, dei Cantoni e dei Comuni continuano a intensificare la collaborazione al fine di garantire una vigilanza efficace e integrale.

La delimitazione delle competenze in materia di protezione dei dati, con particolare riferimento alla questione relativa all'applicabilità della legislazione federale rispetto a quella cantonale, ha continuato a essere oggetto di confronti tra l'IFPDT e le autorità di protezione dei dati partner (cfr. 31° rapporto d'attività, n. III). Queste distinzioni sono state trattate in particolare nel quadro dei rapporti contrattuali di lavoro all'interno di enti privati ai quali sono delegati compiti pubblici o che hanno contratti di prestazioni con un Cantone o con istituzioni pubbliche cantonali. Discussioni al riguardo sono state ad esempio condotte nell'ambito dei trasporti pubblici o delle case di riposo e case di cura.

Le autorità di protezione dei dati si sono inoltre consultate regolarmente sul tema dell'introduzione e/o della gestione di piattaforme di sistemi di banche dati comuni. Ciò ha richiesto un'analisi giuridica e tecnica più approfondita, in particolare per quanto concerne la chiara ripartizione delle responsabilità e dei ruoli, come nel caso

della gestione da parte della Confederazione di una piattaforma che tratta dati personali provenienti dai Cantoni in virtù di obblighi legali cantonali. Alcuni esempi sono i progetti POLAP (cfr. n. 1.2), Justitia (cfr. n. 1.1) ed eVoting (cfr. n. 1.1). Nell'ambito del progetto POLAP, l'IFPDT e privatim hanno inoltre pubblicato una presa di posizione (IFPDT del 27.03.2024; privatim del 23.02.2024, disponibile in francese e tedesco).

Scambio con privatim

Infine, l'IFPDT ha partecipato come membro associato alle assemblee delle autorità cantonali per la protezione dei dati (Conferenza degli incaricati svizzeri per la protezione dei dati; privatim) in cui sono stati trattati temi d'attualità quali il cloud e le conseguenze giuridiche delle violazioni della protezione e sicurezza dei dati.

Scambi annuali con i consulenti per la protezione dei dati della Confederazione

Per il secondo anno consecutivo l'IFPDT ha organizzato un evento informativo rivolto ai consulenti per la protezione dei dati della Confederazione.

In quanto servizio di contatto, i consulenti per la protezione dei dati della Confederazione sono chiamati ad avere scambi regolari con l'IFPDT ed è pertanto essenziale che le novità relative alla protezione dei dati, siano esse di natura legale, tecnica o pratica, vengano comunicate loro apertamente, in particolare ai fini dell'adempimento dei loro compiti legali. Questo evento offre loro anche l'occasione di incontrare i colleghi e confrontarsi sulle sfide quotidiane legate alla loro funzione.

Incontri annuali con le associazioni per la protezione dei dati in Svizzera

Come ogni anno l'IFPDT ha incontrato le associazioni per la protezione dei dati al fine di approfondire le sfide attuali. Tale confronto con la realtà delle imprese private si rivela fondamentale in quanto consente di analizzare le loro prassi e le difficoltà riscontrate. Inoltre, questi scambi offrono all'IFPDT l'opportunità di acquisire una visione dettagliata delle priorità e degli interessi delle diverse regioni linguistiche.

Cooperazione internazionale

Gli scambi internazionali continuano a rivestire un ruolo di primaria importanza, soprattutto alla luce della presenza di aziende tecnologiche globali nel mercato svizzero e delle complesse questioni transfrontaliere relative all'attuazione.

In tale contesto, l'IFPDT mantiene una presenza attiva e significativa negli importanti organismi internazionali, con particolare attenzione alla cooperazione con le autorità per la protezione dei dati dell'UE e dello SEE. Lo scambio con tali autorità è considerato cruciale dall'Icaricato. Nell'anno in esame, quest'ultimo ha preso parte alle riunioni informali degli Stati che beneficiano di una decisione d'adeguatezza dell'UE (i cosiddetti «Adequacy Groups») alle quali hanno partecipato da un lato l'UE e dall'altro l'autorità per la protezione dei dati del Regno Unito.

Protezione dei dati



1.1 Digitalizzazione e diritti fondamentali

CONSULENZA

Progetto CEBA della Cancelleria federale

Nell'anno in rassegna, l'IFPDT ha continuato a seguire dal punto di vista della vigilanza il progetto «Cloud Enabling Büroautomation», in breve CEBA. L'accento è stato posto sulla verifica della valutazione d'impatto sulla protezione dei dati redatta dall'Amministrazione federale e sulle prime serie di formazioni destinate al personale federale. Il progetto «Cloud Enabling Büroautomation» (CEBA), iniziato nel 2019, è gestito dal settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale (CaF). L'obiettivo del progetto è quello di sostituire il pacchetto di prodotti «Microsoft Office LTSC Professional Plus 2021», attualmente impiegato nelle postazioni di lavoro dell'Amministrazione federale, con la soluzione «Micro-soft Office 365» (M365) basata sul cloud. Il

settore TDT ha coinvolto tempestivamente l'IFPDT nel progetto. Già nell'ultimo Rapporto d'attività è stato quindi possibile informare l'opinione pubblica in merito a questo progetto di trasferimento nel cloud pubblico (cfr. 31° Rapporto d'attività, n. 1.1, e comunicato del 7 marzo 2023).

Dopo che, dall'inizio del progetto, l'Incaricato è riuscito a fare in modo che il TDT esaminasse a medio termine delle alternative a Microsoft Office 365, la sua attività di consulenza in materia di vigilanza riguarda ora l'adeguamento e la precisazione della valutazione d'impatto sulla protezione dei dati (VIPD) redatta dal TDT nonché le prime serie di formazioni destinate al personale federale.

L'IFPDT chiede che sia esaminata la proporzionalità di una soluzione basata sul cloud a livello di Confederazione e che siano analizzati e valutati i rischi rilevanti dal profilo della legislazione sulla protezione dei dati, in particolare per quanto riguarda l'accesso da parte di autorità straniere e la dipendenza dai fornitori di cloud che dominano il mercato. Le nostre prese di posizione relative alle versioni continuamente aggiornate della VIPD hanno portato a una migliore descrizione dei rischi fondamentali e a una definizione più chiara delle misure necessarie a minimizzare i rischi. Attualmente il TDT si

sta occupando delle relative precisazioni e aggiunte. Contemporaneamente vengono svolti audit indipendenti, i cui risultati saranno pure integrati nella prossima versione della VIPD.

Un'importante misura per minimizzare i rischi del progetto CEBA è rappresentata dall'etichettatura dei documenti che contengono dati personali sensibili e che devono quindi continuare a essere trattati nei centri di calcolo della Confederazione. A tale scopo è necessario istruire correttamente il personale federale. Alcuni collaboratori dell'IFPDT hanno seguito i primi corsi di formazione per accertarci che fossero rispettati i requisiti di protezione dei dati e sicurezza. In quanto unità organizzativa accorpata amministrativamente alla CaF, in un secondo momento anche l'IFPDT usufruirà delle prestazioni legate alla migrazione a M365 e di questi corsi di formazione.

AMMINISTRAZIONE DIGITALE SVIZZERA (ADS)

Questioni giuridiche correlate ai nuovi compiti

L'Amministrazione digitale Svizzera (ADS) ha assunto i compiti della Conferenza svizzera sull'informatica (CSI). L'IFPDT e le autorità cantonali responsabili della protezione dei dati chiariscono le modalità di collaborazione con l'ADS nell'ambito delle rispettive competenze federali.

Nell'anno in esame è stato completato il trasferimento dei compiti della Conferenza svizzera sull'informatica (CSI) all'Amministrazione digitale Svizzera (ADS), ugualmente finanziata e gestita congiuntamente dalla Confederazione e dai Cantoni. L'ADS ha quindi avviato anche la definizione delle condizioni di collaborazione con i fornitori nel settore delle tecnologie dell'informazione e della comunicazione (TIC) assumendo nel contempo il ruolo di azionista di maggioranza di eOperations Svizzera SA.

Questo ha portato l'IFPDT e le autorità cantonali responsabili della protezione dei dati a interrogarsi sulla natura giuridica dell'Amministrazione digitale Svizzera, così come sulle relative ripercussioni sul piano giuridico e sulla ripartizione delle competenze. Si è dunque posto il quesito se l'ADS debba essere considerata una società semplice costituita ai sensi del Codice delle obbligazioni senza personalità giuridica in base alla convenzione quadro di diritto pubblico che stabilisce il suo mandato di prestazioni, un organo pubblico oppure un organo federale pubblico ai sensi della LPD.

FRODE ELETTORALE

Pratiche irregolari in relazione alla raccolta di firme

A seguito di diversi articoli pubblicati dai mezzi di informazione e di molteplici segnalazioni di cittadini, nell'ambito della sua vigilanza l'IFPDT si è occupato del caso di presunta falsificazione e raccolta sospetta di firme nel contesto di iniziative popolari e referendum.

L'IFPDT ha in particolare analizzato le questioni della protezione dei dati in relazione con i diritti politici previsti dalla legge. Ha esaminato chi ha accesso ai dati e quali sono le finalità del trattamento in occasione della raccolta delle firme. Attualmente, dalle informazioni in possesso dell'IFPDT risulta che non si tratta di una problematica legata alla protezione dei dati. Di fatto, sembrerebbe che la presunta frode sia associata a firme o indirizzi inventati, nonché a firmatari che non esistono più. Ciò esclude ogni possibile collegamento con una persona fisica identificata o identificabile e significa che tali informazioni non sono dati personali e che la legge sulla protezione dei dati non si applica in questo caso.

VOTO ELETTRONICO

Definizione chiara delle competenze

In caso di votazioni elettroniche spetta ai Cantoni vigilare sul rispetto delle norme in materia di protezione dei dati. Dal 2004 Confederazione e Cantoni portano avanti il progetto relativo al voto elettronico. Il 26 giugno 2019 il Consiglio federale ha incaricato la Cancelleria federale (CaF) di riorganizzare la fase sperimentale del voto elettronico. Il rapporto finale congiunto sulla riorganizzazione e la ripresa delle prove prevedeva una revisione delle basi legali per il voto elettronico. La revisione parziale dell'ordinanza sui diritti politici (ODP) e la revisione totale dell'ordinanza della Cancelleria federale concernente il voto elettronico (OVE) sono entrate in vigore il 1° luglio 2022. In base all'articolo 14 OVE sono i Cantoni a dover assumere la responsabilità globale per il corretto svolgimento degli scrutini per via elettronica.

Nell'ambito del progetto, alla Confederazione o alla Cancelleria federale spetta il compito di fornire l'autorizzazione di principio per svolgere le prove del voto elettronico (art. 27a – 27q ODP). Al fine di garantire la sicurezza del voto elettronico, tenendo conto degli ultimi sviluppi, la Confederazione e i Cantoni gestiscono un catalogo congiunto delle

misure che viene costantemente verificato, adeguato e pubblicato e illustra gli sviluppi previsti nel settore del voto elettronico e le necessità d'intervento individuate.

La Cancelleria federale, inoltre, è responsabile della verifica dei sistemi impiegati per il voto elettronico. Attualmente viene utilizzato il sistema della Posta Svizzera. Ogni Cantone può tuttavia decidere in modo autonomo il sistema da impiegare. Attualmente i Cantoni che dispongono dell'autorizzazione necessaria per il voto elettronico sono quattro, ovvero San Gallo, Basilea Città, Turgovia e i Grigioni.

Dal momento che, per quanto riguarda il voto elettronico, la Cancelleria federale svolge soltanto il ruolo di ente di certificazione, ma la responsabilità di verificare la sicurezza dei sistemi è dei Cantoni, la verifica del rispetto delle norme in materia di protezione dei dati spetta unicamente alle autorità cantonali.

ID-E

Partecipazione dell'IFPDT al progetto di legge sull'identità elettronica

Come negli anni precedenti, l'IFPDT ha accompagnato, dal punto di vista della vigilanza, i lavori relativi al progetto di legge sull'identità elettronica (Id-e). L'IFPDT ha continuato in particolare a sostenere il principio della non tracciabilità dell'Id-e al fine di garantire una protezione supplementare della sfera privata. La non tracciabilità comporta l'impossibilità di collegare transazioni diverse effettuate con un'Id-e.

Nel quadro della revisione della legge sull'identità elettronica, l'IFPDT aveva espresso la preoccupazione che la creazione dell'Id-e avrebbe potuto condurre a raccolte eccessive di dati personali tramite i canali digitali. In effetti, l'accesso a tutti i dati contenuti nell'Id-e di un cliente, ad esempio per verificare la sua età durante un semplice acquisto online di prodotti vietati ai minori (in particolare alcolici), sarebbe considerato eccessivo e quindi illegittimo. Sarebbe sufficiente un semplice accesso alla sola informazione in merito alla maggiore età dell'acquirente.

Motivo per cui l'IFPDT ha sostenuto il principio della non tracciabilità dell'Id-e, che garantisce una protezione supplementare della sfera privata impedendo l'accesso a dati non necessari. Per l'attuazione dell'identità elettronica l'IFPDT ha quindi chiesto l'attuazione vincolante di tale principio, il quale è stato accettato dalle autorità e integrato nella legge adottata il 20 dicembre 2024 dalle Camere federali.

SCAMBIO ELETTRONICO DI ATTI GIURIDICI

Progetto Justitia 4.0 della Confederazione e dei Cantoni

L'IFPDT sta seguendo la creazione della piattaforma justitia.swiss, che dovrebbe consentire la comunicazione elettronica nell'ambito giudiziario.

Con justitia.swiss si dovrebbe riuscire a creare una piattaforma online per la comunicazione elettronica tra tutti i soggetti coinvolti in un procedimento giudiziario, ovvero tra autorità giudiziarie, avvocati e altre persone coinvolte. La piattaforma intende implementare lo scambio elettronico di atti giuridici e l'esame elettronico degli atti.

Su richiesta dei Cantoni nell'anno in rassegna l'IFPDT ha contribuito a creare condizioni quadro il più possibile uniformi per i progetti pilota pianificati e in parte già in corso nei Cantoni e presso la Confederazione e, allo stesso

tempo, a garantire che la piattaforma operi nel rispetto delle norme sulla protezione dei dati.

Poiché da qui al momento della piena operatività di justitia.swiss, prevista non prima del 2026, dovranno essere risolti altri problemi giuridici, tecnici e organizzativi, l'IFPDT, in accordo con i Cantoni e insieme all'Ufficio federale di giustizia e all'organizzazione del progetto di justitia.swiss, ha assunto il coordinamento del progetto per quanto riguarda gli aspetti concernenti la protezione dei dati.

Secondo la legge federale concernente le piattaforme per la comunicazione elettronica in ambito giudiziario (LCEG), che entrerà in vigore al più presto il 1° gennaio 2026, l'IFPDT in futuro eserciterà da solo la sorveglianza in base alle norme in materia di protezione dei dati sulla piattaforma justitia.swiss. Attualmente i responsabili dei controlli preliminari sui progetti pilota di justitia.swiss in corso nei singoli Cantoni sono ancora gli incaricati per la protezione dei dati cantonali. La sorveglianza dovrebbe però essere trasferita il prima possibile all'IFPDT ponendo in vigore anticipatamente le disposizioni della LCEG che sono necessarie. Solo a quel punto sarà possibile effettuare un progetto pilota unitario della Confederazione sotto la sorveglianza dell'IFPDT.

CIBERCRIMINALITÀ

Ciberattacco a OneLog

Il servizio di login OneLog non è stato disponibile per circa una settimana a causa di un ciberattacco avvenuto il 24 ottobre 2024. Per garantire la sicurezza dei dati dei numerosi utenti, il titolare del trattamento ha aggiornato costantemente l'IFPDT in merito alle misure attuate e alle azioni intraprese successivamente.

Il 25 ottobre 2024 l'incaricato della protezione dei dati di OneLog ha comunicato all'IFPDT che il servizio di login OneLog aveva subito un attacco informatico. A questa sono seguite altre comunicazioni, attraverso le quali il titolare del trattamento ha informato e tenuto aggiornato l'IFPDT su quanto rilevato in relazione all'evento. In base alla guida per la notifica di violazioni della sicurezza dei dati e l'informazione alle persone interessate secondo l'articolo 24 LPD,

CIBERATTACCO

sono considerate notifiche volontarie quelle che, pur non comportando un rischio elevato per le persone interessate secondo la valutazione del titolare del trattamento, sono comunque portate all'attenzione dell'IFPDT per altre ragioni (cfr. passaggio sulla notifica delle violazioni della sicurezza dei dati). Tali notifiche si rivelano particolarmente rilevanti per tutte le persone interessate e anche dal punto di vista dell'interesse pubblico quando, pur non emergendo rischi significativi dall'analisi condotta in base ai dati interessati, la notifica potrebbe suscitare l'interesse dei media, ad esempio perché coinvolge un ampio numero di persone.

OneLog è un servizio offerto da Alleanza digitale svizzera. L'Alleanza, che riunisce diverse imprese mediatiche svizzere, ha avviato la fase pilota del suo progetto per la realizzazione di una soluzione di login centralizzata nella primavera 2021. L'IFPDT ne ha parlato nel suo 28° rapporto d'attività (cfr. 28° rapporto d'attività, n. 1.1).

Chiusura degli accertamenti preliminari informali nei confronti di Concevis AG e dell'Ufficio federale di statistica (UST)

L'IFPDT ha ultimato gli accertamenti preliminari nei confronti di Concevis e dell'Ufficio federale di statistica. Non sono emerse gravi lacune e si ritiene poco probabile che i dati interessati dall'attacco siano stati effettivamente letti dai pirati informatici. L'IFPDT ha tuttavia rilevato alcuni aspetti da migliorare.

Nel novembre 2023 Concevis, fornitore svizzero di soluzioni software, era stato vittima di un attacco ransomware che aveva interessato in particolare alcuni dati dell'Ufficio federale di statistica (UST). L'IFPDT aveva dunque avviato un accertamento preliminare informale

nei confronti di Concevis e un altro nei confronti dell'UST (cfr. 31° rapporto d'attività, n. 1.2).

L'analisi dell'IFPDT ha permesso di concludere che non vi era la necessità di avviare un'inchiesta formale ai sensi dell'articolo 49 LPD, non essendo emerse gravi lacune. Inoltre, i dati interessati dall'attacco erano criptati, rendendo poco probabile che gli autori dell'attacco abbiano potuto accedervi.

L'IFPDT ha tuttavia rilevato che alcuni aspetti relativi al trattamento dei dati tra l'UST e Concevis avrebbero dovuto essere definiti più chiaramente. Ha pertanto sottolineato l'importanza che i contratti stipulati dalle unità amministrative della Confederazione con i fornitori di prestazioni definiscano in maniera precisa l'intero ciclo di vita dei dati, dalla loro raccolta alla loro distruzione. Ha inoltre rilevato la necessità di disciplinare in modo esplicito la possibilità per l'Ufficio o per i prestatori esterni di procedere a controlli e a verifiche. Infine, l'IFPDT ha rammentato all'UST e a Concevis le raccomandazioni di portata generale formulate nel caso Xplain (cfr. n. 1.2).

Nuove prassi e attività di vigilanza

Prassi dell'IFPDT in materia di diritti delle persone interessate

Chiunque può domandare al titolare del trattamento se dati personali che lo concernono sono oggetto di trattamento. Questo strumento essenziale previsto dalla legge sulla protezione dei dati mira a garantire la trasparenza e a consentire alle persone interessate di verificare il trattamento dei propri dati personali. Tuttavia, alla luce della quantità di denunce ricevute, l'IFPDT constata che spesso questo strumento è trascurato dai titolari del trattamento.

L'IFPDT ha ricevuto diverse denunce relative a potenziali violazioni del diritto di accesso. In numerosi casi ha constatato che i titolari del trattamento non hanno risposto a domande d'accesso o si sono limitati a rinviare alle informazioni generali

contenute nella loro dichiarazione relativa alla protezione dei dati anziché trasmettere le informazioni stabilite dalla legge.

Nell'ambito della sua attività di vigilanza, l'IFPDT è intervenuto invitando i titolari del trattamento a dare seguito alle domande d'accesso e ad adottare le misure necessarie a garantire la conformità della loro prassi di concessione del diritto d'accesso alle prescrizioni della LPD. In un caso ha aperto un'inchiesta formale.

Il diritto d'accesso (art. 25 LPD)

Elemento fondamentale della legge sulla protezione dei dati, il diritto d'accesso consente a chiunque di ottenere dai titolari del trattamento informazioni riguardo ai propri dati personali trattati.

Corollario di questo diritto è l'obbligo per i titolari del trattamento di fornire informazioni: se il titolare del trattamento dispone di dati personali relativi al richiedente, deve trasmetterglieli entro 30 giorni. Deve inoltre fornire informazioni in merito all'identità del titolare del trattamento, allo scopo del trattamento, alla durata di conservazione dei dati personali, alle

informazioni disponibili sulla provenienza dei dati personali nonché, se del caso, sui destinatari o sulle categorie di destinatari cui sono comunicati dati personali. Il termine può essere prorogato, ma quello nuovo deve essere comunicato entro il suddetto termine di 30 giorni.

È inoltre essenziale che il titolare del trattamento comunichi i dati personali trattati in quanto tali al fine di consentire alle persone interessate di verificare quali dati sono trattati, di accertarne l'esattezza e di assicurarsi della liceità del trattamento nonché, se del caso, di

domandarne la rettifica o la cancellazione.

In casi specifici previsti dall'articolo 26 LPD, il titolare del trattamento può rifiutare, limitare o differire la comunicazione di tali informazioni. In tal caso deve indicare il motivo della decisione al fine di permettere alla persona interessata di comprendere le ragioni della restrizione dell'accesso e di verificarne la legittimità.

Si noti inoltre che il titolare del trattamento si espone a conseguenze penali se comunica informazioni inesatte o incomplete (violazione degli obblighi di informare).

Obbligo di informazione

Nell'ambito del disegno di legge sui dati dei passeggeri aerei (D-LDPA), l'IFPDT ha sollevato (oltre a vari altri aspetti) la problematica dell'obbligo di informazione delle autorità (v. anche n. 1.6). Nel messaggio concernente la LDPA è pertanto precisato che i passeggeri aerei devono essere informati per iscritto dalle imprese di trasporto aereo del fatto che i loro dati vengono trattati non solo in relazione al volo, ma anche conformemente alla LDPA. L'informazione può essere contenuta nelle condizioni generali di contratto delle imprese di trasporto aereo. L'obbligo di informazione ai sensi dell'articolo 5 D-LDPA è giustificato anche se si tratta di una ripetizione: i dati dei passeggeri aerei sono trattati in due contesti totalmente diversi (gestione tecnica della prenotazione del volo/attuazione della LDPA), per scopi diversi (prenotazione del volo/lotta alle gravi forme di criminalità) e sotto responsabilità di natura diversa (impresa di trasporto aereo/fedpol). Lo scopo del trattamento dei dati deve essere chiaro leggendo l'informazione (cfr. art. 6 cpv. 3 LPD). Ulteriori dettagli da fornire alle persone interessate emergeranno dall'attuazione dell'ordinanza sulla protezione dei dati.

Diritto di cancellazione

In riferimento alla cancellazione dei dati, nell'anno in rassegna l'IFPDT ha constatato che le richieste vengono ottemperate sia dai titolari del trattamento dei dati personali privati che all'interno dell'Amministrazione federale. In singoli casi le difficoltà derivano più da circostanze tecniche che dalla disponibilità a cancellare i dati. Ciò accade, ad esempio, quando un privato condivide una piattaforma di dati con altri fornitori e la persona interessata desidera cancellare i dati di un solo fornitore, in quanto in tal caso nella pratica possono verificarsi dipendenze di natura tecnica.

Attività di sorveglianza e campagne in base alla nuova LPD

La nuova legge sulla protezione dei dati ha rafforzato i diritti delle persone interessate e conferito all'IFPDT ulteriori compiti e poteri, che attuerà attraverso gli strumenti e le attività di sorveglianza elencati di seguito:

Strumenti

Sul sito Internet dell'IFPDT sono disponibili i seguenti strumenti:

- **formulari per il deposito di una denuncia:** attraverso i formulari persone interessate e soggetti terzi possono segnalare presunte violazioni della LPD;
- **portali di notifica per i titolari del trattamento:** attraverso i nostri portali di notifica i titolari del trattamento possono comunicarci una violazione della sicurezza dei dati («data breach») o la nomina di un consulente per la protezione dei dati.

Attività di sorveglianza

In base al promemoria concernente l'apertura di un'inchiesta per violazione delle disposizioni sulla protezione dei dati, le attività di sorveglianza possono essere così classificate:

- **inchiesta formale:** le inchieste che devono essere svolte in base alle norme di procedura amministrativa della Confederazione servono a indagare su trattamenti di dati personali che, in base a indizi sufficienti, potrebbero violare le norme di protezione dei dati della Confederazione;
- **accertamenti preliminari informali:** nell'ambito degli accertamenti informali preliminari, l'IFPDT verifica se vi sono le condizioni per l'apertura di un'inchiesta formale;
- **intervento a bassa soglia:** gli interventi a bassa soglia sono comunicazioni scritte inviate ai titolari del trattamento per invitarli a contribuire su base volontaria, in modo tale che per un determinato trattamento, nei casi di accertamenti dei fatti semplici, sia garantita la conformità alle norme in materia di protezione dei dati.

Campagne

Prima di avviare d'ufficio delle attività di sorveglianza contro titolari del trattamento privati o organi federali, l'IFPDT può richiamare l'attenzione di questi soggetti sui rischi in materia di protezione dei dati e sulle misure che si possono adottare per ridurli o anticipare loro delle precisazioni sulla sua procedura di sorveglianza attraverso campagne di sensibilizzazione.

Promemoria e guide

Se necessario le precisazioni circa la procedura di sorveglianza sono documentate all'interno di promemoria e guide. Nell'anno in rassegna queste ultime sono state integrate dalle seguenti pubblicazioni:

- Foglio informativo: Pianificare e motivare l'accesso online ai dati personali (18 giugno 2024);
- Guida dell'IFPDT concernente il trattamento di dati mediante cookie e tecnologie simili (22 gennaio 2025);
- Guida per la notifica di violazioni della sicurezza dei dati e l'informazione alle persone interessate secondo l'articolo 24 LPD (6 febbraio 2025)

Attività di sorveglianza in cifre

Nell'esercizio 2024/2025 l'IFPDT ha ricevuto oltre 1000 denunce. Per i dati statistici, cfr. tabella 9 a pagina 91.

Campagna di sensibilizzazione sull'utilizzo del numero AVS

L'IFPDT ha lanciato una campagna di sensibilizzazione riguardo agli obblighi dei dipartimenti federali e della Cancelleria federale in caso di utilizzo sistematico del numero AVS. La campagna rammenta in particolare a tali organi l'obbligo di effettuare analisi periodiche dei rischi.

Nell'ambito di una strategia proattiva, l'IFPDT ha lanciato una campagna di sensibilizzazione presso i dipartimenti federali e la Cancelleria federale riguardo all'utilizzo del numero AVS. Tale campagna è intesa, da un lato, a richiamare le disposizioni legali che disciplinano l'utilizzo sistematico del numero AVS al di fuori delle assicurazioni sociali e, dall'altro lato, a verificarne l'attuazione tramite verifiche a campione.

Alcune disposizioni specifiche introdotte dalla legge federale sull'assicurazione per la vecchiaia e per i superstiti (LAVS) impongono infatti agli utenti una serie di obblighi tecnici e organizzativi. Tra tali misure, l'articolo 153e LAVS stabilisce due obblighi distinti. Da un lato, i dipartimenti federali e la Cancelleria federale hanno l'obbligo di svolgere periodicamente analisi dei rischi per le banche dati da essi gestite che tengano conto in particolare del rischio di collegamenti illeciti tra banche dati. Dall'altro lato, per gli scopi delle analisi dei rischi tali unità devono tenere un elenco delle banche dati in cui è utilizzato sistematicamente il numero AVS.

In quanto servizi di contatto dell'IFPDT ai sensi dell'articolo 28 dell'ordinanza sulla protezione dei dati (OPDa), il 26 settembre 2024 i consulenti per la protezione dei dati di tutti i dipartimenti federali e della Cancelleria federale hanno ricevuto una comunicazione scritta da parte dell'IFPDT con cui si ricordava loro gli obblighi legali secondo la LAVS. Ulteriori chiarimenti sono stati forniti nella seduta interdipartimentale del 30 ottobre 2024.

L'avvio di questa campagna è stato inoltre presentato ai consulenti per la protezione dei dati degli uffici federali il 26 novembre 2024 in occasione di una riunione informativa.

Obbligo di designare un rappresentante secondo l'articolo 14 LPD

L'IFPDT ha invitato le imprese estere che trattano grandi quantità di dati di persone in Svizzera a designare un rappresentante in Svizzera.

Per assicurarsi che la legge si applichi a tutte le fattispecie che esplicano effetti in Svizzera anche se si verificano all'estero, l'articolo 14 LPD precisa i casi in cui deve essere designato un rappresentante in Svizzera. Tale designazione ha in particolare lo scopo di garantire un interlocutore sul territorio svizzero alle persone interessate e alle autorità, nonché di limitare i casi in cui vi è una minore protezione dei residenti in Svizzera dovuta unicamente al fatto che il titolare del trattamento ha sede o domicilio all'estero.

Pertanto, tutte le imprese private che effettuano un trattamento di dati personali legato a un'offerta di merci o prestazioni o finalizzato a porre sotto osservazione il comportamento di persone in Svizzera, e tale trattamento è su grande scala, periodico e comporta un rischio elevato per la personalità delle persone interessate, devono designare un rappresentante in Svizzera.

L'IFPDT è quindi intervenuto in maniera mirata presso numerose imprese internazionali rispondenti ai criteri previsti dalla legge al fine di verificare la designazione del rispettivo rappresentante nonché la pubblicazione dei relativi dati di contatto.

Sul sito dell'IFPDT sono disponibili ulteriori informazioni sull'obbligo di designare un rappresentante secondo l'articolo 14 LPD (v. Protezione dei dati > Conoscenze di base).

Notifica di violazioni della sicurezza dei dati

L'IFPDT ha pubblicato una guida per la notifica di violazioni della sicurezza dei dati e aperto due inchieste nei confronti di titolari del trattamento che non hanno informato gli interessati riguardo a una siffatta violazione.

Dall'entrata in vigore della riveduta legge sulla protezione dei dati, i titolari del trattamento devono notificare all'IFPDT ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. Nell'anno in esame, l'IFPDT ha ricevuto 275 notifiche secondo l'articolo 24 capoverso 1 LPD.

Sia in virtù della vecchia legge sulla protezione dei dati, sia di quella vigente, i titolari del trattamento hanno segnalato violazioni, sebbene non prevedano un rischio elevato per le persone interessate. Si tratta di segnalazioni volontarie, ad esempio perché la violazione potrebbe suscitare un'eco media-tica o perché persone interessate o informatori (whistleblower) potrebbero annunciarsi all'IFPDT.

In caso di notifiche obbligatorie, l'IFPDT verifica sommariamente se le misure attuate o pianificate dal titolare del trattamento sono sufficienti a proteggere le persone interessate e a ridurre i danni. Se necessario, l'IFPDT chiede maggiori dettagli sui fatti o esige ulteriori misure per la protezione di dette persone. Verifica inoltre se esse sono state adeguatamente informate in merito all'incidente. Nel caso di segnalazioni volontarie per le quali il titolare del trattamento non ha identificato un rischio elevato per le persone interessate, in linea di principio verifica soltanto se esiste un obbligo di informare nei confronti degli interessati e, all'occorrenza, come esso è stato adempiuto.

Nell'anno in esame l'IFPDT ha constatato che tra i titolari del trattamento regnava incertezza sulla nozione di «rischio elevato», che comporta un obbligo di notifica all'IFPDT, e sulla sua distinzione dalla nozione di «necessità di proteggere», che rende necessario informare le persone interessate. Ad alcuni titolari del trattamento non è inoltre apparso chiaro quali compiti debbano svolgere in relazione alla presa di conoscenza e all'esame di notifiche obbligatorie e di segnalazioni volontarie e all'attuazione degli obblighi di informare nei confronti di suddette persone.

Al fine di fornire ai titolari del trattamento un ausilio nell'adempimento dei propri obblighi e per fare chiarezza sul loro ruolo, il 22 gennaio 2025 l'IFPDT ha pubblicato una guida sulla gestione delle violazioni della sicurezza dei dati. In tale documento, precisa i criteri secondo cui i titolari del trattamento devono valutare se sussiste un obbligo di notifica all'IFPDT. La guida specifica inoltre che le persone interessate

devono essere informate se possono o devono prendere dei provvedimenti per ridurre o scongiurare un danno derivante da una violazione della sicurezza dei dati. Ad esempio se devono modificare dati di accesso o password, bloccare carte di credito, esaminare criticamente estratti conto o messaggi e richieste (più precisamente e-mail di phishing).

L'IFPDT può esigere che il titolare del trattamento informi le persone interessate se, a suo giudizio, è necessario proteggerle o se, a causa del loro numero elevato o di una copertura mediatica, sussiste un interesse pubblico a un'informazione da parte sua. L'IFPDT è autorizzato a impartire tale ordine indipendentemente dal fatto che la violazione gli sia stata comunicata prima dal titolare del trattamento in modo volontario o in adempimento dell'obbligo di notifica o che non sia stato affatto informato.

L'IFPDT ha aperto un'inchiesta nei confronti di due titolari del trattamento secondo l'articolo 49 segg. LPD, poiché non avevano informato, o non lo avevano fatto a sufficienza, della violazione le persone interessate, sebbene ciò sembrava necessario per la loro protezione. Entrambi i titolari del trattamento hanno sostenuto che non era dato un obbligo di informare e anche dopo richiesta dell'IFPDT si sono rifiutati di informare suddette persone della violazione. Le procedure sono ancora in corso.

Violazioni della sicurezza dei dati in cifre

Nell'esercizio 2024/2025 l'IFPDT ha ricevuto 363 notifiche di violazioni della sicurezza dei dati. I dati esatti relativi alle segnalazioni di violazioni dei dati sono riportati nel capitolo 3.1.

Aumentano i controlli sulle VIPD

Dopo l'entrata in vigore della revisione della legge federale sulla protezione dei dati, svariati organi federali hanno inviato le proprie valutazioni d'impatto sulla protezione dei dati (VIPD) all'IFPDT chiedendo un parere. La VIPD è un documento che deve essere predisposto quando si presume che il trattamento di determinati dati comporti un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

La valutazione d'impatto sulla protezione dei dati (VIPD) è uno strumento che permette ai titolari del trattamento di rilevare, valutare e trattare i rischi in materia di protezione dei dati. Se dalla VIPD emerge che, nonostante le misure pianificate dal titolare, il trattamento dei dati previsto comporta comunque un rischio elevato per la personalità o i diritti fondamentali della persona interessata, occorre richiedere un parere all'IFPDT.

Sono esentati da tale obbligo i titolari del trattamento privati che si sono rivolti ai rispettivi consulenti per la protezione dei dati. Per loro l'IFPDT già nel 2023 aveva pubblicato un promemoria sulla VIPD. I feedback ricevuti dai privati circa questo strumento e il suo utilizzo sono stati in larga parte positivi e diversi soggetti hanno creato modelli d'esempio e strumenti di valutazione automatizzati. L'IFPDT ha

accolto con favore queste iniziative private, in particolare perché permettono di apportare le necessarie modifiche alla VIPD in modo più semplice.

Le VIPD nei progetti della Confederazione

Come previsto svariati organi federali ci hanno inviato le loro VIPD chiedendo un parere, perché, in base alle linee guida in materia del Consiglio federale, tale documento deve essere allegato alle consultazioni degli uffici in merito ai progetti di legge (ad es. anche nel caso della consultazione relativa alla legge sui dati dei passeggeri, LDPA, cfr. n. 1.6).

Attraverso le integrazioni presentate, l'IFPDT ha voluto fornire soprattutto un riassunto che spiegasse in modo chiaro al Consiglio federale e al Parlamento quali sono i rischi derivanti dal trattamento dei dati previsto e le misure adottate per limitarne gli effetti, in modo tale che gli organi politici possano prendere le dovute decisioni consapevoli dei rischi residui.

Attuazione dell'obbligo di verbalizzazione

Con la nuova legge sulla protezione dei dati (LPD) e la rispettiva ordinanza (OPDa), il 1° settembre 2023 è entrato in vigore anche l'obbligo di verbalizzazione sancito dall'articolo 4 OPDa. Tale norma stabilisce che, in caso di trattamento automatico di dati personali, il titolare del trattamento e il suo responsabile del trattamento sono tenuti a verbalizzare i processi come la registrazione, la modifica, la lettura, la comunicazione, la cancellazione e la distruzione dei dati. Grazie ai dati verbalizzati è possibile accettare, indagare e fare luce sui casi di violazione della protezione dei dati.

L'obbligo di verbalizzazione si applica, tra l'altro, anche all'intera Amministrazione federale con le sue molteplici applicazioni. Questo obbligo è già in vigore da più di 20 anni per il trattamento di dati personali degni di particolare protezione e per i profili della personalità. Inoltre, è un elemento della protezione IT di base (n. T2.1 c) e n. 5) che deve essere attuato da tutte le unità amministrative della Confederazione. Nei sistemi informativi di grandi dimensioni dell'Amministrazione federale, come ad esempio il sistema di gestione degli affari GEVER, la verbalizzazione è una prassi comune anche per i dati personali ordinari.

Disposizione transitoria per l'introduzione della verbalizzazione della lettura

Per conciliare l'introduzione della funzione di verbalizzazione richiesta dall'articolo 4 capoverso 2 OPDa con i cicli di sviluppo dei sistemi TIC, l'articolo 46 OPDa prevede una disposizione transitoria: per i sistemi che non rientrano nel campo d'applicazione della direttiva Schengen (UE) 2016/680, l'estensione dell'obbligo di verbalizzazione entra in vigore solo dopo tre anni dall'entrata in vigore dell'OPDa (quindi a partire dal 1° settembre 2026) o alla fine del ciclo di vita del relativo sistema. In questo modo l'obbligo può essere sospeso finché non saranno comunque necessarie delle modifiche al sistema.

L'obiettivo di questa disposizione è sgravare temporaneamente dall'obbligo una parte delle applicazioni, in modo tale che i sistemi informativi della Confederazione non debbano essere adeguati tutti contemporaneamente a partire dal 1° settembre 2026.

Sfide e misure

L'obbligo di verbalizzazione si applica sia ai titolari del trattamento sia ai loro responsabili del trattamento, che, in caso di trattamento automatico di dati personali, dovranno verbalizzare i processi come la registrazione, la modifica, la lettura, la comunicazione, la cancellazione e la distruzione dei dati. La verbalizzazione garantisce che vi sia trasparenza sui trattamenti dei dati effettuati ed è importante per poter intervenire rapidamente in presenza di violazioni della protezione dei dati. I dati verbalizzati servono infatti ad accettare, indagare e analizzare eventuali violazioni di questo tipo.

L'obbligo di verbalizzazione può però comportare un onere notevolmente maggiore per i gestori delle applicazioni. In particolare, il progressivo adeguamento e gli interventi per rendere scalabile l'attuale infrastruttura IT ai nuovi requisiti richiederà un impegno aggiuntivo.

L'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ha preparato, sulla base di valori empirici, una stima dei costi che nell'ambito della consultazione degli uffici in merito all'OPDa ha portato alla richiesta di introdurre delle limitazioni in base al rischio all'obbligo di verbalizzazione. Nel corso del 2025 l'IFPDT organizzerà delle tavole rotonde per confrontarsi con gli uffici federali interessati, così da tenere debitamente in considerazione queste richieste nel rispetto delle disposizioni legali vigenti.



← 2



1.2 Giustizia, polizia, sicurezza

CIBERCRIMINALITÀ

Le inchieste nei confronti della ditta Xplain e degli uffici federali fedpol e UDSC si sono concluse con l'adozione delle raccomandazioni

Nel quadro delle tre inchieste contro fedpol e UDSC nonché contro la ditta Xplain, l'IFPDT ha rilevato violazioni alla legge sulla protezione dei dati. Dai risultati pubblicati delle inchieste emerge, da un lato, che dati personali di fedpol e dell'UDSC sono stati trasmessi alla ditta privata Xplain senza le necessarie misure di protezione dei dati e, dall'altro, che quest'ultima li ha successivamente conservati contravvenendo alle norme di protezione dei dati e in parte anche ai contratti stipulati.

Nei suoi rapporti, l'IFPDT conclude che né l'Ufficio federale di polizia (fedpol) né l'Ufficio federale della dogana e della sicurezza dei confini (UDSC) avevano stabilito in modo chiaro con Xplain se fosse consentito, ed eventualmente a quali condizioni, memorizzare dati personali sul server di Xplain nel quadro delle attività di supporto fornite da quest'ultima. Sarebbe, tuttavia, stato necessario stabilire esplicitamente in quale misura i dati personali potevano essere trasmessi a Xplain ed essere

memorizzati dalla stessa. In sostanza, i dati personali giungevano a Xplain nel quadro di casi di supporto, senza che quest'ultima avesse definito requisiti precisi per la trasmissione e la sicurezza dei dati. Sul server dell'azienda si sono quindi accumulati dati non strutturati provenienti dagli uffici federali interessati. L'IFPDT ha inoltre constatato che la quantità di dati personali trasmessi nell'ambito di tale processo era eccessivamente alta (cfr. in merito anche il 31° rapporto d'attività, n. 1.2 nonché i comunicati stampa del 21.2.2023, 14.7.2023 e 1.5.2024).

Raccomandazioni per l'esternalizzazione

Nell'ambito dell'utilizzo e dello sviluppo delle sue applicazioni digitali, l'Amministrazione federale collabora con aziende private alle quali viene affidato il trattamento di dati personali. Il riesame dell'attacco ransomware subito da Xplain in un'ottica di vigilanza giuridica evidenzia chiaramente l'entità dei rischi e i possibili danni derivanti da tale tipo di trasmissione di dati. L'adozione delle raccomandazioni vincola l'Amministrazione federale e tutti i suoi fornitori di servizi privati a rilevare questi rischi elevati e a ridurli tempestivamente a un livello accettabile, prendendo provvedimenti idonei.

Secondo quanto è emerso dalle tre inchieste, è necessario dunque che siano rispettati i seguenti principi della legislazione federale in materia di protezione dei dati:

- in qualità di «titolari del trattamento» ai sensi del diritto in materia di protezione dei dati, gli organi federali che collaborano con aziende private che assumono il ruolo di «responsabili del trattamento» (p. es. nell'ambito della fornitura di servizi di supporto) sono tenuti a valutare se sia necessario che dati personali escano dall'infrastruttura TIC protetta dell'Amministrazione

federale o che fornitori privati accedano a tale infrastruttura. Devono inoltre verificare se sia possibile anonimizzare i dati personali prima della loro trasmissione e valutare gli ulteriori provvedimenti tecnici o organizzativi da adottare per evitare eventuali violazioni della protezione dei dati;

- dopo aver analizzato i rischi rilevanti in termini di protezione dei dati e definito i provvedimenti idonei per mitigarli, gli organi federali e i fornitori privati devono documentare in modo completo e comprensibile i loro processi di attuazione (p. es. flussi di dati, anonimizzazione e modalità di accesso). Gli organi federali sono inoltre tenuti a definire nei contratti stipulati con i fornitori privati i provvedimenti tecnici e organizzativi necessari, pattuendo, se necessario, pene convenzionali; ▪ nell'ambito del trattamento di dati personali, i fornitori privati responsabili del trattamento devono rispettare gli obblighi e le condizioni contrattuali in merito all'entità, all'intensità e alla durata del trattamento. A questo fine sono considerati provvedimenti idonei i piani per la cancellazione tempestiva dei dati, la sensibilizzazione e la formazione dei collaboratori, nonché periodiche revisioni interne o esterne.

Fedpol e l'UDSC, così come Xplain, hanno adottato integralmente le raccomandazioni dell'IFPDT relative all'attacco ransomware subito da Xplain alla fine di maggio 2024 (cfr. comunicato stampa del 4.6.2024).

Gli accertamenti dei fatti contro l'UDSC e fedpol in merito alla legittimità degli accessi effettuati dal personale dell'UDSC al registro nazionale di ricerca RIPOL gestito da fedpol sono stati separati dalla procedura riguardante Xplain e sono ancora in corso.

Controlli all'interno dell'Amministrazione federale

Nel suo comunicato stampa del 4 giugno 2024 relativo alla chiusura della procedura riguardante Xplain, l'IFPDT ha esortato l'Amministrazione federale e i suoi fornitori di servizi privati a riesaminare la loro collaborazione per quanto riguarda il trattamento di dati personali in base ai risultati delle tre inchieste. In tale contesto sono stati inoltre annunciati controlli in tutta l'Amministrazione federale.

A settembre 2024 l'IFPDT ha effettuato i primi controlli campione all'interno dell'Amministrazione federale.

LEGISLAZIONE

Revisione della legge sulle attività informative

La legge federale sulle attività informative (LAIn) sarà modificata allo scopo di ridefinire e ampliare il trattamento dei dati nell'ambito delle attività informative. In seguito all'inchiesta amministrativa concernente l'acquisizione di informazioni da parte dell'ambito Ciber del Servizio delle attività informative della Confederazione (SIC), il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS)

Piattaforma POLAP per lo scambio di dati in ambito di polizia

Nella sua decisione 1C_63/2023 del 17 ottobre 2024, il Tribunale federale ha confermato le critiche che l'IFPDT aveva formulato a più riprese nel periodo di rapporto 2023/2024 al riguardo del previsto collegamento tra i sistemi di informazione delle polizie cantonali tramite POLAP, una piattaforma informativa con partecipazione della Confederazione (v. in merito anche il 31° Rapporto d'attività, n. 1.2).

Il Tribunale federale era stato adito mediante ricorso in una causa che verteva su una regolamentazione del Cantone di Lucerna volta a permettere il collegamento dei sistemi cantonali a POLAP in previsione della sua entrata in funzione. Il Tribunale federale ha annullato la regolamentazione ritenendo, da un lato, che gli accessi previsti non disponessero di una base legale sufficientemente determinata e, dall'altro, che le possibilità estese di accesso mediante procedura di richiamo violassero il principio di proporzionalità e i diritti degli interessati garantiti nel contesto delle procedure di assistenza amministrativa.

Le autorità della Confederazione e dei Cantoni competenti in materia di protezione dei dati hanno raccomandato di rivedere il progetto di convenzione della CDDPG concernente lo scambio di dati in ambito di polizia con coinvolgimento della Confederazione, raccomandazione che non è ancora stata attuata. Inoltre manca tuttora la base legale esplicita annunciata da fedpol per la gestione della piattaforma di consultazione, che è parte integrante della Strategia nazionale per la lotta alla criminalità organizzata. L'IFPDT parte dal presupposto che la Confederazione e i Cantoni continueranno i loro lavori nel corso del prossimo periodo di rendiconto e si attende di essere tenuto al corrente, unitamente alle autorità cantonali partner, in merito agli sviluppi previsti e consultato tempestivamente su tutte le questioni concernenti la protezione dei dati.

ha diviso in due parti i lavori in corso per la revisione LAIn. Per quanto riguarda la prima parte e gli adeguamenti del diritto di accesso disciplinati al suo interno, l'IFPDT ha già espresso il proprio parere lo scorso anno (cfr. 29° rapporto d'attività, n. 1.2).

La revisione prevede la ridefinizione del trattamento dei dati nell'ambito delle attività informative. Nel progetto di legge sono infatti riportate le categorie di dati personali trattati al posto dei singoli sistemi d'informazione. Entro luglio 2025 dovrebbe essere svolta un'ulteriore consultazione relativa alla seconda parte della revisione. L'IFPDT accompagna i lavori.



1.3 Economia e società

TRACCIAMENTO TRASVERSALE ALLA PIATTAFORMA

Presa di posizione di Ricardo e TX Group riguardo alle raccomandazioni

Nell'anno in esame, l'IFPDT ha pubblicato il suo rapporto finale dopo aver offerto a Ricardo e a TX Group l'opportunità di prendere posizione in merito alle raccomandazioni formulate. L'Icaricato sta valutando le ulteriori azioni a seguito del rigetto delle sue conclusioni.

Nella primavera del 2024, l'IFPDT ha concluso il procedimento condotto secondo il diritto previgente, relativo alla piattaforma d'asta Ricardo e al tracciamento trasversale effettuato

all'interno della piattaforma a fini di pubblicità mirata, avviato nei confronti di Ricardo e di TX Group (TX).

Nel suo rapporto finale, l'IFPDT ha raccomandato in particolare a Ricardo di adeguare la piattaforma affinché gli utenti siano informati in modo chiaro e trasparente riguardo al tracciamento effettuato da TX e alle relative finalità, nonché di ottenere il consenso degli utenti prima di comunicare i dati a TX per scopi pubblicitari mirati. L'IFPDT ha invitato TX a cancellare i dati già

trasmessi in tale contesto qualora non fosse in possesso del consenso richiesto (cfr. 31° rapporto d'attività, n. 1.3).

Le due società hanno espresso le proprie osservazioni in merito al rapporto finale e alle raccomandazioni dell'IFPDT. Nelle rispettive prese di posizione, Ricardo e TX contestano la qualifica dei dati quali dati personali e, di conseguenza, l'applicazione della legge sulla protezione dei dati. Entrambe le società hanno comunicato l'intenzione di non conformarsi alle raccomandazioni, ritenute infondate o prive di oggetto, in quanto riferite a una situazione ormai superata e a una legge nel frattempo abrogata.

Guida concernente il trattamento di dati mediante cookie e tecnologie simili

L'utilizzo di cookie e tecnologie simili da parte dei gestori di siti web e app e il relativo trattamento dei dati riguarda chiunque navighi quotidianamente su Internet. L'IFPDT era entrato nel dettaglio di questo tipo di trattamento dei dati basandosi sulla precedente LPD durante gli accertamenti dei fatti riguardo la piattaforma d'asta Ricardo e contro Digitec Galaxus. Con la revisione della legge sulla protezione dei dati, che ha sostituito il termine profilo della personalità con i termini profilazione e profilazione a rischio elevato, si pone ora la domanda in merito ai nuovi aspetti a cui i gestori di siti Internet e di app devono prestare attenzione nell'ambito dell'utilizzo di cookie e tecnologie simili.

Per fornire chiarimenti a questo riguardo e in merito alla sua attività di vigilanza in base alla nuova normativa, il 22 gennaio 2025 l'IFPDT ha pubblicato una guida, destinata principalmente ai titolari del trattamento privati, ma che contiene anche riferimenti specifici alle disposizioni speciali applicabili agli organi federali.

La guida spiega:

- il modo in cui la disposizione speciale dell'articolo 45c della legge sulle telecomunicazioni deve essere applicata cumulativamente alle disposizioni della LPD;
- quali sono le responsabilità dei gestori dei siti Internet in caso di impiego di servizi e cookie di terze parti;
- il modo in cui è possibile adempiere ai propri obblighi di informare;
- e il modo in cui si possono garantire i diritti di configurazione delle persone interessate e come possono essere attuati dal profilo tecnico per ottenere un consenso che rende legittimo il trattamento o come può essere riconosciuto il diritto di opposizione garantito dalla legge.

ACCOUNT UTENTI

L'IFPDT si è riservato la facoltà di adottare misure adeguate a imporre gli adeguamenti necessari della piattaforma Ricardo, qualora dovesse riscontrare il perdurare delle inadempienze evidenziate nel suo rapporto finale. Il 22 gennaio 2025 ha pubblicato una guida sull'utilizzo dei cookie contenente indicazioni concrete sui requisiti da rispettare per garantire la conformità con la nuova LPD.

Su richiesta di Ricardo e di TX, nell'ottobre 2024 l'IFPDT ha pubblicato una versione censurata del suo rapporto finale, accompagnato da un comunicato stampa. In seguito a una richiesta di accesso ai sensi della legge sulla trasparenza (LTrans), la versione integrale del rapporto è stata resa pubblica sul sito Internet dell'IFPDT nel marzo 2025.

L'IFPDT segue l'attuazione delle raccomandazioni accolte dalla piattaforma di e-commerce

Il 15 aprile 2024 l'IFPDT ha concluso il suo accertamento dei fatti sulla piattaforma di e-commerce svizzera Digitec Galaxus con l'emanazione di raccomandazioni formali. Al momento sta seguendo l'attuazione della raccomandazione accolta dall'azienda, che dovrebbe avvenire nel secondo trimestre del 2025.

La raccomandazione accolta dalla piattaforma online svizzera Digitec Galaxus riguarda la mancata possibilità di opporsi al trattamento dei dati oggetto dell'inchiesta, in particolare a scopo di marketing. Per effettuare un ordine sul sito, infatti, l'azienda richiedeva la creazione di un account utente, ma il trattamento dei dati che ne deriva non è assolutamente necessario per l'esecuzione del contratto di acquisto, pertanto porre come condizione per l'acquisto la creazione di un account utente viola il principio della proporzionalità (cfr. 31° rapporto d'attività, n. 1.3). L'IFPDT ha quindi racco-

mandato a Digitec Galaxus di modificare il trattamento dei dati, per garantire che i trattamenti dei dati effettuati non ingeriscano più del necessario nel diritto all'autodeterminazione informativa dei clienti.

A dicembre 2024 Digitec Galaxus ha presentato all'IFPDT una possibile soluzione per l'attuazione della raccomandazione accolta, che era stata formulata applicando ancora la vecchia LPD. Digitec Galaxus ha comunicato che le raccomandazioni saranno attuate concretamente nel secondo trimestre del 2025. Il 22 gennaio 2025 l'IFPDT ha pubblicato una guida completa all'impiego dei cookie contenente suggerimenti concreti che Digitec Galaxus deve rispettare per garantire la conformità alle norme in materia di protezione dei dati a seguito dell'entrata in vigore della nuova LPD.

CAMPAGNA ONLINE

Inchiesta sull'associazione Bürgerforum Schweiz

L'IFPDT ha esaminato i trattamenti di dati dell'associazione «Bürgerforum Schweiz» in relazione alla campagna online «Pfarrer-Check». Oggetto dell'inchiesta è la raccolta di dati di contatto di parroci e di altre persone attive nell'ambito ecclesiastico finalizzata all'invio di un questionario. A ciò si aggiunge la gestione di una banca dati in Internet che rende pubblico, tra l'altro, chi ha ricevuto il questionario e quali risposte ha eventualmente fornito. Poiché alcune persone sono state inserite nella banca dati contro la loro volontà, l'IFPDT ha ordinato un provvedimento amministrativo sul quale il Tribunale amministrativo federale è ora chiamato a decidere.

Nel corso del 2023 l'IFPDT è venuto a conoscenza dei trattamenti di dati dell'associazione Bürgerforum Schweiz in relazione alla campagna online «Pfarrer-Check». L'associazione raccoglie dati personali di persone attive nell'ambiente ecclesiastico (parroci, membri di un consiglio parrocchiale o del sinodo, dipendenti delle università, operatori che lavorano con i giovanili ecc.) i cui indirizzi sono pubblicamente reperibili, per sottoporre loro un questionario. Le

domande sono intese a verificare se le persone interpellate condividono le visioni di Bürgerforum in merito alla fede. L'associazione, che gestisce una banca dati pubblicamente accessibile contenente tali informazioni, si è rifiutata di accogliere la richiesta delle persone, che figurano nella sua banca dati contro la loro volontà, di cancellare i dati che le concernono (cfr. 31° rapporto d'attività, n. 1.3).

A fine 2023 l'IFPDT ha aperto un'inchiesta formale per esaminare in maniera più approfondita il trattamento di dati in questione e verificarne la conformità con il diritto in materia di protezione dei dati, giungendo alla conclusione che l'associazione ha violato il principio di proporzionalità pubblicando nella banca dati pubblicamente accessibile anche i dati di persone che sono state soltanto «registerate» o semplicemente «interpellate». Secondo l'IFPDT, questi dati

non sono né adatti a ottenere informazioni affidabili sulle convinzioni religiose delle persone interessate, né necessari a dimostrare la rappresentatività del sondaggio. La loro pubblicazione richiede pertanto una giustificazione ai sensi della legge sulla protezione dei dati.

L'IFPDT ritiene che non sussista un interesse pubblico o privato prevalente che giustifichi l'inserimento nella banca dati di persone che sono pubblicamente elencate altrove con lo statuto di «registrato» o «interpellato». Indipendentemente dal fatto che figurino su un altro sito pubblicamente accessibile, per essere registrate nella banca dati le persone devono aver fornito il proprio consenso preventivo legalmente valido. Se una persona ha presentato una richiesta di cancellazione, i suoi dati devono essere cancellati. Nella primavera del 2024 l'IFPDT ha ordinato un provvedimento amministrativo in tal senso (cfr. 31° rapporto d'attività, n. 1.3) contro il quale, nell'anno in esame, l'associazione Bürgerforum ha interposto ricorso al Tribunale amministrativo federale, la cui decisione è ancora in sospeso.



MERCATO IMMOBILIARE

Domande inammissibili nei moduli d'iscrizione per la locazione di un alloggio

I moduli d'iscrizione per la locazione di un alloggio, messi a disposizione dai locatori, devono essere conformi alla protezione dei dati. L'IFPDT chiarisce la situazione giuridica secondo la nuova LPD e ammonisce gli amministratori di immobili i cui moduli contengono domande che ingeriscono eccessivamente nei diritti della personalità dei candidati interessati alla locazione di un alloggio.

Già negli anni Novanta, l'IFPDT aveva emanato delle raccomandazioni in merito alla gestione dei dati personali degli interessati alla locazione di alloggi

(cfr. 4° rapporto d'attività 1996/1997, pag. 49 [non disponibile in italiano]). La raccolta di dati riguardanti le persone interessate alla locazione è in linea di massima autorizzata nella misura in cui tali informazioni siano appropriate per scegliere, secondo criteri oggettivi, un locatario adeguato. Il trattamento dei dati deve essere in particolare trasparente e rispettare lo scopo previsto; quest'ultimo è definito dalla possibilità di concludere il contratto di locazione. Conformemente al principio di proporzionalità, possono quindi essere rilevati e trattati soltanto i dati oggettivamente necessari al raggiungimento di tale scopo. Il trattamento dei dati non può violare inutilmente la sfera privata degli interessati. Una decisione presa nel 1996 dall'allora Commissione per la protezione dei dati ha confermato in gran parte l'opinione dell'IFPDT e rappresenta da quel momento la base della sua prassi plurienale.

Nell'anno in esame, l'IFPDT ha avuto nuovamente l'occasione di affrontare questa tematica e, a seguito della revisione della legge sulla protezione dei dati, di verificare l'attualità della sua prassi sulla base di esempi concreti. Numerose persone interessate hanno presentato segnalazioni

riguardanti i moduli d'iscrizione per la locazione di un alloggio e anche i media hanno più volte segnalato all'IFPDT esempi discutibili. Nell'anno in rassegna l'IFPDT ha quindi messo in atto una campagna comprendente misure a tre livelli.

In adempimento del suo incarico di sensibilizzazione, ha in particolare adattato il «Promemoria concernente i moduli d'iscrizione per la locazione di un alloggio» per fare chiarezza sui requisiti legali in materia di protezione dei dati. Ha semplificato alcune formulazioni e aggiunto degli esempi che illustrano come i locatori possono raccogliere e trattare i dati degli interessati alla locazione di un alloggio rispettando i principi della LPD.

Nel quadro del suo mandato di consulenza, l'IFPDT ha avuto uno scambio di vedute con l'Associazione Svizzera dell'economia immobiliare (SVIT) e l'Associazione svizzera dei proprietari fondiari (HEV), ribadendo la propria posizione in merito all'inammissibilità delle domande relative a stato civile, nazionalità, luogo d'origine, religione, attuale situazione abitativa e copie del documento d'identità. Le motivazioni del settore hanno però convinto l'IFPDT che una copia dell'estratto del registro delle esecuzioni può essere richiesta a tutti gli interessati già durante la procedura di candidatura e non, come ritenuto in precedenza dall'IFPDT, solo al locatario scelto. È però importante che le copie riguardanti tutti i candidati all'alloggio non scelti siano subito cancellate. Il promemoria è stato adattato di conseguenza in questo punto ed è anche stato trasmesso all'Associazione Svizzera Inquilini.

L'IFPDT ha colto l'occasione per attirare l'attenzione del settore su altri problemi legati alla protezione dei dati nel quadro del processo di locazione di alloggi, come ad esempio la comunicazione di informazioni relative all'attuale locatario per organizzare una visita

dell'abitazione oppure le fotografie dell'abitazione occupata scattate senza il consenso del locatario. Dopo questo scambio di vedute, la SVIT ha aggiunto questi punti nelle sue raccomandazioni settoriali concernenti i dati personali nei moduli d'iscrizione per la locazione di un alloggio.

Nell'ambito del suo mandato di vigilanza, l'IFPDT ha analizzato i moduli d'iscrizione per la locazione di alloggi di diverse agenzie immobiliari della Svizzera tedesca e della Svizzera francese che gli sono state segnalate. Laddove erano richiesti dati che violavano il principio di proporzionalità, l'IFPDT

ha contattato per iscritto i responsabili nell'ottica di un intervento «a bassa soglia». In particolare sono state rilevate domande concernenti la nazionalità, lo stato civile o la presenza di una curatela. Sono state anche poste domande inammissibili sull'attuale situazione abitativa, per esempio sulla durata del contratto di locazione, sul numero di stanze o sull'importo del canone di locazione. Alcune agenzie immobiliari richiedevano inoltre sistematicamente i conteggi dello stipendio degli ultimi tre mesi o l'originale dell'estratto del registro delle esecuzioni, oppure i loro moduli comprendevano una dichiarazione di consenso generale che permetteva ai futuri locatori di raccogliere tutte le ulteriori informazioni necessarie sui candidati. In un singolo caso, l'agenzia immobiliare ha addirittura incaricato un investigatore privato di effettuare presso terzi accertamenti riguardanti un candidato.

Anche se la maggior parte degli interventi dell'IFPDT sono stati efficaci, non tutte le agenzie immobiliari contattate si sono dichiarate disposte ad adeguare volontariamente la loro prassi. A seguito della crescente digitalizzazione del settore immobiliare, l'IFPDT continuerà quindi a essere confrontato anche



1.4 Salute

DOPING

Trasmissione di dati medici di atleti svizzeri

La trasmissione sistematica delle cartelle sanitarie all'Agenzia mondiale antidoping (AMA) a fini di controlli puntuale risulterebbe sproporzionata e non si baserebbe su una base giuridica sufficiente. L'AMA aveva chiesto a Swiss Sport Integrity (SSI) di adottare tale misura. Tuttavia, a seguito dell'intervento dell'IFPDT, SSI potrà continuare a seguire la prassi attuale.

Nell'ambito della lotta contro il doping Swiss Sport Integrity (SSI) collabora con l'AMA, la quale ha in particolare il compito di vigilare sul rispetto del Programma mondiale antidoping. L'AMA ha effettuato un audit di SSI a seguito del quale ha ordinato l'adozione di una serie di misure. Una di esse riguardava i dati degli atleti in possesso di un'esenzione a fini terapeutici (EFT), ossia l'esenzione speciale che consente a un atleta di assumere una sostanza dopante nell'ambito di un trattamento medico. Secondo tale misura, SSI sarebbe stata tenuta a trasmettere sistematicamente all'AMA le cartelle sanitarie di tutti gli atleti con EFT per consentire controlli puntuali. Finora SSI trasmetteva unicamente una sintesi concisa della situazione medica dell'atleta, mentre la

cartella sanitaria era inviata soltanto qualora l'AMA richiedesse effettivamente un controllo specifico su un atleta. Tale modifica della prassi avrebbe quindi comportato un trattamento dei dati molto più esteso, motivo per cui SSI ha ritenuto necessario consultarsi con l'IFPDT.

In una comunicazione successivamente invitata dal SSI all'AMA, l'IFPDT ha sottolineato che ogni trattamento di dati personali deve rispettare il principio di proporzionalità. Dopo una valutazione del caso, l'Incaricato ha concluso che la modifica richiesta

dall'AMA non fosse proporzionata. In particolare, l'invio sistematico delle cartelle sanitarie di tutti gli atleti con EFT non è necessario all'attività di sorveglianza dell'AMA, che si limita a effettuare controlli mirati. La prassi attuale risulta adeguata e consente all'AMA di svolgere i controlli quando lo ritiene opportuno, pertanto la modifica richiesta non risponde a un bisogno essenziale. Al contempo, va sottolineato l'interesse degli atleti a trasmettere i loro dati personali degni di particolare protezione soltanto in caso di effettivo controllo. In tale contesto, l'IFPDT ha peraltro ricordato che ogni trasmissione di dati a terzi, soprattutto all'estero (l'AMA ha sede in Canada), comporta un rischio aggiuntivo: tale rischio dovrebbe essere giustificato da un interesse preponderante, condizione che non si applica al caso in questione.

Infine, l'IFPDT ha anche osservato che SSI non disponeva verosimilmente di una base legale sufficientemente specifica per autorizzare una trasmissione sistematica di dati come richiesto.

L'AMA ha preso atto della posizione dell'IFPDT accettando che SSI mantenga la prassi attuale e ha deciso di chiudere la procedura a sua carico.

MODULI DEI PAZIENTI

Tra obbligo di informare e consenso

Il modulo di consenso sottoposto ai pazienti in occasione di una visita presso un medico o un altro terapeuta suscita numerosi interrogativi. Alla luce della confusione generata talvolta da tale modulo che riporta diversi aspetti giuridici, l'IFPDT intende sensibilizzare i fornitori di prestazioni, nonché le loro associazioni mantello, in merito ai requisiti della LPD a tale riguardo.

Nell'anno in rassegna l'IFPDT è stato regolarmente contattato su questioni inerenti i moduli di consenso dei pazienti. L'Incaricato pubblicherà a breve sul suo sito Internet un'informativa all'attenzione dei fornitori di prestazioni, nonché delle loro associazioni mantello, affinché se necessario adattino i propri moduli ai requisiti della legge federale sulla protezione dei dati (LPD).

A grandi linee, nell'ottica della protezione dei dati occorre distinguere tra i requisiti legati all'obbligo di informare e quelli del consenso.

L'obbligo di informare

Per i medici e gli altri terapeuti l'obbligo di informare non è nuovo: esisteva infatti già nella vecchia LPD in relazione al trattamento dei dati personali degni di particolare protezione, quali i dati sanitari. Con l'entrata in vigore della nuova LPD l'obbligo di informare è stato ampliato a tutte le categorie di dati personali.

Le informazioni da fornire devono comprendere tutte le indicazioni necessarie a garantire la trasparenza del trattamento e permettere alla persona interessata di far valere i propri diritti. Devono inoltre essere adeguate alle situazioni e includere perlomeno i dati di cui all'articolo 19 capoverso 2 LPD. Il livello di dettaglio dipende dal tipo di dati raccolti, dalla natura e dall'ampiezza del trattamento, dal rischio di lesione e dalla gravità della lesione della personalità.

L'obbligo di informare non è sottoposto ad alcun requisito formale. L'informazione deve essere trasparente, concisa, comprensibile e facilmente accessibile. Anche se l'informazione può essere fornita oralmente, per motivi di prova legati al rispetto dell'obbligo può essere opportuno documentare l'informazione o procedere in forma scritta. Tuttavia il paziente è libero di leggere (o meno) il documento e non è tenuto a confermarne la ricezione o a fornire il proprio consenso. In pratica, sono sufficienti precisazioni in un modulo o la trasmissione di una scheda informativa specifica (eventualmente da firmare per presa conoscenza).

Il consenso

Anche in questo ambito la nuova LPD non introduce modifiche sostanziali. Il consenso non è in linea di principio un presupposto per il trattamento, ma è previsto in quanto motivo giustificativo in particolare in occasione della comunicazione di dati personali degni di particolare protezione a terzi. Negli altri casi, il trattamento può eventualmente essere giustificato da un interesse privato preponderante se il trattamento è in relazione diretta con la conclusione o l'esecuzione di un contratto.

Per essere valido, oltre a dover essere fornito prima o al momento dell'inizio del trattamento per cui è richiesto, il consenso deve essere libero e informato: la persona interessata deve ricevere come minimo le informazioni di cui all'articolo 19 LPD. In funzione del contesto e della natura dei dati trattati, è talvolta necessario aggiungere precisazioni affinché la persona interessata sia in grado di valutare la portata del consenso. Il consenso deve inoltre essere specifico: deve essere fornito per uno o più trattamenti determinati e coprire tutte le finalità del trattamento. Non può essere fornito in modo generico per qualsiasi trattamento futuro.

La forma del consenso resta libera. Non è quindi necessario che sia scritta. Il titolare del trattamento deve tuttavia fornire la prova del consenso. Vi è quindi un interesse a documentare il consenso anche se non è dipendente dalla forma.

CARTELLA INFORMATIZZATA DEL PAZIENTE

Revisione completa della legge e finanziamento transitorio

Lo sviluppo della cartella informatizzata del paziente (CIP) prosegue. L'avamprogetto di revisione totale della legge in consultazione ha mostrato che è auspicata una maggiore centralizzazione. Su tale base, il Consiglio federale ha deciso che sarà ora compito della Confederazione mettere a disposizione l'infrastruttura tecnica e assicurarne lo sviluppo. Nel frattempo, il Parlamento ha approvato un finanziamento transitorio per la gestione e lo sviluppo della CIP. L'IFPDT segue il dossier.

Nell'estate del 2023 il Consiglio federale ha posto in consultazione l'avamprogetto di revisione completa della legge federale sulla cartella informatizzata del paziente (LCIP) in merito al quale l'IFPDT aveva preso posizione (cfr. 31° rapporto d'attività 2023/2024, n. 1.4). In tale contesto, erano prospettate diverse misure per continuare a migliorare e a sviluppare la cartella informatizzata del paziente, ad esempio l'obbligo di affiliazione per tutti i fornitori di prestazioni di cura o l'introduzione di un modello opt-out (diritto di opposizione in sostituzione del con-

senso esplicito). La revisione contiene inoltre un disciplinamento più chiaro dei ruoli della Confederazione e dei Cantoni nell'ambito della CIP.

Alla luce delle critiche pervenute riguardo alla struttura decentralizzata della CIP, il Consiglio federale mira ora a una maggiore centralizzazione della cartella informatizzata. Pertanto, nella sua seduta del 27 settembre 2024 ha deciso che sarà ora compito della Confederazione mettere a disposizione l'infrastruttura tecnica e assicurarne lo sviluppo. Al momento le diverse infrastrutture tecniche della CIP sono messe a disposizione dalle comunità e comunità di riferimento, le quali ricorrono a fornitori di piattaforme informatiche differenti.

Il messaggio concernente la revisione totale include questa modifica e sarà verosimilmente sottoposto al Parlamento nell'autunno del 2025.

Finanziamento transitorio, consenso e accesso ai servizi di ricerca dei dati

Considerato che la revisione totale della legge necessaria allo sviluppo della cartella informatizzata del paziente richiederà diversi anni, al fine di incoraggiare la diffusione e l'utilizzo immediato della CIP, il Consiglio federale ha presentato al Parlamento una revisione separata della LCIP concernente un finanziamento transitorio per gli offerenti di CIP (le comunità di riferimento). Per favorirne la gestione e lo sviluppo, nella primavera del 2024 il Parlamento ha approvato un aiuto finanziario di 30 franchi per ogni

CIP aperta, che sarà versato per un periodo di cinque anni dall'entrata in vigore di tale revisione. Il finanziamento transitorio è entrato in vigore il 1° ottobre 2024.

Questa revisione parziale permette inoltre di sancire la CIP nella legislazione come strumento dell'assicurazione obbligatoria delle cure medico-sanitarie (AOMS), facilitando la procedura di apertura delle cartelle. I pazienti possono ora esprimere il proprio consenso all'apertura di una CIP mediante il proprio strumento d'identificazione elettronica di un emittente certificato; non è più necessario fornire una firma autografa o elettronica. Inoltre i Cantoni avranno accesso al servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute per verificare il rispetto dell'obbligo degli ospedali, delle case per partorienti e delle case di cura, nonché dei medici ammessi dopo il 1° gennaio 2022 di affiliarsi a una comunità certificata o a una comunità di riferimento.

L'IFPDT continuerà a seguire attivamente lo sviluppo della CIP e a vigilare sul rispetto delle disposizioni sulla protezione dei dati, in particolare in occasione delle consultazioni degli uffici in materia di attuazione o nel quadro di questioni specifiche.

1.5 Lavoro

DIRITTO IN MATERIA DI PERSONALE FEDERALE

Piattaforma di segnalazione

L'IFPDT è intervenuto con diverse prese di posizione affinché il trattamento dei dati nell'ambito delle denunce e segnalazioni di illeciti o irregolarità effettuate dagli impiegati della Confederazione sia regolamentato in maniera più precisa a livello di legge.

Nel quadro del progetto di revisione della legge sul personale federale (LPers), l'IFPDT ha preso posizione a favore di un miglioramento delle disposizioni che disciplinano il trattamento dei dati nell'ambito delle denunce e segnalazioni di illeciti o irregolarità da parte di impiegati pubblici. Gli impiegati della Confederazione sono infatti tenuti a denunciare tutti i crimini e i delitti perseguitibili d'ufficio che constatano o sono loro segnalati nell'esercizio della loro funzione. Devono comunicarli ai loro superiori, al Controllo federale delle finanze (CDF) o alle autorità di perseguitamento penale. Possono inoltre segnalare altre irregolarità constatate o loro segnalate nell'esercizio della loro funzione.

Nella sua versione attuale l'articolo 22a LPers, che prevede le segnalazioni sull'apposita piattaforma del CDF, presenta alcune lacune. Sebbene il compito legale del CDF sia disciplinato dalla LPers e il registro delle segnalazioni sia

effettivamente notificato all'IFPDT, il trattamento dei dati non è di per sé definito nella legge, la quale prevede unicamente che «il CDF accerta i fatti e adotta i provvedimenti necessari». Il trattamento dei dati personali degni di particolare protezione effettuato dal CDF deve quindi essere regolamentato in modo dettagliato nella legge. Tanto più che le segnalazioni possono essere nominative e alcune di esse implicheranno persone specifiche e dati degni di particolare protezione, quali casi di indiscrezioni o di crimini di natura penale (corruzione, uso improprio di fondi, irregolarità in appalti pubblici ecc.).

Tenendo conto delle prese di posizione dell'IFPDT emesse durante le procedure di consultazione degli uffici, sono state apportate modifiche a livello dei progetti di revisione di tre diverse leggi federali. Tali modifiche riguardano

le precisazioni necessarie sia sulle segnalazioni e sulle relative procedure, sia sui trattamenti dei dati che ne derivano.

Di conseguenza, il progetto di modifica dell'articolo 22a LPers è stato completato con precisazioni sulle condizioni delle denunce e delle segnalazioni e chiarimenti riguardo agli organi presso i quali possono essere effettuate. In particolare, è stata disciplinata chiaramente a livello di legge la possibilità per gli impiegati del Dipartimento federale degli affari esteri (DFAE) di avvalersi direttamente della piattaforma di segnalazione del DFAE.

Sono state inoltre introdotte disposizioni specifiche sul trattamento dei dati effettuato dal CDF nel quadro delle sue attività relative alle segnalazioni e denunce in un nuovo articolo 10a della legge sul Controllo delle finanze (LCF; RS 614.0). Questo progetto di disposizione disciplina in particolare la gestione della piattaforma di segnalazione, il trattamento dei dati degni di particolare protezione effettuati al suo interno, nonché le comunicazioni dei dati ad altre autorità.

Infine, il trattamento dei dati associati alle segnalazioni trasmesse tramite la piattaforma del DFAE è stato regolamentato nella legge federale sul trattamento dei dati personali da parte del Dipartimento federale degli affari esteri (RS 235.2).

DIRITTO IN MATERIA DI PERSONALE FEDERALE

È stata in particolare inserita nel progetto una nuova sezione 10 intitolata «Persone connesse a segnalazioni di crimini, delitti e irregolarità» al fine di disciplinare il trattamento dei dati che il DFAE effettuerà in relazione alle segnalazioni di cui all'articolo 22a LPers sulla sua piattaforma.

Queste precisazioni, elaborate sulla base delle prese di posizione dell'IFPDT e introdotte nel quadro delle revisioni di tali leggi federali, assicureranno la certezza del diritto in materia di trattamento dei dati nell'ambito delle denunce e segnalazioni di illeciti o irregolarità da parte di impiegati pubblici e apparteranno al quadro legale l'adeguata densità normativa.

Profilazione nel contesto di valutazioni e ricerca attiva di personale

Nell'ambito della revisione della legge sul personale federale, l'IFPDT si è adoperato esprimendo diversi pareri affinché la base legale per la profilazione nel contesto di valutazioni e della ricerca attiva di personale sia sufficientemente precisa e trasparente. Si è inoltre dichiarato favorevole allo svolgimento preliminare di valutazioni d'impatto sulla protezione dei dati per siffatti metodi di trattamento dei dati, che valutino i rischi connessi e definiscano misure di protezione idonee.

Nell'ambito della revisione della legge sul personale federale (LPers), l'IFPDT si è pronunciato su diversi aspetti della protezione dei dati. Con l'entrata in vigore della nuova LPD, il termine «profilo della personalità» è stato soppresso e sono stati introdotti i termini «profilazione» e «profilazione a rischio elevato». La LPers deve quindi essere adeguata alla nuova terminologia. Due attività sono in primo piano: la valutazione (valutazioni e test di personalità di candidati e impiegati) e la ricerca attiva di personale. Mentre la valutazione è

già prevista dalla LPers vigente, non è ancora sancito dalla legge il processo di ricerca attiva di personale, cioè il trattamento di informazioni su persone che non sono né candidati né impiegati.

Affinché anche in futuro la Confederazione in quanto datore di lavoro possa utilizzare valutazioni nel settore del reclutamento, delle esigenze di promozione e del potenziale di sviluppo, ad esempio per stimare l'idoneità di un dipendente per un progetto o una promozione o per raccomandare agli impiegati una carriera professionale, la disposizione della LPers ha dovuto essere adeguata alla nuova nozione di profilazione.

Inoltre è necessaria una base legale per la ricerca attiva di personale, in modo che i datori di lavoro possano utilizzare i social media (come ad esempio LinkedIn) per cercare il personale idoneo e valutare l'idoneità di una persona per un posto specifico.

SORVEGLIANZA DEL PERSONALE

A seconda delle circostanze, siffatti trattamenti dei dati possono costituire non soltanto una profilazione, ma anche una a rischio elevato, poiché anche informazioni di per sé innocue possono rapidamente condensarsi in un'immagine completa di una persona che consente di valutare aspetti essenziali della personalità. È pertanto necessario creare una base legale sufficientemente precisa e trasparente per rispettare i principi di legalità e trasparenza. In particolare, per le diverse operazioni devono essere determinate le categorie di dati particolarmente sensibili necessarie a tal fine e quindi definite dalla legge. In seguito al parere dell'IFPDT, l'Ufficio federale del personale (UFPER) ha integrato e precisato di conseguenza la disposizione.

L'IFPDT ha inoltre sostenuto che per i metodi di trattamento previsti dalla revisione della legge devono essere svolte valutazioni d'impatto sulla protezione dei dati poiché, a causa della natura e dell'entità del trattamento, la profilazione può comportare un rischio elevato per la personalità delle persone in questione. Si devono dunque identificare i rischi connessi e descrivere le

misure di protezione appropriate per affrontarli. L'UFPER ha quindi eseguito le analisi dei rischi richieste, individuandone diversi e definendo relative misure per mitigarli. Ne fanno parte, tra le altre, il disciplinamento legale delle autorizzazioni di accesso, misure in materia di sicurezza dei dati, la formazione e la sensibilizzazione dei collaboratori, l'introduzione di istruzioni nonché la verbalizzazione dei trattamenti. I risultati dell'analisi dei rischi sono stati presentati nel messaggio del Consiglio federale all'attenzione delle Camere federali.

Rispetto dei principi di protezione dei dati nell'ambito della sorveglianza del personale

L'impiego di sistemi di sorveglianza sul posto di lavoro ha portato a numerosi interventi dell'IFPDT. Perché l'utilizzo di questi sistemi sia conforme alla normativa in materia di protezione dei dati è necessario, in particolare, che i dati siano trattati solo nella misura strettamente necessaria e che i collaboratori siano adeguatamente informati. Nell'anno in rassegna l'IFPDT è stato più volte contattato in riferimento alla conformità dei sistemi di videosorveglianza alle norme in materia di protezione dei dati. In alcuni casi è intervenuto nell'ambito di indagini preliminari e interventi a bassa soglia, richiamando l'attenzione sui principi della protezione dei dati. Inoltre, ha aperto un'inchiesta su un sistema di sorveglianza.

Il datore di lavoro è autorizzato a trattare i dati del lavoratore solo nella misura in cui questi riguardano la sua



65797 km

D / B
PARK
N R

idoneità al rapporto di lavoro oppure sono necessari all'esecuzione del contratto di lavoro (principio di proporzionalità). Ciononostante, il datore di lavoro deve proteggere la salute e la personalità dei lavoratori. Sono pertanto vietati sistemi di sorveglianza volti a monitorare in modo mirato il comportamento dei dipendenti. Se invece i sistemi di sorveglianza devono essere installati per altri motivi, è necessario che questi siano configurati in modo da non pregiudicare la salute e la libertà di movimento dei dipendenti. La sorveglianza deve quindi essere limitata allo stretto necessario. Nel caso di un impianto di videosorveglianza, ad esempio, ciò significa che le registrazioni non possono essere utilizzate per controllare il comportamento dei lavoratori e che il datore di lavoro deve avere un legittimo interesse aziendale

per farne uso, che prevale sull'interesse del lavoratore alla tutela della sua personalità. Le videocamere devono essere posizionate e impostate in modo tale che l'area registrata sia ridotta al minimo indispensabile e che i lavoratori possano uscire dall'inquadratura. Inoltre, di principio le registrazioni non sono consentite nelle zone di ristoro.

Oltre a questo, è importante anche la trasparenza. Prima di iniziare a utilizzare questi sistemi, i collaboratori devono essere informati in modo esauriente e comprensibile sul tipo, sullo scopo e sul raggio di azione del sistema di sorveglianza impiegato. Spesso però nella pratica si osservano lacune a questo riguardo: i lavoratori in molti casi non vengono informati, o non a sufficienza, in merito all'impiego di misure di sorveglianza.

Il rispetto di questi principi è fondamentale perché nei rapporti di lavoro è possibile fare appello al consenso solo in misura limitata quando si parla di misure di sorveglianza ritenuto che il lavoratore, data la sua posizione subordinata, spesso non è libero di decidere.

Sorveglianza del personale

La sorveglianza del personale è un tema di cui l'IFPDT si occupa regolarmente: la registrazione digitale del tempo di lavoro, il tracciamento GPS o l'accesso alle e-mail di lavoro dei dipendenti sono solo alcuni esempi di situazioni che spesso sollevano questioni relative alla protezione dei dati. Nel corso dell'anno si è conclusa la procedura di accertamento dei fatti relativa alla registrazione digitale del tempo di lavoro presso un'impresa di pulizia di edifici (v. 27° Rapporto d'attività, n. 1.6).

1.6 Trasporti

PROGETTO SWISSCOM BROADCAST

L'IFPDT chiede delle risposte in merito alla rete di droni di Swisscom

Con la rete di droni svizzera di Swisscom Broadcast nei prossimi anni sarà realizzata una nuova infrastruttura per voli automatizzati con i droni, che consentirà l'utilizzo dei droni «as a Service», ad esempio per ispezioni all'interno di infrastrutture, interventi di polizia o per la protezione di vaste aree.

Per garantire che durante l'utilizzo di questa infrastruttura i dati personali siano trattati in conformità con la normativa in materia, l'IFPDT ha svolto degli accertamenti presso Swisscom Broadcast, l'azienda che fornisce il servizio. Dall'indagine è emerso che il gestore della rete di droni adotta le misure necessarie per garantire la protezione dei dati. In particolare, prima della messa in esercizio di una rete di droni è previsto un esame preliminare dei rischi, nonché una valutazione dell'impatto sulla protezione dei dati in caso di rischi elevati per la personalità o i diritti fondamentali degli interessati. L'IFPDT continuerà a seguire la realizzazione di questa infrastruttura e si confronterà regolarmente con il gestore.

BIOMETRIA

Riconoscimento facciale presso l'aeroporto di Zurigo

Il riconoscimento facciale presso l'aeroporto di Zurigo può essere introdotto soltanto se è presente una base legale. Dal momento che il progetto implica un rischio potenzialmente elevato per la personalità e i diritti fondamentali degli interessati, l'IFPDT ha analizzato nel dettaglio il progetto.

Flughafen Zürich AG ha informato l'IFPDT di avere in programma l'acquisizione di una tecnologia che consente l'identificazione dei passeggeri aerei attraverso un riconoscimento facciale automatizzato e ha chiesto all'Icaricato di fornire una prima valutazione di questo progetto in base alle norme in materia di protezione dei dati. Dal momento che per il controllo delle carte d'imbarco dei passeggeri aerei, e quindi per la loro identificazione, si farebbe ricorso a dati biometrici, che ai sensi della LPD sono considerati dati personali degni di particolare protezione, questo tipo di trattamento in generale comporterebbe rischi elevati per la personalità e i diritti fondamentali degli interessati.

L'aeroporto di Zurigo svolge la sua attività in base a una concessione d'esercizio secondo la legge federale sulla navigazione aerea; pertanto, è da considerarsi un organo federale ai sensi della LPD. Perché gli organi federali possano trattare dati personali degni di particolare protezione è tuttavia necessaria una base all'interno di una

legge formale. La legge sulla navigazione aerea attualmente in fase di revisione, rifacendosi ai regolamenti in vigore a livello internazionale, prevederà la possibilità di impiegare dati biometrici per il controllo delle carte d'imbarco. Fino alla sua entrata in vigore, però, manca una base legale formale. L'impiego di questa tecnologia è quindi consentito soltanto alle condizioni quadro previste dalla LPD per i progetti pilota.

Stando a quanto affermato dall'aeroporto di Zurigo, il riconoscimento facciale previsto dovrebbe essere utilizzato soltanto per i controlli delle carte d'imbarco e su base volontaria. Inoltre, all'interno dell'aeroporto di Zurigo le zone nelle quali i passeggeri in futuro potranno farsi registrare attraverso i propri dati biometrici saranno opportunamente segnalate. L'IFPDT ha analizzato con cura le condizioni quadro sia legali che tecniche del trattamento e, se il progetto verrà attuato, seguirà l'aeroporto di Zurigo dal punto di vista della sorveglianza di legge.

PASSENGER NAME RECORDS

Legge sui dati dei passeggeri aerei

Attualmente in Svizzera non è possibile utilizzare in modo sistematico i dati di chi viaggia a bordo di un aereo a causa dell'assenza di una base legale. Tuttavia, tale base sarà istituita con l'entrata in vigore della legge sui dati dei passeggeri aerei (LDPA). Il Consiglio nazionale e il Consiglio degli Stati hanno approvato la legge il 21 marzo 2025. Il termine per il referendum scade il 10 luglio 2025.

Al momento della prenotazione di un volo i passeggeri devono comunicare alle compagnie aeree o alle agenzie di viaggio determinati dati personali, tra cui nome e cognome, dati di contatto (inclusi l'indirizzo e il recapito telefonico), agenzia di viaggio e informazioni sulle modalità di pagamento. La raccolta di questi dati (in inglese «Passenger Name Records» o «PNR») è disciplinata da norme internazionali dell'ONU, dell'Organizzazione dell'aviazione civile internazionale (OACI) e dell'UE e contribuisce alla lotta contro il terrorismo e altre gravi forme di criminalità. Gli Stati Uniti hanno deciso che la Svizzera dovrà obbligatoriamente comunicare questi dati per rimanere nel «Visa Waiver Program» (VWP), il programma che consente l'ingresso negli USA senza visto per motivi professionali o turistici (v. articolo relativo a BTLE e EDPB al n. 1.7).

Oltre al disegno di legge sui dati dei passeggeri aerei (LDPA), l'IFPDAT ha esaminato anche la valutazione d'impatto sulla protezione dei dati elaborata dall'ufficio federale competente. Le precisazioni che ha richiesto sono state integrate. L'IFPDAT continuerà a seguire il progetto.

PIATTAFORMA PER I TP NOVA

Controlli sulle FFS

L'IFPDAT ha verificato l'implementazione sulla piattaforma di distribuzione centrale NOVA delle modifiche da lui richieste in merito alla protezione dei dati. In relazione alla segnalazione del 2022 di una vulnerabilità sulla piattaforma centrale di distribuzione NOVA, gestita dalle FFS per conto dell'organizzazione di settore dei trasporti pubblici Alliance SwissPass (cfr. 29° rapporto d'attività, n. 1.7 e 31° rapporto d'attività, n. 1.6), l'IFPDAT ha chiesto alle FFS di effettuare un audit per verificare se le regole sulla cancellazione in NOVA fossero state integrate così come richiesto.

A partire dal 1° gennaio 2024, l'organizzazione di settore ha inoltre introdotto standard vincolanti in materia di sicurezza delle informazioni, noti come Prescrizione 591, che le imprese di trasporto collegate a NOVA sono tenute a rispettare. Le imprese di trasporto già associate dovevano comprovare attraverso un'autovalutazione il rispetto delle relative prescrizioni entro la fine di giugno 2024. L'IFPDAT ha quindi chiesto alle FFS di presentare un rapporto anche riguardo a tale adempimento.

Le FFS hanno informato l'IFPDAT che all'inizio del 2024 è stato effettuato un audit, dal quale è emerso che le norme relative alla cancellazione erano state pienamente implementate in tutte le applicazioni NOVA. Inoltre erano state realizzate tutte le strutture necessarie per consentire l'esecuzione degli audit sulla Prescrizione 591 e un costante sviluppo continuo. Nel corso del 2025 sarà fornito un quadro più oggettivo della situazione attuale. L'IFPDAT continuerà a seguire il progetto.



1.7 Internazionale

Data la presenza sul mercato svizzero di aziende del settore tecnologico attive a livello globale, l'IFPDT si trova ad affrontare numerose questioni di carattere transfrontaliero concernenti l'esecuzione per le quali, grazie alla modernizzazione degli atti legislativi in materia di protezione dei dati, sono ora disponibili a livello nazionale, europeo e mondiale strumenti migliori che devono essere sfruttati.

Per l'applicazione della LPD e degli accordi di diritto pubblico internazionale alle aziende attive in tutto il mondo la collaborazione transfrontaliera con le autorità estere di controllo della protezione dei dati è indispensabile. Grazie allo scambio più rapido delle informazioni nell'ambito dell'assistenza amministrativa internazionale è possibile sia fornire una migliore protezione giuridica alle persone interessate dal trattamento dei dati, sia migliorare la certezza del diritto per i soggetti che sono responsabili di tale trattamento.

Nel contesto informale dei cosiddetti «adequacy groups», l'IFPDT si è confrontato anche su questo tema con le autorità competenti in materia di protezione dei dati di quegli Stati che l'UE ha riconosciuto formalmente provvisti di una legislazione in materia di protezione dei dati e di

misure esecutive della stessa che garantiscono un livello di protezione equivalente. Per quanto riguarda le piattaforme social e altre offerte di grandi aziende internazionali, ha illustrato alcune soluzioni attraverso le quali sarebbe possibile accelerare l'assistenza amministrativa transfrontaliera e semplificare la notificazione di documenti.

Da un lato, la Convenzione europea sulla notificazione all'estero dei documenti in materia amministrativa (RS 0.172.030.5 – CENA94), applicabile anche alla vigilanza sulla protezione dei dati, consente una notificazione più semplice dei documenti tra gli Stati contraenti. Dall'altro, la LPD attribuisce all'IFPDT la competenza per dichiarare alle autorità estere competenti in materia di protezione dei dati che nel loro caso la Svizzera consente la notificazione diretta dei documenti se garantiscono all'IFPDT di accordargli il medesimo diritto.

«DATA SCRAPING»

Dichiarazione comune finale sull'estrazione di dati

Dopo aver pubblicato una dichiarazione comune sull'estrazione di dati nel 2023, l'IFPDT e i suoi omologhi di altre 16 autorità hanno collaborato con alcune delle maggiori imprese di media sociali al mondo. Tale collaborazione si è conclusa con la pubblicazione di una dichiarazione finale contenente nuove indicazioni per il settore.

L'estrazione massiccia di dati personali («data scraping») dalle piattaforme dei media sociali, in particolare per alimentare i sistemi di intelligenza artificiale, suscita crescenti preoccupazioni. In tale ottica, le autorità di protezione dei dati del mondo intero hanno integrato la dichiarazione comune del 2023 aggiungendo una dichiarazione finale. In essa sono fornite indicazioni supplementari per aiutare le imprese ad assicurare che le informazioni personali dei loro utenti siano protette dall'estrazione illegale di dati, e in particolare che le organizzazioni:

- si conformino alle leggi sulla protezione dei dati e delle informazioni personali quando utilizzano le informazioni personali (comprese quelle provenienti dalle proprie piattaforme) per sviluppare modelli linguistici di grandi dimensioni per mezzo dell'intelligenza artificiale;

SWISS-US DPF

- si dotino di una serie di misure di protezione combinate, le rivedano e le aggiornino regolarmente per tenere conto dell’evoluzione delle tecniche e delle tecnologie di «data scraping»;
- si accertino che il «data scraping» a fini commerciali o di utilità sociale sia legittimo e conforme a rigorose modalità contrattuali.

La prima dichiarazione, firmata nel 2023 (cfr. 31° rapporto d’attività, n. 1.7), è poi stata sottoposta alle società madri di YouTube, TikTok, Instagram, Threads, Facebook, LinkedIn, Weibo e X (ex Twitter).

Questo approccio ha dato vita a un dialogo tra le autorità di protezione dei dati e diverse di queste imprese di media sociali, nonché con l’alleanza per l’attenuazione degli effetti dell’estrazione non autorizzata di dati (Mitigating Unauthorized Scraping Alliance), un’organizzazione volta a lottare contro il «data scraping» non autorizzato. Le autorità di protezione dei dati hanno quindi potuto comprendere meglio le sfide che le organizzazioni devono affrontare per proteggersi dal «data scraping» illegale, in particolare il crescente livello di sofisticazione degli autori di queste pratiche, i costanti progressi di tale tecnologia e la difficoltà di distinguere gli operatori non autorizzati dagli utenti autorizzati.

In generale, le imprese di media sociali hanno confermato alle autorità di protezione dei dati l’attuazione di buona parte delle misure contenute nella dichiarazione iniziale. Tra le misure aggiuntive presentate nella dichiarazione comune finale sono da rilevare l’utilizzo di elementi di concezione delle piattaforme che rendono più difficile il «data scraping» automatizzato, misure di protezione che si avvalgono dell’intelligenza artificiale e soluzioni a costo inferiore che le piccole e medie imprese potrebbero utilizzare per rispettare gli obblighi in materia di protezione dei dati.

Quadro di riferimento per la comunicazione di dati personali negli Stati Uniti

Dopo l’intesa su un quadro di riferimento per la trasmissione di dati personali negli Stati Uniti raggiunta nel 2023 dall’Unione europea e dal Regno Unito con gli Stati Uniti (v. 31° Rapporto d’attività, n. 1.7), il 15 settembre 2024 è entrato in vigore l’analogo «Data Privacy Framework» (Swiss-US DPF) tra la Svizzera e gli Stati Uniti. Questi ultimi sono quindi stati inseriti nell’elenco, sotto-posto all’approvazione del Consiglio federale, degli Stati che garantiscono una protezione adeguata dei dati, fermo restando che l’idoneità concerne soltanto le imprese statunitensi certificate in base a questo framework.

Il quadro di riferimento giuridico su cui si basa la decisione di adeguatezza del Consiglio federale comprende, oltre al DPF, anche l’«executive order» 14086 (decreto presidenziale) relativo all’introduzione di un meccanismo di ricorso in due fasi, garanzie aggiuntive per le persone interessate e diverse disposizioni d’esecuzione attraverso le quali il ministero della giustizia statunitense concretizza le garanzie sancite dal decreto presidenziale.

Il meccanismo di ricorso in due fasi dovrebbe permettere, da un lato, di migliorare le possibilità di protezione giuridica evidenziate dalla sentenza



«Schrems II» e, dall’altro, di colmare le lacune del vecchio «Swiss-US Privacy Shield». Nella prima fase, il «Civil Liberties Protection Officer» (CLPO; l’incaricato statunitense per la tutela delle libertà civili) dell’«Office of the Director of National Intelligence» (ODNI; l’ufficio del direttore dell’intelligence nazionale) esamina i ricorsi individuali. Una volta che il CLPO ha terminato la sua inchiesta, la persona interessata può richiedere che la decisione sia esaminata in una seconda fase dall’appena creata «Data Protection Review Court» (DPRC; corte di revisione in materia di protezione dei dati).

Ricorso all’IFPDT

Per tutta la durata della procedura le autorità americane e la persona interessata in Svizzera comunicano tra loro esclusivamente tramite l’IFPDT. Nella prima fase, la persona interessata presenta il proprio ricorso all’IFPDT il quale, prima di trasmettere il ricorso al CLPO-ODNI, ne verifica la completezza, e in particolare se soddisfa i requisiti

previsti per i ricorsi qualificati («qualifying complaint»). Per poter essere considerato tale, il ricorso deve essere presentato in forma scritta. Inoltre, il ricorrente deve dimostrare la sua identità e fornire le informazioni essenziali per permettere una verifica del ricorso. Non è necessario che il ricorrente presenti delle prove a conferma del sospetto di un’ingerenza da parte delle autorità statunitensi, è sufficiente una ragionevole verosimiglianza. Infine, il ricorrente deve indicare anche i mezzi specifici attraverso i quali i suoi dati sarebbero stati trasmessi negli Stati Uniti. Se tutti i requisiti sono soddisfatti, l’IFPDT trasmette il ricorso al CLPO-ODNI.

Al termine dell’esame da parte del CLPO, il ricorrente viene informato per il tramite dell’IFPDT che il suo caso è stato esaminato e che, rispettivamente, non sono state riscontrate violazioni oppure che il CLPO-ODNI ha disposto un’adeguata misura di riparazione. Attraverso queste risposte standard sempre dello stesso tenore non viene né confermato né negato che il ricorrente sia stato oggetto di attività da parte dei servizi di intelligence statunitensi. La persona interessata riceve una risposta standard dello stesso tenore tramite l’IFPDT anche nel caso in cui il ricorso sia inoltrato alla DPRC. Una procedura

analogia con risposte standard si applica anche in Svizzera per il trattamento delle richieste di informazioni ai sensi della legge federale sulle attività informative.

Imprese statunitensi non certificate

In caso di trasmissione di dati provenienti dalla Svizzera a imprese statunitensi non certificate sono ancora necessarie garanzie aggiuntive ai sensi dell’articolo 16 capoverso 2 LPD, che assicurino una protezione dei dati appropriata (p. es. clausole contrattuali tipo o regolamenti interni sulla protezione dei dati vincolanti). È tuttavia opportuno evidenziare che le garanzie e le possibili vie legali introdotte dall’«executive order» 14086 si applicano a tutte le trasmissioni di dati dalla Svizzera agli Stati Uniti e non soltanto a quelle che avvengono in base alla decisione di adeguatezza del Consiglio federale ai sensi dell’articolo 16 capoverso 1 LPD.

SCHENGEN**Valutazione della Svizzera**

Dal 20 al 24 gennaio 2025 un gruppo di esperti europei ha visitato la Svizzera quale Stato associato a Schengen per valutare l'applicazione dell'acquis di Schengen nell'ambito della protezione dei dati.

Un gruppo composto da esperti delle autorità di controllo in materia di protezione dei dati degli Stati membri di Schengen (approccio peer-to-peer), da un osservatore del Garante europeo della protezione dei dati (GEPD) e da una rappresentante della Commissione europea ha fatto visita alla Svizzera per valutare l'applicazione dell'acquis di Schengen nell'ambito della protezione dei dati.

Nel quadro del programma di valutazione pluriennale 2023–2029, tutti gli Stati membri di Schengen vengono valutati per stabilire le loro prestazioni complessive nell'applicazione dell'acquis di Schengen nei settori gestione delle frontiere esterne, assenza di controlli alle frontiere interne, politica in materia di visti, rimpatri, sistemi IT su larga scala a sostegno dell'applicazione dell'acquis di Schengen, cooperazione di polizia, cooperazione giudiziaria in materia penale e protezione dei dati. Il concetto di valutazione Schengen di terza generazione mira a ottenere un quadro completo dell'applicazione dell'acquis di Schengen rafforzando così la fiducia reciproca all'interno dello spazio Schengen. La valutazione non viene più effettuata ogni cinque, ma ogni sette anni (v. 31° Rapporto d'attività, n. 1.7).

La parte della valutazione che riguarda la protezione dei dati è volta ad accertare che i requisiti in materia di protezione dei dati previsti dall'acquis di Schengen siano stati attuati in modo efficace.

L'IFPDT ha partecipato attivamente ai lavori relativi a questa valutazione Schengen della Svizzera. Il 20 gennaio 2025 ha ricevuto gli esperti europei nei suoi uffici, ha presentato loro il suo ruolo e le attività che svolge e ha risposto alle domande ancora in sospeso.

Il diritto europeo prevede che, quattro settimane dopo la conclusione dell'attività di valutazione, la Commissione europea trasmetta alla Svizzera il progetto di relazione di valutazione e i progetti delle raccomandazioni. In seguito, la Svizzera ha due settimane di tempo per esprimere le proprie osservazioni in merito. La relazione di valutazione analizza gli aspetti qualitativi, quantitativi, operativi, amministrativi e organizzativi ed elenca le pratiche dimostratesi valide, le lacune e gli ambiti da migliorare, riscontrati durante la valutazione.

SCHENGEN**Gruppi di coordinamento del controllo dei sistemi d'informazione SIS, VIS ed Eurodac**

Il gruppo di coordinamento del controllo del sistema VIS è stato integrato nel «Coordinated Supervision Committee», ora responsabile dei sistemi di informazione EES ed ETIAS.

Il gruppo di coordinamento del controllo del sistema VIS (VIS SCG) è stato integrato nel «Coordinated Supervision Committee» (CSC) e si compone delle stesse autorità responsabili della protezione dei dati, tra cui è presente anche la Svizzera. La presidenza e il segretariato sono stati trasferiti dal Garante europeo della protezione dei dati (GEPD) al Comitato europeo per la protezione dei dati (EDPB). In futuro il CSC si occuperà anche dei sistemi di informazione EES («Entry/Exit System»), il nuovo sistema di ingressi-uscite, ed ETIAS («European Travel Information and Authorisation System»), il sistema europeo di informazione e autorizzazione ai viaggi.

Attualmente l'EDPB sta valutando il numero dichiarato la prima volta dagli Stati membri di Schengen di richieste di informazioni, di rettifica o di cancellazione pervenute in merito ai dati trattati nel SIS. Il rapporto, che dovrebbe essere completato nel corso del 2025, riporterà il numero dei casi in cui sono state fornite informazioni oppure i dati sono stati rettificati o cancellati.

SCHENGEN

L'entrata in funzione del sistema EES, prevista per il 10 novembre 2024, è stata posticipata data la mancanza di un sistema centrale sufficientemente stabile e resistente a livello europeo. Nei diversi Stati membri e associati a Schengen l'introduzione del sistema di informazione sarà graduale e dovrebbe essere completata a ottobre 2025.

Un rappresentante dell'IFPDT ha inoltre partecipato alla valutazione dell'Ungheria.

SCHENGEN**Gruppo di coordinamento delle autorità svizzere per la protezione dei dati**

Il gruppo di coordinamento Schengen delle autorità federali e cantonali svizzere responsabili della protezione dei dati, all'interno del quale l'autorità omologa del Liechtenstein ha lo statuto di osservatore, si è riunito due volte sotto la presidenza dell'IFPDT.

L'IFPDT ha informato le sue autorità partner cantonali sugli esiti delle sedute del gruppo di coordinamento del controllo europeo relative agli attuali sistemi d'informazione SIS e VIS, così come sullo stato di avanzamento delle attività di implementazione del sistema di ingressi-uscite (EES) e del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS). Il gruppo ha anche fatto visita all'Ufficio federale di polizia (fedpol) e all'Ufficio SIRENE annesso. Inoltre ha preparato i testi relativi ai sistemi SIS e VIS da pubblicare sulle pagine web cantonali e aggiornato le linee guida per i controlli SIS.

SCHENGEN**Attività a livello nazionale**

Sono stati completati i controlli presso fedpol quale punto d'accesso centrale del sistema centrale d'informazione visti (C-VIS) e dei file di registro presso il Corpo delle guardie di confine. L'IFPDT, inoltre, ha condotto anche un controllo dei file di registro SIS presso l'Ufficio centrale Armi di fedpol.

Il controllo effettuato presso l'Ufficio federale di polizia (fedpol) riguardava i dati trattati dalla Centrale operativa in qualità di punto d'accesso centrale al sistema C-VIS. Nel corso dei controlli l'IFPDT non ha rilevato trattamenti indebiti di dati personali e ha quindi potuto chiudere l'inchiesta senza emanare alcuna decisione.

SCHENGEN

Durante i controlli sui file di registro e sul trattamento dei dati presso il Corpo delle guardie di confine, l'IFPDT ha rilevato un accesso indebito al SIS. Ha chiesto all'Ufficio federale della dogana e della sicurezza dei confini (UDSC) di apportare modifiche alla gestione delle autorizzazioni e di effettuare controlli interni. L'IFPDT ne seguirà l'attuazione.

L'IFPDT ha effettuato controlli a campione sui file di registro dell'Ufficio centrale Armi di fedpol per verificare la liceità degli accessi effettuati dal personale autorizzato. Ha richiesto dunque al consulente per la protezione dei dati di fedpol i file di registro relativi a tutti gli accessi effettuati da tutto il personale nel periodo compreso tra il 4 e l'8 settembre 2024 e li ha analizzati. Nel suo rapporto finale del 19 dicembre 2024 l'IFPDT ha dichiarato di non aver riscontrato alcun accesso indebito.

BTLE ed EDPB

Quale sottogruppo di lavoro del Comitato europeo per la protezione dei dati (EDPB), il gruppo «Border Travel and Law Enforcement» (BTLE) si occupa di tematiche relative all'acquis di Schengen e di questioni più ampie in relazione all'accordo di Schengen. In qualità di Stato associato a Schengen la Svizzera partecipa ai lavori.
Nell'anno in esame il sottogruppo di lavoro BTLE ha concluso i lavori riguardanti le linee guida relative all'articolo 37 della Direttiva (UE) 2016/680 («Law Enforcement

Directive», LED) (v. 31° Rapporto d'attività, n. 1.7). L'articolo 37 LED stabilisce i requisiti legali (le garanzie) per i trasferimenti di dati in un Paese terzo al di fuori dello spazio EU/SEE. Le linee guida relative all'articolo 37 LED sono state approvate e adottate dall'EDPB a giugno 2024.

Inoltre, l'IFPDT ha partecipato anche ai lavori per l'attuazione della Direttiva (UE) 2016/681 («Passenger Name Record», PNR) in base alla sentenza PNR (C-817/19) della Corte di giustizia dell'Unione europea (CGUE). La sentenza riguarda l'uso dei dati del codice di prenotazione (dati PNR) al fine di prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi, e impone importanti limitazioni

CONSIGLIO D'EUROPA

al trattamento dei dati personali per fare in modo che l'applicazione della direttiva PNR sia in linea con la Convenzione europea dei diritti dell'uomo (CEDU). Alcune importanti limitazioni sono, tra le altre, l'uso esclusivo dei dati per reati di terrorismo e reati gravi nonché il termine massimo di cinque anni per la conservazione di tutti i dati del codice di prenotazione, che deve essere rigorosamente rispettato (v. anche articolo al n. 1.6).

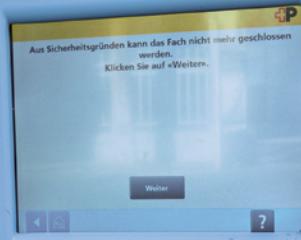
Al momento si sta inoltre lavorando sulle linee guida dell'EDPB relative al rapporto tra l'«AI Act» e le norme europee in materia di protezione dei dati (RGPD, LED).

Entrata in vigore della Convenzione 108+ prevista

L'entrata in vigore della Convenzione modernizzata in materia di protezione dei dati (Convenzione 108+) è prevista per la fine del 2026. In occasione delle sedute plenarie del Comitato consultivo del Consiglio d'Europa sulla Convenzione sulla protezione dei dati è stato approvato il terzo e ultimo modulo delle clausole contrattuali tipo per la trasmissione transfrontaliera di dati personali e le linee guida per il trattamento dei dati in relazione alle elezioni e alle votazioni. L'entrata in vigore della Convenzione modernizzata del Consiglio d'Europa in materia di protezione dei dati (Convenzione 108+) è stata ulteriormente posticipata, ma dovrebbe avvenire nel corso del 2026. Come spiegato nell'ultimo rapporto d'attività, la Convenzione entrerà in vigore solo quando il protocollo sarà stato ratificato da 38 Stati aderenti (v. 31° rapporto d'attività, n. 1.7). La Convenzione è aperta anche agli Stati che non sono membri del Consiglio d'Europa e in tal senso ha un impatto anche extra-europeo. A fine marzo 2025 la Convenzione era stata ratificata da 33 Stati, mentre 13 Stati l'avevano firmata ma non ancora ratificata. In numerosi Stati, tuttavia, la procedura di ratifica è nelle ultime fasi; per tale motivo è lecito supporre che l'entrata in vigore avverrà entro la fine del 2026. Con la Convenzione modernizzata (C108+) il Comitato consultivo sarà sostituito da un comitato della convenzione e sarà introdotto un meccanismo di valutazione.

L'IFPDT ha partecipato a entrambe le sedute plenarie e alle riunioni del Comitato consultivo della Convenzione 108+. Durante la seduta plenaria di giugno 2024 il Comitato ha approvato il terzo e ultimo modulo delle clausole contrattuali tipo per la trasmissione transfrontaliera di dati personali, che si applica alla comunicazione dei dati tra due responsabili del trattamento. Il primo modulo riguarda invece la comunicazione dei dati tra due titolari del trattamento, mentre il secondo modulo quella tra un titolare e un responsabile del trattamento. I tre moduli saranno riuniti in un unico documento. L'IFPDT ha riconosciuto le clausole contrattuali tipo del Consiglio d'Europa e le ha pubblicate sul proprio sito Internet. In aggiunta sono state approvate anche le linee guida per garantire la tutela dei diritti delle persone fisiche quando i loro dati personali sono trattati ai fini della registrazione e dell'autentificazione presso le urne.

All'ordine del giorno della seduta plenaria di novembre 2024 vi erano anche le elezioni per il rinnovo dell'ufficio del Comitato consultivo. Alla presidenza è stata eletta la rappresentante dell'autorità responsabile della protezione dei dati dell'Argentina. La rappresentante dell'IFPDT è stata confermata prima vicepresidente.



S

M



SPRING CONFERENCE**Conferenza europea dei commissari per la protezione dei dati**

Durante l'annuale conferenza primaverile («Spring Conference») le autorità europee di protezione dei dati si riuniscono per discutere di tematiche relative alla loro attività di vigilanza. Nel 2024 l'evento è stato organizzato dall'autorità per la protezione dei dati lettone e si è svolto a Riga dal 14 al 16 maggio.

Alla 32° «Spring Conference» hanno partecipato oltre 130 delegati e tre organizzazioni provenienti da 45 Paesi. I partecipanti si sono confrontati sulla loro attività di vigilanza e sulla cooperazione transfrontaliera che, dati gli sviluppi tecnologici, sta acquisendo sempre più importanza.

L'Incaricato federale ha partecipato alla tavola rotonda sulle modalità di cooperazione tra Stati SEE e Stati non-SEE e sulle sfide derivanti dal fatto che i grandi gruppi tecnologici attivi a livello mondiale trattano dati personali in diverse zone economiche.

ECHW**Workshop su casi pratici**

L'«European Case Handling Workshop» (ECHW) è un sottogruppo di lavoro della «Spring Conference». Nell'ambito di questo incontro annuale tra esperti si discute di casi tratti dall'attività pratica di vigilanza. L'ECHW 2024 è stato organizzato dall'autorità per la protezione dei dati estone e si è tenuto a Tallinn il 5 e il 6 dicembre 2024.

Durante i workshop si è discusso, tra l'altro, di casi concernenti l'impiego di videocamere in spazi pubblici e complessi residenziali, dello svolgimento delle valutazioni d'impatto sulla protezione dei dati e della definizione di dati personali sui social media. La rappresentante dell'IFPDT ha presentato un caso di studio sull'uso delle telecamere per il riconoscimento facciale negli spazi pubblici con aspetti di diritto comparato.

OCSE**Working Party on Data Governance and Privacy in the Digital Economy**

L'OCSE si impegna nella ricerca e nell'analisi nell'ambito della gestione dei dati e promuove il dibattito internazionale riguardo al diritto in materia di protezione dei dati alla luce degli sviluppi e delle sfide più recenti. Una delle priorità dell'OCSE è rafforzare la fiducia negli scambi di dati tra Paesi diversi e garantire che questi avvengano in modo sicuro ed efficiente. Attraverso il suo lavoro l'OCSE mira a promuovere un contesto digitale globale che permetta la trasmissione semplice e sicura dei dati oltre i confini nazionali.

Una delle priorità dell'OCSE è garantire un livello elevato di protezione e controllo sui dati, soprattutto in caso di trasmissione oltre i confini nazionali. L'obiettivo dell'OCSE è sviluppare standard e linee guida in grado di soddisfare le esigenze in termini di sicurezza dei dati e, al contempo, sostenere l'innovazione e il libero flusso di informazioni. L'OCSE si propone dunque di contribuire a creare un ambiente improntato alla fiducia e alla trasparenza in cui sia possibile valorizzare appieno il potenziale delle tecnologie digitali, garantendo al contempo la protezione dei diritti e delle libertà degli utenti.

Gruppo di lavoro per la gestione dei dati e la protezione della sfera privata

All'interno del gruppo di lavoro dell'OCSE l'IFPDT può fare affidamento su un suo rappresentante che si occupa della governance dei dati e della protezione della sfera privata nell'economia digitale («Working Party on Data Governance and Privacy in the Digital Economy», DGP). Tale gruppo è assoggettato al comitato dell'OCSE per la politica del mondo digitale («Committee on Digital Economy Policy», CDEP) e si compone dei delegati dei 38 Stati membri dell'OCSE, tra cui figurano in particolare i rappresentanti dei governi e delle autorità di protezione dei dati. Il gruppo collabora con gli altri gruppi di lavoro del CDEP e altri organismi dell'OCSE ed è responsabile dello sviluppo e della promozione di strategie empiriche per

la gestione dei dati e la protezione della sfera privata. Attraverso il suo lavoro mira a massimizzare i benefici sociali ed economici derivanti da un utilizzo efficace e su larga scala dei dati, affrontando al contempo i rischi associati e superando le sfide legate alla protezione della sfera privata.

Una delle principali attività del DGP consiste nell'analizzare l'accesso delle autorità ai dati dei privati, con l'obiettivo di favorire l'efficienza nello svolgimento dei compiti pubblici e, allo stesso tempo, di garantire una protezione efficace dei dati. Ha inoltre approfondito la complessa interazione tra diversi quadri normativi digitali con l'intento di creare strutture di governance efficienti e coerenti. Inoltre si è occupato del ruolo degli intermediari di dati fidati («data intermediaries»), il cui compito è consentire uno scambio sicuro ed efficiente dei dati assumendo un ruolo neutrale. Particolare attenzione è stata dedicata all'integrazione dell'intelligenza artificiale (IA) nei sistemi digitali e al significato delle tecnologie per il miglioramento della protezione dei dati («Privacy Enhancing Technologies», PET). Il DGP ha inoltre esaminato le dinamiche dei pagamenti transfrontalieri, al fine di ottimizzare l'efficienza e la sicu-

rezza di queste transazioni in un contesto economico globalizzato. L'obiettivo è quello di ottenere una panoramica degli effetti che governance dei dati, leggi in materia di protezione dei dati e regolamenti finanziari esercitano sui pagamenti transfrontalieri. In questo modo le autorità competenti per la protezione dei dati potrebbero acquisire una migliore comprensione del funzionamento di questo settore e delle sfide che deve affrontare per garantire la conformità alle norme e ai regolamenti.

SYMPOSIUM

Privacy Symposium a Venezia

L'estrazione massiccia di dati, la protezione della sfera privata nel quadro dell'azione umanitaria e la cooperazione internazionale e regionale sono stati al centro dei dibattiti del Privacy Symposium.

Con oltre 300 partecipanti che condividono le proprie prospettive, il Privacy Symposium offre un luogo di scambio per i professionisti della protezione dei dati, gli esperti, le autorità e i ricercatori.

L'IFPDT è intervenuto in diverse tavole rotonde, in particolare in materia di:

- estrazione di dati («data scraping»), insieme ad altre autorità di protezione dei dati firmatarie della dichiarazione comune sull'estrazione di dati (v. sopra la sezione dedicata al «data scraping»);
- protezione dei dati nell'azione umanitaria, insieme a organizzazioni internazionali e autorità di protezione dei dati (v. box dedicato al GT AID); in questo contesto i partecipanti si sono soffermati sulla relazione tra la protezione dei dati e l'azione umanitaria, dall'assistenza in risposta alle catastrofi al monitoraggio delle tendenze di spostamento, in cui i dati svolgono un ruolo fondamentale per assicurare interventi umanitari efficaci;

AMVP

Proteggere la vita privata nell'era digitale

Il potere dell'informazione è stato al centro dei dibattiti dell'Assemblea mondiale per la protezione della vita privata, che in occasione della sua riunione annuale ha adottato quattro risoluzioni su questioni essenziali.

Imperniata sul tema centrale «Il potere della i», la conferenza dell'Assemblea mondiale per la protezione della vita privata (AMVP) si è concentrata su otto tematiche importanti: individuo, innovazione, informazione, integrità, indipendenza, internazionale, interculturale e indigeno.

Nel corso della sessione aperta al pubblico, al centro del dibattito vi è stata la questione del rispetto e dell'equilibrio tra il potere dell'informazione e la necessità per i cittadini di controllare i propri dati personali. Gli argomenti affrontati hanno riguardato la determinazione dei danni alla vita privata, la protezione dei dati, la salute mentale, l'impatto della tecnologia sulle autorità di regolamentazione, nonché i vantaggi e le sfide degli strumenti di trasferimento dei dati. In parallelo, i partecipanti si

sono confrontati sul ruolo della confidenzialità dei dati nelle crisi umanitarie, sulla riduzione delle disparità in materia di diritto alla vita privata (esplorando le diverse dimensioni della confidenzialità della diversità), sulla condivisione dei dati tra governi e terze parti ecc., in un dialogo costruttivo volto sia a rafforzare l'efficacia dei modelli giuridici esistenti, sia a promuovere i mezzi per migliorarli in funzione dei cambiamenti tecnologici.

Nella sessione a porte chiuse l'AMVP ha adottato quattro risoluzioni:

- approvare e incoraggiare l'utilizzo di meccanismi di certificazione della protezione dei dati;

- i principi relativi al trattamento delle informazioni personali nell'ambito delle neuroscienze e delle neurotecnicologie;
- la libera circolazione dei dati in totale fiducia e la regolamentazione efficace dei flussi mondiali di dati;
- le nuove regole e procedure dell'AMVP.

L'AMVP, di cui l'IFPDT è membro, è stata istituita nel 1979. Riunisce le autorità di protezione dei dati di oltre 100 Paesi e ha lo scopo di discutere le principali sfide in materia di protezione della vita privata e il modo in cui gli organismi di regolamentazione possono lavorare efficacemente, sia individualmente sia congiuntamente, per proteggere la vita privata in un mondo sempre più incentrato sui dati. La sua 46a edizione si è tenuta dal 29 ottobre al 1° novembre 2024 a St-Hélier (Jersey).

Nuova presidente e statuto aggiornato

Le autorità appartenenti all'Associazione francofona delle autorità per la protezione dei dati personali (AFAPDP) hanno eletto una nuova presidente e adottato il nuovo statuto dell'associazione. Altresì all'ordine del giorno: l'assistenza alle autorità malgasce per la creazione di una commissione dedicata.

In occasione della loro assemblea generale i membri hanno eletto, all'unanimità, una nuova presidente, la commissaria della Repubblica di Mauritius Drudeisha Madhub. Prima donna a capo della rete, è anche la prima rappresentante dell'area Africa- Oceano Indiano dalla nascita dell'AFAPDP.

AMVP – GT AID

Rafforzare la protezione della vita privata nel contesto delle emergenze

GT AID, il gruppo di lavoro dell'AMVP dedicato all'azione umanitaria e presieduto dall'IFPDT, ha potenziato la sua azione di sensibilizzazione per la protezione della vita privata nel contesto delle emergenze. Ha in particolare organizzato una tavola rotonda dedicata a questo tema in occasione del Privacy Symposium di Venezia e ha contribuito alla 3a edizione del manuale del Comitato internazionale della Croce Rossa (CICR) sulla protezione dei dati personali nell'azione umanitaria. Nell'ambito della sua attività

di promozione della protezione della vita privata su scala mondiale ha partecipato a numerose tavole rotonde, tra cui quella dell'atelier delle organizzazioni internazionali sulla protezione dei dati organizzata congiuntamente dal Garante europeo della protezione dei dati (GEPD) e dalla Banca mondiale. Il gruppo ha inoltre stilato un elenco dei Paesi africani dotati di una legge sulla protezione dei dati personali e di un'autorità di protezione, con i punti di contatto in seno a tali autorità.

INCONTRI BILATERALI

Nel quadro di un gruppo di lavoro, l'IFPDT ha partecipato all'elaborazione dell'aggiornamento dello Statuto dell'associazione risalente al 2013, che è stato successivamente adottato.

I membri hanno inoltre discusso l'assistenza alle autorità malgasce in materia di «protezione dei dati personali» nell'ambito del progetto dell'Organizzazione internazionale della Francofonia volto alla modernizzazione dell'ecosistema dello stato civile del Madagascar. Si tratta in particolare di contribuire alla creazione della Commissione malgascia dell'informatica e delle libertà (Commission malagasy de l'information et des libertés, CMIL).

L'AFAPDP riunisce le autorità indipendenti di 26 Paesi, tra cui la Svizzera, accomunati dalla lingua, dalla tradizione giuridica e da valori condivisi. Questa 16a assemblea generale si è tenuta a St-Hélier (Jersey) il 28 novembre 2024.

Scambi tra omologhi

Nell'anno in rassegna, l'IFPDT ha ricevuto due delegazioni estere a Berna per discutere le sfide comuni e la cooperazione bilaterale.

Nel giugno 2024, l'Incaricato ha accolto il suo omologo austriaco neoeletto, Matthias Schmidl, per uno scambio di

opinioni. Le discussioni hanno riguardato le sfide comuni e la cooperazione bilaterale nell'ambito della digitalizzazione e della protezione dei dati, nonché la libertà d'informazione e il principio di trasparenza.

Nell'agosto 2024 l'Incaricato ha accolto il suo omologo somalo, Mohamed Ali, primo incaricato del Paese. La legge somala sulla protezione dei dati è stata infatti adottata nel marzo 2023. I due hanno discusso delle prime esperienze della nuova autorità preposta alla protezione dei dati e delle sfide generali in questo ambito in un mondo digitale.

Principio di trasparenza

2.1 In generale

La legge sulla trasparenza (LTras) ha lo scopo di promuovere la trasparenza sulle attribuzioni, l'organizzazione e l'attività dell'Amministrazione garantendo al pubblico l'accesso ai documenti ufficiali (art. 1 LTras). L'obiettivo è promuovere la fiducia nello Stato e nelle autorità facilitando la comprensione dell'operato dell'Amministrazione e aumentando così l'accettazione dell'operato dello Stato.

Secondo i dati forniti dall'Amministrazione federale riguardanti le domande di accesso ai documenti ufficiali pervenute nel 2024, emerge un persistente bisogno da parte dei media e della società di disporre di informazioni dettagliate e di un'Amministrazione (o attività amministrativa) trasparente. Tale esigenza si manifesta con particolare chiarezza nel fatto che le domande hanno raggiunto un nuovo record storico. Nell'anno in rassegna, infatti, le domande di accesso presentate alle autorità federali sono state quasi il 30 per cento in più rispetto all'anno

precedente. Secondo quanto comunicato dalle autorità, l'incremento ha avuto ripercussioni anche sull'onere sostenuto per trattare le domande. Nel complesso è emerso dunque che l'attuazione del principio di trasparenza rappresenta un compito impegnativo e complesso. Le cifre riportate di seguito (v. n. 2.2) evidenziano che, in continuità con quanto osservato negli ultimi anni, anche nell'anno in esame il numero di casi in cui è stato accordato un accesso completo è rimasto su livelli elevati.

Se i richiedenti o terzi interessati non concordano con le modalità di accesso decise dalle autorità, la LTras offre la possibilità di presentare una domanda di mediazione all'Icaricato. Nel 2024 si

è registrato il numero più alto di procedure di mediazione dall'entrata in vigore della LTras: l'Icaricato ha infatti ricevuto 202 domande di mediazione, ovvero il 53 per cento in più rispetto all'anno precedente. L'obiettivo della procedura di mediazione è trovare rapidamente un accordo tra gli interessati. Anche nel 2024 le mediazioni orali in loco si sono dimostrate efficaci: nel 76 per cento dei casi si è riusciti a chiudere le sedute di mediazione con una soluzione consensuale.

Il persistente elevato numero di domande di mediazione, unitamente alle crescente complessità delle problematiche giuridiche cui è necessario rispondere, ha determinato ritardi nell'esecuzione delle stesse. Di conseguenza per il 72 per cento delle procedure l'Icaricato non è riuscito a rispettare il termine legale di 30 giorni. Questa tendenza negativa è destinata ad aggravarsi, rendendo pertanto sempre più difficile rispondere alla volontà del legislatore di avere procedure rapide (v. n. 2.3).

All'inizio del 2025 si è verificata nuovamente una situazione spiacevole, in cui la persona che aveva presentato la richiesta, un politico locale non si è presentato alla seduta di mediazione senza fornire alcuna giustificazione. L'Incarnato ha manifestato il suo rammarico per tale negligenza, che ha comportato un inutile dispendio di tempo e di risorse sia per lui che per i suoi collaboratori legali e per l'autorità competente. In caso di assenza ingiustificata del richiedente la normativa prevede che la procedura di mediazione venga, infatti, stralciata dal ruolo.

Altrettanto spiacevole è stato il caso di un'autorità che non ha rispettato l'accordo scritto convenuto con la persona richiedente durante la seduta di mediazione. Se un'autorità non adempie ai propri obblighi contrattuali, la persona richiedente può richiedere l'accesso concordato ai documenti ufficiali al Tribunale amministrativo federale tramite un'azione.

Anche nel 2024 si sono osservati tentativi da parte dell'Amministrazione di escludere settori dell'attività amministrativa o determinate categorie di documenti dal principio di trasparenza dell'Amministrazione. Una panoramica delle riserve previste da leggi speciali ai sensi dell'articolo 4 LTras è riportata al numero 2.5.

Particolarmente rilevante è l'esclusione del Servizio d'inchiesta svizzero sulla sicurezza (SISI) dal campo d'applicazione della LTras deciso dal Consiglio federale in virtù dell'articolo 2 capoverso 3 LTras (v. n. 2.4). Secondo l'Incarnato il problema centrale in questo caso risiede nel fatto che l'Amministrazione

si esclude autonomamente dalla trasparenza dell'Amministrazione, anticipando così una decisione che, in ogni caso, dovrà essere presa dal legislatore nell'ambito della revisione parziale della legge sulla navigazione aerea. L'IFPDT, inoltre, non ritiene sia necessario introdurre questa limitazione senza condizioni della LTras. Introducendo simili riserve, infatti, si compromette il principio di trasparenza e, conseguentemente, la trasparenza dell'Amministrazione, che è uno degli obiettivi cui è finalizzato.

Si rileva, in generale, che il cambio di paradigma dal principio del segreto a quello di trasparenza, introdotto con la LTras è attuato e applicato in modo attivo dalla maggior parte dell'Amministrazione.

2.2 Domande di accesso: forte incremento nel 2024

Secondo le cifre comunicate dalle autorità federali, nell'anno in rassegna sono pervenute 2186 domande di accesso (nel 2023 erano state 1701), facendo quindi registrare un aumento del 29 per cento rispetto al 2023. A queste si aggiungono 46 domande di accesso, che sono state evase nel 2024 ma che erano state presentate negli anni precedenti. In 1159 casi (52 %) le autorità hanno concesso l'accesso completo ai documenti (nel 2023: 830, pari al 48 %), mentre in 474 casi (21 %) un accesso parziale o differito (nel 2023: 402, pari al 23 %). In 179 casi (8 %) l'accesso è stato del tutto negato (nel 2023: 176, pari al 10 %). Secondo i dati forniti dalle autorità, 133 domande di accesso (6 %) sono state ritirate (nel 2023: 73, pari al 4 %), 102 erano ancora pendenti alla fine del 2024 e in 185 casi non esisteva alcun documento ufficiale.

In sintesi, l'Icaricato ha quindi rilevato che nell'anno in rassegna in oltre la metà dei casi è stato accordato un accesso completo ai documenti. Se si esclude l'anno precedente, quindi, nel 2024 si è confermata la tendenza consolidata negli anni passati. Anche il numero di casi in cui l'accesso è stato completamente negato, che nel corso degli anni si è attestato intorno al dieci per cento, si è mantenuto stabile a un basso livello.

Dipartimenti e uffici federali

Nel 2024 alcune unità amministrative si sono trovate al centro dell'interesse dei media e della società. Dati i compiti che svolgono, soprattutto il DDPS (527), il DATEC (324) come pure il DFAE (306) hanno ricevuto un gran numero di domande di accesso. Secondo le autorità, talvolta si trattava di domande di notevole entità e complessità. Stando a quanto riportato, in molti casi è stato necessario un coordinamento interno tra gli uffici o i dipartimenti.

A livello di uffici, dalle cifre comunicate si evince che quello che ha ricevuto il maggior numero di domande di accesso nel 2024 è stato l'UFSPO con 317 casi, seguito dal settore dei PF con 143, dall'UFAM con 139 e dalla CaF con 94. Sette autorità hanno dichiarato di non aver ricevuto nessuna domanda di accesso nell'anno in rassegna. All'IFPDT stesso sono state inoltrate 29 domande di accesso: in 18 casi è stato accordato l'accesso completo, in un caso è stato

completamente negato, in 4 casi è stato accordato un accesso parziale e 6 domande erano ancora pendenti alla fine del 2024.

L'importo degli emolumenti riscossi nel 2024 per l'accesso ai documenti ufficiali ammonta a un totale di 9950 franchi ed è pertanto decisamente inferiore rispetto all'importo dell'anno precedente (-30 %), quando si era arrivati a 14 226,20 franchi. Mentre la CaF, il DFAE, il DFGP, il DDPS, i Servizi del Parlamento e il Ministero pubblico della Confederazione non hanno riscosso alcun emolumento, gli altri quattro dipartimenti hanno fatturato ai richiedenti una parte del tempo impiegato (DFI: fr. 4250; DEFR: fr. 3600; DFF: fr. 2000; DATEC: fr. 100).

Da evidenziare a tale riguardo che soltanto per 7 delle 2232 domande di accesso trattate è stato riscosso un emolumento. Rispetto all'anno precedente, nel quale in 19 casi era stato riscosso un emolumento, si tratta di un calo notevole, sia per quanto riguarda il numero di casi, sia in relazione all'ammontare totale degli emolumenti. La riscossione di emolumenti continua comunque a rappresentare un'eccezione (0,3 %). La prassi amministrativa, secondo cui i documenti ufficiali possono essere consultati in linea di principio

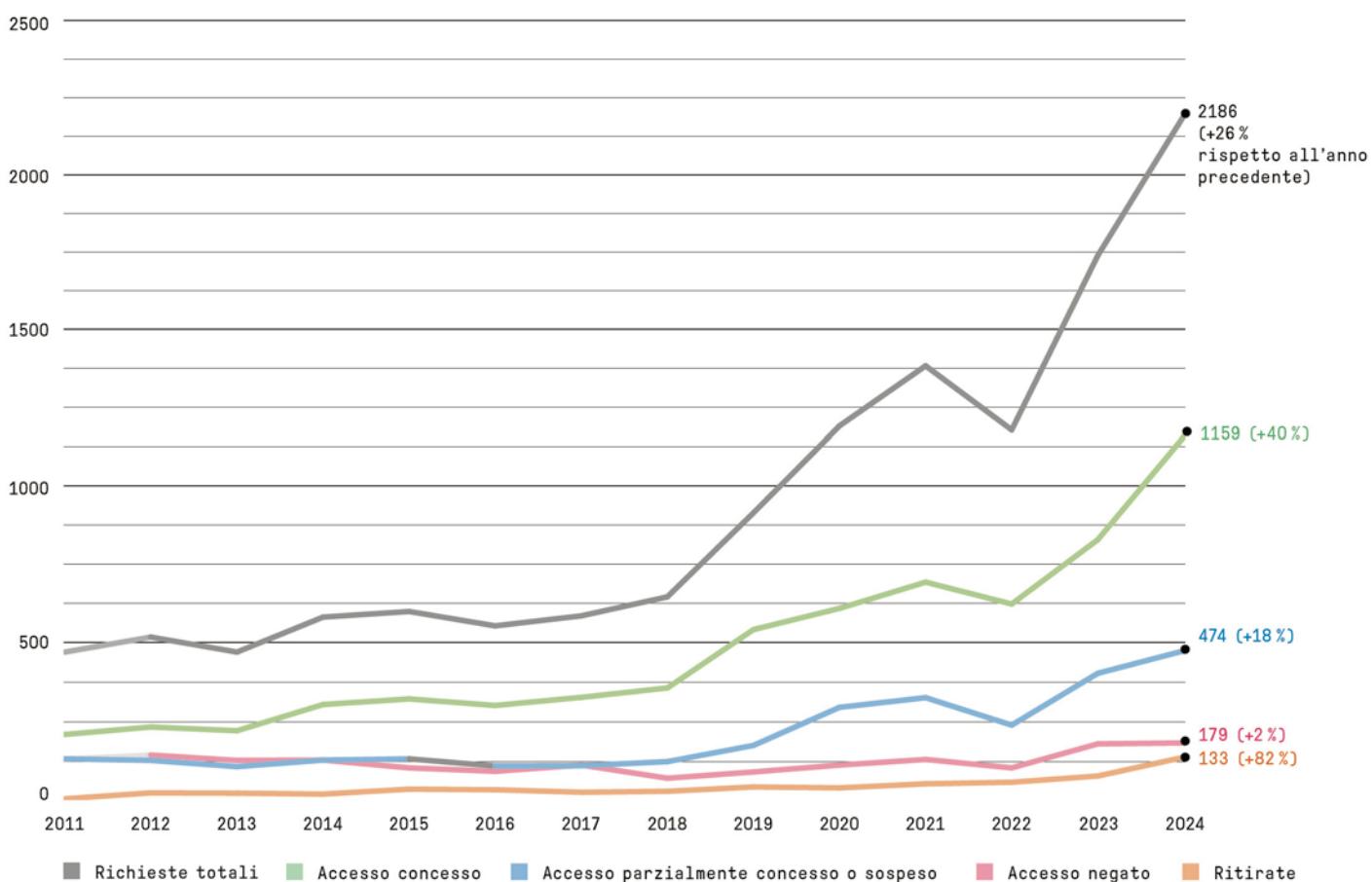
gratuitamente, è ancorata nella legge sulla trasparenza dal 1° novembre 2023. In via eccezionale è possibile riscuotere degli emolumenti qualora una domanda di accesso richieda un'elaborazione particolarmente onerosa.

Per quanto riguarda il tempo dedicato al trattamento delle domande di accesso, l'Incaricato rammenta che le autorità non sono tenute a registrarlo e che non esistono prescrizioni applicabili all'intera Amministrazione federale per una registrazione uniforme. I dati

forniti all'Incaricato su base volontaria rispecchiano quindi solo in parte le ore di lavoro effettivamente prestate. Tuttavia, secondo tali dati il tempo impiegato nell'anno in rassegna, ossia 7256 ore, è nuovamente aumentato in maniera sostanziale rispetto all'anno precedente (6469 ore).

Il fatto che l'onere indicato dalle autorità per la gestione delle domande di accesso non corrisponda integralmente al tempo effettivamente impiegato risulta chiaramente, a titolo esemplificativo, dai dati forniti dall'UFSP. Oltre al tempo impiegato comunicato periodicamente dalle unità specializzate dell'UFSP (482 ore), l'UFSP ha comunicato all'Incaricato un onere elevato per il trattamento delle domande di accesso (comprese le procedure di mediazione

Figura 1: Valutazione delle domande di accesso – evoluzione dal 2011





4b
Arbeitsfläche

3
Institutsarbeiten

e di ricorso) e il supporto giuridico offerto dalla sua consulente per la trasparenza pari ad almeno 3,6 posti a tempo pieno. Lo stesso dovrebbe quindi valere anche per altre autorità.

Un aumento significativo si rileva anche in relazione al tempo necessario comunicato per la preparazione delle procedure di mediazione: 1271 ore

rispetto alle 730 dell'anno precedente (cfr. in merito 2022: 1006 ore; 2021: 865 ore; 2020: 569 ore).

Servizi del Parlamento

Stando ai dati comunicati, nell'anno in rassegna i Servizi del Parlamento hanno ricevuto cinque domande di accesso. In un caso è stato accordato l'accesso completo e in un altro è stato accordato l'accesso parziale. In due casi l'accesso è stato completamente negato e in un altro non esisteva alcun documento ufficiale.

Ministero pubblico della Confederazione

Il Ministero pubblico della Confederazione ha comunicato di aver ricevuto otto domande nel 2024. In tre casi è stato accordato l'accesso completo, mentre in altri due è stato completamente negato. Tre casi erano ancora pendenti alla fine del 2024

Figura 2: Emolumenti riscossi dall'entrata in vigore della LTras



2.3 Procedure di mediazione: notevole aumento delle domande di mediazione

Nel 2024 sono state presentate all’Incaricato 202 domande di mediazione, il numero più alto registrato dall’entrata in vigore della LTras. Facendo un confronto con le richieste presentate nel 2023 (132) è stato dunque registrato un aumento del 53 per cento. La maggior parte delle domande è stata presentata da privati (66) e giornalisti (61). I dati in questione consentono le seguenti constatazioni: i casi in cui l’Amministrazione federale ha rifiutato completamente o in parte l’accesso oppure l’ha differito o ha dichiarato che non erano disponibili documenti ufficiali sono stati 838 e 202 volte, in altre parole, nel 24 per cento dei casi, si è giunti alla presentazione di una domanda di mediazione.

Nel 2024 sono state evase 157 domande di mediazione facendo segnare anche in questo caso una cifra record. Di queste, 130 erano state presentate nell’anno in rassegna e 27 l’anno precedente. In 92 casi è stato possibile giungere a un accordo. L’Incaricato ha inoltre emanato 31 raccomandazioni, che hanno permesso di concludere 32 procedure per le quali non era stato possibile giungere a un accordo.

Tra i casi conclusi vanno annoverate anche 15 domande che non sono state presentate entro il termine previsto, 10 casi in cui non erano soddisfatti i

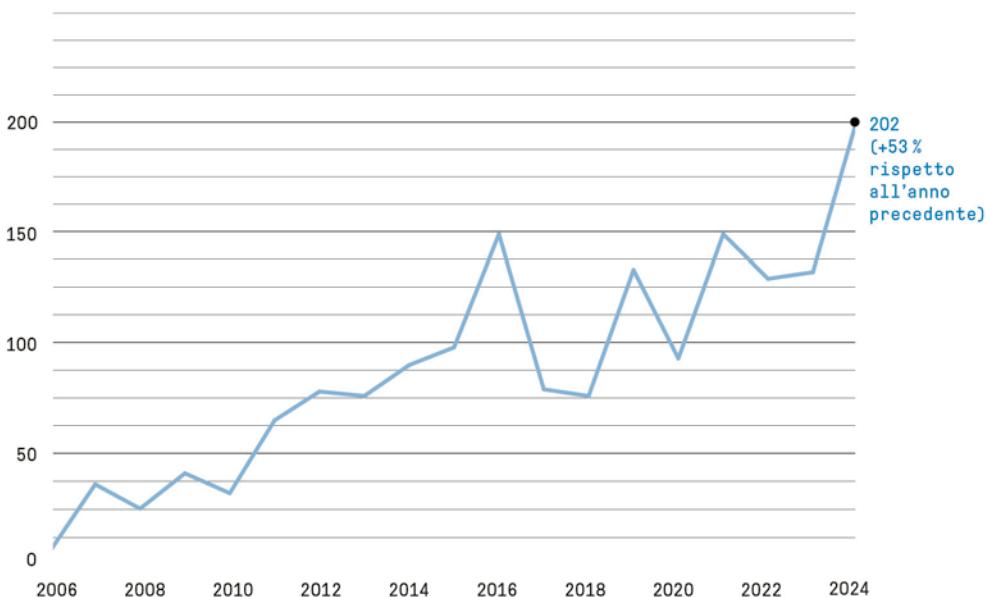
requisiti per l’applicazione della LTras e 8 domande di mediazione che sono state ritirate. Infine 10 procedure di mediazione sono state sospese in accordo tra le parti o su richiesta del richiedente.

Percentuale di soluzioni consensuali

Le soluzioni consensuali presentano numerosi vantaggi: consentono di chiarire la situazione e di accelerare la procedura di accesso nonché di agevolare l’eventuale futura collaborazione tra i partecipanti.

L’efficacia delle sedute di mediazione è particolarmente evidenziata dalla percentuale di soluzioni consensuali raggiunte, la quale risulta superiore a

Figura 3: Richieste di mediazione dall’entrata in vigore della LTras



quella delle raccomandazioni formulate. Nell'anno in rassegna è stato possibile pervenire a 92 soluzioni consensuali e l'Icaricato ha emanato 31 raccomandazioni per risolvere 32 casi. Rispetto alle raccomandazioni, le soluzioni consensuali corrispondono al 74 per cento. Nell'anno in rassegna, nelle 82 sedute di mediazione svolte si è potuti giungere a un'intesa in 62 casi (76%).

Ciò dimostra in modo evidente che la mediazione orale svolta dall'IFPDT permette di giungere a soluzioni consensuali. Dal momento che l'organizzazione di sedute di mediazione risulta vantaggiosa per tutte le parti coinvolte, sarebbe opportuno proseguire su questa via.

Nota: tutte le raccomandazioni dell'anno in rassegna sono disponibili sul sito Internet dell'Icaricato (www.lincaricato.ch).

Tabella 1: Soluzioni consensuali

2024	74 %
2023	47 %
2022 (influsso coronavirus)	51 %
2021 (influsso coronavirus)	44 %
2020 (influsso coronavirus)	34 %
2019	61 %
2018	55 %

Durata delle procedure di mediazione

Tabella 3 riportata qui di seguito, le procedure sono classificate in tre gruppi in funzione della loro durata; tuttavia, nella durata di elaborazione

non si considera il periodo in cui una procedura di mediazione è stata sospesa su richiesta o previo accordo delle parti coinvolte. La sospensione si verifica, in particolare, quando successivamente alla seduta un'autorità rivede la propria posizione o è tenuta a consultare terze parti interessate. Qualora la seduta venga differita su richiesta di una delle parti (p. es. a causa di assenza per vacanze, malattia ecc.), anche l'eventuale prolungamento della procedura derivante da tale differimento non è incluso del calcolo della durata.

Dalla tabella si evince che il 28 per cento delle procedure di mediazione concluse nel 2024 è stato evaso entro il termine legale di 30 giorni. Nel 45 per cento dei casi la procedura di mediazione è durata da 31 a 99 giorni e nel 27 per cento dei casi 100 o più giorni.

Soltanto per 16 delle 44 domande di mediazione evase entro il termine di 30 giorni (36 %), durante la procedura è stato effettuato un esame materiale dell'oggetto della mediazione. Nei restanti 28 casi (64 %) non è stata condotta alcuna valutazione nel merito; questi casi erano, in particolare, palesemente esclusi dal campo di applicazione della LTras o

non adempivano ai requisiti formali necessari per l'avvio di una procedura di mediazione.

Il ritardo nel disbrigo delle procedure degli anni precedenti e il numero elevato di nuove domande ha causato anche nel 2024 un allungamento della durata delle procedure. Oltre a ciò, va considerato che il numero delle domande di mediazione pervenute è soggetto a oscillazioni. Mentre a giugno e a ottobre è giunto all'Incaricato un numero elevato di domande (rispettivamente 30 e 26), ad agosto ne sono state inoltrate solo 8 e a dicembre 9.

Negli anni precedenti alla pandemia, il termine legale di 30 giorni per evadere le procedure di mediazione veniva generalmente rispettato nei casi in cui le sedute si concludevano con successo, ovvero con il raggiungimento di un'intesa fra le parti. Seppure questo non si applichi all'anno in rassegna, nei casi in cui la procedura è stata evasa con il raggiungimento di un'intesa tra le parti, il termine legale di 30 giorni è

stato rispettato nel 20 per cento dei casi (2023: 35%). A causa delle risorse di personale disponibili e dei ritardi nel disbrigo delle procedure, nel 95 per cento dei casi è stato necessario fissare la seduta di mediazione dopo il decorso del termine legale. Nei casi in cui l'Incaricato ha dovuto emanare una raccomandazione scritta in assenza di una soluzione consensuale, non è mai riuscito a farla pervenire agli interessati entro 30 giorni dalla ricezione della domanda, ovvero entro il termine legale.

Altri fattori che hanno determinato il superamento del termine legale sono stati il volume consistente delle domande di accesso, il numero elevato di terzi coinvolti nella procedura o la complessità giuridica delle questioni trattate. Poiché in questi casi il trattamento spesso risulta particolarmente oneroso, secondo l'articolo 12a dell'ordinanza sulla trasparenza (OTras; RS 152.31) l'Incaricato è libero di prolungare ragionevolmente il termine legale.

Se il superamento del termine breve di 30 giorni in casi complessi o in procedure con numerose parti coinvolte (ossia con più parti terze interessate) è considerato un aspetto intrinseco del sistema, in quanto la legge prevede la possibilità di una proroga, i ritardi accumulatisi successivamente, dovuti esclusivamente all'incremento significativo delle richieste di mediazione, sono da considerarsi, dal punto di vista giuridico, casi di giustizia ritardata.

Tabelle 2: Tempo di elaborazione delle procedure di mediazione

Tempo di elaborazione in giorni	Periodo 2014 – agosto 2016*	Fase pilota 2017	Periodo 2018	Periodo 2019	Periodo 2020	Periodo 2021	Periodo 2022	Periodo 2023	Periodo 2024
entro 30 giorni	11%	59%	50%	57%	43%	42%	25%	27%	28%
da 31 a 99 giorni	45%	37%	50%	38%	30%	51%	42%	35%	45%
100 o più giorni	44%	4%	0%	5%	27%	7%	33%	38%	27%

* Fonte: presentazione dell'Incaricato, evento per i dieci anni della LTras, 2 settembre 2016

Numero di casi pendenti

I dati riportati qui di seguito forniscono informazioni sul numero di casi pendenti alla fine dei rispettivi anni in rassegna. A inizio gennaio 2025 erano pendenti 66 procedure di mediazione, di cui 10 sospese (1 risalente al 2019, 1 al 2021, 2 al 2022 e 6 all'anno in rassegna). 19 di questi casi sono stati conclusi entro la chiusura di redazione del presente rapporto.

Tabella 3: Procedure di mediazione pendenti

Fine 2024	66 (di cui 19 evase entro la chiusura di redazione e 10 sospese)
Fine 2023	31 (di cui 17 evase entro la chiusura di redazione e 9 sospese)
Fine 2022	41 (di cui 16 evase entro la chiusura di redazione e 13 sospese)
Fine 2021	27 (di cui 14 evase entro la chiusura di redazione e 8 sospese)
Fine 2020	17 (di cui 9 evase entro la chiusura di redazione e 8 sospese)
Fine 2019	43 (di cui 40 evase entro la chiusura di redazione e 3 sospese)
Fine 2018	15 (di cui 13 evase nel febbraio 2019 e 2 sospese)

2.4 Procedura legislativa

RAPPORTO DELLA CDG-S

**Il Consiglio federale
rinuncia a esaminare in
modo più approfondito
se sia possibile riconoscere
all'IFPDT il diritto di
pronunciare decisioni**

Nel rapporto redatto nel contesto delle accuse di irreperibilità di e-mail all'interno della Segreteria generale del Dipartimento federale dell'interno (SG-DFI), la Commissione della gestione del Consiglio degli Stati (CdG-S) ha evidenziato la mancanza di principi uniformi per la classificazione e l'archiviazione dei documenti all'interno dell'Amministrazione federale nonché la necessità di fare chiarezza in merito. La Commissione ha fornito cinque raccomandazioni ed è giunta alla conclusione che sarebbe necessario rafforzare il diritto dell'Icaricato di consultare i documenti ufficiali. Il Consiglio federale ha reso noto tramite rapporto il proprio parere riguardo alle cinque raccomandazioni.

Nel suo rapporto del 10 ottobre 2023 («Archiviazione e classificazione di documenti e procedura per le domande di accesso secondo la LTras: accertamenti generali in merito alle norme applicabili e nel contesto delle accuse di irreperibilità di e-mail all'interno della SG-DFI») la CdG-S ha trattato le basi legali concernenti la conservazione, la classificazione e l'archiviazione dei documenti (legge sull'archiviazione) e l'accesso ai documenti ufficiali (legge sulla trasparenza). Nei suoi ultimi rapporti d'attività l'IFPDT si era già espresso in modo esaustivo al riguardo (cfr. 31° rapporto d'attività, n. 2.4 e 30° rapporto d'attività, n. 2.4).

Nel suo rapporto la Commissione ha fornito al Consiglio federale le seguenti cinque raccomandazioni, tre delle quali sono direttamente correlate alla legge sulla trasparenza:

- nella raccomandazione 1 la CdG-S ha invitato il Consiglio federale a valutare se sia necessario modificare le disposizioni di legge relative al diritto di consultazione di documenti legati sia alla funzione degli impiegati federali che alla sfera privata, in particolare per quanto riguarda i magistrati;
- nella raccomandazione 4 la CdG-S ha invitato il Consiglio federale a esaminare se la LTras sia o debba essere applicabile anche ai procedimenti penali già conclusi e, se del caso, a chiarire questo punto in occasione della prossima revisione della legge;

- nella raccomandazione 5 la CdG-S ha invitato il Consiglio federale a vagliare l'opportunità di modificare la LTras riconoscendo all'IFPDT un diritto di intervento o un diritto di pronunciare decisioni qualora il suo diritto di consultazione non venga rispettato.

Nel suo parere del 10 gennaio 2024 il Consiglio federale aveva comunicato alla CdG-S che accoglieva l'invito a esaminare quanto indicato nelle raccomandazioni dalla 1 alla 4. Respingeva invece la proposta di vagliare l'opportunità di riconoscere all'Icaricato il diritto di pronunciare decisioni come suggerito nella raccomandazione 5, proponendo invece di esaminare le possibilità di intervento dell'Icaricato nei casi in cui gli venga negato il diritto di consultazione.

Il Consiglio federale ha quindi incaricato il Dipartimento federale di giustizia e polizia (DFGP) di valutare le raccomandazioni entro la fine del 2024 e di

avanzare proposte sulle possibili misure tramite rapporto. Durante una consultazione preliminare e una consultazione degli uffici del DFGP, l'IFPDT ha potuto esprimere le proprie considerazioni sulla bozza del rapporto, in particolare, in merito alle singole raccomandazioni e alle asserzioni del Consiglio federale:

- riguardo alla raccomandazione 1 il Consiglio federale ha espresso delle riserve in quanto ritiene che, nel caso dei documenti legati non soltanto all'attività d'ufficio ma anche alla sfera privata di una persona, debba essere sempre verificato caso per caso se sussista il diritto all'accesso in base alla legge sulla trasparenza o alla consultazione in base alla legge sull'archiviazione. A suo avviso non sussiste alcuna necessità di adeguare la legge. Secondo il Consiglio federale la raccomandazione 1 della CdG-S riguarda un aspetto specifico del coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza e i rispettivi diritti di consultazione. Durante le consultazioni a riguardo l'Incaricato ha fatto presente che a suo avviso sarebbe indispensabile procedere a una revisione (parziale) dei testi di legge per disciplinare il coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza garantendo la necessaria certezza del diritto, soprattutto perché le due procedure di consultazione si differenziano in

modo sostanziale sia sul piano materiale sia su quello procedurale, come riconosciuto anche dal Consiglio federale nel suo rapporto;

- riguardo alla raccomandazione 4 e all'applicabilità della legge sulla trasparenza abbiamo constatato che non sono state prese in considerazione le nostre osservazioni che facevano riferimento alla giurisprudenza, in base alla quale il Tribunale federale avrebbe già deciso le modalità di attuazione dell'articolo 3 capoverso 1 lettera a LTras. Interpretando in modo restrittivo la motivazione riportata all'articolo 3 capoverso 1 lettera a LTras per cui gli atti processuali dovrebbero essere esclusi, nella sua interpretazione il Tribunale è giunto alla conclusione che soltanto gli atti procedurali in senso stretto sono esclusi dal campo d'applicazione della legge sulla trasparenza. Per quanto riguarda i requisiti necessari per una tale eccezione elaborati dal Tribunale, il fatto che un procedimento sia ancora in corso o già concluso non ha

alcun tipo di rilevanza. Secondo l'Incaricato la questione dell'accesso agli atti procedurali, in questo modo, è chiarita in modo definitivo dal Tribunale federale;

- per quanto riguarda la raccomandazione 5, il Consiglio federale ha confermato la valutazione che aveva già espresso l'11 gennaio 2024 e ha respinto la possibilità di valutare in modo più approfondito l'eventualità di concedere all'Incaricato la facoltà di pronunciare decisioni. Per motivare la sua posizione ha sottolineato che, come stabilito dalla legge sulla trasparenza, la procedura di mediazione è una procedura semplice, informale e non pregiudiziale; pertanto, dare all'Incaricato la facoltà di pronunciare decisioni non sarebbe conforme al sistema. Durante la consultazione degli uffici l'IFPDT ha anche evidenziato che rinunciando a esaminare più nel dettaglio la possibilità di concedere la facoltà di pronunciare decisioni non viene soddisfatta la richiesta della CdG-S di sottoporre a esame, oltre alla questione dei diritti di intervento dell'Incaricato, anche quella relativa a uno specifico diritto di pronunciare decisioni. La nostra richiesta di un esame adeguato non è stata soddisfatta.

Il rapporto del 13 dicembre 2024 del Consiglio federale destinato alla CdG-S è stato approvato e pubblicato dal DFGP nella forma proposta.

Limitazione del principio di trasparenza in caso di «whistleblowing»

La revisione della legge sul personale federale attualmente all'esame del Parlamento prevede ampie limitazioni del principio di trasparenza, segnatamente per quanto concerne la gestione delle segnalazioni da parte di chi denuncia episodi di «whistleblowing». L'Incaricato si è più volte pronunciato contro le limitazioni previste.

Il 28 agosto 2024 il Consiglio federale ha trasmesso al Parlamento il messaggio concernente la modifica della legge sul personale federale (LPers). Oltre a modifiche nell'ambito della previdenza professionale, la revisione prevede anche misure volte a rafforzare la protezione dei dati in relazione alla profilazione e a promuovere la digitalizzazione nella gestione del personale (cfr. n. 1.5).

Inoltre, con la revisione il Consiglio

federale intende apportare modifiche puntuali volte ad aumentare l'efficienza nell'applicazione del diritto sul personale federale.

All'articolo 22a capoverso 7 del progetto di modifica della legge sul personale federale (P-LPers), il Consiglio federale propone di introdurre una misura legislativa volta a incrementare l'efficienza escludendo dal campo d'applicazione della legge sulla trasparenza i documenti che comprovano una segnalazione secondo l'articolo 22a P-LPers (segnalazioni, denunce e protezione relative al «whistleblowing»), che sono presentati insieme a una tale segnalazione o che sono allestiti in base ad essa. L'Ufficio federale del personale (UFPER), responsabile del progetto, sostiene che la limitazione del principio di trasparenza sia necessaria per garantire a lungo termine la fiducia nello strumento del «whistleblowing». Inoltre, nel caso dei suddetti documenti, la mancata applicazione del principio di trasparenza servirebbe a tutelare le persone accusate di un comportamento illecito attraverso una segnalazione.

Nel corso di due consultazioni degli uffici e di una consultazione intermedia l'Incaricato ha sottolineato invano che i legittimi interessi privati sono tutelati anche in caso di applicazione della legge sulla trasparenza. Come spiegato dall'IFPD, inoltre, lo strumento del «whistleblowing» gode già di grande fiducia, soprattutto perché la norma in

materia di cui all'articolo 22a LPers è entrata in vigore il 1° gennaio 2011. Gli obblighi di denuncia e segnalazione sanciti da tale norma per gli impiegati federali in caso di reati perseguitibili d'ufficio e il diritto di segnalazione in caso di irregolarità di altro tipo sono stati ampiamente utilizzati sin dall'introduzione di tale disposizione. Come dimostrano le valutazioni statistiche del Controllo federale delle finanze (CDF), infatti, il numero di casi è costantemente aumentato. All'Incaricato non è quindi chiaro in che modo il mantenimento delle regole attualmente in vigore, senza riserva ai sensi dell'articolo 4 LTras, debba o possa causare un calo della fiducia. In più, secondo l'Incaricato, la legge sulla trasparenza offre sufficienti opzioni per garantire la tutela delle informazioni sensibili e dei dati personali sia di coloro che fanno ricorso allo strumento del «whistleblowing» sia di chi potrebbe essere oggetto di segnalazioni (cfr. art. 7 e 9 LTras).

L'IFPD ritiene quindi che non sia

AVIAZIONE

necessario mantenere la riservatezza su tutte le segnalazioni e su tutti gli eventuali allegati, così come su tutti gli altri documenti che vengono prodotti a seguito della segnalazione, compresi i documenti e i rapporti conclusivi eventualmente preparati successivamente e relativi a una segnalazione. Anche perché in questo modo si andrebbe contro il principio della proporzionalità di cui all'articolo 5 Cost. Secondo l'Incaricato la riserva prevista al principio di trasparenza non è giustificata dato il legittimo interesse pubblico a un trattamento approfondito delle segnalazioni di comportamenti illeciti ad opera di impiegati dell'Amministrazione.

L'IFPDT sottolinea infine che gli organi di segnalazione («whistleblowing») non dovrebbero rimanere nell'ombra, perché sono tenuti per legge a effettuare controlli sulle unità e/o sugli impiegati dell'unità amministrativa interessata dalla segnalazione e quindi sono particolarmente sotto i riflettori dell'opinione pubblica.

Nel messaggio trasmesso dal Consiglio federale al Parlamento e attualmente in fase di deliberazione parlamentare è ancora presente la limitazione

Limitazione del principio di trasparenza nella vigilanza sull'aviazione civile

La vigilanza sull'aviazione civile sarà in gran parte esclusa dal principio di trasparenza. Nella consultazione degli uffici e nel corso della procedura di consultazione l'Incaricato ha espresso il proprio parere contrario alla limitazione prevista.

Elaborato dall'Ufficio federale dell'aviazione civile (UFAC), il progetto posto in consultazione di modifica della legge sulla navigazione aerea prevede ampie limitazioni al principio di trasparenza, segnatamente nell'ambito della vigilanza dell'UFAC prevista per legge. In base all'articolo 107d capoverso 2 del progetto posto in consultazione concernente la modifica della legge sulla navigazione aerea (LNA), la legge sulla trasparenza non dovrebbe essere applicabile per l'accesso ai dati personali e ai dati di persone giuridiche contenuti nei documenti ufficiali elencati qui di seguito e nemmeno se l'accesso ai documenti ufficiali elencati qui di

seguito compromette la sicurezza aerea e la sicurezza dell'aviazione: rapporti relativi ad audit, ispezioni, perizie e controlli dell'UFAC (lett. a), segnalazioni di eventi trasmesse all'UFAC sulla base del regolamento (UE) n. 376/2014¹¹ e la relativa documentazione (lett. b) e documenti ufficiali concernenti inchieste sulla sicurezza del Servizio d'inchiesta svizzero sulla sicurezza (SISI) (lett. c).

L'Incaricato, che in qualità di autorità di vigilanza è assoggettato alla legge sulla trasparenza, ha respinto le disposizioni proposte, perché la LTras offre sufficienti strumenti per proteggere le informazioni sensibili anche nell'ambito dell'attività di vigilanza e nell'ambito delle inchieste sulla sicurezza (cfr. art. 7 e 9 LTras). In generale è stato anche sottolineato che il legislatore non ha sancito volutamente la confidenzialità tra autorità di vigilanza e assoggettati alla vigilanza nelle eccezioni alla legge sulla trasparenza.

Per giustificare la limitazione del principio di trasparenza, l'UFAC ha sostenuto che le persone assoggettate alla vigilanza adempirebbero ai loro obblighi di segnalazione soltanto con la certezza che queste informazioni non saranno divulgate. Questa premessa, non pertinente alla luce della posizione qui espressa, non tiene conto del fatto che in uno Stato di diritto occorre par-

AVIAZIONE

tire dal presupposto che gli obblighi legali d'informazione e di notifica sono rispettati. L'UFAC, inoltre, non riconosce neanche il fatto che possibili violazioni della legge da parte delle persone assoggettate alla vigilanza non giustificano in alcun caso limitazioni nell'applicazione della legge sulla trasparenza. L'Icaricato ritiene poi inammissibile e pretenzioso che l'UFAC giustifichi la propria proposta sostenendo che i rapporti spesso contengono dettagli tecnici difficili da comprendere per il grande pubblico. In conclusione, l'IFPDT non ha individuato alcun motivo plausibile che giustifichi l'intenzione dell'UFAC di escludere totalmente la trasparenza dell'amministrazione e quindi di tenere segrete in modo incondizionato parti sostanziali dell'attività di vigilanza.

L'IFPDT ha fatto inoltre presente che le autorità con compiti di vigilanza, audit, controllo o ispezione sono oggetto di particolare interesse da parte dell'opinione pubblica, poiché sono tenute per legge a vigilare su altre unità amministrative e/o soggetti privati. Soprattutto in contesti così sensibili, quindi, l'Icaricato non può che opporsi quando le autorità di vigilanza cercano di autoescludersi dal campo d'applicazione della legge sulla trasparenza parlando del «pericolo di

inosservanza degli obblighi di segnalazione» e menzionando l'«eccessiva complessità per la popolazione». Nell'ambito della revisione parziale 1+ della legge sulla navigazione aerea, tra il 2014 e il 2015 era già stato proposto di introdurre una restrizione altrettanto ampia del principio di trasparenza, alla quale l'Icaricato si era opposto in modo deciso (cfr. 22° rapporto d'attività, n. 2.2.2). Ciononostante, dopo la decisione di non introdurre simili disposizioni, l'UFAC non ha fornito spiegazioni volte a giustificare la necessità di una misura di questo tipo alla luce dell'evoluzione della situazione in questi anni.

Dal momento che dopo la consultazione degli uffici l'UFAC non ha voluto inserire le posizioni divergenti dell'IFPDT nel rapporto esplicativo concernente il progetto di modifica della legge, per motivi di trasparenza l'Icaricato si è visto costretto a far pervenire il proprio parere anche nell'ambito della procedura di consultazione.

Modifica dell'ordinanza concernente le inchieste sulla sicurezza in caso di eventi imprevisti nei trasporti (OIET)

Con la modifica entrata in vigore il 1° gennaio 2025, il Consiglio federale ha escluso il Servizio d'inchiesta svizzero sulla sicurezza (SISI) dal campo d'applicazione della legge sulla trasparenza. Durante la consultazione degli uffici, l'Icaricato si è opposto a questa limitazione del principio di trasparenza, tuttavia senza successo.

In base all'articolo 2 capoverso 3 lettera a LTras il Consiglio federale può escludere delle unità dell'Amministrazione federale dal campo d'applicazione personale della legge sulla trasparenza se è necessario per l'adempimento dei compiti loro affidati. Rifacendosi a questa opzione, nel nuovo articolo 54a dell'ordinanza concernente le inchieste sulla sicurezza in caso di eventi imprevisti nei trasporti (OIET), il Consiglio federale ha stabilito che il SISI è escluso dal campo d'applicazione della legge sulla trasparenza nella misura in cui tratta dati concernenti persone fisiche e giuridiche.

VIGILANZA FINANZIARIA

Il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC), responsabile della modifica all'ordinanza, ha dichiarato che questa esclusione dal campo d'applicazione della legge sulla trasparenza era necessaria perché l'unico modo per far sì che il SISI continuasse a ricevere le informazioni di cui ha bisogno per garantire la sicurezza dei trasporti, era garantire a chi denuncia che le informazioni trasmesse non fossero divulgate. Questa argomentazione è stata addotta più volte dall'Amministrazione federale per giustificare la necessità (apparente) di limitare la trasparenza dell'Amministrazione. Come più volte spiegato dall'Icaricato, le motivazioni addotte non sono convincenti (v. il contributo

sulla revisione della LNA e 31° rapporto d'attività, n. 2.4 e 22° rapporto d'attività, n. 2.2.2). Il DATEC, inoltre, non ha spiegato perché le disposizioni d'eccezione della legge sulla trasparenza non sarebbero sufficienti a garantire al SISI di poter adempiere ai propri compiti.

Con l'esclusione del SISI dal campo d'applicazione personale della legge sulla trasparenza, l'Amministrazione si sottrae al principio di trasparenza. Tale scelta sorprende particolarmente in quanto l'UFAC e il DATEC già nell'ambito della revisione parziale della LNA (v. sopra), e quindi a livello di legge, avevano proposto l'introduzione di una disposizione di legge specifica che escludesse il SISI dal campo d'applicazione della legge sulla trasparenza. In questo modo, quindi, il Consiglio federale anticipa il processo decisionale del Parlamento.

Dopo l'entrata in vigore il 1° gennaio 2025 della norma che esclude il SISI dal campo d'applicazione in base all'articolo 54a OIET, nei commenti a questa disposizione il DATEC ha spiegato che in ogni caso tale norma ha carattere puramente provvisorio, in quanto le limitazioni al campo d'applicazione del principio di trasparenza, dovrebbero in linea di massima spettare unicamente al potere legislativo.

Nuova legge federale sulla trasparenza delle persone giuridiche

La legge sulla trasparenza delle persone giuridiche mira a introdurre un registro centrale per l'identificazione degli aenti economicamente diritto effettivi delle persone giuridiche. Nonostante l'intervento dell'Icaricato, il progetto di legge prevede un'esclusione della legge sulla trasparenza.

Il 22 maggio 2024 il Consiglio federale ha trasmesso al Parlamento il messaggio concernente una nuova legge federale sulla trasparenza delle persone giuridiche e sull'identificazione degli aenti economicamente diritto (LTPG). Questa prevede la creazione di un registro con informazioni aggiornate sugli aenti economicamente diritto degli enti

DIRITTO DI NECESSITÀ

giuridici registrati. L'obiettivo è quello di rafforzare ulteriormente il dispositivo di lotta contro il riciclaggio di denaro, il finanziamento del terrorismo e la criminalità economica.

L'Incaricato esprime rammarico in merito al fatto che una volta conclusa la procedura di consultazione (cfr. 31° rapporto d'attività, n. 2.4) il Consiglio federale ha escluso esplicitamente l'applicazione della legge sulla trasparenza. Secondo l'articolo 53 capoverso 4 del progetto di legge, la LTras non si applicherebbe pertanto ai dati del registro per la trasparenza relativi a persone fisiche o giuridiche.

La Segreteria di Stato per le questioni finanziarie internazionali (SFI), responsabile del progetto, ha giustificato la limitazione del principio di trasparenza sostenendo che lo scopo del registro per la trasparenza è principalmente quello di migliorare la lotta contro il riciclaggio di denaro e il finanziamento del

terrorismo. Secondo la SFI un maggiore accesso al registro non apporterebbe alcun valore aggiunto e costituirebbe un pregiudizio sproporzionato dei diritti alla protezione della personalità.

Nel corso della consultazione degli uffici l'Incaricato ha sottolineato invano che i legittimi interessi privati rimangono tutelati anche in caso di applicazione della legge sulla trasparenza, dal momento che la norma garantisce esplicitamente la protezione dei segreti d'affari (art. 7 cpv. 1 lett. g LTras) e della sfera privata, così come dei dati personali delle persone fisiche e giuridiche (art. 7 cpv. 2 LTras, art. 9 cpv. 2 LTras in combinato disposto con art. 36 LPD e art. 57s LOGA). L'IFPDT ha fatto inoltre presente che le banche dati o i registri utilizzati dalle autorità per lo svolgimento dei compiti pubblici sono in linea di principio coperti dal diritto di accesso secondo la legge sulla trasparenza. Secondo l'Incaricato, quindi, regolamentare in modo diverso il registro per la trasparenza senza fornire sufficienti motivazioni sarebbe contrario al sistema o al concetto di trasparenza.

Nel progetto di legge trasmesso dal Consiglio federale al Parlamento e attualmente oggetto d'esame parlamentare è ancora presente la limitazione del principio di trasparenza. Tuttavia la posizione dell'Incaricato è stata inserita all'interno del messaggio del Consiglio federale.

Ricorso al diritto di necessità: Rapporto del consiglio federale

Nel suo rapporto in adempimento del postulato del 19 giugno 2024, il Consiglio federale è giunto alla conclusione che proprio in tempi di crisi il principio di trasparenza assume un'importanza fondamentale e dovrebbe essere escluso soltanto in casi eccezionali. La posizione dell'Incaricato è riportata nel rapporto.

Negli ultimi due decenni il Consiglio federale ha fatto più volte ricorso al diritto sancito dalla Costituzione che gli permette di adottare ordinanze di necessità (cfr. art. 184 cpv. 3 e art. 185 cpv. 3 Cost.). Nell'ambito del piano di salvataggio per le aziende elettriche e dell'acquisizione di Credit Suisse da parte di UBS, il Consiglio federale ha escluso dal campo d'applicazione della

LTras le attività trasferite all’Amministrazione tramite lo stesso diritto di necessità. Il Parlamento ha incaricato il Consiglio federale di evidenziare le basi legali e i limiti del diritto di necessità e di accertare un’eventuale necessità d’intervento.

Nel suo rapporto del 19 giugno 2024 il Consiglio federale è giunto alla conclusione che il diritto di accesso sancito dalla LTras dovrebbe essere escluso soltanto in casi eccezionali attraverso il diritto di necessità. Il Consiglio federale ritiene infatti che questo strumento, introdotto dal legislatore per permettere ai cittadini di controllare l’Amministrazione, assuma un ruolo centrale soprattutto in tempi di crisi. Eventuali limitazioni al diritto di accesso devono dunque essere debitamente motivate.

Durante la consultazione degli uffici l’Incaricato ha espresso il proprio parere sulla bozza del rapporto dell’Ufficio federale di giustizia (UFG). L’Incaricato chiedeva principalmente che venissero stralciati due passaggi riguardanti una valutazione giuridica su

questioni che fino a quel momento non erano state ancora chiarite. Nel suo parere, inoltre, l’IFPDT criticava ancora una volta le motivazioni esposte nel rapporto per giustificare l’esclusione della legge sulla trasparenza, in cui si affermava che altrimenti non sarebbe stato possibile garantire il rispetto degli obblighi di notifica previsti dalla legge (cfr. contributo in merito alla revisione della LNA nonché 31° rapporto d’attività, n. 2.4 e 22° rapporto

d’attività, n. 2.2.2). L’Incaricato ha accolto con favore il fatto che sono state apportate le modifiche richieste e che la sua posizione sia stata riportata nel rapporto.

Nella sua comunicazione del 6 aprile 2023 l’IFPDT aveva già dichiarato che dai motivi addotti per il sostegno del settore elettrico e di quello finanziario sulla base del diritto di necessità, non emerge l’esigenza di escludere l’applicazione della legge sulla trasparenza attraverso il diritto di necessità. Questa valutazione è stata confermata anche nella sua raccomandazione del 27 novembre 2023 in merito all’accesso ai documenti per l’acquisizione di Credit Suisse da parte di UBS. Bisogna infine ricordare che, nel suo rapporto del 17 dicembre 2024 sulla gestione delle autorità federali nel contesto della crisi di Credit Suisse, la Commissione parlamentare d’inchiesta (CPI) aveva sollevato dei dubbi circa la proporzionalità dell’esclusione della LTras e aveva esortato il Consiglio federale a rispettare il principio di trasparenza dell’Amministrazione anche nell’emanazione del diritto di necessità (raccomandazione n. 17 del rapporto).

2.5 Riserve di disposizioni speciali ai sensi dell'articolo 4 LTras

La legge sulla trasparenza prevede un coordinamento con altre disposizioni contenute in leggi federali speciali, che prevedono una regolamentazione specifica in relazione all'accesso a documenti ufficiali. Conformemente all'articolo 4 LTras, restano salve le disposizioni

previste in altre leggi federali che dichiarano segrete determinate informazioni (lett. a) o prevedono condizioni divergenti da quelle previste dalla legge sulla trasparenza per l'accesso a determinate informazioni (lett. b). Pertanto le disposizioni della legge sulla trasparenza non sono applicabili per l'accesso a tali informazioni.

La prevalenza di una disposizione di legge nel senso di una disposizione speciale secondo l'art. 4 LTras deve essere determinata per ogni caso specifico interpretando le disposizioni pertinenti.

Tabella 4: Disposizioni speciali ai sensi dell'articolo 4 LTras

Atto normativo (forma breve) e abbreviazione	n. RS	Art. / cpv.	Data di entrata in vigore
Legge sulla sicurezza delle informazioni (LSIn)	128	Art. 4 cpv. 1 bis	(aperto)
Messaggio concernente la modifica della legge sul personale federale (LPers)	177.220.1	Art. 22a cpv. 7 E-LPers	Messaggio del 28 agosto 2024 Stato: deliberazione nel parlamento
Messaggio concernente la legge federale sulla trasparenza delle persone giuridiche e sull'identificazione dei titolari effettivi (LTPG)		Art. 53 cpv. LTras	Messaggio del 22 maggio 2024 Stato: deliberazione nel parlamento
Modifica della legge federale sull'assicurazione malattie LAMal (misure di contenimento dei costi - pacchetto 2)	832.10 831.20	Art. 52c LAMal (norma di delega) Art. 52d cpv. 5 LAMal Disposizione transitoria LAMal cpv. 4 Art. 14 ^{quinquies} cpv. 2 u. 3 LAI (norma di delega) Art. 14 ^{sexies} Abs. 5 LAI Disposizione transitoria LAI cpv. 1	Approvato dal Parlamento il 21 marzo 2025.
Legge federale sugli aiuti finanziari concessi a titolo sussidiario per salvare le imprese di rilevanza sistematica del settore dell'energia elettrica (LAiSE)	734.91	Art. 20 cpv. 4	1° ottobre 2022
Legge federale sugli appalti pubblici (LAPub)	172.056.1	Art. 48 cpv. 1 (accesso esplicito prescritto); Art. 11 lett. e (si applica solo come disposizione speciale durante la procedura di aggiudicazione)	1° gennaio 2021
Legge sulle fideiussioni solidali COVID-19 (LFiS-COVID-19)	951.26	Art. 12 cpv. 2	19 dicembre 2020
Legge federale sull'organizzazione dell'infrastruttura ferroviaria (OIF) (atto mantello)			
Legge federale sulle ferrovie (Lferr)	742.101	Art. 14 cpv. 2	1° luglio 2020
Legge sugli impianti a fune (LIFT)	743.01	Art. 24e	1° luglio 2020

Atto normativo (forma breve) e abbreviazione	n. RS	Art. / cpv.	Data di entrata in vigore
Legge sul trasporto di viaggiatori (LTV)	745.1	Art. 52a	1° luglio 2020
Legge federale sulla navigazione interna (LNI)	747.201	Art. 15b	1° luglio 2020
Legge federale sulle attività informative (LAIn)	121	Art. 67	1° settembre 2017
Legge sulle derrate alimentari (LDerr)	817.0	Art. 24 Disposizione speciale ai sensi del messaggio concernente la legge federale sulle derrate alimentari e gli oggetti d'uso del 25 maggio 2011	1° maggio 2017
Legge federale sulla promozione della ricerca e dell'innovazione (LPRI)	420.1	Art. 13 cpv. 4 (cfr. sentenza del TAF n. A-6160/2018 del 4 novembre 2019 consid. 4.)	1° gennaio 2014
Legge sulle banche (LBCR)	952.0	Art. 47 cpv. 1	1° gennaio 2009 (lett. a e b) e 1° luglio 2015 (lett. c)
Legge sui brevetti (LBI)	232.14	Art. 90 OBI, che si basa sull'art. 65 cpv. 2 LBI (cfr. sentenza del TF n. 4A_249/2021 del 10 giugno 2021)	1° luglio 2008
Ordinanza sui brevetti (OBI)	232.141		
Entrata in vigore della legge sulla trasparenza			1° luglio 2006
Legge sul Parlamento (LParl)	171.10	Art. 47 cpv. 1 (cfr. sentenza del TAF n. A-6108/2016 del 28 marzo 2018 consid. 3.1.)	1° dicembre 2003
Legge sul controllo dei beni a duplice impiego (LBDI)	946.202	Art. 4 e 5 (cfr. sentenza del TAF n. A-5133/2019 del 24 novembre 2021 consid. 5.3.2.4.)	1° ottobre 1997
Legge federale sull'imposta federale diretta (LIFD)	642.11	Art. 110 cpv. 1	1° gennaio 1995
Legge federale sull'imposta preventiva (LIP)	642.21	Art. 37 cpv. 1	1° gennaio 1967
Legge federale sulle tasse di bollo (LTB)	641.10	Art. 33 cpv. 1	11° luglio 1974
Legge sull'IVA (LIVA)	641.20	Art. 74 cpv. 1	1° gennaio 2010
Legge federale sull'armonizzazione delle imposte dirette dei Cantoni e dei Comuni (LAID)	642.14	Art. 39 cpv. 1 (cfr. GAAC 2016.1 (pag. 1-14), edizione del 26 gennaio 2016: «Secret fiscal et accès à des documents officiels»)	1° gennaio 1993
Legge sulla statistica federale (LStat)	431.01	Art. 14 (cfr. sentenza del TF n. 1C_50/2015 del 2 dicembre 2015 consid. 4.2. e segg.)	1° agosto 1993

Tabella 5: NESSUNA disposizione speciale ai sensi dell'articolo 4 LTras

Atto normativo (forma breve) e abbreviazione	n. RS	Art. / cpv.	Data di entrata in vigore
Legge federale sulla sicurezza dei prodotti (LSPro)	930.11	Art. 10 cpv. 4 in combinato disposto con l'art. 12 (cfr. sentenza del TF 1C_299/2019 del 7 aprile 2020 consid. 5.5.)	1° luglio 2010
Legge sui revisori (LSR)	221.302	Art. 19 cpv. 2 (cfr. sentenza del TF n. 1C_93/2021 del 6 maggio 2022 consid. 3.6.)	1° settembre 2007
Legge sulle telecomunicazioni (LTC)	784.10	Art. 24f (cfr. sentenza del TAF A-516/2022 del 12 settembre 2023 consid. 6.5)	1° aprile 2007
Legge federale sulla parte generale del diritto delle assicurazioni sociali (LPGA)	830.1	Art. 33 (nel presente caso nessuna disposizione speciale ai sensi dell'art. 4 LTras: cfr. sentenza del TAF n. A-5111/2013 del 6 agosto 2014 consid. 4.1 e segg.; A-4962/2012 del 22 aprile 2013 consid. 6.1.3)	1° gennaio 2003
LATer	812.21	Art. 61 e 62 (cfr. sentenza del TF n. 1C_562/2017 del 2 luglio 2018 consid. 3.2; sentenza del TAF n. A-3621/2014 del 2 settembre 2015 consid. 4.4.2.3 e segg.)	1° gennaio 2002
Legge federale sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità (LPP)	831.40	Art. 86 (cfr. sentenza del TF n. 1C_336/2021 del 3 marzo 2022 consid. 3.4.3.)	1° gennaio 2001



L'IFPDT

3.1 Compiti e risorse

Prestazioni e risorse nell'ambito della protezione dei dati

Effettivi del personale

L'effettivo dell'IFPD è stabile dal 2023, anno di entrata in vigore della nuova LPD, rimanendo pertanto invariato a 33 posti a tempo pieno.

Tabella 6: Posti attribuibili per trattare questioni riguardanti la LPD

2023	33
2024	33
2025	33

Prestazioni

Secondo il nuovo modello di gestione dell'Amministrazione federale (NMG), i compiti dell'IFPD, quale autorità di protezione dei dati competente per gli organi federali e l'economia privata, sono attribuiti ai quattro gruppi di prestazioni «consulenza», «vigilanza», «informazione» e «legislazione».

Nell'anno in rassegna, ovvero dal 1° aprile 2024 al 31 marzo 2025, le risorse di personale impiegate presso l'IFPD che potevano essere destinate alla protezione dei dati sono state ripartite nei gruppi summenzionati nel modo seguente:

Tabella 7: Servizi protezione dei dati

Consulenza alla Confederazione	20,8%
Consulenza a privati	18,0%
Collaborazione con autorità esterne	15,1%
Collaborazione con i Cantoni	1,2%
Totale Consulenza	55,1%
Vigilanza	20,2%
Certificazione	0,1%
Totale Vigilanza	20,3%
Informazione	12,5%
Formazione / conferenze	2,6%
Totale Informazione	15,1%
Legislazione	9,5%
Totale Legislazione	9,5%
Totale Protezione dei dati	100,0%

Consulenza

Nel settore della consulenza l'IFPD si trova ad affrontare un continuo incremento delle richieste derivanti dal proprio mandato legale, in virtù del quale è chiamato ad accompagnare grandi progetti digitali. In tale contesto, esercita la sua funzione di consulente sia in seno all'Amministrazione federale, partecipando a progetti quali CEBA (v. n. 1.1), POLAP (v. n. 1.2), il sistema di riconoscimento facciale presso l'aeroporto di Zurigo (v. n. 1.6) o ancora Justitia 4.0 (v. n. 1.1), sia presso aziende pubbliche (FFS, Swisscom; v. n. 1.6) e private. Nell'ambito di tali progetti, l'IFPD è spesso chiamato a condurre valutazioni d'impatto sulla protezione dei dati. Nell'anno in rassegna, le risorse di personale impiegate nella consulenza ammontavano al 55,1 per cento, un valore leggermente superiore rispetto all'anno precedente (53,3%).

Per quanto riguarda i diversi gruppi di prestazioni, la valutazione delle risorse deve fondarsi sui seguenti obiettivi di efficacia:

Tabella 8: Obiettivi di efficacia IFPD in materia di protezione dei dati

Gruppo di prestazioni	Obiettivi di efficacia
Consulenza	L'IFPD dispiega una presenza conforme alle attese per la consulenza a privati e per il monitoraggio di progetti sensibili in materia di protezione dei dati dell'economia e delle autorità federali.
Vigilanza	L'IFPD dispiega una densità di controlli credibile.
Informazione	L'IFPD sensibilizza l'opinione pubblica in modo proattivo sui rischi legati alla tecnologia e alle applicazioni nel contesto della digitalizzazione. Dispone di un sito Internet moderno e di facile consultazione nonché di portali di notifica.
Legislazione	DL'IFPD esercita attivamente e tempestivamente la propria influenza nell'elaborazione di tutte le norme speciali e di tutti i regolamenti che hanno un impatto in materia di protezione dei dati, a livello nazionale e internazionale. Sostiene le cerchie interessate nella formulazione di regole di buona prassi.

Vigilanza e campagne

Il numero di denunce trattate nell'anno in rassegna dai tre team dell'ambito direzionale Protezione dei dati ha raggiunto quota 1053.

Inoltre, la quota di risorse impiegate nelle attività e nelle procedure di vigilanza era pari al 20,3 per cento, il che corrisponde a un netto aumento rispetto al valore medio pari al 15 per cento degli anni in rassegna successivi al 2015. Conformemente a quanto previsto nel quadro della pianificazione dei suoi obiettivi strategici, l'IFPDT ha

rafforzato la sua attività di vigilanza, come evidenziato anche dai dati statistici. La tabella sottostante illustra le differenti attività di vigilanza dell'IFPDT, che spaziano dagli interventi a bassa soglia agli accertamenti preliminari, fino alle inchieste formali.

Sono state avviate due campagne volte a sensibilizzare su temi specifici il maggior numero possibile di persone, organi federali o imprese private. In particolare, è stata lanciata una campagna rivolta agli organi federali (v. anche il tema prioritario a tale proposito) sull'utilizzo del numero AVS al di fuori del contesto delle assicurazioni sociali. Inoltre, è stata avviata una campagna sui moduli di iscrizione relativi alla locazione di appartamenti, che è stata pubblicata e comunicata alle persone interessate (v. n. 1.3).

Violazioni della sicurezza dei dati

Nell'anno in rassegna, sono stati segnalati all'IFPDT 344 casi di violazioni della sicurezza dei dati tramite il modulo online (rispetto ai 245 dell'anno precedente), il che rappresenta un aumento significativo.

19 segnalazioni sono state trasmesse all'IFPDT tramite altri canali, quali la posta elettronica o tradizionale. In 26 casi la segnalazione è stata spontanea.

Nell'anno in rassegna è stato calcolato anche il tempo che intercorre tra il verificarsi di una violazione della sicurezza dei dati e la segnalazione all'IFPDT: in circa il 40 per cento dei casi la segnalazione è avvenuta entro sei giorni. Dopo 21 giorni è stato segnalato circa l'80 per cento delle violazioni della sicurezza dei dati.

Tabella 9: Attività di vigilanza e campagne (cfr. p. 22)

Denunce	1053
di cui	1023 contro privati 30 contro la Confederazione 788 trattate 265 pendenti
Interventi a bassa soglia	108
di cui	90% messi in atto su base volontaria
Accertamenti preliminari	20
Inchieste	9
di cui	6 aperte 3 concluse con misure amministrative
Decisioni pendenti presso il TAF	2
Campagne	2
di cui	1 per la Confederazione 1 per privati

Tabella 10: Notifiche di violazioni della sicurezza dei dati

Totale	363
di cui spontanee	26
entro 6 giorni	40%
entro 21 giorni	80%

Informazione

Nell'anno in rassegna le risorse impiegate per il gruppo di prestazioni «Informazione» sono state nuovamente ridotte in misura proporzionale del 15,1 per cento rispetto all'anno precedente (17,8%).

Legislazione

Gli adeguamenti del trattamento dei dati personali conseguenti alla trasformazione digitale degli uffici federali comportano l'introduzione nel diritto federale di prescrizioni nuove e rivedute sul trattamento dei dati, in merito alle quali l'IFPDT si esprime nell'ambito di procedure di consultazione. In tale contesto, occorre sottolineare l'impegno profuso dai diversi team dell'IFPDT dato che la maggior parte delle consultazioni richiede un'analisi interdisciplinare (protezione dei dati, informatica, questioni internazionali e principio di trasparenza). Inoltre, quando i progetti

sono associati a grandi progetti informatici o il trattamento previsto potrebbe comportare un rischio residuo elevato per la personalità o i diritti fondamentali della persona interessata, occorre effettuare anche delle valutazioni d'impatto. Nell'anno in rassegna abbiamo partecipato a 271 consultazioni degli uffici.

Tabella 11: Consultazioni degli uffici

Total	274
di cui concluse	250

Prestazioni e risorse nell'ambito della legge sulla trasparenza

L'effettivo del personale impiegabile per mediazioni e raccomandazioni secondo la legge sulla trasparenza rimane invariato a sei posti a tempo pieno. L'Incaricato continuerà ad adoperarsi per ridurre ulteriormente nei prossimi esercizi in esame le pratiche accumulate a causa del persistente numero elevato di domande di mediazione. Se e con quali tempi ciò accadrà dipende, da un lato, dalla evoluzione quantitativa delle richieste di mediazione e dalla loro complessità e, dall'altro lato, dalle risorse di personale disponibili.

Tabella 12: Posti attribuiti per trattare le questioni relative al principio di trasparenza

2023	5,4
2024	6,2
2025	6,2

Partecipazione a deliberazioni delle commissioni e audizioni da parte di commissioni parlamentari

Nel periodo in esame l’Incaricato ha partecipato alle seguenti audizioni e deliberazioni delle commissioni:

- aprile 2024: CAG-S sulla legge federale sul mezzo d’identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull’Id-e)
- aprile 2024: sottocommissioni CDF-S e CDF-N sul consuntivo 2023
- aprile 2024: CIP-S sulla legge federale sul sistema nazionale di consultazione degli indirizzi delle persone fisiche (Legge sul servizio nazionale degli indirizzi, LSI)
- maggio 2024: CIP-N sull’adeguamento della legislazione in materia di protezione dei dati prevedendo un disciplinamento per le decisioni parzialmente automatizzate basate sull’intelligenza artificiale
- giugno 2024: CIP-S sulla legge federale sul sistema nazionale di consultazione degli indirizzi delle persone fisiche (Legge sul servizio nazionale degli indirizzi, LSI)
- giugno 2024: sottocommissione CdG-S/N sul rapporto d’attività dell’IFPDT 2023/2024
- giugno 2024: CIP-N sulla legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi (Legge sui dati dei passeggeri aerei, LDPA)
- giugno 2024: CAG-S sulla legge federale sul mezzo d’identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull’Id-e)
- agosto 2024: CPS-N sulla legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi (Legge sui dati dei passeggeri aerei, LDPA)
- agosto 2024: CIP-S sulla legge federale sul mezzo d’identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull’Id-e)
- agosto 2024: CdG-N visita del nostro servizio da parte della sottocommissione DFGP/CaF
- ottobre 2024: sottocommissioni CDF-S e CDF-N sul preventivo 2025
- ottobre 2024: CIP-N sulla legge federale sul sistema nazionale di consultazione degli indirizzi delle persone fisiche (Legge sul servizio nazionale degli indirizzi, LSI)
- ottobre 2024: CIP-N sulla legge sul personale federale (LPers)

Visita di servizio della Sottocommissione DFGP/CaF della Commissione della gestione del Consiglio nazionale

Le Commissioni della gestione (CdG) esercitano, su mandato delle Camere federali, l'alta vigilanza sulla gestione del Consiglio federale e dell'Amministrazione federale, dei tribunali della Confederazione e di altri organi incaricati di compiti federali.

È in tale contesto che il 27 agosto 2024 la Sottocommissione DFGP/CaF ha potuto scambiarsi con l'Icaricato federale nonché i quadri dell'IFPDT in merito alle missioni, ai compiti e alle competenze dell'IFPDT e alle attività in corso. Tale visita ha consentito in particolare di discutere le sfide attuali e di informarsi sulla soddisfazione degli impiegati. Ha inoltre offerto l'opportunità all'IFPDT di presentare i temi d'attualità importanti in relazione al principio di trasparenza e alla protezione dei dati.

Il consulente per la protezione dei dati dell'IFPDT

Il consulente per la protezione dei dati dell'IFPDT ha il compito di rispondere alle richieste di informazioni e di verificare i trattamenti dei dati personali da parte dell'IFPDT quale autorità, come pure di raccomandare misure correttive qualora venisse accertata una violazione delle norme sulla protezione dei dati. Inoltre, il consulente per la protezione

dei dati fornisce sostegno all'esame, all'applicazione e all'aggiornamento dei regolamenti sul trattamento.

Nell'anno in rassegna, il consulente per la protezione dei dati ha ricevuto in totale sedici richieste di informazioni e una richiesta di cancellazione. Il consulente ha provveduto a fornire le informazioni richieste a sei persone interessate entro il termine stabilito. Le restanti richieste riguardavano dati personali che l'IFPDT non possedeva né a cui aveva accesso. È frequente che i cittadini ritengano che l'IFPDT abbia accesso a tutte le banche dati e a tutti i dati personali gestiti dall'Amministrazione federale, ma ciò non corrisponde alla realtà.

17:32

5G 53

Abbrechen

Fotos

Sammlungen

Fertig

Q Mediathek durchsuchen ...



Beschränkter Zugriff auf deine Mediathek

„Instagram“ kann nur auf die Objekte zugreifen, die du auswählst. Die App kann Inhalte zu deiner Mediathek hinzufügen, selbst wenn keine Objekte ausgewählt sind.



3.2 Comunicazione

Nel 2024 l'IFPDT ha pubblicato 15 contributi brevi e 5 comunicati stampa. Per quanto riguarda la legge sulla trasparenza ha emesso e pubblicato sul proprio sito Internet 30 raccomandazioni. In merito al principio di trasparenza nell'Amministrazione, il Tribunale amministrativo federale si è espresso 14 volte e il Tribunale federale una volta. Una parte dell'Amministrazione federale persiste nel chiedere che le attività delle autorità siano parzialmente o completamente escluse dall'ambito di applicazione della legge sulla trasparenza. L'IFPDT ha redatto un elenco al riguardo che ha pubblicato sul suo sito Internet.

Comunicati stampa

Al termine delle sue procedure formali l'IFPDT è solito diffondere un comunicato stampa. Nel 2024 questi documenti hanno riguardato la conclusione delle inchieste nei confronti di fedpol e dell'UDSC in ambito federale, nonché contro le ditte Xplain, Digitec Galaxus e la piattaforma di aste Ricardo a livello privato. Tutte le procedure sono state concluse in conformità con la normativa previgente.

Comunicazioni «in breve»

Sette contributi brevi riguardavano la protezione dei dati fuori dai confini nazionali. L'IFPDT, ad esempio, è intervenuto sul caso di Meta, che intendeva utilizzare i dati degli utenti in Svizzera senza il loro consenso per migliorare il proprio sistema di intelligenza artificiale. Alla luce delle crescenti preoccupazioni riguardo l'estrazione massiva di dati personali dalle piattaforme di social media (il cosiddetto «data scraping»), in particolare a supporto dei sistemi d'intelligenza artificiale, l'IFPDT e altre 16 autorità omologhe di altri Paesi hanno delineato le migliori strategie

che le imprese di social media possono adottare per proteggere i dati personali in maniera più efficace.

Informazione e sensibilizzazione

Dopo il lancio del suo nuovo sito Internet nel 2023, l'IFPDT ha continuato a offrire informazioni e strumenti utili, con particolare attenzione alle novità introdotte dalla revisione totale della legge sulla protezione dei dati, senza trascurare i progressi della digitalizzazione e i fenomeni tecnologici ad essa correlati, come l'intelligenza artificiale. Tra questi ricordiamo la guida concernente il trattamento dei dati mediante cookie e tecnologie simili, la guida per la notifica di violazioni della sicurezza dei dati e l'informazione alle persone interessate

secondo l'articolo 24 LPD, il promemoria concernente l'apertura di un'inchiesta da parte dell'IFPDT per violazione delle disposizioni sulla protezione dei dati e il foglio informativo sulla pianificazione e sulla motivazione dell'accesso online ai dati personali.

Sito Internet

A seguito della migrazione su un nuovo software, il sito Internet è stato oggetto di un ulteriore restyling e offre ora, grazie a FAQ dettagliate, un supporto rapido e costante. I nuovi moduli di contatto permettono ai diversi gruppi di utenti di sottoporre le proprie problematiche all'IFPDT in modo semplice e diretto. I portali di notifica continuano a essere utilizzati efficacemente (v. statistiche). Tutte le guide e le spiegazioni sono raccolte nella sezione Documentazione.

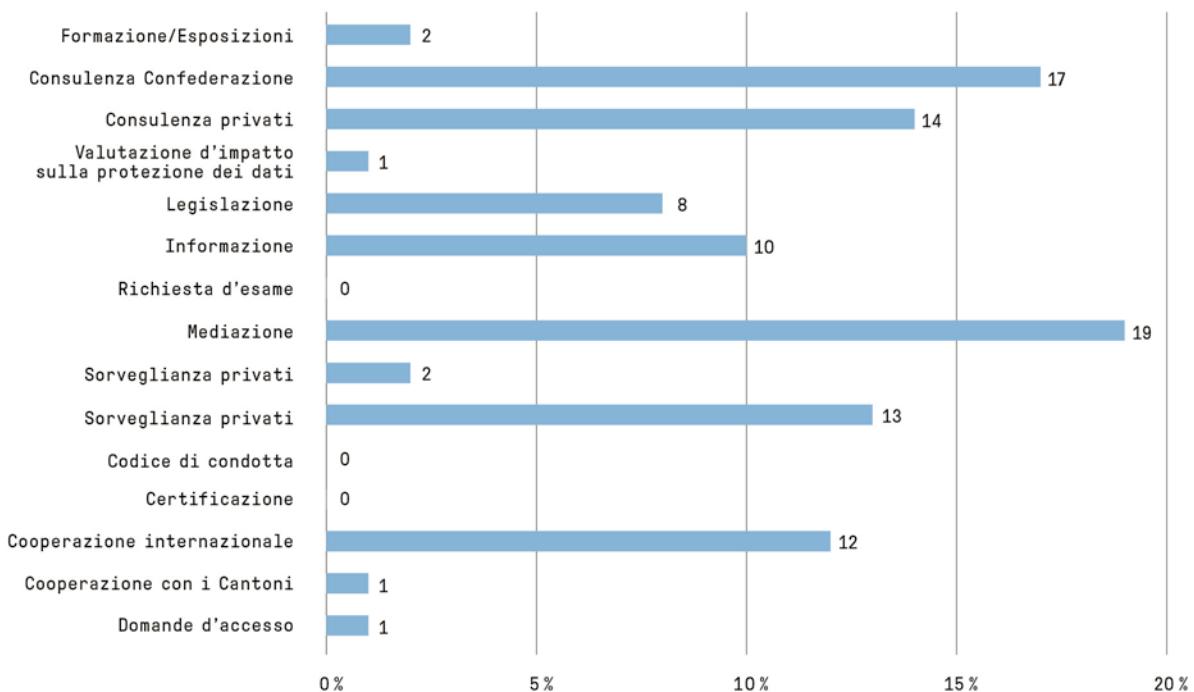
Attività mediatica

Nell'anno 2024 l'IFPDT ha risposto a circa 200 domande dei media. Le notizie riguardanti la protezione e la sicurezza dei dati, così come quelle sulla legge sulla trasparenza e sull'importanza della trasparenza nell'Amministrazione, hanno contribuito a sensibilizzare la popolazione e costituiscono un elemento fondamentale dell'attività di comunicazione dell'IFPDT, soprattutto nei casi in cui sorgono controversie. Per tale motivo, l'Incarnicato federale si rivolge spesso all'opinione pubblica esprimendo pareri critici a nome dei cittadini interessati.

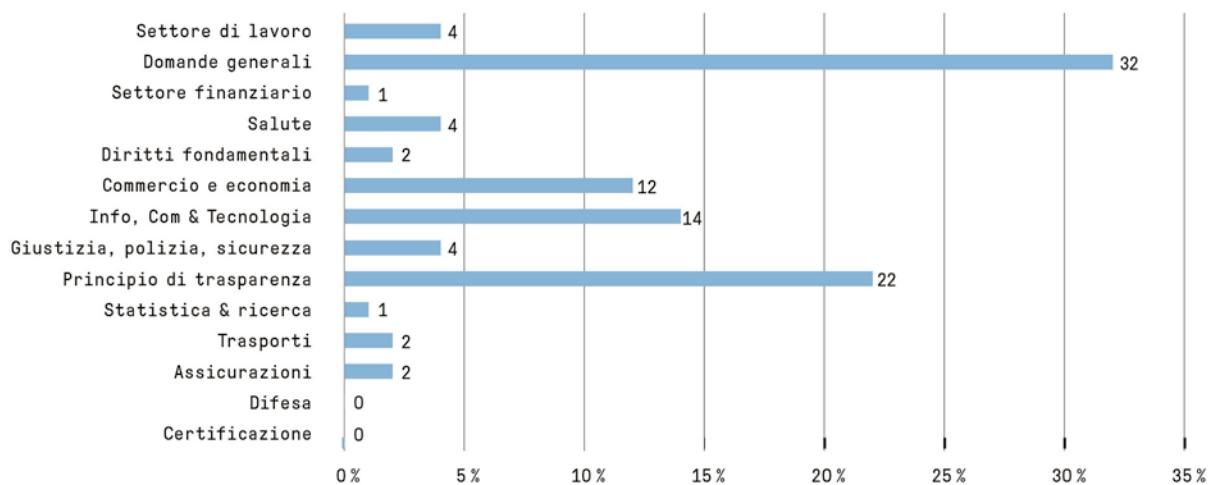
3.3 Statistiche

Statistiche sulle attività dell'IFPDT dal 1° aprile 2024 al 31 marzo 2025

Carico di lavoro per compiti in %



Carico di lavoro per materie in %

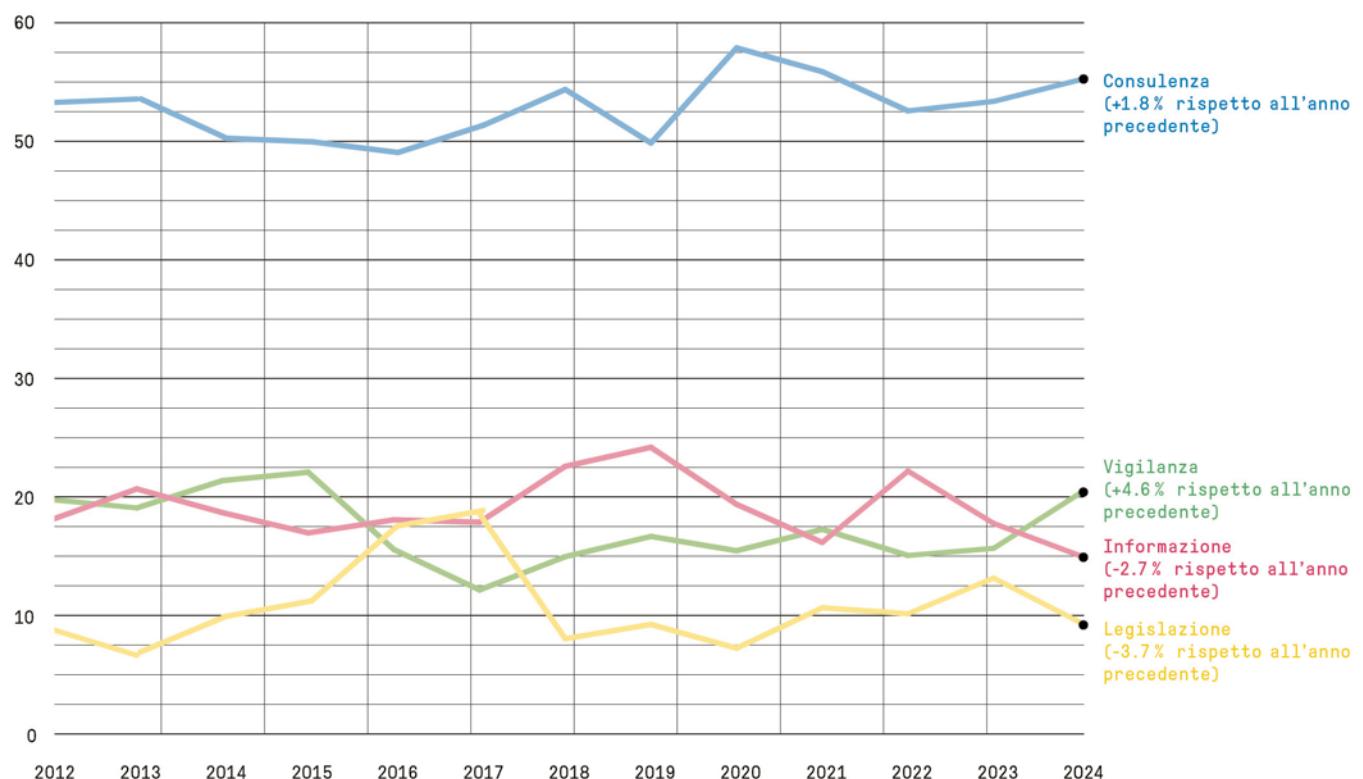


Numero d'operazioni d'affari

Procedure di mediazione	184
Consultazioni d'ufficio	274
Servizi di consulenza	1248
Indagini su denuncia	1087
Procedure di ricorso	9
Conferenze ed eventi	49
Richieste dei media	170
Chiamate alla hotline	1180
Richieste con modulo di contatto	1823
Richieste via e-mail	914
Richieste entrate per posta	604
Totale di entrate da persone fisiche	3668
Totale di rifiuti standard	584
Percentuale di rifiuti standard	16%

Paragone pluriennale

(in percentuale)



**Panoramica delle domande d'accesso secondo la legge sulla trasparenza
dal 1° gennaio al 31 dicembre 2024**

Dipartimento	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
CaF	123	68	12	30	1	8	4
DFAE	306	137	27	77	6	15	44
DFI	292	131	17	79	19	25	21
DFGP	212	111	20	37	10	3	31
DDPS	527	366	23	90	10	8	30
DFF	145	54	28	43	4	5	11
DEFR	290	146	25	35	63	13	8
DATEC	324	142	23	82	20	22	35
MPC	8	3	2	0	0	3	0
SP	5	1	2	1	0	0	1
Totale 2024 (%)	2232	1159 (52)	179 (8)	474 (21)	133 (6)	102 (5)	185 (8)
Totale 2023 (%)	1738 (100)	830 (48)	176 (10)	402 (23)	73 (4)	96 (6)	161 (9)
Totale 2022 (%)	1180 (100)	624 (53)	99 (8)	236 (20)	53 (5)	69 (6)	99 (8)
Totale 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (4)	78 (6)	115 (8)
Totale 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Totale 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Totale 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Totale 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	-
Totale 2016 (%)	554 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	-
Totale 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	-
Totale 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	-

**Statistica delle domande d'accesso secondo la legge sulla trasparenza
dal 1° gennaio al 31 dicembre 2024**

		Numero di domande	Inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	94	0	50	11	26	1	2	4
	IFPDT	29	0	18	1	4	0	6	0
	Totale	123	0	68	12	30	1	8	4
Dipartimento federale degli affari esteri DFAE	DFAE	306	0	137	27	77	6	15	44
	Totale	306	0	137	27	77	6	15	44
Dipartimento federale dell'interno DFI	SG DFI	22	0	13	2	4	0	1	2
	UFU	8	1	8	0	0	0	0	0
	UFC	15	0	9	2	2	0	2	0
	AFS	2	1	2	0	0	0	0	0
	METEO CH	3	0	3	0	0	0	0	0
	BN	0	0	0	0	0	0	0	0
	UFSP	85	0	21	4	41	4	13	2
	UST	4	0	4	0	0	0	0	0
	UFAS	32	0	21	0	6	1	0	4
	USAVERG	42	0	23	2	8	3	3	3
	MNS	0	0	0	0	0	0	0	0
	SWISS MEDIC	70	8	25	5	18	11	3	8
	SUVA	7	0	2	2	0	0	1	2
	compenswiss	2	0	0	0	0	0	2	0
Totale		292	10	131	17	79	19	25	21
Dipartimento federale di giustizia e polizia DFGP	SG DFGP	34	1	19	0	6	1	0	8
	DFGP	54	2	25	10	4	2	0	13
	FEDPOL	35	0	9	10	11	0	2	3
	METAS	2	0	2	0	0	0	0	0
	SEM	61	0	39	0	12	6	0	4
	Servizio SCPT	2	0	1	0	1	0	0	0
	ISDC	4	0	3	0	0	0	0	1
	IPI	4	0	4	0	0	0	0	0
	CFCG	6	0	4	0	0	1	1	0
	CAF	2	0	2	0	0	0	0	0
	ASR	5	0	2	0	3	0	0	0
	CSI	3	0	1	0	0	0	0	2
	CNPT	0	0	0	0	0	0	0	0
Totale		212	3	111	20	37	10	3	31

		Numero di domande	inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS	SG DDPS	87	5	19	7	39	5	5	12
	Difesa	38	0	9	0	19	3	0	7
	SIC	16	0	2	1	10	0	0	3
	AVI-AIn	12	1	2	7	2	1	0	0
	armasuisse	18	1	2	4	9	1	2	0
	UFSPO	317	0	311	2	0	0	1	3
	UFPP	8	0	4	0	4	0	0	0
	swisstopo	4	0	3	0	0	0	0	1
	UUC	2	0	2	0	0	0	0	0
	SEPOS	23	0	11	2	7	0	0	3
	UFCS	2	0	1	0	0	0	0	1
Totale		527	7	366	23	90	10	8	30
Dipartimento federale delle finanze DFF	SC DFF	27	1	9	6	8	1	0	3
	AFF	11	0	6	2	2	0	1	0
	UFPER	5	0	4	0	1	0	0	0
	AFC	20	0	7	3	8	0	1	1
	UDSC	32	5	8	9	10	0	3	2
	UFCL	12	0	7	4	1	0	0	0
	UFIT	4	0	2	0	1	0	0	1
	CDF	18	0	8	4	3	2	0	1
	SFI	11	0	1	0	7	0	0	3
	PUBLICA	4	0	1	0	2	1	0	0
	UCC	1	0	1	0	0	0	0	0
Totale		145	6	54	28	43	4	5	11

		Numero di domande	inoltrate negli anni precedenti							
			Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile		
Dipartimento federale dell'economia, della formazione e della ricerca DEFRI	SG DEFR	20	0	6	2	4	2	4	2	
	SECO	51	1	16	10	16	8	1	0	
	SEFRI	11	0	6	2	1	0	0	2	
	UFAG	22	2	12	2	3	2	0	3	
	Agroscope	3	0	2	0	0	0	1	0	
	UFAE	0	0	0	0	0	0	0	0	
	UFAB	4	0	4	0	0	0	0	0	
	SPR	8	0	3	1	4	0	0	0	
	COMCO	16	0	9	1	3	0	2	1	
	CIVI	3	0	3	0	0	0	0	0	
	UFDC	1	0	1	0	0	0	0	0	
	FNS	4	1	1	2	1	0	0	0	
	IUFFP	0	0	0	0	0	0	0	0	
Consiglio dei PF	143	0	81	5	2	50	5	0	0	
	Innosuisse	4	0	2	0	1	1	0	0	
Totale		290	4	146	25	35	63	13	8	

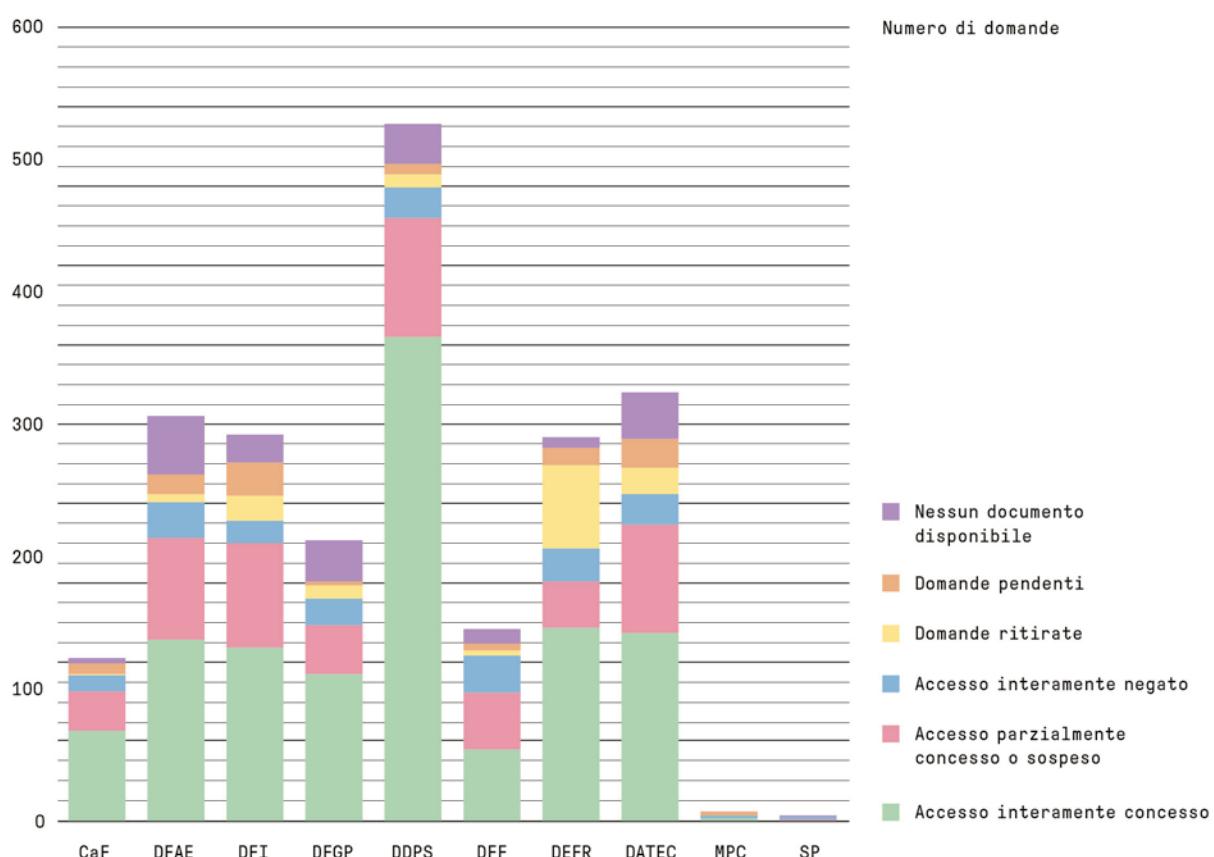
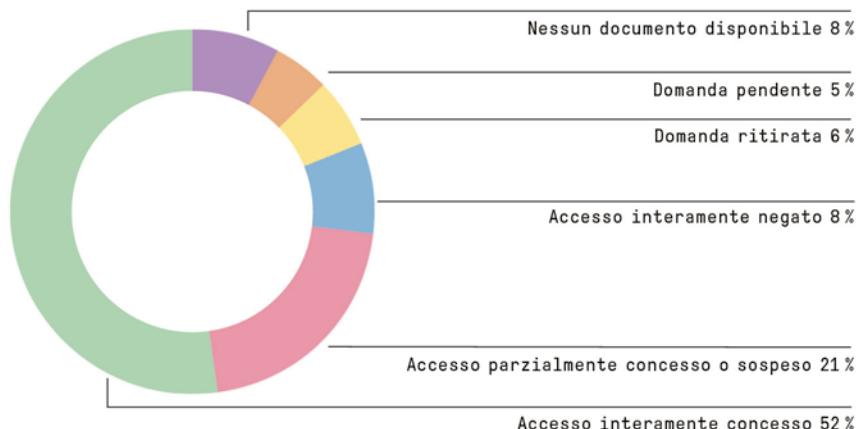
		SG DATEC	31	1	13	2	3	0	1	12
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	UFA	19	0	9	0	5	1	2	2	
	UFAC	26	2	10	4	6	3	0	3	
	UFE	19	1	9	0	6	2	2	0	
	USTRA	27	0	23	0	2	1	0	1	
	UFCOM	34	2	7	2	11	5	3	6	
	UFAM	144	5	58	14	43	8	11	10	
	ARE	9	0	8	1	0	0	0	0	
	ComCom	2	0	1	0	1	0	0	0	
	IFSN	7	3	2	0	3	0	2	0	
	ESTI	1	0	0	0	0	0	1	0	
	PostCom	3	2	1	0	2	0	0	0	
	AIRR	0	0	0	0	0	0	0	0	
	IFO	0	0	0	0	0	0	0	0	
	SUST	2	0	1	0	0	0	0	1	
Totale		324	16	142	23	82	20	22	35	

		Numero di domande	inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Ministero pubblico della Confederazione MPC Bundesanwalt-schaft BA	MPC	8	0	3	2	0	0	3	0
	Totale	8	0	3	2	0	0	3	0
Servizi del Parlamento SP	SP	5	0	1	2	1	0	0	1
	Totale	5	0	1	2	1	0	0	1
	Somma totale	2232	46	1159	179	474	133	102	185

Numero di domande di mediazione secondo la categoria di richiedenti

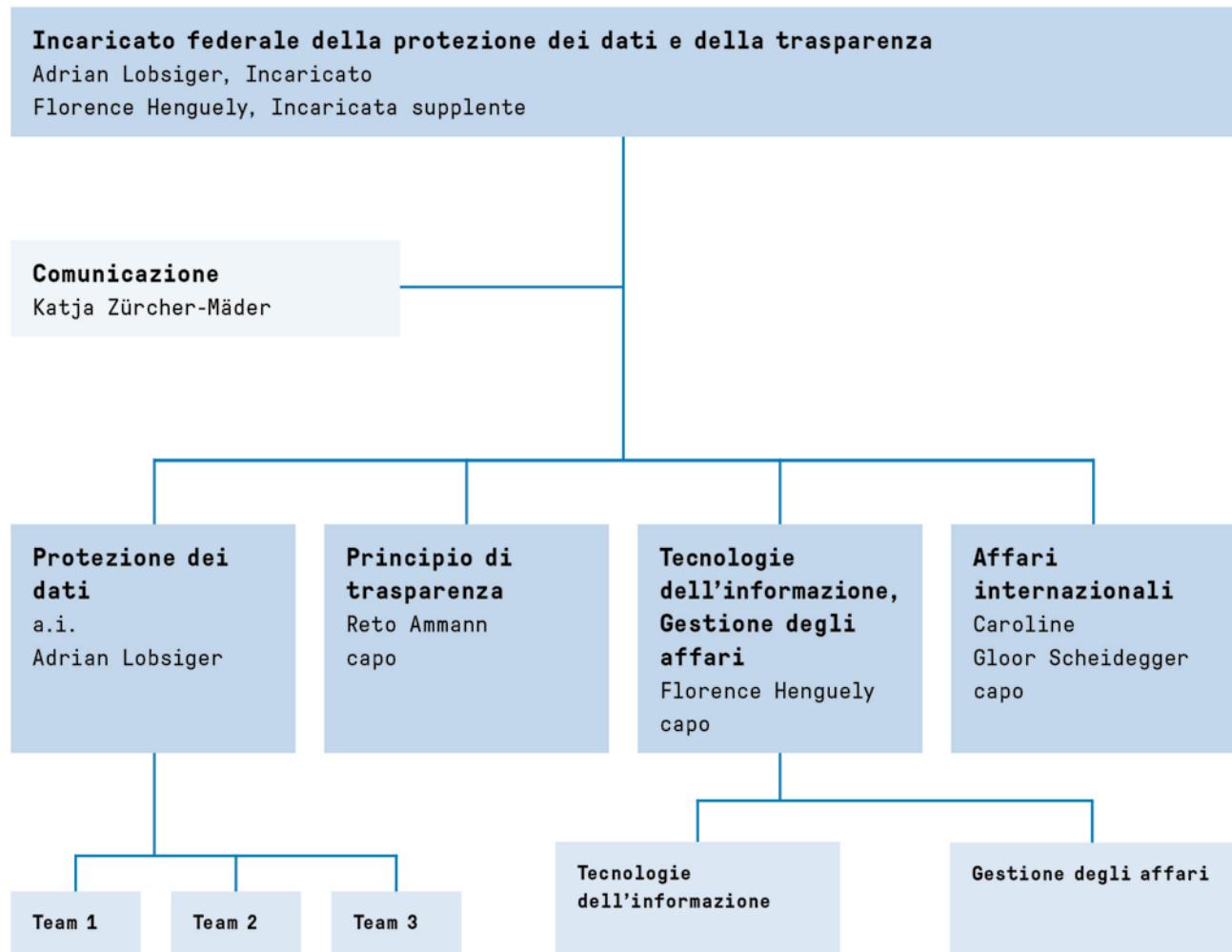
Categoria di richiedenti	2024	2023	2022	2021	2020	2019	2018	2017
Media	61	74	47	53	31	34	24	21
Privati (o nessuna assegnazione esatta possibile)	66	31	37	49	42	40	26	35
Parti interessate (associazioni, organizzazioni, società ecc.)	16	8	9	16	5	7	9	14
Avvocati	45	16	27	12	7	5	4	2
Aziende	14	3	9	19	7	47	13	7
Università	0	0	0	0	1	0	0	0
Totale	202	132	129	149	93	133	76	79

**Domande d'accesso dell'intera amministrazione federale
dal 1° gennaio al 31 dicembre 2024**



3.4 Organizzazione dell'IFPDT (Stato 31 marzo 2025)

Organigramma



Personale dell'IFPDT

Numero di dipendenti	44		
FTE	37.2		
per sesso			
Donne	22	50%	
Uomini	22	50%	
per livello di occupazione			
1-89%	29	65.91%	
90-100%	15	34.09%	
per lingua			
Tedesco	31	70.45%	
Francese	12	27.27%	
Italiano	1	2.27%	
per età			
20-49 anni	25	56.82%	
50-65 anni	19	43.18%	
Posizioni dirigenziali			
Donne	5	55.56%	
Uomini	4	44.44%	
	Total	9	

Abbreviazioni

ADS Amministrazione digitale svizzera	LCF Legge sul Controllo delle finanze	Privatim Conferenza degli incaricati svizzeri per la protezione dei dati dei Cantoni
AMVP Assemblea mondiale per la protezione della vita privata	LCIP Legge federale sulla cartella informatizzata del paziente	RA Rapporto annuale dell'IFPDT
CEPD Comitato europeo per la protezione dei dati	LDPA Legge sui dati dei passeggeri aerei	SIC Servizio delle attività informative della Confederazione
CIP Cartella informatizzata del paziente	LNA Legge federale sulla navigazione aerea	SIS II Sistema d'informazione Schengen di seconda generazione
DataReg Registro delle attività di trattamento degli organismi federali	LPD Legge federale sulla protezione dei dati	TDT Settore Trasformazione digitale e governance delle TIC della Cancelleria federale
Fedpol Ufficio federale di polizia	LPers Legge sul personale federale	TIC Tecnologie dell'informazione e della comunicazione
GDPR Regolamento generale sulla protezione dei dati	LSIn Legge sulla sicurezza delle informazioni	UDSC Ufficio federale della dogana e della sicurezza dei confini
GEPD Garante europeo della protezione dei dati	LTPG Legge sulla trasparenza delle persone giuridiche	UFCS Ufficio federale della cibersicurezza
IA Intelligenza artificiale	LTras Legge federale sul principio di trasparenza dell'amministrazione	VIPD Valutazione d'impatto sulla protezione dei dati
Id-e Identità elettronica	OPDa Ordinanza sulla protezione dei dati	VIS Sistema centrale d'informazione visti
IFPDT Incaricato federale della protezione dei dati e della trasparenza	OTras Ordinanza sul principio di trasparenza dell'amministrazione	
LAIn Legge federale sulle attività informative	PNR Dati dei passeggeri aerei (Passenger Name Records)	
LAVS Legge federale sull'assicurazione per la vecchiaia e per i superstiti		

Elenco delle illustrazioni

Figure	Tabelle	
Figura 1: Valutazione delle domande di accesso – evoluzione dal 2011 p. 69	Tabella 1: Soluzioni consensuali p. 73	Tabella 9: Attività di vigilanza e campagne p. 91
Figura 2: Emolumenti riscossi dall'entrata in vigore della LTras p. 71	Tabella 2: Tempo di elaborazione delle procedure di mediazione p. 74	Tabella 10: Notifiche di violazione della sicurezza dei dati p. 91
Figura 3: Richieste di mediazione dall'entrata in vigore della LTras p. 72	Tabella 3: Procedure di mediazione pendenti p. 75	Tabella 11: Consultazioni degli uffici ... p. 92
	Tabella 4: Disposizioni speciali ai sensi dell'articolo 4 LTras p. 84-85	Tabella 12: Posti attribuiti per trattare le questioni relative al principio di trasparenza p. 93
	Tabella 5: NESSUNA disposizione speciale ai sensi dell'articolo 4 LTras p. 86	
	Tabella 6: Posti attribuibili per trattare questioni riguardanti la LPD p. 90	
	Tabella 7: Servizi protezione dei dati .. p. 90	
	Tabella 8: Obiettivi di efficacia dell'IFPDT in materia di protezione dei dati p. 90	

Impressum

Il presente rapporto è disponibile in quattro lingue e anche in versione elettronica su Internet (www.lincaricato.ch).

Distribuzione: UFCL, Pubblicazioni federali, CH-3003 Berna

www.bundespublikationen.admin.ch

Art.-Nr. 410.032.I

Layout: Ast & Fischer AG, Wabern

Fotografia: Monika Flückiger

Caratteri: Pressura, Documenta

Stampa: Ast & Fischer AG, Wabern

Carta: PlanoArt®, senza legno, extra bianco



Cifre chiave

Prestazioni protezione dei dati

55.1% **20.3%** **15.1%** **9.5%**

Consulenza

Vigilanza

Informazione

Legislazione

Vigilanza

108 **19** **9** **2**

Interventi a bassa soglia

Accertamenti preliminari

Inchieste formali ai sensi dell'art. 49 LPD

pendenti dinanzi al TAF

Domande d'accesso all'IFPDT

18 **4** **1** **0** **6** **0**

interamente concesso

parzialmente concesso o sospeso

interamente negato

ritirato

pendente

nessun documento disponibile

Incaricato federale della protezione dei dati e della trasparenza
Feldeggweg 1
CH-3003 Berna

E-mail: info@edoeb.admin.ch
Sito Internet: www.lincaricato.ch
 @EDÖB – PFPDT – IFPDT
Telefono: +41 (0)58 462 43 95 (lu–ve, 10–11:30)
Fax: +41 (0)58 465 99 96