28° Rapporto d'attività 2020/21

Incaricato federale della protezione dei dati e della trasparenza

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapporto d’attività 2020/2021 dell’Incaricato federale della protezione dei dati e della trasparenza

L’Incaricato fa rapporto all’Assemblea federale periodicamente e secondo i bisogni. Trasmette contemporaneamente il rapporto al Consiglio federale (art. 30 LPD).

Il presente rapporto riguarda il periodo dal 1° aprile 2020 al 31 marzo 2021.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Premessa

Il periodo in rassegna è stato caratterizzato da una persistente pandemia e dalle misure adottate dal Consiglio federale e dall'Amministrazione per proteggere la popolazione e sostenere l'economia.

In un simile contesto non deve certo sorprendere il fatto che l'attività di vigilanza della nostra autorità di protezione dei dati si sia concentrata sugli strumenti digitali della lotta contro la pandemia, come la «SwissCovid App» o i certificati di vaccinazione, test e guarigione. Anche nell'ambito dell'esecuzione della legge sulla trasparenza il nostro lavoro quotidiano è stato contrassegnato dalla pandemia di COVID-19: un'alta percentuale delle domande di mediazione pervenuteci ha infatti riguardato l'accesso a documenti ufficiali concernenti ad esempio l'acquisto di mascherine o vaccini.

Mentre per combattere la tenace pandemia lo Stato interveniva nella sfera privata e nell'autodeterminazione informativa della popolazione con una serie di misure attuate a un ritmo incalzante, da parte nostra abbiamo sempre insistito sulla trasparenza nell'operato delle autorità. Visto che quando affronta una crisi l'Amministrazione deve stabilire priorità, abbiamo proceduto in modo pragmatico, chiedendo per esempio agli operatori dei media di usare pazienza per quanto riguarda la documentazione a posteriori dell'attività dell'Ufficio federale della sanità pubblica.

È ancora presto per stilare un bilancio dei danni causati da questa pandemia che mina la libertà. Ma su un punto non ci sono dubbi: anche la nostra autorità ha tratto gli opportuni insegnamenti dalle disavventure digitali che hanno provocato stupore e indignazione in questa crisi. Le critiche ai servizi dello Stato e ai loro dirigenti non possono tuttavia farci dimenticare le carenze della digitalizzazione asincrona del nostro Paese. Pensiamo in primo luogo alla mancanza di un servizio di base per un'identità elettronica accertata ufficialmente, la quale è indispensabile proprio per garantire una gestione dei dati sanitari moderna e conforme ai principi della protezione dei dati.

Adrian Lobsiger
Incaricato federale della protezione dei dati e della trasparenza

Berna, 31 marzo 2021

Protezione dei dati

Principio di trasparenza

L'IFPDT

Testi e immagini con riferimento a Corona

Sfide attuali
I Digitalizzazione

La crisi di coronavirus, persistente nonostante la disponibilità dei vaccini, e l'accelerazione della digitalizzazione negli ambiti del lavoro e del consumo hanno contrassegnato anche durante l'anno in rassegna l'impiego delle tecnologie dell'informazione e della comunicazione (TIC) da parte della popolazione svizzera.

Tecnologia ed economia

Il potenziale tecnico ed economico per ingerenze nella sfera privata e nei diritti di autodeterminazione della popolazione permane elevato.

La realtà digitale è impostata sulla trasmissione a velocità molto elevate di segnali in Internet che vengono trasformati in caratteri, immagini, suoni o vibrazioni da miliardi di apparecchi portatili (cosiddetti dispositivi «smart») e resi in tal modo percettibili ai sensi umani. La curiosità, la voglia di giocare e la sete di sapere vengono appagate dall'attuale disponibilità e dalla grande diffusione di informazioni.

Le persone possono essere tuttavia rapidamente infastidite nel ricevere richieste per un particolare uso di dati o nel caso in cui entra in gioco la protezione della sfera intima. I privati e le imprese provvedono quindi a rendere inaccessibile una parte dei loro dati o a crittografarli, ciò che rappresenta a sua volta una spina nel fianco per i servizi d'intervento e la polizia. Anche i detentori di dispositivi smart sono viepiù confrontati a richieste di enti privati o autorità che chiedono loro di mostrare il loro apparecchio per confronti automatici di dati – cosiddetti «scan» – ciò che può creare disagio al pensiero che vi siano contenute numerose tracce della loro attività digitale. Non tutti sono quindi disposti a mostrare il proprio dispositivo smart dotato di un determinato programma. Vi sono anche persone che, a causa della loro età, della loro salute o di loro disabilità nemmeno sono in grado di farlo.

Nell'attuale fase di lotta contro la pandemia è ipotizzabile che queste persone si sentano maggiormente sotto pressione. In vista della riapertura degli esercizi e della soppressione dei divieti di manifestazioni è presumibile che l'accesso a determinati beni e prestazioni dipenderà dalla presentazione del risultato del test COVID-19 o della vaccinazione contro il COVID-19. Per impedire che la popolazione si veda imporre l'obbligo di portare con sé uno smartphone, l'IFPDT chiede che le siano messi a disposizione, a condizioni sopportabili, metodi alternativi di rilevamento dei dati sulla salute oltre a quello digitale. Tali opzioni sono importanti poiché va considerato che i trattamenti sistematici di dati personali nel contesto della pandemia caratterizzeranno l'autodeterminazione della popolazione in materia d'informazione ben oltre l'attuale crisi. Considerata la vasta diffusione di dispositivi smart è prevedibile che la crisi possa trasformarsi in un trampolino di lancio per interessi commerciali e di autorità per i quali appare verosimile l'accessibilità illimitata a questi apparecchi in quanto strumenti mobili di identificazione e di documentazione. Al fine di impedire che i dispositivi smart degenerino diventando cavigliere elettroniche, l'Incaricato ha chiesto pubblicamente che siano autorizzati anche vettori d'informazione convenzionali, ad esempio cartacei, sia per il rilevamento dei dati di contatto nell'ambito del tracciamento dei contatti sia per la presentazione di risultati dei test e delle vaccinazioni (v. le nostre comunicazioni sulle liste di ospiti e sulla raccolta di dati relativi alla salute da parte di privati). Tali riflessioni sono state determinanti anche per il legislatore quando, nella primavera 2020, aveva sancito nella legge sulle epidemie il principio secondo cui nessuno può far dipendere una prestazione dall'uso dell'applicazione SwissCovid.

Gli effetti di vasta portata generati dalla progressiva automatizzazione nel trattamento di grandi quantità di dati sono emersi in modo significativo nell'anno in rassegna anche in occasione di elezioni e votazioni. Quando si ricorre alla tecnica meccanica e digitale per lo spoglio di grandi quantità di voti, le preoccupazioni primarie dell'elettorato riguardano la trasparenza e l'attendibilità di queste procedure e sollevano quindi tipici interrogativi dal profilo della protezione dei dati. La sfiducia sempre più diffusa nei con-

fronti delle procedure automatizzate ha contribuito anche ai disordini intervenuti alla fine delle elezioni presidenziali satunitensi. Prendendo volutamente di mira aspetti astratti e tecnici della trasmissione, dello spoglio e della valutazione dei dati discreditandoli con critiche generali e sistemiche, gli allora legali della Casa Bianca hanno contribuito ad alimentare l'insicurezza di un pubblico che, nei forum di Internet, si trovava confrontato a una raffica di credenze relative ad algoritmi truccati e macchinazioni varie. Questo scenario lascia presumere che, con la progressiva automatizzazione delle elezioni e delle votazioni, acquisiranno importanza strumenti di lavoro propri di una moderna protezione dei dati che richiedono un pur minimo intervento umano nello svolgimento di procedure automatizzate con esiti decisionali.

Società e politica in materia di dati

Il 7 marzo 2021 il popolo svizzero ha respinto chiaramente la legge federale sui servizi di identificazione elettronica (Ie). Mentre il Consiglio federale e il Parlamento hanno tentato invano di conquistare la fiducia della popolazione quanto al coinvolgimento di soggetti privati per il rilascio dell'identificazione elettronica (Ie), il comitato referendario si era invece imposto argomentando principalmente che tale rilascio debba competere esclusivamente alle autorità. Il fatto che il Popolo si sia dichiarato favorevole a una maggiore direzione dello Stato nell'ambito di un progetto digitale chiave, potrebbe essere riconducibile alla sua legittima aspettativa di un'attività statale e di un conseguente trattamento dei dati personali che siano svolti nei limiti definiti dalla legge e di un diligente orientamento al principio di legalità da parte delle autorità.

Queste aspettative della popolazione contrastano in parte con le esperienze raccolte dall'IFPDT. Nella nostra attività di consulenza e di vigilanza constatiamo che, a causa delle sfide poste dalla trasformazione digitale in atto, l'Amministrazione federale ha difficoltà crescenti nell'applicare il principio di legalità e pone inoltre in dubbio i requisiti definiti dalla prassi del Tribunale federale in merito alla chiarezza delle basi legali per il trattamento dei dati. Per tali ragioni non è più sostenibile continuare a iscrivere nella legge contenuti, categorie, scopi, intensità e durata dei trattamenti dei dati personali da parte delle autorità poiché ciò richiede presumibilmente il mantenimento di «depositi di dati» e «interruzioni dei media» ormai obsoleti che ostacolerebbero il collegamento flessibile alla rete da parte dell'Amministrazione come pure lo svolgimento efficiente della sua attività.

Va osservato tuttavia che, così come non mette in discussione la digitalizzazione dell'Amministrazione, l'Incaricato ritiene altresì legittima l'esigenza della stessa di disporre di basi legali moderne che non limitino inutilmente la libertà degli uffici sui piani organizzativo e tecnologico. Mediante un'attività di consulenza orientata alle soluzioni, l'IFPDT sottolinea che norme di legge formulate in modo generale e astratto e tecnologicamente neutro non ostacolano minimamente la trasformazione digitale. L'Incaricato sostiene inoltre gli sforzi dell'Amministrazione volti a semplificare le strutture di sistemi consolidatisi nel tempo.

«La popolazione non può essere spinta all'obbligo di portare con sé uno smartphone.»

Nonostante questo riconoscimento nei confronti della trasformazione digitale, la vigilanza sulla protezione dei dati della Confederazione non può dispensare l'Amministrazione dal dedurre lo scopo, l'entità e l'intensità dei trattamenti digitali dei dati personali da un mandato degli organi politici, iscritto nella legge in modo comprensibile per i cittadini. È inoltre indispensabile che, disciplinando il trattamento dei dati da parte delle autorità, il legislatore democraticamente legittimato stabilisca i limiti di competenza necessari sui piani politico e istituzionale attribuendo responsabilità, limitando l'accesso diretto ai dati personali e disciplinando lo scambio di informazioni nell'ambito dell'assistenza amministrativa. Anche dalla nuova legge sulla protezione dei dati si evince del resto che la trasformazione digitale dell'Amministrazione va attuata evitando di annacquare il principio di legalità: nella stessa il legislatore del 2020 aveva riaffermato la promessa secondo cui gli organi federali tratteranno dati sensibili dei cittadini unicamente qualora ciò fosse previsto da una legge sottoposta a referendum, dalla quale risultassero chiaramente gli scopi, l'entità, le modalità, i contenuti dei dati e l'intensità del trattamento.

Durante l'anno in rassegna l'IFPDT ha avuto tra l'altro un colloquio con l'Amministrazione federale delle dogane sul tema dei requisiti riguardanti il principio di legalità. La discussione verteva sui margini di manovra del futuro Ufficio federale delle dogane e della sicurezza dei confini, il cui personale tratterà grandi quantità di dati personali sensibili e, come i collaboratori dell'Ufficio federale di polizia e del Servizio d'informazione della Confederazione, sarà armato e avrà competenze di polizia.

L'elaborazione di dati personali da parte delle autorità della Confederazione preposte alla sicurezza implica elevati rischi per la sfera privata e l'autodeterminazione informativa della popolazione, dato che tali autorità procedono in modo occulto alla raccolta di una parte delle loro informazioni e, a seconda del risultato della valutazione dei dati, infliggono misure coercitive incisive alle persone interessate. In tale contesto, riguardo alla trasformazione digitale di questi Uffici, la vigilanza sulla protezione dei dati della Confederazione non può tollerare concessioni nell'osservanza dei requisiti di chiarezza posti alle norme legali e sanciti dal Tribunale federale in materia di trattamenti di dati personali da parte di autorità di polizia. È unicamente grazie a leggi sufficientemente chiare che può essere impedita una confusione di competenze nell'ambito della trasformazione digitale delle autorità di sicurezza della Confederazione e del corpo cantonale di polizia. Qualora il collegamento digitale di dati personali trattati all'interno del tessuto federalistico delle autorità di sicurezza in adempimento di scopi così diversi tra loro, quali la prevenzione di minacce da parte della polizia di sicurezza, il perseguimento penale ad opera della polizia criminale, la protezione dello Stato grazie ad attività d'informazione e l'esecuzione di numerose leggi speciali, venisse lasciato alla discrezione delle autorità, ne risulterebbe una concentrazione poco trasparente dei poteri di polizia, in contrasto con l'attribuzione delle competenze sancite dalla Costituzione federale.

Limitare per legge il trattamento dei dati di polizia della Confederazione a determinate categorie in funzione dei compiti è tanto più importante in quanto, improntata a una complessità tramandata dalla sua storia, l'organizzazione delle autorità di sicurezza a livello di Confederazione si distanzia in maniera singolare dalla situazione nei Cantoni. Mentre qui i rilevamenti di dati personali sono svolti in maniera occulta e coercitiva da un unico corpo di polizia i cui compiti e le cui competenze sono desumibili dalla legge cantonale in materia di polizia, la Confederazione ripartisce i suoi poteri di polizia, come menzionato, tra una moltitudine di unità armate che trattano dati personali sulla base di leggi tra loro molto diverse. Da ormai molti

«Le autorità di sicurezza della Confederazione hanno sempre più difficoltà a rispettare il principio di legalità.»

anni, nei suoi rapporti d'attività l'Incaricato federale della protezione dei dati e della trasparenza deplora l'assenza di una normativa federale comparabile alle vigenti leggi cantonali in materia di polizia e la mancanza di chiarezza generata dalla moltitudine di leggi federali speciali che riducono la trasparenza del trattamento di dati personali da parte delle autorità di sicurezza della Confederazione in modo difficilmente sostenibile dal profilo della legislazione sulla protezione dei dati. Nell'ambito della trasformazione digitale questa frammentazione legislativa ha comportato difficoltà sempre maggiori per queste autorità nel mantenere una chiara visione d'assieme dei trattamenti di dati effettuati a più livelli. L'Incaricato vede in questa situazione un'ulteriore spiegazione delle difficoltà incontrate dalle autorità di sicurezza della Confederazione nell'applicare il principio di legalità.

Legislazione

Con l'approvazione della revisione totale della legge federale sulla protezione dei dati, il 25 settembre 2020, le Camere federali hanno portato a termine i loro lunghi lavori di revisione della legislazione in materia di protezione dei dati (cfr. tema prioritario I).

II Attività di consulenza, controllo e mediazione

Affinché possa, nella sua veste di autorità di vigilanza, assicurare che i dati personali siano trattati non in base alle capacità tecniche bensì all'intensità legalmente consentita, l'IFPDT chiede ai responsabili delle applicazioni digitali di ridurre al minimo, già allo stadio pianificatorio e progettuale, i rischi elevati per la protezione dei dati e forniscano la pertinente documentazione all'autorità di vigilanza in materia di protezione dei dati e ai relativi responsabili aziendali. Seguendo questo orientamento abbiamo portato avanti la nostra consulenza nell'ambito della vigilanza legale su un numero notevole di progetti di big data a cura di autorità federali e imprese private, promuovendo un impiego autoresponsabile di strumenti di lavoro moderni quali la valutazione dell'impatto sulla protezione dei dati nonché la figura del responsabile aziendale della protezione dei dati.

Nell'anno in rassegna l'IFPDT ha dato la priorità assoluta all'accompagnamento e al controllo, intesi come vigilanza legale, di numerosi progetti digitali nell'ambito dell'attuale lotta contro la pandemia (evidenziati in giallo nel presente rapporto). La pandemia ha sollecitato l'IFPDT anche nel suo ruolo di Incaricato della trasparenza, che lo ha visto confrontato a numerose richieste di mediazione inerenti, tra l'altro, a documenti ufficiali per l'acquisto di mascherine o di vaccini e le quali, a seguito dell'obbligo generale del telelavoro, hanno reso in gran parte necessaria l'adozione di raccomandazioni scritte.

Sei dei 15 grandi progetti seguiti dall'IFPDT in virtù dei suoi obblighi di consulenza erano in relazione alla trasformazione digitale ordinata dal Consiglio federale per l'Amministrazione federale, la quale sta tentando di recuperare i ritardi nella digitalizzazione deplorati da rappresentanti della politica e dei media soprattutto in relazione alla lotta contro la pandemia. Oltre ai progetti menzionati dell'Ufficio federale della sanità pubblica, l'IFPDT ha seguito progetti di digitalizzazione di numerosi altri organi federali ponendo la priorità sulle autorità di sicurezza (cfr. n. 1.2 e 3.1).

Dopo la netta diminuzione registrata nel periodo 2015/16, le spese relative ai compiti di controllo sono leggermente aumentate negli ultimi anni stabilizzandosi su un livello basso a causa della scarsa dotazione di mezzi. Anche nell'anno in rassegna l'IFPDT non ha potuto soddisfare nella misura auspicata le legittime aspettative del pubblico. Benché aspiri a una stretta collaborazione con il Centro nazionale per la cibersicurezza, l'IFPDT non dispone di fondi sufficienti (cfr.n. 3.1) per effettuare sistematicamente prove di campionatura e controlli della sicurezza tecnica che si rivelerebbero particolarmente utili proprio nell'ambito dell'archiviazione di dati sensibili sulla salute. In tale contesto va ricordato il caso della Fondazione «mievaccinazioni».

III Cooperazione nazionale e internazionale

Cooperazione nazionale

Nel quadro della lotta contro l'attuale pandemia sono emersi problemi di delimitazione delle competenze federali e cantonali nel tracciamento dei contatti come pure nel trattamento di dati personali in relazione con i test e le vaccinazioni riguardanti il COVID-19. Grazie ai contatti intrattenuti tra gli incaricati cantonali della protezione dei dati e l'IFPDT è sempre stato possibile trovare soluzioni per un procedimento coordinato e pragmatico.

Cooperazione internazionale

La lotta alla pandemia e la conseguente gestione dei dati sulla salute pongono problemi comparabili in materia di protezione dei dati in numerosi Stati che ne sono colpiti, ragione per cui l'IFPDT ha seguito attentamente gli sviluppi intervenuti a livello internazionale ricorrendo anche ai suoi contatti con i suoi partner esteri.

Consiglio d'Europa

Determinato a impegnarsi attivamente presso il Consiglio d'Europa, l'IFPDT ha preso parte alle sedute del Comitato consultivo della Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (Convenzione 108). Nel contempo una rappresentante dell'IFPDT è stata eletta presso l'Ufficio del Comitato consultivo della Convenzione 108 il quale dirige i lavori del Comitato tra le sedute plenarie.

Valutazione del livello di protezione dei dati

Atteso per fine maggio 2020, il rapporto della Commissione europea concernente l'adeguatezza del livello di protezione dei dati della Svizzera ha subito ritardi ma è atteso ancora prima dell'estate 2021.

Con il Regno Unito, uscito dall'UE, la Svizzera ha potuto portare a termine con successo ancora nell'anno in rassegna i negoziati relativi ai riconoscimenti reciproci dell'adeguatezza del livello di protezione dei dati.

Soppressione dello scudo Svizzera-USA per la privacy quale livello adeguato di protezione dei dati

Il 16 luglio 2020 la Corte di giustizia dell'Unione europea (CGUE) ha emesso la sentenza attesa con trepidazione riguardante la trasmissione di dati dall'UE agli USA (Schrems II). Essa ha dichiarato non valida la decisione di esecuzione 2016/1250 della Commissione UE sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy concernente le imprese USA certificate sotto tale regime.

Le sentenze della CGUE non hanno validità per la Svizzera. Sullo sfondo delle sue valutazioni periodiche dello scudo Svizzera-USA per la privacy e dei riconoscimenti dell'adeguatezza tra la Svizzera e l'UE, l'IFPDT ha tuttavia constatato che tale regime non offre più una protezione adeguata alle persone interessate in Svizzera. Ha quindi esortato le imprese svizzere a effettuare la trasmissione di dati negli USA sulla base di garanzie contrattuali e valutazioni dell'impatto dei rischi relativi a progetti.

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali

Valutazione d'impatto sulla protezione dei dati concernente la SwissID

Nell'anno in rassegna lo SwissSign Group AG ha sottoposto per conoscenza all'IFPDT la sua valutazione d'impatto sulla protezione dei dati concernente la SwissID.

A causa dell'importanza sistemica della «SwissID» di SwissSign Group AG, in passato l'IFPDT ha avuto riunioni periodiche con i responsabili dell'impresa e in quest'ambito si è tra l'altro adoperato affinché, per i servizi strettamente Single-Sign-On (SSO) della «SwissID», fosse possibile una registrazione anonima. SwissSign Group AG ha adottato questo principio nella sua politica in materia di protezione dei dati. Le sue Condizioni generali saranno a breve debitamente adeguate.

Nell'anno in esame SwissSign Group AG ha presentato all'IFPDT la valutazione d'impatto sulla protezione dei dati commissionata a un consulente esterno per la protezione dei dati. Dall'esame svolto dall'IFPDT emerge che il documento descrive in modo dettagliato le procedure di trattamento dei dati personali, valuta i rischi delle misure riguardanti i diritti fondamentali ed elenca le misure di protezione della personalità.

L'IFPDT ha preso atto che, secondo il titolare del trattamento, la valutazione d'impatto sulla protezione dei dati è conclusa e il trattamento dei dati in relazione alla «SwissID» è ammissibile in considerazione dei rischi e delle misure descritte.

Progetto degli editori di media svizzeri per un accesso comune a portali in rete

L'Alleanza digitale svizzera porta avanti i suoi lavori per la realizzazione di una soluzione SSO uniforme per i portali in rete di editori di media. Nel quadro di una discussione l'IFPDT ha illustrato possibilità di miglioramenti.

Realizzando un progetto SSO (Single-Sign-On) l'Alleanza digitale svizzera si adopera affinché in futuro, mediante un unico login comune, gli utenti possano accedere a varie offerte web di diversi editori di media svizzeri. L'Alleanza, che riunisce diverse imprese mediatiche svizzere, ha ulteriormente sviluppato il suo progetto per la realizzazione del SSO centrale, di cui nella primavera 2021 viene avviata una fase pilota. Nel quadro di precedenti presentazioni del progetto e delle relative discussioni abbiamo esposto all'Alleanza digitale svizzera il nostro punto di vista in merito agli aspetti del progetto essenziali alla protezione dei dati, illustrando possibilità di miglioramenti.

Il progetto si protrarrà oltre la conclusione dell'anno in rassegna. Anche nel prosieguo dei lavori ci adopereremo affinché nella struttura della soluzione SSO sia tenuto conto in modo ottimale della protezione della personalità.

Iniziative cloud per attuare la strategia TIC della Confederazione

L'IFPDT ha accompagnato l'elaborazione di obiettivi strategici e linee guida per la trasformazione digitale in seno all'Amministrazione federale. La realizzazione delle necessarie infrastrutture informatiche comprende anche la garanzia dell'impiego sicuro di servizi cloud pubblici («public clouds»), a complemento dell'opzione già esistente di poter gestire e trattare applicazioni e dati nei centri di calcolo dell'Amministrazione federale («private clouds»). Chiediamo che i requisiti in materia di protezione dei dati siano già considerati al momento della pubblicazione del bando di concorso.

La digitalizzazione richiede l'utilizzo di una moltitudine di applicazioni e servizi che devono presentare un'elevata agilità, flessibilità ed estensibilità. Per poter adempiere queste esigenze, l'impiego di soluzioni cloud sia pubbliche che private offre un contributo importante poiché tali soluzioni mettono a disposizione in tempo reale i servizi e gli strumenti necessari, con la possibilità di procurarsi da sé i componenti (per i termini utilizzati v. box). L'Amministrazione federale usa già oggi, in misura limitata, servizi cloud facilmente estensibili di varia natura. Un sondaggio svolto nel quarto trimestre del 2019 presso i Dipartimenti e la Cancelleria federale ha mostrato che in futuro aumenterà proprio il fabbisogno di servizi cloud pubblici.

È proprio utilizzando questi servizi cloud pubblici che le unità amministrative dell'Amministrazione federale centrale possono accedere in modo efficiente e rapido a soluzioni innovative e relativamente economiche, nonché alle più recenti tecnologie. Si apre così la strada a nuove possibilità di mettere a disposizione in modo rapido e agile prestazioni amministrative digitali. Di conseguenza, le prestazioni operative TIC possono essere ottimizzate e esternalizzate almeno nei settori in cui non vigono elevati requisiti di sicurezza. Per questo motivo è sorta in seno all'Amministrazione federale la necessità di creare, accanto alle esistenti soluzioni cloud private, un'opzione strategica per l'utilizzo di servizi cloud pubblici. Si trattava inoltre di svolgere un'analisi accurata sul fabbisogno, l'impostazione, la necessità e la fattibilità di un'infrastruttura pubblica, ma esclusivamente svizzera, di cloud e dati denominata «Swiss Cloud».

Ma proprio l'utilizzo di servizi cloud pubblici comporta una maggiore dipendenza da offerenti attivi per lo più a livello mondiale. Ciò riguarda sia la dipendenza tecnologica sia la disponibilità di dati e applicazioni. In tale contesto occorre necessariamente chiedersi in che modo possano essere garantite la sovranità sui propri dati e la protezione dalle fughe di dati.

Per tener conto di questa problematica, mediante numerose aggiunte ai criteri per l'acquisto di cloud pubblici l'IFPDT si è adoperato affinché la protezione dei dati e la sicurezza dei dati siano garantite già dagli offerenti lungo tutta la catena di trasformazione. Si è pure impegnato in modo determinante a favore dell'elaborazione di requisiti riguardanti l'affidabilità di tali servizi cloud dal punto di vista della sicurezza informatica e della protezione dei dati. Vista la portata del progetto, l'IFPDT ha ritenuto indispensabile esigere che gli offerenti presentino specifiche certificazioni in materia di protezione dei dati già nelle offerte.

È evidente che le riflessioni inerenti alla protezione dei dati devono essere integrate già in una fase molto precoce dei progetti che implicano il trattamento di dati personali. L'IFPDT continuerà a seguire da vicino le iniziative cloud e verificherà l'attuazione dei criteri e requisiti richiesti.

Servizi cloud

Mentre in passato quasi ogni azienda aveva il proprio centro di calcolo, oggi si ricorre spesso ai servizi cloud. Per cloud o cloud computing (nuvola informatica) s'intende la fornitura attraverso la rete Internet di prestazioni quali spazio di memoria, potenza di calcolo oppure software applicativi. Un cloud è quindi un'infrastruttura informatica online, nella quale vengono esternalizzati dati o interi ambienti di sistema. Le diverse soluzioni di cloud computing si differenziano in base all'uso previsto e al livello d'integrazione desiderato.
I principali vantaggi di un cloud sono i seguenti:

- elevata scalabilità, ossia la possibilità di aumentare o ridurre la capacità di memoria e la potenza di calcolo in funzione dei bisogni;
- elevata disponibilità e sicurezza grazie all'utilizzo delle più moderne tecnologie;
- sicurezza degli investimenti, dato che l'ambiente è mantenuto da chi lo fornisce e non sono necessari grandi investimenti per un'infrastruttura di server propria.

Possibili usi del cloud

Per i servizi cloud esistono diversi tipi di prestazioni che si differenziano in base alle esigenze dei singoli utenti. I principali usi sono:

- private cloud: è per lo più allestito nel centro di calcolo dell'azienda ed è utilizzato soltanto da un'azienda. Solitamente è gestito dall'azienda stessa o, se necessario, da un fornitore esterno ed è accessibile soltanto a gruppi chiaramente definiti di persone. Il cloud privato soddisfa i severi requisiti di sicurezza e di protezione dei dati ed è quindi particolarmente adatto per i dati sensibili come le informazioni confidenziali concernenti il personale o i dati aziendali riservati.
- public cloud: è un'offerta di un fornitore liberamente accessibile che rende i suoi servizi aperti e accessibili a tutti via Internet. Tutti gli utenti condividono la stessa infrastruttura. I noti archivi online come Dropbox oppure Google Drive, ma anche i provider di posta elettronica come Gmail oppure Hotmail si basano su un cloud pubblico.
- hybrid cloud: è una soluzione mista tra un cloud privato e uno pubblico. L'utente riceve un cloud pubblico, nel quale è integrato un ambiente privato per i dati e le applicazioni sensibili. La forma ibrida è apprezzata perché consente di archiviare i dati altamente sensibili in un cloud privato e di esternalizzare più facilmente e in modo più economico i dati meno sensibili.
- multicloud: collega tra loro più servizi cloud consentendo di utilizzare in parallelo le soluzioni di diversi fornitori di cloud. Il multicloud offre molte più possibilità rispetto alla forma ibrida.

Livello d'integrazione del cloud

Nel cloud computing si distinguono in genere tre cosiddetti livelli di servizio cloud, basati gli uni sugli altri. A partire dall'infrastruttura passando per la piattaforma fino ad arrivare al software, questi livelli di servizio formano tre strati sovrapposti e definiscono nel contempo l'architettura del cloud.

- Infrastructure as a Service: in questo caso le risorse come potenza di calcolo, capacità di memoria o di rete sono ottenute dal cloud. Se i server locali sono stati precedentemente spostati nel cloud, ora il cloud sostituisce l'hardware in loco, mentre il supporto per il sistema operativo e le applicazioni rimane in azienda.
- Plattform as a Service: in questo caso dal cloud si ottengono anche il sistema operativo e le applicazioni relative al sistema come backup, antivirus, applicazioni di manutenzione ecc. Anziché sviluppare software sul proprio ambiente, le aziende possono utilizzare ambienti completi di sviluppo e di fornitura nel cloud.
- Software as a Service: all'utente viene fornita un'applicazione cloud con tutte le sue infrastrutture e piattaforme informatiche sottostanti. L'utente ottiene così tutti i componenti informatici dal fornitore.

L'ingresso dell'Amministrazione federale nel cloud deve avvenire nel rispetto della protezione dei dati

La «Strategia cloud dell'Amministrazione federale» spianerà la strada a una digitalizzazione dell'Amministrazione federale basata sul cloud computing. L'IFPDT ha espresso il proprio parere sul documento di strategia e ha potuto inserirvi le sue esigenze principali dal profilo della protezione dei dati.

L'Organo direzione informatica della Confederazione (ODIC) è stato incaricato dal Consiglio federale di redigere un documento di strategia che concretizza la visione cloud della Confederazione e prescrive linee guida e principi vincolanti per l'acquisizione di applicazioni cloud da parte delle singole unità amministrative. L'IFPDT ha ricevuto una versione provvisoria del documento per consultazione preliminare e ha individuato in diversi punti un potenziale di miglioramento. Ha constatato in particolare che il documento si è focalizzato soprattutto sui requisiti da porre alla sicurezza dell'informazione, trattando solo superficialmente altri aspetti giuridici attinenti alla protezione dei dati.

Abbiamo perciò proposto alcune integrazioni affinché nel documento di strategia vengano inclusi i requisiti relativi alla protezione dei dati in relazione a una delocalizzazione dei trattamenti di dati in un cloud. Le nostre proposte miravano soprattutto a evidenziare i rischi supplementari insiti in una delocalizzazione dei trattamenti di dati a fornitori esteri di public cloud situati in Paesi privi di un livello di protezione dei dati adeguato.

In tal senso, secondo le nostre proposte, il documento dovrà prevedere che – nel valutare se e con quali misure il trattamento di dati mediante applicazioni cloud sia ammesso – vada effettuata una valutazione d'impatto sulla protezione dei dati se nel cloud vengono trattati dati personali. Questo meccanismo consentirà di verificare la conformità giuridica dell'applicazione

cloud, applicando criteri quali l'ubicazione dei server, il diritto in vigore nel Paese in questione e le misure tecniche e organizzative previste. Le nostre osservazioni e proposte di modifica sono state integrate nella versione finale del documento.

Sia l'Amministrazione federale sia gli utenti privati di soluzioni di public cloud sono confrontati sempre più spesso con questioni simili da quando il regime dello scudo per la privacy è stato riesaminato (cfr. il testo sullo scudo per la privacy, tema prioritario II nel presente rapporto) e non si può partire dal presupposto che le clausole contrattuali standard garantiscano negli Stati Uniti un livello di protezione dei dati adeguato. Molti fornitori risiedono infatti proprio negli USA.

CORONA

Accesso da parte dell'UFSP ai dati sulla mobilità detenuti da Swisscom

Dopo che il 21 marzo 2020 il Consiglio federale aveva vietato gli assembramenti di oltre cinque persone nello spazio pubblico, l'UFSP ha verificato mediante informazioni detenute da Swisscom se questa misura di protezione dal contagio di coronavirus fosse rispettata. L'IFPDT è giunto alla conclusione che Swisscom aveva permesso all'UFAS di accedere esclusivamente a dati anonimizzati.

Swisscom ricorre alla piattaforma Mobility Insights (MIP) per elaborare statistiche di gruppo anonimizzate basate su dati aggregati sulla mobilità al fine di analizzare i comportamenti in questo ambito sul territorio svizzero. Dopo che era stato reso noto che nell'ambito della lotta alla pandemia doveva essere garantito all'Ufficio federale della sanità pubblica (UFSP) l'accesso a tali dati – per farsi un'idea e verificare se in Svizzera vi erano ancora grandi assembramenti di persone – l'IFPDT ha avviato accertamenti preliminari nell'ambito dei quali ha anche svolto un'ispezione presso l'UFSP.

Le analisi di Swisscom, rese accessibili con un ritardo di almeno otto ore sotto forma di visualizzazioni, mostrano l'andamento temporale della presenza dei proprietari di telefoni cellulari in quadranti di 100 metri x 100 metri, ma solo se in tali quadranti sono presenti più di 20 cellulari di abbonati Swisscom. I dati relativi alla localizzazione vengono anonimizzati e aggregati appena possibile e all'UFSP non vengono mai mostrati i dati in chiaro su cui si basano le visualizzazioni. Le visualizzazioni accessibili all'UFSP non consentono di risalire all'identità delle persone e sono dunque anonime. Di conseguenza nella valutazione del 3 aprile 2020 l'IFPDT ritiene pertanto che l'elaborazione dei dati da parte di Swisscom e la trasmissione di dati anonimi all'UFSP siano ammesse dalla legislazione sulla protezione dei dati (cfr. la nostra comunicazione del 3 aprile 2020).

Sulla base di queste informazioni l'IFPDT ha concluso che non vi erano indizi che potessero indurlo a procedere a un accertamento formale dei fatti. L'IFPDT era invece del parere che le informazioni accessibili al pubblico sulla collaborazione tra l'UFSP e Swisscom e sulla relativa elaborazione dei dati fossero scarse e non facilmente reperibili. Ha pertanto esortato Swisscom a fornire al pubblico informazioni più dettagliate sulla procedura di elaborazione dei dati. Swisscom ha risposto a questa richiesta e ha preparato delle FAQ sull'utilizzo della piattaforma Mobility Insights da parte UFSP.

Programma Gestione dei dati a livello nazionale

La gestione dei dati pubblici sarà più semplice ed efficiente attraverso l'utilizzo multiplo dei dati. Con questo obiettivo il Consiglio federale, nell'ambito del programma Gestione dei dati a livello nazionale, ha lanciato diversi progetti pilota. L'IFPDT è in contatto con l'Ufficio federale di statistica, responsabile del programma, e si adopera in favore di un'attuazione conforme alla protezione dei dati.

L'obiettivo del programma Gestione dei dati a livello nazionale (NaDB) è di mettere le persone e le imprese in condizione di comunicare determinate informazioni alle autorità una volta sola (principio «once only»), in modo tale da sgravarle. Inoltre, un utilizzo multiplo dei dati consentirà di ridurre l'onere amministrativo nell'amministrazione pubblica. Per raggiungere l'obiettivo s'intende agevolare lo scambio di dati tra le autorità.

Nell'ambito della consultazione degli uffici, l'IFPDT ha innanzitutto espresso il proprio parere sui rapporti concernenti quattro progetti pilota su temi quali garanzia della qualità dei dati aziendali, statistiche dei salari, dati fiscali e processi, ruoli e responsabilità. Ha sottolineato inoltre che, in considerazione dell'utilizzo multiplo di informazioni contemplato dal programma, la protezione dei dati riveste un'importanza particolare. Ritiene tuttavia che l'utilizzo multiplo celi notevoli rischi legati alla protezione dei dati. Occorre assicurare in particolare che il principio «once only» non porti ad allargare la cerchia delle persone legittimate ad accedere ai dati. Si deve inoltre disciplinare in modo vincolante chi può elaborare quali dati a quale scopo, nonché distinguere chiaramente tra elaborazione di dati a fini statistici e ad altri fini. Dev'essere infine trasparente il modo in cui sono disciplinati il rilevamento e il successivo trattamento dei dati nonché le possibilità di accesso.

La consultazione degli uffici è stata seguita da uno scambio tra l'Ufficio federale di statistica, incaricato dell'attuazione, e l'IFPDT durante il quale sono stati discussi ancora una volta questi aspetti. L'Incaricato continuerà a seguire l'attuazione del programma NaDB in veste consultiva e rimarrà a disposizione degli uffici responsabili come interlocutore.

CORONA

Promemoria concernente l'uso conforme alla protezione dei dati di soluzioni in materia di conferenze audio e video

A causa della pandemia le applicazioni relative a conferenze audio e video hanno attecchito molto rapidamente. L'enorme quantità di utenti ha reso queste piattaforme digitali un interessante bersaglio di attacchi. Nella scelta del software è perciò importante prestare attenzione alla sicurezza delle informazioni e alla protezione dei dati. Oltre a essere in parte soggetti a successivi trattamenti abusivi, i dati personali sono esposti a rischi quanto alla loro sicurezza, che non sempre risulta riconoscibile, o attraverso l'uso di piattaforme che presentano addirittura notorie lacune.

Il promemoria dell'IFPDT (cfr. la nostra comunicazione del 10 aprile 2020 «Misure per un impiego sicuro delle soluzioni di audio e videoconferenza») è rivolto a tutti i gruppi di utenti – sia nel settore privato sia in quello aziendale – e li aiuta a proteggere i loro dati personali e a impedire effetti indesiderati. L'IFPDT raccomanda nello stesso misure di protezione nell'ambito dell'utilizzazione, ad esempio nella gestione dell'ID di meeting e della relativa password, nell'uso della videocamera o nella presentazione dello schermo. Il promemoria fornisce inoltre indicazioni per una valutazione e un'introduzione di una soluzione di audio- e di videoconferenza. In tal modo è consigliabile, ad esempio, esaminare la gestione dei metadati, la crittografia o la sicurezza del fornitore di servizi. Prima dell'implementazione nell'impresa andrebbero inoltre chiarite in un regolamento le disposizioni relative all'utilizzazione. L'impresa è inoltre tenuta a informare in modo trasparente i collaboratori sullo svolgimento di eventuali registrazioni o sorveglianze.

Vista la tentazione di integrare le soluzioni impiegate ad hoc durante la pandemia anche nell'infrastruttura TIC esistente, l'Incaricato raccomanda di acquisire tali soluzioni nell'ambito di progetti ordinari o per il tramite dei responsabili TI, affinché la conformità possa essere assicurata. La soluzione di audio- e videoconferenza utilizzata deve disporre di impostazioni di sicurezza che consentano uno standard elevato di protezione dei dati, in particolare in relazione con i segreti commerciali e professionali.

App di incontri: trattamento dei dati

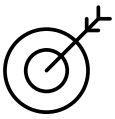
L'IFPDT ha avviato una procedura presso un fornitore svizzero di app di incontri per verificare i suoi metodi di trattamento e la sua gestione delle richieste di cancellazione.

Secondo i dati forniti dall'Ufficio federale di statistica, in Svizzera le app e i siti Internet di incontri assumono un ruolo sempre più importante nella ricerca di un partner: quasi il venti per cento delle coppie che negli ultimi cinque anni hanno visto nascere la loro relazione si sono conosciute online tramite un servizio di ricerca partner, un'app di incontri o una rete sociale[1]. App e siti Internet di incontri si caratterizzano per il fatto di presentare partner adatti basandosi sui dati personali forniti dai clienti che trattano del tutto o in parte automaticamente avvalendosi di un algoritmo.

Per aumentare le possibilità di avere successo nella ricerca di un partner, gli utenti sono invitati a fornire informazioni in parte molto sensibili sulla propria persona come, ad esempio, dati sulla propria visione del mondo, la religione, il consumo di alcool. Il trattamento di simili dati personali cela così rischi elevati perché se ne possono trarre conclusioni su aspetti importanti della personalità degli utenti.

[1] Ufficio federale di statistica (ed.): Erhebung zu Familien und Generationen 2018. Erste Ergebnisse. Neuchâtel 2019, pag. 9 (soltanto in tedesco) https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/erhebungen/efg.assetdetail.10467788.html (consultato il 14.04.2020)

Nella primavera 2021 l'IFPDT ha avviato un accertamento dei fatti presso un fornitore di una simile app di incontri con sede in Svizzera. A questa decisione siamo giunti dopo avere ricevuto comunicazioni di persone che attiravano la nostra attenzione sul fatto che non avevano alcuna possibilità di cancellare il proprio conto tramite l'app e che le richieste in tal senso rivolte al fornitore dell'app non venivano elaborate. Oltre a chiarire questo punto, il nostro accertamento dei fatti mira anche a verificare che il fornitore osservi altre disposizioni afferenti al diritto in materia di protezione dei dati. Tutto ciò in considerazione dei requisiti di trasparenza e sicurezza del trattamento nonché dell'eventuale comunicazione di dati personali a terzi.



L'IFPDT prevede nuovi portali di notifica

In seguito all'introduzione di nuovi obblighi di notifica nella LPD riveduta, l'IFPDT lancerà a breve due portali di notifica online sui quali si potranno notificare le perdite di dati e comunicare i consulenti per la protezione dei dati.

La legge sulla protezione dei dati riveduta stabilisce nuovi obblighi di notifica per i titolari del trattamento dei dati nei confronti dell'IFPDT. Questi comprendono la registrazione del trattamento dei dati da parte degli organi federali, la comunicazione dei consulenti per la protezione dei dati e la notifica di violazioni della sicurezza dei dati. L'IFPDT s'impegna a mantenere il più basso possibile l'onere derivante da questi nuovi obblighi consentendo agli interessati di effettuare online le notifiche in modo semplice e sicuro.

In primo luogo è necessario adeguare il registro delle collezioni di dati notificate all'IFPDT, dato che in futuro soltanto gli organi federali saranno tenuti a notificare i loro registri delle attività di trattamento all'IFPDT. Il portale di notifica e ricerca www.datareg.admin.ch sarà debitamente rinnovato per adattarsi alle nuove direttive.

Saranno inoltre introdotti due nuovi portali di notifica. In un primo portale web saranno registrati in modo strutturato ed efficiente i consulenti per la protezione dei dati nominati dai titolari del trattamento. Il portale adotta i principi del chiosco self-service, in cui i titolari del trattamento registrano, mutano e cancellano autonomamente i dati di contatto dei consulenti per la protezione dei dati. Nel secondo portale saranno registrate le notifiche di violazione della sicurezza dei dati che comportano un rischio elevato per gli interessati. L'Incaricato si aspetta un aumento del numero di notifiche di questo tipo. Anche questo portale permetterà di registrare le notifiche in modo strutturato e semplice e, grazie all'automazione, garantirà un risparmio di risorse nella valutazione dei dati. L'obiettivo è garantire risposte tempestive agli eventi segnalati.

La nuova legge federale sulla protezione dei dati dal punto di vista dell'IFPDT

Entro la data di entrata in vigore della nuova LPD (v. box) l'economia privata e le autorità federali dovranno adeguare alle nuove disposizioni il modo in cui trattano i dati personali. Nel febbraio 2021 l'IFPDT ha stabilito e pubblicato quelle che considera essere le novità più significative (cfr. la nostra comunicazione «Nuova legge federale sulla protezione dei dati dal punto di vista dell'IFPDT»). Raccomanda di osservare diversi punti.

Soltanto dati di persone fisiche

Analogamente al nuovo regolamento europeo sulla protezione dei dati (RGPD), la LPD riveduta mira esclusivamente a proteggere la personalità delle persone fisiche i cui dati personali sono oggetto di trattamento e non contempla più i dati delle persone giuridiche.

Dati personali degni di particolare protezione

La definizione di dati personali degni di particolare protezione è estesa ai dati genetici e ai dati biometrici che identificano in modo univoco una persona fisica.

Privacy by design e by default

Nella LPD riveduta sono stati introdotti i concetti di «protezione dei dati sin dalla progettazione» (privacy by design) e di «protezione dei dati per impostazione predefinita» (privacy by default). Il nuovo testo normativo obbliga le autorità e le imprese ad attuare i principi di trattamento contenuti nella LPD sin dalla progettazione. Le applicazioni devono tra l'altro essere impostate in modo tale che i dati siano anonimizzati o cancellati in maniera standardizzata. La protezione dei dati per impostazione predefinita protegge gli utenti di offerte online private che non esaminano le condizioni d'utilizzazione né i diritti di opposizione che ne derivano. In questo caso il trattamento di dati personali è circoscritto al minimo indispensabile per lo scopo perseguito, fintanto che gli utenti non autorizzino un trattamento più ampio.

Valutazione d'impatto sulla protezione dei dati

Le valutazioni d'impatto sulla protezione dei dati non sono un elemento nuovo nel diritto svizzero della protezione dei dati; gli organi federali sono già oggi tenuti a effettuarle. Se un trattamento può comportare un rischio elevato per la personalità o per i diritti fondamentali della persona interessata, ai sensi dell'articolo 22 della LPD riveduta anche i titolari privati del trattamento devono effettuare previamente una valutazione d'impatto sulla protezione dei dati. Il rischio elevato, in particolare in caso di utilizzazione di nuove tecnologie, risulta dal tipo, dall'entità, dalle circostanze e dallo scopo del trattamento. Sussiste un rischio elevato in particolare nel caso in cui è prevista una profilazione a rischio elevato oppure un trattamento su vasta scala di dati personali degni di particolare protezione. Secondo l'articolo 23 della LPD riveduta il titolare deve chiedere previamente il parere dell'IFPDT se dalla valutazione d'impatto sulla protezione dei dati emerge che, nonostante i provvedimenti previsti dal titolare, il trattamento previsto comporta ancora un rischio elevato per la personalità o i diritti fondamentali della persona interessata. Se l'IFPDT ha obiezioni riguardo alla valutazione d'impatto stessa, suggerirà al titolare del trattamento precisazioni e aggiunte.

Codice di condotta

All'articolo 11 la LDP riveduta incentiva le associazioni professionali, di settore ed economiche a sviluppare un proprio codice di condotta e a sottoporlo per parere all'IFPDT. I pareri sono pubblicati e possono contenere obiezioni o raccomandare modifiche o precisazioni. Un parere positivo dell'IFPDT funge da base alla presunzione giuridica che la condotta riportata nel codice sia conforme alla legislazione sulla protezione di dati. I codici di condotta formulati in maniera troppo generale non possono invece dispensare da rischi che non sono specificati nel testo.

Certificazioni

Conformemente all'articolo 13 della LDP riveduta, i fornitori di programmi o sistemi di trattamento di dati personali potranno, come i gestori degli stessi, far certificare i propri sistemi, prodotti e servizi. La certificazione permette alle aziende ad esempio di comprovare che rispettano il principio della protezione dei dati per impostazione predefinita e che dispongono di un sistema adeguato di gestione della protezione dei dati.

Registro delle attività di trattamento

L'articolo 12 della LPD riveduta prevede che i titolari e i responsabili del trattamento tengano ognuno un registro delle rispettive attività di trattamento. Il nuovo testo normativo ne definisce il contenuto minimo. Il registro deve essere sempre aggiornato. Nell'ordinanza il Consiglio federale prevede eccezioni per le imprese con meno di 250 collaboratori i cui trattamenti di dati personali comportano un rischio esiguo di violazione della personalità delle persone interessate.


ABHOLEN / PICK UP

Comunicazione di dati personali all'estero

L'articolo 16 della LPD riveduta stabilisce che i dati personali possono essere comunicati all'estero soltanto se il Consiglio federale ha constatato che la legislazione dello Stato destinatario garantisce una protezione adeguata dei dati. A tale scopo pubblica un elenco stabilito secondo il diritto vigente dall'IFPDT. Se lo Stato destinatario non figura nell'elenco del Consiglio federale, i dati possono comunque esservi comunicati, come avvenuto finora con il diritto vigente, se la protezione dei dati viene assicurata in modo adeguato con altri strumenti.

Se si prevede di pubblicare i dati all'estero – anche in caso di memorizzazione su sistemi esteri (cloud) – devono essere indicati i Paesi in questione, indipendentemente dal fatto che offrano o meno una protezione dei dati adeguata. In questo ambito la LPD è più severa del RGPD.

Ampi obblighi d'informazione

In adempimento dell'obiettivo di trasparenza perseguito dalla revisione, l'articolo 19 della LPD riveduta estende l'obbligo di informazione per le imprese. In linea di massima in futuro il titolare privato deve precedentemente informare in ogni caso e in modo adeguato la persona interessata sulla prevista raccolta di dati personali anche se i dati non sono raccolti presso di essa. La LPD vigente prescrive questo obbligo di informazione solo in caso di dati personali degni di particolare protezione e profili della personalità. Le imprese devono dunque esaminare e tenere aggiornate le proprie dichiarazioni relative alla protezione dei dati. Se il trattamento comporta decisioni individuali automatizzate, ai sensi dell'articolo 21 LPD riveduta il titolare del trattamento deve rispettare nuovi obblighi di informazione nei confronti della persona interessata e accordarle i diritti di essere sentita e di riesaminare la decisione.

Diritto d'accesso della persona interessata

La nuova LPD ha esteso il diritto della persona interessata di chiedere se dati personali che la concernono sono oggetto di trattamento. L'articolo 25 della LPD riveduta presenta un elenco più esteso delle informazioni che il titolare del trattamento deve comunicare, ad esempio sulla durata di conservazione dei dati personali della persona interessata.

Obbligo di notifica di violazioni della sicurezza dei dati

Conformemente all'articolo 24 della LPD riveduta il titolare del trattamento deve notificare all'IFPDT ogni violazione della sicurezza dei dati che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata. La notifica deve pervenire quanto prima all'IFPDT, dopo che il titolare ha redatto una previsione delle possibili conseguenze della violazione e ha valutato se la persona interessata debba essere informata della violazione e in che modo.

Maggiori poteri di vigilanza

La nuova LPD prevede che l'Incaricato debba in linea di principio aprire un'inchiesta su tutte le violazioni. Potrà pronunciare decisioni contro trattamenti dei dati insufficienti e, in determinati casi, dovrà essere consultato. In futuro potranno essere comminate multe fino a 250 000 franchi.

Inchiesta per violazione delle disposizioni sulla protezione dei dati

In futuro l'IFPDT sarà tenuto a svolgere d'ufficio un'inchiesta in caso di violazioni della nuova LPD da parte di organi federali o di privati (art. 49 cpv. 1 LPD riveduta). Nella LPD vigente si applica ancora la limitazione secondo la quale l'IFPDT svolge di propria iniziativa un'inchiesta con accertamento dei fatti contro privati solo quando il metodo di trattamento può violare i diritti della personalità di un numero considerevole di persone. Questa soglia di intervento definita quale «errore di sistema» viene abolita. Tuttavia anche nella nuova LPD se la violazione delle disposizioni sulla protezione dei dati è di poca importanza, l'IFPDT può rinunciare ad aprire un'inchiesta (art. 49 cpv. 2 LPD riveduta). Inoltre, come avvenuto finora, può rinunciare a misure formali quando, dopo un primo scambio di informazioni, il titolare del trattamento riconosce la lacuna che gli è stata notificata e vi pone rimedio in tempo utile. Date le risorse limitate di cui dispone, si può prevedere che anche dopo l'entrata in vigore della nuova legge in generale l'IFPDT intenda determinare delle priorità nel trattamento di notifiche in base al principio dell'opportunità.

Decisioni

Ai sensi dell'articolo 51 capoverso 1 LPD riveduta, l'IFPDT potrà svolgere procedure secondo la legge federale sulla procedura amministrativa[1] e ordinare formalmente a organi federali o titolari privati di trattamenti di dati di adeguare, sospendere o cessare del tutto o in parte il trattamento nonché di cancellare o distruggere del tutto o in parte i dati personali. Può ad esempio ordinare che un'impresa informi la persona interessata della violazione notificata della sicurezza dei dati. Fino ad ora l'IFPDT aveva solo la competenza di emanare raccomandazioni e di adire il Tribunale amministrativo federale in caso di mancata ottemperanza.

Consultazione

L'IFPDT non è né un'autorità di approvazione né un servizio di omologazione per applicazioni, prodotti, regolamentazioni e progetti. Tuttavia la nuova legge prevede in svariati articoli che i titolari debbano consultare l'IFPDT prima della conclusione definitiva di lavori e la realizzazione di progetti. Devono dunque essergli sottoposti per parere codici di condotta nonché valutazioni d'impatto sulla protezione dei dati in caso di elevati rischi residui.

Pareri spontanei e informazione del pubblico

A parte i pareri nel quadro di consultazioni formali, l'IFPDT può continuare ad esprimersi in modo spontaneo su nuove tecnologie, questioni di digitalizzazione o pratiche di trattamento di determinati settori e pubblicare la propria opinione e la propria valutazione. Inoltre, in caso di interesse generale l'IFPDT informa il pubblico, come avvenuto finora, delle proprie constatazioni e misure (anche nell'ambito di indagini formali).

Emolumenti

L'articolo 59 LPD riveduta disciplina le prestazioni dell'IFPDT per le quali i privati dovranno versare emolumenti: ad esempio per un parere in merito ad un codice di condotta o per una valutazione d'impatto sulla protezione dei dati o ancora per l'approvazione di clausole tipo di protezione dei dati e di norme interne d'impresa vincolanti. L'IFPDT potrà però riscuotere dai privati emolumenti anche per servizi di consulenza generale.

Sanzioni

Nella nuova LPD sono previste multe per privati fino a 250 000 franchi (art. 60 LPD riveduta). Sono punibili atti od omissioni intenzionali, ma non quelli colposi. Il mancato rispetto degli obblighi di informare, di concedere l'accesso e di collaborare nonché la violazione degli obblighi di diligenza e del segreto professionale sono punibili a querela di parte. Invece il mancato rispetto di provvedimenti amministrativi dell'IFPDT è perseguito d'ufficio. In linea di massima sono punibili con multa soltanto le persone fisiche, ma in futuro potranno esserlo anche le imprese stesse fino a 50 000 franchi, se la ricerca della persona fisica all'interno dell'impresa o dell'organizzazione comporterebbe un onere sproporzionato.

Nel regime previsto dalla nuova LPD l'IFPDT continuerà a non avere la facoltà di pronunciare sanzioni. Le persone che si sono rese colpevoli sono sanzionate dalle autorità di perseguimento cantonali. L'IFPDT può sporgere denuncia e avvalersi nel procedimento dei diritti dell'accusatore privato (art. 65 cpv. 2 LPD riveduta), ma non ha il diritto di querela.

[1] Legge federale del 20 dicembre 1968 sulla procedura amministrativa (PA), RS 172.021.

Un lungo cammino verso la meta

Nella sessione autunnale 2020 il Parlamento ha licenziato la legge federale sulla protezione dei dati sottoposta a revisione totale come pure le modifiche di altri atti normativi sulla protezione dei dati. Il Consiglio federale porrà in vigore la nuova LPD e le relative ordinanze d'esecuzione probabilmente nel secondo semestre del 2022

Genesi

La prima legge federale del 19 giugno 1992 sulla protezione dei dati è entrata in vigore a metà del 1993. Dopo la revisione parziale del 2008, il cui obiettivo era quello di informare meglio la popolazione sul trattamento dei suoi dati, è divenuto ben presto chiaro che il rapido sviluppo tecnologico avrebbe reso necessarie ulteriori modifiche. Per garantire alla popolazione una protezione al passo con i tempi nella vita quotidiana, caratterizzata da cloud computing, big data e reti sociali, era indispensabile procedere a una modifica generale della LPD.

Nell'autunno del 2017 il Consiglio federale ha licenziato il disegno di revisione totale della legge e lo ha trasmesso alle Camere federali.

Obiettivi della revisione

Oltre al rafforzamento dei diritti delle persone interessate, nel suo messaggio il Consiglio federale ha posto l'accento sul cosiddetto approccio basato sui rischi come principio guida della revisione: lo Stato e le imprese devono rilevare tempestivamente i rischi per la sfera privata e l'autodeterminazione informativa e inserire i requisiti della protezione dei dati sin dalla fase pianificatoria dei loro progetti digitali. Occorre documentare i rischi elevati e le misure tecniche e organizzative adottate per eliminarli o mitigarli. La nuova LPD dovrebbe quindi promuovere l'autoregolazione, esentando da alcuni obblighi gli attori dei settori che emanano un codice di condotta vincolante. Non da ultimo mira a rafforzare i poteri di vigilanza dell'IFPDT.

Dibattimento a tappe

A inizio 2018 il Parlamento ha deciso di suddividere la revisione in due tappe: in un primo momento le disposizioni sul trattamento dei dati applicabili agli organi federali come fedpol sono state adeguate per rispettare i termini d'attuazione dei trattati internazionali. Questi lavori sono sfociati nella cosiddetta legge sulla protezione dei dati in ambito Schengen (LPDS), entrata in vigore il 1° marzo 2019 (cfr. 27° rapporto d'attività, n. 1.2).
La revisione totale della LPD è stata fatta soltanto in un secondo momento. Nella sessione autunnale 2019 il Consiglio nazionale, in qualità di prima Camera, ha adottato la revisione totale della legge che le Camere federali hanno in seguito licenziato il 25 settembre 2020, dopo aver appianato di tutte le divergenze. Nel redigere la nuova LPD il Consiglio federale e il Parlamento hanno tenuto conto della Convenzione 108[1] ampliata del Consiglio d'Europa e del Regolamento generale sulla protezione dei dati dell'Unione europea (RGPD)[2]. A causa della sua portata extraterritoriale, dalla sua entrata in vigore nel maggio 2018 il RGPD è già stato applicato da gran parte dell'economia svizzera. Nonostante questo allineamento al diritto europeo, la nuova LPD rispecchia la tradizione giuridica svizzera, in quanto ha un alto grado di astrazione ed è formulata in modo neutrale sotto il profilo tecnologico. Si differenza dal RGPD non soltanto per la sua brevità, ma anche per una terminologia in parte diversa.

In generale si presume che, dopo il rinnovo delle rispettive legislazioni sulla protezione dei dati, la Svizzera e l'UE riconosceranno reciprocamente l'equivalenza dei loro livelli di protezione dei dati, cosicché lo scambio informale di dati personali attraverso le frontiere nazionali continuerà ad essere possibile. Al termine della redazione del presente rapporto d'attività era ancora in sospeso la questione del rinnovo della decisione di riconoscimento dell'UE nei confronti della Svizzera risalente al 2000.

[1] Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale, conclusa a Strasburgo il 28 gennaio 1981, approvata dall'Assemblea federale il 5 giugno 1997. L'ampliamento della Convenzione è stato approvato dalle Camere federale nell'estate del 2020. Il Consiglio federale potrà ratificarla soltanto dopo l'entrata in vigore della nuova LPD.

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

1.2 Giustizia, polizia, sicurezza

Domande di informazioni presso il Servizio delle attività informative della Confederazione (SIC)

Dopo che nel 2019 si è visto confrontato con un numero insolitamente elevato di domande d'accesso che inizialmente è riuscito a trattare con grande ritardo, per evadere le pendenze il SIC ha adottato misure particolari che l'IFPDT ha accompagnato dal profilo del diritto della vigilanza.

A fine 2019 diversi media hanno diffuso la notizia che il SIC riceveva molte più domande del solito concernenti registrazioni nei suoi sistemi d'informazione. Il via l'avevano dato tra l'altro articoli precedenti i cui titoli parlavano di «spionaggio» di diversi politici. La Delegazione delle Commissioni della gestione delle due Camere (DelCG) ha quindi effettuato accertamenti in proposito, mentre l'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn) ha verificato la tenuta dei dossier concernenti i politici nel sistema di gestione degli affari del SIC.

Dopo essere venuto a conoscenza, sulla base di reclami dei cittadini, che i tempi del SIC per trattare le domande d'accesso erano molto lunghi, l'IFPDT ha contattato il Servizio. Il SIC ha sostenuto davanti all'IFPDT di aver ricevuto dal 2019 un numero di domande dieci volte maggiore del solito. Secondo il SIC in poco più di un anno gli sarebbero arrivate oltre mille domande. Il Servizio avrebbe fatto di tutto per evadere le domande pendenti nell'arco di qualche settimana. Nel frattempo aveva istituito un gruppo di lavoro per adeguare le procedure operative in modo che le numerose domande pendenti potessero essere smaltite senza che la qualità ne risentisse.

Nel giugno 2020 il SIC ha comunicato all'IFPDT tra l'altro che, grazie alle risorse supplementari rese disponibili per evadere le pendenze, da maggio 2020 era possibile rispondere puntualmente alle nuove domande d'accesso. Il SIC ha inoltre reso noto che sono ancora pendenti circa 50 domande di vecchia data che vengono evase man mano.

Adottato il messaggio concernente la revisione della legge sui profili del DNA

Con la revisione della legge sui profili del DNA il Consiglio federale intende consentire alle autorità di acquisire maggiori informazioni da una traccia di DNA in caso di indagini penali. La richiesta dell'IFPDT di avere un quadro legislativo più severo è stata soddisfatta.

Il 4 dicembre 2020 il Consiglio federale ha adottato il messaggio concernente la revisione della legge sui profili del DNA. Con la revisione il Consiglio federale vuole consentire alle autorità di desumere più informazioni da una traccia di DNA nel caso di inchieste penali. Dopo estese audizioni, il 26 gennaio 2021 la Commissione della politica di sicurezza del Consiglio nazionale (CPS-N) ha deciso senza voti contrari di entrare in materia sul progetto. Ritiene che le autorità inquirenti disporranno così di metodi efficaci per svolgere in modo più rapido e più mirato le indagini. La Commissione sottolinea la proporzionalità del progetto dato che i risultati dell'analisi del fenotipo si applicheranno soltanto per chiarire fattispecie penali che prevedono una pena detentiva massima superiore a tre anni. Nella prassi attuale, in alcuni casi da una traccia di DNA è possibile desumere soltanto il sesso. D'ora in poi potranno essere dedotte anche le probabilità del colore degli occhi, dei capelli e della pelle, la possibile discendenza biogeografica e

l'età. Come richiesto dall'IFPDT, sarà sancito nella legge quali caratteristiche è consentito esaminare.

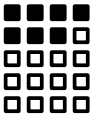
L'IFPDT aveva espresso il proprio parere sul progetto di modifica del Dipartimento federale di giustizia e polizia (DFGP) e richiesto un quadro legislativo più severo (circa la prima consultazione degli uffici, cfr. 27° rapporto d'attività, n. 1.2). Nella procedura di consultazione – come aveva già fatto in relazione all'avamprogetto – l'Incaricato aveva sostenuto che a ordinare la fenotipizzazione e la ricerca di legami di parentela doveva essere il giudice dei provvedimenti coercitivi. Si tratta di strumenti che implicano notevoli ingerenze nei diritti fondamentali e che possono essere impiegati soltanto per accertare gravi crimini contro l'incolumità fisica, la libertà o l'integrità sessuale. Accoglie quindi con favore il fatto che tale richiesta sia stata presa in considerazione nonostante il DFGP l'avesse in origine respinta.

Progetto di legislazione concernente il controllo dei telefoni cellulari nella procedura d'asilo

Il progetto di legislazione avviato con l'iniziativa parlamentare 17.423 intende conferire alla Segreteria di Stato della migrazione (SEM) competenze più ampie che le consentano di controllare supporti mobili di dati per accertare l'identità dei richiedenti nelle procedure d'asilo e di allontanamento. A tal proposito l'Incaricato ha sin dall'inizio espresso preoccupazioni di natura generale. Pur accogliendo con favore i miglioramenti apportati nel frattempo, continua a respingere per principio il progetto.

L'iniziativa parlamentare 17.423 presentata il 17 marzo 2017 dal consigliere nazionale Rutz chiede di modificare le basi legali in modo da consentire alla SEM di analizzare supporti mobili di dati di richiedenti l'asilo. Le Commissioni delle istituzioni politiche delle due Camere hanno dato seguito all'iniziativa. Su questa base è stata elaborata la modifica della legge sull'asilo e della legge sugli stranieri che conferirà alla SEM competenze più ampie che le consentano di controllare supporti mobili di dati per accertare l'identità dei richiedenti nelle procedure d'asilo e di allontanamento.

Nella procedura di consultazione l'IFPDT ha espresso il proprio parere sul progetto manifestando preoccupazioni di natura generale (v. rapporto del 4 giugno 2020, solo in tedesco). Ha fatto presente che, nel caso della valutazione dei supporti elettronici di dati, si tratta di una grave ingerenza nella sfera privata di molte persone, la quale deve fondarsi su sufficienti basi legali formali. L'IFPDT ha inoltre espresso dubbi sul fatto che le misure siano in grado di sortire l'effetto auspicato e che il disciplinamento proposto possa essere attuato conformemente ai diritti fondamentali alla luce dei principi costituzionali di eguaglianza e proporzionalità, tanto più che, a differenza del diritto processuale penale, la procedura amministrativa d'asilo e di allontanamento non contempla garanzie procedurali vere e proprie per il sequestro e la valutazione di supporti elettronici di dati. La misura non dovrebbe nemmeno obbligare indirettamente a portare su di sé e mettere a disposizione in qualsiasi momento dispositivi intelligenti.



Le autorità interessate, tra cui in particolare la SEM, hanno accolto la critica in modo costruttivo aderendo ampiamente alle richieste dell'IFPDT. Si è così rinunciato al ritiro obbligatorio di supporti elettronici di dati e si è creata una base legale formale per la misura. Come richiesto dall'Incaricato, ora si disciplina espressamente che la valutazione di dispositivi mobili di dati finalizzata ad accertare l'identità è una misura sussidiaria che deve essere presa in ogni caso nel rispetto della proporzionalità e che il rifiuto di un richiedente l'asilo di concedervi l'accesso può essere preso in considerazione soltanto nella verifica della credibilità. Alle persone interessate spettano diritti di presenza e di informazione. È stato possibile rafforzare

anche la posizione di terzi, i cui dati personali sono coinvolti nella valutazione. L'Incaricato si rallegra infine che le sue preoccupazioni di natura generale concernenti l'adeguatezza e l'efficacia della misura prevista vengano prese in considerazione grazie a un obbligo di valutazione.

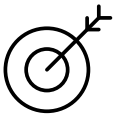
Per l'Incaricato non è tuttavia ancora chiaro come il principio di sussidiarietà e di proporzionalità possa essere attuato nella pratica. Secondo il rapporto esplicativo sulla modifica delle basi legali saranno altre le misure intese ad accertare l'identità ad essere adottate qualora si rivelassero meno onerose rispetto alla valutazione elettronica di dati. Per giudicare la proporzionalità di una misura dovrebbe infine essere determinante quale procedura di valutazione risulta essere la meno gravosa. Qui occorre rilevare che, secondo il progetto di legge, la valutazione di dati personali può essere automatizzata utilizzando un software specifico. La valutazione di supporti elettronici di dati potrebbe dunque avvenire regolarmente, se non addirittura come procedura standard. Non bisogna tuttavia anteporre l'efficienza alla tutela delle libertà fondamentali. L'Incaricato si attiene perciò al suo rifiuto di principio del progetto. Fa inoltre notare, al di là del contesto del diritto d'asilo, che spesso le misure limitative delle libertà vengono introdotte dapprima nei confronti delle minoranze, per poi essere estese progressivamente in altri contesti ad ampie cerchie della popolazione.

Intervento dell'IFPDT presso l'Amministrazione federale delle dogane: regolamentazione insufficiente del trattamento dei dati nella nuova legge sulla polizia doganale

L'Amministrazione federale delle dogane elabora una revisione di legge con cui intende istituire il quadro giuridico per l'impiego di tecnologie digitali d'avanguardia e nel contempo creare la necessaria flessibilità organizzativa per riuscire in futuro a reagire più rapidamente ed efficacemente alle mutate situazioni. L'IFPDT accoglie favorevolmente questi sforzi, lamenta tuttavia una predisposizione insufficiente di regole per il trattamento dei dati in questo progetto di ampio portata.

L'11 settembre 2020 il Consiglio federale ha posto in consultazione la «legge sui compiti d'esecuzione dell'UDSC» (LE-UDSC), facente parte di un pacchetto legislativo con cui intende istituire la base giuridica per il programma di digitalizzazione e trasformazione (DaziT) dell'Amministrazione federale delle dogane. Si tratta di un progetto di ampia portata rilevante sotto il profilo finanziario e sensibile nell'ottica della protezione dei dati. Nel nuovo Ufficio federale delle dogane e della sicurezza dei confini (UDSC) confluiranno l'Amministrazione delle dogane e il Corpo delle guardie di confine ad essa integrato. Tutto il personale avrà attribuzioni di polizia e quindi competenze coercitive in materia di raccolta dei dati.

Durante la seconda consultazione degli uffici che si è svolta dal 5 al 25 marzo 2020 (per quanto riguarda la prima consultazione degli uffici si veda il 27° rapporto d'attività, n. 2.4), l'IFPDT ha invano segnalato all'Amministrazione federale delle dogane che dal suo punto di vista le disposizioni previste in materia di trattamento dei dati personali contenevano gravi lacune. Tali disposizioni trascuravano in particolare la facoltà assicurata ai cittadini, secondo la legislazione in materia di protezione dei dati, di valutare sia i trattamenti di dati da parte dello Stato suscettibili di ingerire nella loro sfera privata e limitarne l'autodeterminazione, sia i diritti di protezione di cui dispongono per opporvisi.



L'Incaricato ha quindi consigliato al Consiglio federale di fare in modo che il Governo e il Parlamento, in quanto organi politici della Confederazione, si riservassero il diritto di disciplinare sia gli aspetti essenziali dei trattamenti di dati, che saranno ora gestiti in un unico sistema della polizia doganale, sia le interfacce verso tale sistema.

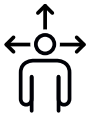
Tenendo conto di queste osservazioni, il Consiglio federale ha incaricato l'Amministrazione di rielaborare le disposizioni sul trattamento dei dati, come indicato nella documentazione per la consultazione. L'Incaricato approva tale passo e intrattiene contatti intensi con l'Amministrazione federale delle dogane e l'Ufficio federale di giustizia al fine di contribuire a colmare le lacune constatate mediante suggerimenti concreti.

1.3 Fiscalità e finanza

L'IFPDT s'impegna dinanzi al Tribunale federale per il diritto all'informazione nell'ambito dell'assistenza amministrativa internazionale in materia fiscale

Nel 2019 il Tribunale amministrativo federale ha accolto un ricorso dell'IFPDT concernente il diritto all'informazione nell'ambito dell'assistenza amministrativa internazionale in materia fiscale. Nella successiva procedura di ricorso dinanzi al Tribunale federale l'Incaricato ha nuovamente perorato la causa a favore del diritto all'informazione. La decisione del Tribunale federale è attesa.

Nell'ambito dell'assistenza amministrativa internazionale in materia fiscale il diritto di essere informati in merito a un procedimento di assistenza amministrativa in corso è collegato alla legittimazione a ricorrere di una persona (cfr. art. 14 Legge sull'assistenza amministrativa fiscale). A fine dicembre 2017 l'IFPDT aveva emanato una raccomandazione formale secondo cui, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, l'Amministrazione federale delle contribuzioni (AFC) deve informare preventivamente anche le persone non formalmente interessate dalla richiesta di assistenza amministrativa (ossia persone terze), i cui nomi non anneriti vanno resi noti all'autorità estera richiedente (cfr. 25° rapporto d'attività, n. 1.9.2). L'IFPDT l'aveva motivata ritenendo che i terzi sono legittimati a difendersi da una trasmissione illegittima dei loro dati mediante ricorso. L'AFC ha respinto la raccomandazione e l'IFPDT ha dapprima sottoposto la questione al Dipartimento federale delle finanze (DFF) per poi presentare ricorso al Tribunale amministrativo federale contro la decisione negativa del DFF (cfr. 26° rapporto d'attività, n. 1.3).



Nella sua sentenza del 3 settembre 2019 il Tribunale amministrativo federale è giunto alla conclusione che, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, in linea di principio devono essere informate preventivamente le persone non interessate dalla domanda di assistenza amministrativa (persone terze), i cui dati non anneriti devono essere resi noti. Disposizioni derogatorie sono da prevedere, secondo il Tribunale amministrativo federale, nei casi in cui l'informazione richiesta può essere comunicata soltanto con un onere eccessivo e tale da non rendere possibile l'assistenza amministrativa o da ritardarne gravemente l'attuazione. L'IFPDT ha accolto con favore la sentenza in quanto essa tutela i diritti fondamentali dei dipendenti delle banche e di altre persone terze.

L'AFC ha interposto ricorso dinanzi al Tribunale federale. Quest'ultimo ha annullato la sospensione della procedura richiesta dall'AFC dopo che il 13 luglio 2020 aveva emesso una decisione di principio (DTF 146 I 172) in un'altra vertenza su una questione analoga. In quella decisione il Tribunale federale aveva fortemente limitato il diritto all'informazione: riteneva che terze persone, i cui dati non anneriti devono essere trasmessi dall'AFC all'autorità estera richiedente, sono legittimate soltanto in via eccezionale, segnatamente in base a circostanze particolari, a difendersi mediante un ricorso. L'AFC non deve perciò informare preventivamente d'ufficio in merito alla trasmissione dei dati tutte le persone terze legittimate a ricorrere, bensì soltanto quelle la cui legittimazione a ricorrere è evidente in base agli atti.

Tenuto conto della più recente giurisprudenza, l'IFPDT ha riconosciuto dinanzi al Tribunale federale che, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, terze persone non sono legittimate a ricorrere in modo generale, ma soltanto eccezionale. È rimasto tuttavia dell'opinione, confermata dal Tribunale amministrativo federale, che in linea di principio debbano essere informate preventivamente d'ufficio in merito alla trasmissione dei loro dati tutte le persone terze. Soltanto così tutte le persone terze, legittimate a ricorrere ai sensi della giurisprudenza del Tribunale federale, possono effettivamente fare uso del loro diritto di ricorso e difendersi contro un'imminente trasmissione di dati. L'IFPDT ha quindi prospettato nuovamente dinanzi al Tribunale federale come attuare l'obbligo di massima in materia d'informazione cui soggiace l'AFC, senza che ne insorga un onere sproporzionato tale da non rendere possibile l'assistenza amministrativa o da ritardarne gravemente l'attuazione. La decisione in merito è attesa.


Restaurants

1.4 Commercio ed economia

Accertamenti sulle implementazioni 5G di Sunrise e Swisscom

L'IFPDT ha potuto concludere due accertamenti dei fatti, condotti indipendentemente l'uno dall'altro, presso le imprese Sunrise e Swisscom circa l'implementazione della nuova tecnologia di telefonia mobile di quinta generazione (5G). Entrambi gli operatori hanno mostrato che la protezione dei dati e la sicurezza tecnica godono della massima attenzione.

Secondo le specifiche tecniche, oltre a una maggiore velocità di trasmissione dei dati la nuova tecnologia di telefonia mobile 5G dovrebbe offrire anche una maggiore sicurezza. Vista l'attualità e la portata di questo cambiamento, nel 2019 l'IFPDT ha avviato due accertamenti formali dei fatti presso gli operatori Swisscom e Sunrise, quando questi hanno pianificato l'introduzione del 5G. Entrambi gli operatori hanno permesso all'IFPDT di farsi un quadro della progettazione e dello stato dell'implementazione e gli hanno trasmesso documentazioni voluminose. Oltre a numerose questioni tecniche, per l'IFPDT erano di particolare importanza i seguenti aspetti: da un lato, già nel 2018 diversi media avevano riferito che nell'ambito dell'implementazione della tecnologia 5G potevano manifestarsi sensibili vulnerabilità e che erano note lacune di sicurezza. Dall'altro vi erano preoccupazioni circa la sicurezza in relazione ai fornitori impiegati, in particolare Huawei. L'IFPDT ha pertanto chiesto alle due imprese controllate di spiegare come affrontano le vulnerabilità conosciute e se vi sono dipendenze rispetto a singoli fornitori – segnatamente Huawei – che pregiudicano la disponibilità (p. es. in seguito a sanzioni commerciali statunitensi), la confidenzialità o la sicurezza dei dati.

Sunrise ha indicato di intrattenere uno scambio permanente con organi e gruppi di lavoro internazionali del settore delle telecomunicazioni e di aver inoltre fatto analizzare la propria implementazione da parte di un'impresa esterna indipendente. Dal punto di vista dell'IFPDT, le misure di miglioramento identificate rivestono grande valore in particolare per conseguire una sicurezza sufficiente e un livello adeguato della protezione dei dati. Ha pertanto raccomandato a Sunrise di concludere l'attuazione di tali misure. Quanto a Huawei, suo partner e fornitore 5G, Sunrise ha eseguito alcune analisi di sicurezza che hanno evidenziato rischi nei settori della disponibilità, della collaborazione e dello spionaggio. Per questi rischi specifici, Sunrise ha definito e attuato diverse misure.

Come per Sunrise, anche per Swisscom l'IFPDT non ha trovato indizi di un'inadeguatezza dell'implementazione dal punto di vista della sicurezza dei dati e della protezione dei dati. Per quanto riguarda la sicurezza dei dati del 5G Swisscom ha eseguito valutazioni di sicurezza interne. Al pari di Sunrise, anche Swisscom intrattiene uno scambio con diversi organi e gruppi di lavoro internazionali e si affida ai loro approcci collaudati che garantiscono un funzionamento sicuro. Swisscom indica Ericsson, suo partner da molti anni, come fornitore principale per la tecnologia 5G e dichiara che i componenti forniti da Huawei e impiegati nella costruzione di antenne sono unicamente elementi passivi privi di elettronica che vengono utilizzati soltanto per la ricezione e la trasmissione dei segnali d'onda.

L'IFPDT giunge alla conclusione che la sicurezza dei dati è stata rispettata adeguatamente dalle imprese controllate e che le considerazioni sulla protezione dei dati rivestono grande importanza nel contesto dell'introduzione della nuova tecnologia. Con l'adattamento completo della tecnologia 5G, i vantaggi rispetto al 4G sono evidenti per quanto riguarda la sicurezza delle informazioni.

Registrazioni errate nella banca dati di una società di riscossione

L'IFPDT ha continuato la procedura di accertamento dei fatti nei confronti di un'importante società di riscossione a causa di probabili errori di registrazione nella banca dati e ha ampliato l'oggetto dell'indagine.

Nel febbraio 2020 l'Incaricato aveva avviato una procedura di accertamento dei fatti nei confronti di una società a causa di probabili errori di registrazione nella banca dati che hanno portato a confondere persone con nome o indirizzo identico o analogo e a causa delle difficoltà che sarebbero insorte nella correzione di tali registrazioni errate (cfr. 27° rapporto d'attività, n. 1.4). Nell'anno in rassegna dalle richieste dei cittadini e dei media è emerso che anche la pratica di considerare in determinati casi la solvibilità di una famiglia nel suo insieme (famiglia di cattivi pagatori) solleva interrogativi in materia di protezione dei dati. L'IFPDT ha quindi deciso di includere questo aspetto nell'accertamento dei fatti in corso. Si ha una famiglia di cattivi pagatori quando, nell'ambito di una verifica di solvibilità, vengono divulgate informazioni negative sulla solvibilità di altre persone che vivono nella stessa economia domestica. Può accadere che, nonostante una solvibilità impeccabile, alcuni clienti di negozi online non possano acquistare merce tramite fattura se nella loro economia domestica vive una persona con una cattiva solvibilità. Questi accertamenti giuridici erano ancora in corso alla fine dell'anno in rassegna.

Esame della capacità creditizia nell'ambito del leasing auto

Per poter concludere un contratto di leasing i clienti devono acconsentire che il fornitore del leasing verifichi la loro capacità creditizia. A questo scopo il fornitore può informarsi anche presso terzi. L'IFPDT avvia i primi accertamenti su questo tipo di trattamento dei dati.

Prima che i clienti possano concludere un contratto di leasing per un'automobile, il fornitore del leasing deve verificare la loro capacità creditizia. A questo scopo deve chiedere determinate informazioni sulla situazione economica dei potenziali clienti. Se l'esito dell'esame della capacità creditizia è negativo, non è possibile concludere il contratto di leasing: lo prescrive la legge sul credito al consumo. L'obiettivo consiste nell'impedire un eccessivo indebitamento dei consumatori. Questo trattamento dei dati soggiace alle disposizioni della LPD e non deve ledere illegittimamente la personalità del cliente e di eventuali terzi. Possono essere trattate in particolare soltanto le informazioni necessarie per poter constatare la capacità creditizia.

Dalle domande dei cittadini l'IFPDT ha appreso che un fornitore di leasing si fa dare il consenso dai clienti al fine di esaminarne la capacità creditizia per poter chiedere a terzi numerose informazioni. È necessario ottenere il consenso per chiedere informazioni anche su terze persone come coniugi o membri della famiglia. L'IFPDT si è chiesto se questo trattamento dei dati si limita a una misura permessa dal punto di vista del diritto sulla protezione dei dati e se la riconoscibilità del trattamento dei dati da parte degli interessati è garantita. L'Incaricato ha perciò chiesto al fornitore di leasing di esprimere il suo parere su diverse questioni. In base alle risposte che otterrà, verificherà se effettuare un accertamento o raccomandare eventuali misure.

Accertamento dei fatti riguardo alla nuova videosorveglianza della Migros

Nell'anno in rassegna l'IFPDT ha analizzato il nuovo sistema di videosorveglianza della Migros nel quadro di un accertamento dei fatti. L'azienda ha dichiarato che non saranno effettuati né riconoscimenti facciali né valutazioni automatizzate di modelli comportamentali o analisi simili. L'IFPDT non ha emanato raccomandazioni, ma ha preteso miglioramenti per quanto riguarda l'informazione dei clienti sul sistema.

Per le aziende i sistemi di videosorveglianza possono rappresentare uno strumento atto a salvaguardare i loro legittimi interessi, come ad esempio la protezione della proprietà. Dall'altro lato nell'opinione pubblica aumenta un certo disagio nei confronti di simili iniziative, non da ultimo a causa delle nuove possibilità di identificazione e analisi offerte dalla tecnica.

Anche il nuovo sistema della Migros è stato criticato nei media ed è stato fonte di insicurezza. Per chiarire le funzioni della nuova videosorveglianza adottata dalla Migros, nell'ambito della sua attività di vigilanza l'IFPDT si è fatto descrivere il sistema e le misure prese dall'azienda per tutelare i diritti della personalità.

Dopo aver valutato il parere della Migros e la documentazione presentata, l'IFPDT ha potuto constatare che il nuovo sistema di videosorveglianza si limita alle funzioni reattive: in un caso sospetto concreto il responsabile della sicurezza di una filiale Migros può rilevare, scegliendo manualmente un'immagine fissa, determinati parametri di una persona sospettata (colore dei capelli, sesso e altezza). Il sistema cerca la stessa combinazione di parametri nelle videoriprese registrate ed entro un lasso di tempo definito. Il materiale fotografico è messo quindi a diposizione del personale addetto alla sicurezza della filiale Migros interessata e può così essere d'ausilio per individuare comportamenti illeciti.

La Migros ha ribattuto che non sono effettuati né riconoscimenti facciali né valutazioni automatizzate di modelli comportamentali o analisi simili. L'identificazione di persone che sono state riprese mediante il sistema di videosorveglianza è possibile soltanto in singoli casi motivati al di fuori del sistema e segue una procedura stabilita dall'azienda.

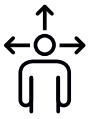
Dato che, considerate le sue funzioni limitate, il nuovo sistema di videosorveglianza non si differenzia sostanzialmente dai sistemi in uso finora, l'IFPDT può prescindere dal formulare raccomandazioni giuridiche in materia di protezione dei dati. Inoltre, le misure e i processi tecnici e organizzativi illustrati dalla Migros sembrano adatti a garantire la sicurezza dei dati personali trattati in relazione al sistema di videosorveglianza.

L'IFPDT ha tuttavia richiesto miglioramenti per quanto riguarda le informazioni sul nuovo sistema che appaiono nelle disposizioni sulla protezione dei dati sulla pagina web della Migros, poiché sono formulate in maniera troppo generica e non ne spiegano le funzioni. Ha inoltre preteso dalla Migros di essere informato anticipatamente e per tempo sui progetti futuri o su eventuali ampliamenti delle funzioni nel settore della videosorveglianza. Al momento in cui è stato redatto questo documento la risposta della Migros non era ancora pervenuta.

Trattamento di dati dei clienti da parte dei negozi online

Abbiamo avviato una procedura nei confronti di un negozio online per controllare se il trattamento di dati dei suoi clienti è conforme alla protezione dei dati. Ci chiediamo inoltre se il trattamento dei dati possa avvenire contro l'espressa volontà degli utenti.

Che la causa sia la chiusura dei negozi durante i lockdown o i rischi legati a un'entrata nei negozi, la pandemia di Coronavirus ha indotto molte persone a effettuare gli acquisti online. Per alcuni i negozi online sono diventati persino l'unica possibilità di comperare determinate merci. Le domande dei cittadini hanno attirato la nostra attenzione sul fatto che presso uno dei maggiori commercianti online svizzeri occorreva allestire un conto clienti accettando tutti i trattamenti dei dati descritti nella dichiarazione di protezione dei dati per poter effettuare un ordine.



Questo significava tra l'altro che i clienti dovevano accettare la registrazione e la valutazione del proprio comportamento d'acquisto in forma individualizzata e personale, il collegamento con altri dati personali (p. es. con dati personali già raccolti nel passato da questa o da altre aziende del gruppo oppure da terzi oppure con dati personali di dominio pubblico) nonché la comunicazione di dati personali ad altre aziende del gruppo. Richieste di opposizione presentate successivamente al servizio clienti non potevano impedire questi trattamenti dei dati. Il gerente del negozio online le respingeva con la motivazione che la dichiarazione di protezione dei dati valeva per tutta la clientela ugualmente e senza eccezioni e che per i clienti i trattamenti non erano opzionali.

Nella primavera del 2020 abbiamo scritto al gerente del negozio online nel quadro di un accertamento preliminare per avere, da un lato, una panoramica sui suoi metodi di trattamento dei dati e, dall'altro, per chiarire le possibilità dei clienti di presentare opposizione. Dopo aver valutato la risposta del gerente abbiamo avviato un accertamento dei fatti. Oltre ad analizzare se il trattamento dei dati da parte del gerente del negozio online e di altre aziende del gruppo è conforme alla protezione dei dati, ci concentriamo sulla questione se simili trattamenti dei dati possano avvenire contro l'espressa volontà degli utenti.

Valutazione giuridica sull'utilizzo dei dati di Ricardo all'interno del TX Group

Nell'ambito di una procedura ancora in corso, l'IFPDT ha valutato dal punto di vista giuridico l'utilizzo che il TX Group fa dei dati raccolti sulla piattaforma d'aste online ricardo.ch. Abbiamo concluso che gli utenti devono dare il proprio consenso ai trattamenti dei propri dati effettuati ai fini di una pubblicità mirata del gruppo. Riteniamo inoltre che attualmente l'informazione trasmessa agli utenti sia insufficiente e che la dichiarazione di protezione dei dati debba essere migliorata.

Nell'ambito della procedura di accertamento dei fatti, avviata nei confronti di Ricardo ed estesa a Tamedia/TX Group, concernente l'utilizzo da parte del TX Group dei dati raccolti sulla piattaforma di aste online ricardo.ch, nel marzo 2020 abbiamo potuto concludere il nostro accertamento dei fatti (cfr. i nostri precedenti rapporti d'attività). Quest'ultimo si basa in particolare sulla nuova dichiarazione di protezione dei dati di ricardo.ch – utilizzata in modo standardizzato dalle società del TX Group – nonché sulle risposte fornite da Ricardo e dal TX Group concernenti i trattamenti dei dati effettuati al loro interno. I risultati della nostra valutazione giuridica dal profilo della legge sulla protezione dei dati (LPD) saranno confluiti in un rapporto finale.

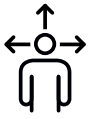
La dichiarazione di protezione dei dati di Tamedia/TX Group, introdotta nel luglio 2017 per ricardo.ch e da allora più volte aggiornata, prevede in particolare che i dati personali raccolti sulla piattaforma ricardo.ch possano essere comunicati alle società del TX

Group o ai loro partner e trattati «per la personalizzazione e per scopi di marketing». Il comportamento online degli utenti può in particolare essere seguito e valutato tramite strumenti d'analisi. Tale trattamento dei dati avverrebbe «principalmente con dati pseudonimizzati o resi anonimi». Il trattamento è finalizzato all'invio o alla visualizzazione sui portali di TX Group di «pubblicità anonima» e al miglioramento della sicurezza dei portali.

Il nostro accertamento dei fatti ha permesso di stabilire che il TX Group (ex Tamedia AG), tratta e analizza alcuni dati degli utenti della piattaforma ricardo.ch per scopi di marketing. I dati raccolti sui vari portali di TX Group consentono di arricchire, in forma aggregata, la banca dati del gruppo. Lo scopo dell'analisi e la combinazione di questi dati in provenienza da fonti diverse è d'inviare agli utenti dei servizi del TX Group o ai loro partner pubblicità mirata, sulla base di una segmentazione effettuata in funzione di attributi socio-demografici (in base ai dati forniti dall'utente al momento della sua registrazione) e dei presunti ambiti d'interesse degli utenti (dedotti dal loro comportamento online sui portali del TX Group e di altri siti partner). La combinazione dei dati all'interno del TX Group è resa possibile attraverso identificatori pseudonimi creati in particolare partendo dagli indirizzi di posta elettronica.

Abbiamo proceduto alla valutazione giuridica dei fatti e siamo giunti, tra l'altro, alle seguenti conclusioni:

- il trattamento dei dati, in particolare la combinazione dei dati effettuata dal TX Group e l'attribuzione dei segmenti agli utenti, è a tutti gli effetti un trattamento di dati personali che soggiace alla legge federale sulla protezione dei dati (LPD). Inoltre, l'insieme dei dati risultanti dalla profilazione può in questo caso costituire un profilo della personalità ai sensi della LPD e sono quindi applicabili le esigenze di protezione più severe previste dalla legge;
- riteniamo che tale profilazione ai fini di una pubblicità mirata richieda il consenso delle persone interessate, che per di più deve essere esplicito. Infatti, anche se il TX Group può far valere degli interessi legittimi, questi non prevalgono in questo caso sul diritto all'autodeterminazione informativa degli utenti della piattaforma ricardo.ch;
- la dichiarazione di protezione dei dati di Ricardo/TX Group e la relativa comunicazione devono essere migliorate, conformemente al principio di trasparenza. In particolare, gli utenti devono capire in modo inequivocabile i trattamenti dei dati effettuati da Ricardo da un lato, e da TX Group dall'altro, quali sono i loro scopi, se esistono o meno mezzi per opporvisi e, in caso affermativo, le possibilità di opposizione devono essere effettivamente applicate.



Stiamo attualmente esaminando le prossime tappe.

Revisione dell'ordinanza sull'energia

Nell'ambito della revisione dell'ordinanza sull'approvvigionamento elettrico (OAEl) l'IFPDT chiede, nell'interesse delle persone coinvolte, un termine massimo di due anni per la conservazione dei dati di misurazione da parte dei gestori di rete. Il DATEC respinge la richiesta, rimandando tra l'altro ai termini quinquennali già esistenti nell'OAEl. È stata registrata una differenza.

Nell'ambito di una consultazione degli uffici riguardante le revisioni dell'ordinanza sull'energia, l'IFPDT riteneva il termine quinquennale di conservazione dei dati dei profili di carico ivi contenuto non proporzionale dal profilo temporale. L'IFPDT è del parere che si tratti di una conservazione di dati a titolo preventivo che riguarda tutti i consumatori di elettricità in Svizzera. Per ottimizzare i consumi di energia elettrica i profili di carico devono essere conservati per cinque anni, anche se si deve partire dal presupposto che la maggioranza degli interessati non li analizzerà mai.

Anche per la gestione della rete e del bilancio nonché per la fatturazione è possibile utilizzare strumenti meno incisivi per raggiungere gli scopi prefissati, come ad esempio un'aggregazione in base alle posizioni tariffali (p. es. tariffa alta/bassa) per le fatture: in questo modo il profilo di carico non sarebbe più rilevante ai fini della fatturazione. Secondo l'OAEl i dati personali e i profili della personalità vengono distrutti dopo 12 mesi sempre che non siano rilevanti ai fini della fatturazione o anonimizzati.

La lunga conservazione quinquennale risulta problematica soprattutto perché nel caso dei profili di carico si tratta di profili della personalità o, secondo la LPD riveduta, di una profilazione, a cui si applicano requisiti maggiori in materia di sicurezza dei dati.

L'IFPDT è perciò del parere che occorra cancellare i dati personali dopo dodici mesi oppure, per motivi di attuabilità, al più tardi dopo due anni, a meno che gli interessati non acconsentano esplicitamente a una durata di conservazione più lunga, ad esempio a scopo di informazione sui dati del profilo di carico per soluzioni di efficienza. Occorrerebbe dunque modificare la disposizione pertinente in modo che la durata di conservazione dei profili di carico continui a essere di dodici mesi e i clienti possano chiedere, mediante un consenso esplicito, una durata più lunga fino a un massimo di cinque anni.

1.5 Salute

Soluzioni cloud per il trattamento di dati dei pazienti: requisiti

Nel settore della sanità è in costante aumento l'impiego di soluzioni cloud per il trattamento di dati dei pazienti. Nell'ambito della sua attività di consulenza l'IFPDT ha evidenziato i punti che i professionisti della salute sono tenuti a osservare quando scelgono una soluzione cloud.

Nell'anno in rassegna l'IFPDT è stato interpellato ripetutamente da medici, psicologi e altre persone che operano nel settore sanitario in relazione all'impiego di soluzioni cloud per il trattamento di dati dei pazienti. Si trattava del trattamento e del salvataggio di dati relativi alla salute in un centro di calcolo gestito da un fornitore esterno (il cosiddetto provider di servizi cloud). Le domande riguardavano soprattutto la conservazione e la trasmissione o la cancellazione di dati dei pazienti (p. es. dopo il decesso di un paziente o la chiusura di uno studio medico).

Nell'ambito della sua attività di consulenza, l'IFPDT fa notare innanzitutto che il medico, anche quando impiega una soluzione cloud, rimane responsabile della sicurezza dei dati anche se da quel momento in poi ha soltanto un controllo limitato sui medesimi. Deve perciò scegliere con cura il provider di servizi cloud e prestare attenzione ai punti seguenti:

- i dati devono rimanere in Svizzera;
- il contratto con il provider di servizi cloud dovrebbe soddisfare i requisiti propri del segreto medico;
- tutte le persone che hanno accesso ai dati dei pazienti devono essere soggette all'obbligo del segreto medico;
- dovrebbe essere possibile in ogni momento cancellare i dati dei pazienti;
- un elenco di tutte le persone che hanno accesso ai dati dovrebbe poter essere richiesto in ogni momento;
- la sicurezza dei dati dovrebbe essere controllata a intervalli regolari e i relativi audit dovrebbero essere disponibili;
- il medico dovrebbe sapere chi è l'interlocutore in materia di protezione dei dati;
- il backup dovrebbe essere effettuato giornalmente;
- tutti i collegamenti devono essere crittati e un'autenticazione a due fattori dovrebbe limitare gli accessi ai dati soltanto alle persone autorizzate.

Infine si può affermare che l'IFPDT dissuade dall'impiego di soluzioni cloud gratuite di uso corrente per scambiare o conservare i dati dei pazienti poiché non soddisfano di norma le condizioni sopra elencate.

CORONA

Accertamento dei fatti a proposito di lemievaccinazioni.ch

Già diversi anni prima della pandemia era stata attivata la piattaforma elettronica lemievaccinazioni.ch gestita da una Fondazione e sostenuta finanziariamente anche dall'Ufficio federale della sanità pubblica (UFSP). La piattaforma era stata pensata come alternativa elettronica al comune libretto di vaccinazione.

Nel contesto della pandemia di COVID-19 la piattaforma ha visto aumentare sensibilmente il numero degli utenti, anche a causa di interfacce messe a disposizione dell'applicazione promossa dall'UFSP fra coloro che desiderano annunciarsi per la vaccinazione. Su incarico dell'UFSP la Fondazione ha inoltre sviluppato e gestito un modulo specifico per la documentazione della vaccinazione contro la COVID-19 (myCOVIDvac).

A fine marzo 2021 l'Incaricato ha preso atto dei risultati di un'inchiesta giornalistica, che ha rilevato possibili gravi lacune nella protezione dei dati e nella sicurezza sulla piattaforma lemievaccinazioni.ch. Dopo aver consultato il Centro nazionale per la cibersicurezza (NCSC), l'Incaricato ha avviato il giorno stesso un accertamento formale dei fatti e raccomandato alla Fondazione di sospendere immediatamente la gestione della piattaforma. Alla fine dell'anno in rassegna il procedimento era ancora pendente e una ripresa dell'esercizio della piattaforma non era ancora in vista.

D'intesa con le autorità cantonali per la protezione dei dati l'Incaricato si è inoltre adoperato affinché altre piattaforme, gestite da privati su mandato o su raccomandazione delle autorità sanitarie federali e cantonali, vengano controllate più da vicino.

CORONA

Sfide in materia di protezione dei dati con un'attenzione particolare a eventuali agevolazioni per persone vaccinate

La disponibilità di vaccini contro la COVID-19 ha suscitato un dibattito pubblico sull'abolizione, per le persone vaccinate, di divieti e di provvedimenti che limitano la libertà. Dal dicembre 2020 l'IFPDT ha sostenuto pubblicamente che l'elaborazione di dati sanitari da parte dello Stato e dell'economia in relazione a eventuali agevolazioni per persone vaccinate debba avvenire sulla base di chiare disposizioni di diritto pubblico e non possa implicare in pratica l'obbligo di avere con sé un telefonino.

In vista di una vaccinazione contro la COVID-19 durante la seconda ondata della pandemia è sorto un dibattito pubblico sull'abolizione, per le persone vaccinate, di divieti e di provvedimenti che limitano la libertà. Dopo aver sentito l'Incaricato le Commissioni delle istituzioni politiche di entrambe le Camere hanno discusso di come applicare queste eventuali agevolazioni sotto il profilo giuridico (cfr. comunicato stampa CIP-S del 23.02.2021).

Lo Stato e i privati con compiti statali possono prevedere differenziazioni a dipendenza dello stato vaccinale soltanto se è disponibile una corrispondente base legale. In virtù della libertà contrattuale, fondamentalmente tali differenziazioni sono per contro possibili fra privati, anche senza una base legale esplicita.

Se fanno dipendere l'accesso a beni o a prestazioni dallo stato vaccinale della loro clientela o dei loro ospiti, i privati elaborano a tal fine costantemente dati sanitari dei loro concittadini con il rischio di ledere, a seconda delle circostanze, la loro personalità. Fin dall'avvio del dibattito pubblico e anche durante le audizioni summenzionate l'Incaricato ha pertanto sostenuto che per questa fattispecie occorra elaborare disposizioni legali. Ha inoltre indicato i requisiti in materia di diritto di protezione dei dati che i privati devono soddisfare se intendono permettere l'accesso a beni o a prestazioni soltanto a chi pubblica il risultato di un test o la prova di essere stato vaccinato (si veda in merito la nostra comunicazione del 22.01.2021).

L'acquisizione e l'ulteriore trattamento dei dati personali devono essere adeguati a soddisfare dal profilo della proporzionalità il conseguimento dello scopo e quindi a proteggere contro la trasmissione e la malattia. Occorre pertanto rinunciare a richiedere dati sanitari per permettere l'accesso a beni o a prestazioni, se non ci si può ragionevolmente aspettare che gli interessati vi rinuncino. Per quanto riguarda il tipo di trattamento l'IFPDT ha infine sottolineato che alle persone che non sono in grado o non vogliono presentare una prova vaccinale sul telefonino occorre offrire, a condizioni paragonabili, alternative ragionevoli al trattamento digitale dei dati personali menzionati.

Quest'ultimo aspetto riveste una certa importanza per l'Incaricato, perché si può supporre che il trattamento sistematico dei dati personali da parte di privati nel contesto della pandemia condizionerà l'autodeterminazione informativa della popolazione ben al di là della situazione attuale.

CORONA

Introduzione di un certificato COVID-19 conforme alla protezione dei dati

Per poter dimostrare l'avvenuta vaccinazione contro la COVID-19, la guarigione da un'infezione da COVID-19 o il risultato del test COVID-19 in vista di viaggi all'estero, il Parlamento federale ha elaborato nel marzo 2021 una disposizione legale per l'introduzione di un certificato COVID-19 armonizzato, non falsificabile e riconosciuto a livello internazionale. Nel quadro del suo obbligo legale di consulenza in materia di vigilanza l'Incaricato segue i lavori dell'Ufficio federale della sanità pubblica (UFSP) per l'implementazione di questo certificato.

Nel corso della seconda ondata della pandemia è emersa l'esigenza di poter certificare preventivamente e in modo affidabile l'avvenuta vaccinazione, la guarigione o il risultato negativo di un test per il coronavirus di persone che intendessero viaggiare al di fuori della Svizzera o che avessero eventuali altre necessità. Fino a quel momento non esistevano in Svizzera disposizioni legislative specifiche che disciplinassero forma e contenuto di un certificato vaccinale. Sono così state offerte anche certificazioni sull'avvenuta vaccinazione contro la COVID-19 o sul risultato di un test in forma cartacea, via SMS, per posta elettronica o mediante registrazione (verificabile) su una pertinente piattaforma. Le varie possibilità non soddisfacevano però tutti i requisiti giuridici in materia di protezione dei dati: l'Incaricato si è così convinto a intervenire nell'ambito del diritto di vigilanza (v. box su «lemievaccinazioni.ch»).

Nel marzo 2021 il legislatore federale ha introdotto un certificato COVID-19 armonizzato e riconosciuto a livello internazionale, approvando il nuovo articolo 6a della legge COVID-19. Questa disposizione stabilisce i requisiti del documento che certifica l'avvenuta vaccinazione contro la COVID-19, la guarigione da un'infezione da COVID-19 o il risultato di un test COVID-19. Secondo il nuovo articolo un certificato di questo tipo dev'essere personale, non falsificabile, verificabile nel rispetto delle norme sulla protezione dei dati e concepito in modo tale da consentire unicamente una verifica decentralizzata o locale della sua autenticità e validità. Tale certificato dovrà quindi poter essere utilizzato per entrare in altri Paesi e uscirne. Nella disposizione del legislatore, secondo cui in futuro il certificato dovrà poter essere utilizzabile non soltanto in forma digitale ma anche in forma cartacea, trova riscontro anche la richiesta dell'Incaricato secondo cui il certificato disponibile in forma elettronica non può implicare in pratica l'obbligo di avere con sé un telefonino.

La disposizione prevede inoltre che la Confederazione possa mettere a disposizione dei Cantoni e di terzi un sistema per il rilascio di certificati. Per sviluppare un sistema di questo genere l'UFSP ha istituito il 29 marzo 2021 un gruppo di progetto, che sarà seguito dall'Incaricato nell'ambito del suo obbligo legale di consulenza in materia di vigilanza. Le sue richieste coincidono ampiamente con la posizione del Comitato europeo per la protezione dei dati (EDPB) e del Garante europeo della protezione dei dati (GEPD) sul «certificato verde digitale», che dovrebbe essere introdotto nell'area dell'UE per i viaggi transfrontalieri. L'IFPDT ha inoltre formulato all'attenzione del gruppo di progetto linee guida sulla protezione dei dati, in modo tale che i certificati vengano concepiti utilizzando il minor numero possibile di dati, così da poterli utilizzare per altri scopi all'interno del Paese. Per altri usi dovrebbero venire elaborate, conformemente all'opinione difesa dall'Incaricato, basi di diritto pubblico che non si rivolgano soltanto alle autorità ma anche ai privati (si veda il testo sopra).

Cartella informatizzata del paziente: certificate le prime comunità di riferimento

In tutte le regioni della Svizzera la cartella informatizzata del paziente (CIP) è ai blocchi di partenza. In questo contesto l'IFPDT ha seguito lo sviluppo delle procedure di certificazione. In seguito ha preso contatto con le nuove comunità di riferimento e ha rafforzato lo scambio con quelle esistenti. Nel frattempo le prime comunità di riferimento sono state certificate.

La CIP è un punto di raccolta virtuale di collegamenti ipertestuali mediante i quali i privati possono disporre in forma digitale dei propri dati sulla salute, quali i rapporti medici e le ricette. I dati sulla salute sono dati personali degni di particolare protezione il cui trattamento presuppone l'esplicito consenso degli interessati.

A sua volta ciò presuppone che i pazienti siano informati in maniera chiara e completa. Per l'IFPDT la corretta attuazione di questo aspetto riveste particolare importanza. Nell'anno in rassegna ha già visionato i relativi documenti delle comunità di riferimento.

La legge federale sulla cartella informatizzata del paziente (LCIP), entrata in vigore il 15 aprile 2017, prevede che i pazienti possano gestire autonomamente tutti i diritti d'accesso a ogni singolo documento. Vanno quindi predisposti correttamente i gradi di riservatezza per ciascun documento, l'attribuzione di ruoli d'utente ai singoli professionisti della salute, le regole inerenti ai rappresentanti e l'impostazione secondo cui nelle situazioni di emergenza l'accesso è possibile soltanto previa autorizzazione del professionista della salute curante. L'IFPDT ha concentrato la sua attenzione anche su questi aspetti e continuerà ad osservare

la regolamentazione dei diritti d'accesso in particolare dopo la conclusione delle procedure di certificazione delle comunità di riferimento, affinché i pazienti mantengano il controllo sui dati anche dopo aver rilasciato il proprio consenso. L'IFPDT rimane comunque in contatto con l'UFSP, gli offerenti dell'infrastruttura tecnica e le autorità cantonali preposte alla protezione dei dati. Questi contatti consentono fra l'altro di chiarire le questioni relative alla competenza derivanti dal fatto che determinati fornitori di prestazioni mediche, quali gli ospedali, sottostanno alla vigilanza cantonale in materia di protezione dei dati, mentre i medici e le comunità di riferimento sono soggetti alla vigilanza dell'IFPDT.

Secondo la pianificazione, le comunità di riferimento avrebbero dovuto essere operative nell'aprile 2020. Tuttavia vi sono stati ritardi dovuti al protrarsi delle procedure di certificazione. A metà novembre 2020 è stata certificata secondo la LCIP la prima comunità di riferimento, la «eHealth Aargau (SteHAG)», seguita a fine dicembre 2020 da un secondo offerente CIP, la comunità di riferimento «Südost» dell'associazione «eSANITA». L'IFPDT ha sollecitato le due comunità di riferimento a illustrare i rischi essenziali finora individuati a proposito della protezione dei dati in relazione alla CIP, le misure attuate per affrontare tali sfide e il modo in cui si assumono la responsabilità per quanto concerne la protezione dei dati in questo campo.

Gli interlocutori principali dell'IFPDT saranno i responsabili della protezione e della sicurezza dei dati, i quali devono istituire le comunità di riferimento sulla base dell'OCIP.

CORONA

App per il tracciamento di prossimità della Confederazione (app SwissCovid)

L'IFPDT era stato interpellato già all'inizio della pandemia di coronavirus dagli ideatori del sistema svizzero di tracciamento di prossimità, da cui è poi scaturita la app SwissCovid, che gli avevano chiesto la sua partecipazione consultativa ai lavori. Il sistema identifica mediante la tecnica di trasmissione bluetooth i contatti rilevanti tra cellulari e li registra localmente. L'IFPDT ha seguito da vicino lo sviluppo della app SwissCovid dai profili prima tecnico dopodiché della legislazione.

Il 21 marzo 2020, pochi giorni dopo che in Svizzera era stata dichiarata la situazione straordinaria ai sensi della legge sulle epidemie (LEp), l'IFPDT era stato contattato dagli ideatori di una app per il tracciamento di prossimità, i quali gli hanno chiesto di valutare il progetto dal punto di vista del diritto in materia di protezione dei dati. I responsabili del progetto, provenienti dal Politecnico federale di Losanna (PFL) e dall'economia privata, volevano in tal modo segnalare alle persone che avevano attivato la app Covid sul loro cellulare di essersi trovate nei paraggi di una persona che aveva parimenti scaricato tale applicazione sul proprio cellulare ed era poi risultata positiva al test del coronavirus. Nel quadro di questa prima valutazione, l'IFPDT ha constatato che, mediante la prevista rinuncia al rilevamento di dati relativi all'ubicazione, l'utilizzazione di codici di identificazione temporanei e la partecipazione facoltativa, il progetto rispettava le esigenze di protezione della sfera privata e di autodeterminazione informativa.

Il PFL e i suoi partner hanno proseguito lo sviluppo dell'applicazione denominata «Decentralized Privacy Preserving Proximity Tracing» (DP-3T). I lavori si sono svolti autonomamente rispetto al progetto europeo «Pan-European Privacy-Preserving Proximity Tracing» (PEPP-PT) e hanno apportato miglioramenti in materia di diritto sulla protezione dei dati, segnatamente grazie all'introduzione di un approccio decentralizzato nell'elaborazione dei dati. Un aspetto particolarmente vantaggioso di tale approccio decentralizzato consisteva nel fatto che, benché non si potesse rinunciare ai server centrali, la trasmissione di dati avrebbe avuto luogo soltanto in forma di chiavi anonime e le registrazioni delle prossimità rilevanti dal profilo epidemiologico sarebbero avvenute soltanto localmente sul cellulare.

Nel corso del progetto la Confederazione ha deciso di introdurre un sistema di tracciamento ufficiale basato sul protocollo DP-3T. In qualità di organo responsabile, l'Ufficio federale della sanità pubblica (UFSP) ci ha quindi coinvolto nei lavori di attuazione della app SwissCovid della Confederazione e ci ha fornito una documentazione completa. I nostri specialisti hanno così potuto riesaminare tecnicamente l'applicazione e la relativa configurazione del sistema, includendo l'attuazione nel sistema a valle (backend-server). In maggio l'IFPDT ha tra l'altro constatato, sulla base di una valutazione d'impatto sulla protezione dei dati, che le condizioni previste dal diritto sulla protezione dei dati erano soddisfatte (cfr. parere dell'IFPDT dell'13 maggio 2020).

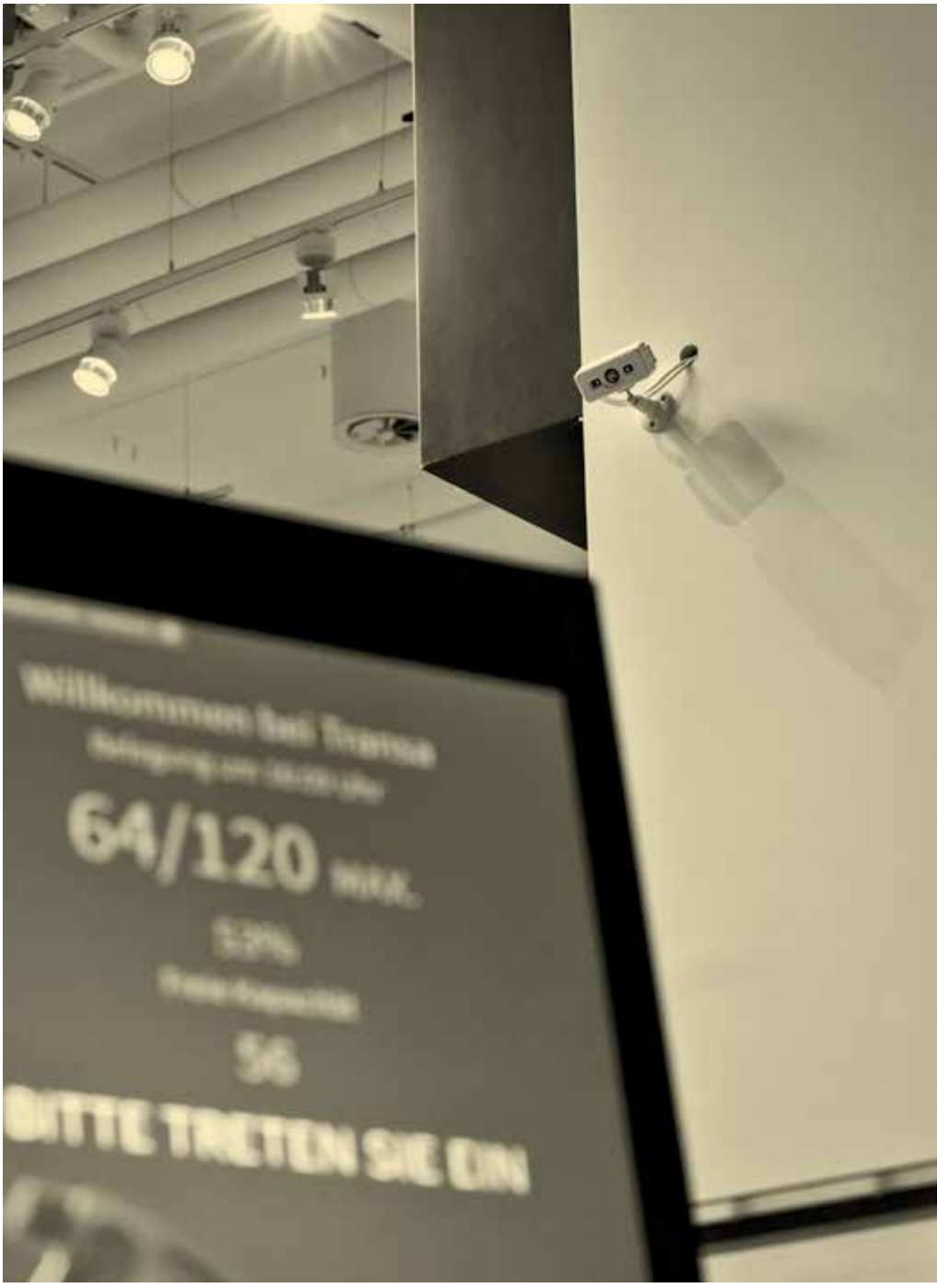
Dopo aver preso atto di un rapporto pubblicato in giugno dal Centro nazionale per la cibersicurezza (NCSC), l'IFPDT ha condiviso tale valutazione. Esso ha sottolineato che l'utilizzazione delle interfacce di programmazione (cosiddette interfacceAPI, application programming interface) di Google e Apple per la app SwissCovid, criticata dalle cerchie vicine alla protezione dei dati e dai media, non poneva rischi significativamente più elevati per la popolazione rispetto all'usuale impiego quotidiano di tali interfacce.

Dopo aver chiesto invano all'Amministrazione di avviare i lavori per istituire nella legge sulle epidemie, in conformità all'articolo 17 LPD, una base legale sufficientemente concreta per l'applicazione, l'IFPDT ha quindi rivolto tale invito alle competenti commissioni parlamentari. Tale base legale è stata quindi iscritta il 25 giugno 2020 a titolo urgente nel nuovo articolo 60ª della legge sulle epidemie.

Secondo tale disposizione l'utilizzazione della app SwissCovid ha carattere facoltativo. Da un lato il legislatore era consapevole delle difficoltà di rendere politicamente

accettabile un regime obbligatorio, il quale non era oltretutto realizzabile vista la possibilità di disattivare in ogni momento la funzione bluetooth. D'altra parte, vietando alle autorità, alle imprese e ai privati di favorire o penalizzare le persone in ragione dell'utilizzazione o meno dell'applicazione da parte loro, il Parlamento ha lanciato un segnale contro l'introduzione di un obbligo fattivo di portare con sé un apparecchio cellulare.

Il 25 giugno 2020 l'app SwissCovid è stata lanciata nelle App-Store di Apple e Google. Mentre ancora parecchi mesi dopo la sua introduzione, parti della popolazione nutrivano grande diffidenza nei confronti dell'applicazione dubitando che fosse conforme ai principi di protezione dei dati, altre voci avevano deplorato che, a causa della protezione dei dati, il legislatore aveva limitato oltre misura l'efficacia di tale applicazione. Confrontato con queste posizioni contrastanti, l'UFSP non è finora riuscito ad aumentare ulteriormente la diffusione dell'applicazione oltre la soglia – invero notevole benché avesse disatteso aspettative più ottimistiche – di circa tre milioni di download e di 1,7 milioni di utenti attivi.



CORONA

Quadro giuridico della raccolta dei dati di contatto

Con i suoi interventi, l'IFPDT ha contribuito a far sì che la registrazione dei dati di contatto per tracciare i contagi da COVID-19, il cosiddetto contact tracing, poggiasse su basi legali sufficientemente specifiche, nel rispetto dei principi della legge sulla protezione dei dati.

Quando l'11 maggio 2020 c'è stata la riapertura di ristoranti, bar, discoteche, centri fitness e altri locali pubblici, molte strutture hanno previsto la registrazione dei dati di contatto per tracciare i contagi come parte dei piani di protezione decisi dal Consiglio federale. Dato che per la raccolta e l'ulteriore trattamento di questi dati non esisteva inizialmente alcuna base legale, l'IFPDT ha sostenuto pubblicamente che, per il momento, tutto ciò poteva avvenire soltanto su base volontaria (cfr. la nostra comunicazione del 19.05.2020 «Coronavirus: piani di protezione»).

Con il suo intervento l'IFPDT ha potuto contribuire a far sì che il Consiglio federale facesse poggiare su una base giuridica sufficientemente specifica l'obbligo di fornire i propri dati di contatto che lo stesso Consiglio federale aveva introdotto il 22 giugno 2020. L'ordinanza COVID-19 situazione particolare ha limitato l'impiego dei dati raccolti (trasmissione ai servizi cantonali competenti per il contact tracing in caso di contagio), ha disciplinato i requisiti di conservazione (garanzia di riservatezza) e la cancellazione automatica dopo 14 giorni e ha stabilito quali dati dovevano essere registrati a livello federale (cognome, nome, domicilio e numero di telefono).

Per aumentare l'efficacia del contact tracing alcuni Cantoni hanno obbligato i gestori di locali a utilizzare una determinata applicazione per la registrazione dei dati di contatto. Oltre a segnalare la necessità di una chiara base legale (cantonale), l'IFPDT ha sottolineato che tali applicazioni devono garantire un trattamento dei dati riconoscibile, limitato allo scopo e sicuro. Ha inoltre ripetutamente evidenziato che i privati non possono di fatto imporre ai propri clienti di avere con sé uno smartphone. Occorre tener presente che vi sono persone riluttanti a mostrare uno smartphone dotato di un determinato programma perché temono un accesso ai dati riguardanti il loro stile di vita digitale. Ve ne sono poi altre che per la loro età, il loro stato di salute o a causa di una disabilità non sono neppure in grado di farlo. A queste persone gli esercizi pubblici devono mettere a disposizione, oltre a quelli digitali, anche metodi di registrazione alternativi come la compilazione di moduli cartacei in condizioni ragionevoli.

Infine, dall'estate del 2020 si sono accumulate le segnalazioni dell'esistenza di problemi di natura giuridica e tecnica nell'uso di alcune applicazioni per la registrazione dei dati di contatto. Questo ha spinto l'IFPDT ad avviare una procedura di accertamento dei fatti su un'applicazione molto utilizzata in alcune regioni della Svizzera. L'IFPDT vuole completare l'inchiesta prima della prossima riapertura del settore della ristorazione, un obiettivo non di poco conto date le formalità della procedura.

1.6 Lavoro

Ammissibilità dei controlli di background nelle procedure di candidatura

Accade sempre più spesso che ditte, soprattutto estere, offrano a datori di lavoro svizzeri interessati la possibilità di consultare banche dati alla ricerca di informazioni su candidati e di fornire infine una raccomandazione di assunzione. L'IFPDT è stato interpellato più volte sull'ammissibilità di simili controlli, i cosiddetti «background check».

Secondo l'articolo 328b CO il datore di lavoro può trattare soltanto quei dati che sono necessari per la procedura di candidatura in corso. Deve inoltre osservare sempre anche i principi di trattamento dei dati contenuti nella LPD, in particolare il principio di proporzionalità e l'obbligo di trasparenza.

Il principio di proporzionalità esige che la consultazione di banche dati e successiva valutazione dei dati trovati siano adeguate, necessarie e ragionevoli per verificare le qualifiche dei candidati. Un controllo di sicurezza relativo alle persone più o meno esteso può essere – in ambiti in cui i lavoratori hanno accesso a informazioni sensibili – adeguato, necessario e ragionevole per limitare determinati rischi, come ad esempio nel settore bancario o in quello della sicurezza. Dove invece non sussistono particolari rischi, come potrebbe essere il caso – fatte salve circostanze particolari – ad esempio del personale insegnante, un controllo di sicurezza approfondito appare sproporzionato.

Indipendentemente dalla questione della proporzionalità, il datore di lavoro è tenuto, in base all'obbligo di trasparenza, a informare la persona interessata in merito al background check e ai trattamenti dei dati e alle valutazioni successivi. Soltanto così si assicura che questa possa verificare la legittimità del trattamento dei dati e la loro esattezza e far valere i propri diritti. Alla luce dell'obbligo di trasparenza non sono perciò ammissibili background check effettuati di nascosto che non vengono comunicati agli interessati.

CORONA

Telelavoro: aspetti legati al diritto in materia di protezione dei dati

Nell'anno in rassegna, a numerosi impiegati è stato ordinato di lavorare entro le proprie quattro mura. Di conseguenza l'IFPDT si è occupato in maniera crescente di questioni legate all'impiego delle diverse soluzioni per svolgere videoconferenze, alla sorveglianza dei collaboratori e all'accesso ai server aziendali svizzeri dall'estero.

La domanda circa le condizioni alle quali è possibile introdurre il telelavoro per gli impiegati trova risposta nelle prescrizioni del diritto in materia di lavoro. Dal punto di vista del diritto sulla protezione dei dati, da questa premessa emergono tuttavia alcune problematiche non irrilevanti, ad esempio in relazione all'impiego di mezzi di telecomunicazione digitali per le conferenze telefoniche e le videoconferenze (v. cap. 1.1, box concernente la guida corrispondente) oppure all'utilizzo di piattaforme per lo scambio di dati. Pur considerando che gli obblighi dei lavoratori possono variare puntualmente, anche in tempi di crisi il datore di lavoro è responsabile della sicurezza informatica e della protezione dei dati, e rimane quindi vincolato ai principi sanciti nella LPD per il trattamento dei dati. Detto questo, incombe pertanto al datore di lavoro scegliere un software che garantisca sufficientemente la sicurezza dei dati personali trattati. Sul proprio sito l'IFPDT ha pubblicato una guida, intitolata «Misure per un impiego sicuro delle soluzioni di audio e videoconferenza», che riassume le principali prescrizioni in materia di protezione dei dati che devono essere rispettate nella scelta delle rispettive piattaforme.

Diverse richieste della popolazione esprimevano il timore che durante il telelavoro gli impiegati potessero essere esposti a una sorveglianza permanente da parte del datore di lavoro. L'IFPDT è consapevole del fatto che, a seconda della soluzione informatica utilizzata, il comportamento di chi lavora a casa potrebbe essere sorvegliato facilmente e in permanenza: ciò sarebbe tuttavia illecito alla luce della LPD e inoltre espressamente vietato dalle norme della legge sul lavoro.

L'IFPDT è infine stato confrontato più volte con la domanda se sia da considerare una comunicazione di dati all'estero il fatto di fare telelavoro dall'estero – dalla residenza di vacanza o, nel caso dei frontalieri, da casa propria – e da lì accedere al server aziendale in Svizzera. Secondo l'IFPDT, fintanto che il lavoratore che accede al server aziendale dalla sua postazione di telelavoro all'estero mediante Virtual Private Network (VPN) si limita a trattare dati personali nella stessa misura in cui lo farebbe normalmente anche negli uffici dell'impresa, e in particolare non rende accessibili i dati a nessuno all'estero, non si tratta di una comunicazione transfrontaliera di dati ai sensi della LPD. La confidenzialità dei dati personali deve essere garantita in ogni caso, indipendentemente dal fatto che i lavoratori facciano telelavoro all'estero o in Svizzera.

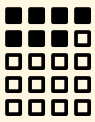
CORONA

Prescrizioni in materia di protezione dei dati a proposito del riconoscimento precoce del coronavirus in ambito lavorativo

In merito ai rapporti di lavoro la pandemia di coronavirus ha sollevato diverse questioni relative alla conformità alla protezione dei dati, ad esempio per quanto riguarda le misurazioni della temperatura sul posto di lavoro o la comunicazione interna in merito ai contagi constatati. A questo proposito è emersa ripetutamente la questione se i provvedimenti adottati fossero proporzionati.

Nel quadro del rapporto lavorativo il datore di lavoro può trattare soltanto quei dati concernenti i lavoratori che sono necessari per lo svolgimento del rapporto lavorativo stesso. In questo ambito il principio di proporzionalità secondo la LPD deve essere sempre rispettato. Ogni trattamento dei dati deve infatti essere appropriato, necessario e ragionevole allo scopo di raggiungere l'obiettivo prefissato, in questo caso evitare infezioni sul posto di lavoro.

Per quanto riguarda le misurazioni della temperatura sul posto di lavoro ci si è chiesti se questo provvedimento fosse effettivamente appropriato per arginare i contagi. Da un lato una temperatura alterata può essere sintomo di un'altra malattia, dall'altro la temperatura corporea può facilmente essere abbassata artificialmente con l'assunzione di medicamenti. Inoltre, non tutte le persone contagiate dal virus presentano sintomi di febbre. La misurazione generalizzata della temperatura appare dunque solo parzialmente appropriata per evitare i contagi sul posto di lavoro. Il datore di lavoro deve pertanto chiedersi se non vi siano provvedimenti meno incisivi che potrebbero portare allo stesso obiettivo. In questi casi l'IFPDT ha normalmente proposto di obbligare i collaboratori ad annunciarsi immediatamente presso una persona di fiducia all'interno dell'azienda non appena si manifestano sintomi tipici di un contagio da coronavirus. Per valutare la questione l'IFPDT si è basato anche sulle raccomandazioni della Swiss National COVID-19 Science Task Force, che ha espressamente sconsigliato la misurazione della temperatura quale provvedimento preventivo isolato.



È ripetutamente sorta anche la domanda di come un datore di lavoro debba o possa comunicare un caso di contagio agli altri collaboratori, affinché quelli che sono stati a contatto con la persona contagiata possano entrare in quarantena. Nei confronti dei lavoratori il datore di lavoro ha un obbligo di tutela che richiede il trattamento di questa informazione, anche se il tracciamento dei contatti incombe in linea di principio alle autorità cantonali (medico cantonale) e non ai datori di lavoro.

1.7 Assicurazioni

Introduzione del Sistema di segnalazione e informazione HIS nel settore delle assicurazioni svizzere

L'IFPDT è stato consultato dall'Associazione svizzera d'assicurazioni in vista dell'introduzione del Sistema di segnalazione e informazione HIS, una banca dati a disposizione delle compagnie di assicurazione che vi partecipano, sviluppata per impedire l'abuso assicurativo. L'IFPDT ha ribadito che tutti i trattamenti di dati in relazione con la gestione dell'HIS devono rispettare il principio di proporzionalità sancito nel diritto sulla protezione dei dati.

La consultazione dell'IFPDT in merito all'HIS è stata già avviata nel 2017/2018 (cfr. 25° rapporto di attività, n. 1.6.2) e viene ora portata avanti.

Le compagnie di assicurazione svizzere che partecipano all'HIS vi notificano persone nel cui caso, in occasione della liquidazione di un sinistro, è stata riscontrata un'irregolarità definita per regolamento, ad esempio una reticenza secondo l'articolo 6 della legge sul contratto d'assicurazione (LCA). In caso di futuri sinistri, cercando la persona interessata nel sistema appare un'indicazione che rimanda a quest'irregolarità, cosicché la compagnia di assicurazione è in grado di verificare in modo approfondito il proprio obbligo di fornire la prestazione nel nuovo caso. I motivi della notifica ottemperano il diritto assicurativo o quello in materia di responsabilità civile, ma non sono di natura penale. Una compagnia di assicurazione può vedere se una persona è notificata nell'HIS soltanto se questa è coinvolta in un nuovo sinistro, tuttavia non al di fuori di un processo di elaborazione di danni, in particolare non prima che venga concluso un contratto con la persona stessa. Vengono notificate nell'HIS non soltanto la persona assicurata, ma anche altre persone eventualmente coinvolte, come «istigatori» o «complici».

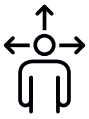
Nell'ambito della sua consultazione, l'IFPDT ha sottolineato in particolare che tutti i trattamenti di dati in relazione all'HIS devono rispettare il principio di proporzionalità secondo il diritto sulla protezione dei dati. Una registrazione nell'HIS deve dunque essere adeguata e necessaria per impedire o scoprire abusi assicurativi e anche la conseguente ingerenza nella sfera privata deve poter essere ragionevolmente accettata dalla persona interessata. I motivi della notifica devono essere rigorosamente circoscritti e chiaramente definiti in un regolamento, nonché essere resi trasparenti. Una notifica può consentire alla compagnia di assicurazione di verificare approfonditamente la pretesa di prestazioni della persona assicurata in un nuovo sinistro, ma non deve comportare la sua condanna a priori. Occorre dunque prendere i provvedimenti necessari per assicurare la correttezza dei dati personali. Compagnie di assicurazione che non si attengono al regolamento ed effettuano ripetutamente notifiche ingiustificate devono poter essere individuate e sanzionate.

I suggerimenti dell'IFPDT sono stati in gran parte attuati. Sono stati ulteriormente precisati soprattutto i motivi alla base di una notifica nell'HIS. Sarà infine la prassi a mostrare in che misura l'HIS sarà in grado di contribuire a impedire abusi assicurativi, in che misura le compagnie di assicurazione si atterranno alle disposizioni regolamentari e se in futuro saranno necessari eventuali adeguamenti dal punto di vista della protezione dei dati.

Trasmissione di dati dei membri agli sponsor

L'IFPDT chiede di produrre un consenso valido per trasmettere i dati agli sponsor nel rispetto della legge. I membri di associazioni devono poter opporsi alla trasmissione dei dati senza che ciò comporti uno svantaggio sproporzionato.

Nell'anno in rassegna l'IFPDT ha ricevuto diverse richieste concernenti la trasmissione agli sponsor di dati relativi all'indirizzo di membri di associazioni per scopi pubblicitari. Ci si chiede se sia ammissibile esigere un contributo più elevato da quei membri



che si sono opposti alla trasmissione dei propri dati. Abbiamo richiamato l'attenzione delle persone e delle associazioni interessate sul fatto che potrebbe insorgere uno svantaggio sproporzionato se l'aumento del contributo è talmente elevato che le persone interessate si sentono praticamente costrette ad acconsentire che i loro dati vengano comunicati.

Già in passato l'IFPDT ha ricordato alle associazioni sportive e agli sponsor la loro responsabilità per la legalità dei trattamenti di dati da essi effettuati (cfr. 22° rapporto d'attività 2014/2015, n. 1.8.5). Senza un consenso valido delle persone interessate, le associazioni non possono trasmettere dati agli sponsor. Affinché una trasmissione di dati possa avvenire conformemente alla legge, tutti gli interessati devono esserne informati previamente e in modo adeguato (vale a dire quali dati verranno comunicati, a quali destinatari, per quale scopo) e devono poter dare il loro consenso. Se questo avviene come opt-out (opzione di rinuncia), è essenziale che i membri abbiano una possibilità semplice di opporsi alla trasmissione dei propri dati senza incorrere in svantaggi sproporzionati. Gli sponsor, a loro volta, devono assicurare per contratto che tratteranno soltanto i dati relativi all'indirizzo di quei membri di associazioni che sono stati loro comunicati sulla base di un consenso efficace.

Utilizzazione sistematica del numero AVS da parte delle autorità: il Parlamento approva la modifica della legge

Il 18 dicembre 2020 il Parlamento ha approvato la modifica della legge federale sull'assicurazione per la vecchiaia e per i superstiti. Il nuovo testo normativo definisce un'ampia cerchia di autorità, organizzazioni e persone autorizzate a utilizzare sistematicamente il numero AVS a 13 cifre (NAVS13) come identificatore personale univoco al di fuori del settore delle assicurazioni sociali. L'Incaricato ha ottenuto garanzie importanti in materia di protezione dei dati.

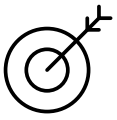
Il 1° febbraio 2017 il Consiglio federale aveva incaricato il Dipartimento federale dell'interno (DFI) di svolgere una consultazione sull'utilizzazione sistematica del NAVS13 da parte di autorità federali, cantonali e comunali. Un gruppo di lavoro interno all'Amministrazione, al quale non siamo stati invitati a partecipare, ha ritenuto che non vi fossero particolari rischi in termini di protezione dei dati. Ciononostante, sia l'IFPDT sia le autorità cantonali preposte alla protezione dei dati erano già contrari al principio dell'utilizzazione sistematica del NAVS13 a causa dei rischi in materia di protezione dei dati.

Assieme all'Ufficio federale di giustizia (UFG) abbiamo quindi richiesto una valutazione dei rischi di un'utilizzazione sistematica del numero AVS che è stata commissionata a David Basin, professore ordinario al PF di Zurigo. Da questa valutazione, datata 27 settembre 2017, è emerso che l'utilizzazione sistematica del NAVS13 presentava rischi non indifferenti in termini di protezione dei dati (cfr. 25° rapporto d'attività, n. 1.1.2). L'esperto raccomandava l'utilizzazione di numeri settoriali, sottolineando tuttavia nel contempo che una simile misura non avrebbe avuto gli effetti auspicati in materia di protezione dei dati se non fosse stata accompagnata da altre misure importanti, come il rinnovo dell'architettura delle banche dati.

A seguito di questa perizia, il 20 ottobre 2017 la Commissione degli affari giuridici del Consiglio nazionale ha presentato un postulato (17.3968) che incaricava il Consiglio federale di illustrare un piano su come affrontare i rischi correlati all'utilizzazione del NAVS13 quale numero d'identificazione personale unico. Il piano doveva inoltre illustrare come fosse possibile migliorare la protezione dei dati quando Cantoni, Comuni e terzi utilizzano i numeri d'identificazione personali e per fare ciò doveva tenere conto del giudizio dell'IFPDT. Nel suo parere del 20 dicembre 2017 il Consiglio federale si è detto cosciente dei problemi legati all'utilizzazione sistematica del NAVS13 e ha dichiarato che avrebbe tenuto conto dello studio Basin e delle osservazioni dell'Incaricato nel suo disegno di legge. Durante la consultazione preliminare degli uffici siamo riusciti a ottenere diverse modifiche del disegno, in particolare quella che obbliga tutte le unità autorizzate a utilizzare sistematicamente il NAVS13 a procedere a un'analisi dei rischi e a tenere un elenco delle banche dati in cui il NAVS13 è registrato. Allo stesso modo, è stata riconosciuta e inserita nel disegno di legge la necessità di rafforzare le misure tecniche e organizzative volte a limitare i rischi di violazione dei dati (cfr. 27° rapporto d'attività, n. 1.7).

Il 7 novembre 2018 il Consiglio federale ha avviato una consultazione sulla modifica della legge sull'AVS, che prevede l'utilizzazione sistematica del NAVS13. Il disegno ha tenuto conto dei requisiti posti dall'Incaricato in merito alla protezione dei dati. Un'autorità può collegare dati fattuali (cognome, nome, data di nascita ecc.) al NAVS13 e verificare la loro esattezza nella banca dati Unique Person Identification (UPI) gestita dall'Ufficio centrale di compensazione (UCC). Tuttavia, non può accedere ad altri registri come il Registro centrale degli assicurati e il Registro centrale delle prestazioni correnti dell'UCC, né ai registri contenenti dati fattuali gestiti da altre autorità. Questo consente di evitare che un'autorità sia in grado di fare collega-

menti tra le varie banche dati e stabilire, sulla base del NAVS13, profili della personalità che per la natura stessa dei dati sarebbero molto precisi. Va quindi accolto positivamente il fatto che tutte le unità a livello federale e cantonale, ma anche le unità decentrate dell'Amministrazione federale, nonché le organizzazioni e le persone di diritto pubblico o privato che non appartengono alle amministrazioni che dispongono di tali banche dati, debbano procedere periodicamente ad analisi dei rischi, tenendo in particolare conto del pericolo di collegamenti non autorizzati di dati. In base a quest'analisi dei rischi vanno definite e attuate misure di sicurezza e di protezione dei dati conformi al livello di rischio e allo stato della tecnica. Le unità designate dal disegno di legge che utilizzano sistematicamente il NAVS13 hanno l'obbligo di tenere un elenco delle banche dati pertinenti che funga in particolare da base per le analisi dei rischi. Oltre alle unità delle amministrazioni federali, cantonali e comunali, la legge autorizza a utilizzare sistematicamente il numero NAVS13 le istituzioni preposte all'educazione, le imprese di assicurazione private (anche nell'ambito dell'assicurazione complementare) e le organizzazioni e le persone di diritto pubblico o privato che non appartengono alle amministrazioni sopraccitate e alle quali sono conferiti compiti amministrativi sulla base del diritto federale, cantonale o comunicale oppure di un contratto, purché il diritto applicabile preveda l'utilizzazione sistematica del numero AVS. Inoltre, il NAVS13 non deve essere utilizzato per scopi prettamente privati. Ciò si applica anche nei casi in cui le persone interessate consentono a privati di utilizzare in modo sistematico il loro numero AVS.



Oltre alle misure sopraccitate, accogliamo con favore il fatto che la legge preveda anche l'obbligo di adottare misure tecniche e organizzative vincolanti per prevenire eventuali utilizzazioni abusive del numero AVS. Come pure il principio contenuto nella legge secondo cui l'accesso a banche dati contenenti il NAVS13 deve essere limitato alle persone che necessitano questo numero per adempiere i loro compiti. Lo stesso vale per le trasmissioni di file contenenti il NAVS13 che devono essere fatte in modo cifrato attraverso una rete pubblica. Incontra i nostri favori anche il fatto che le autorità, le organizzazioni e persone autorizzate a utilizzare il numero AVS dovranno definire la procedura da seguire in caso di accesso abusivo a banche dati o di utilizzazione abusiva delle medesime e che il loro personale dovrà essere istruito a utilizzare il numero AVS conformemente alla legge. Infine, apprezziamo pure il fatto che la legge preveda che il mancato rispetto di questi doveri potrà essere sanzionato penalmente.

Dopo la procedura di consultazione il disegno non è stato più modificato in modo sostanziale. Nel dicembre 2020, poco prima della votazione finale dell'Assemblea federale, il Parlamento ha ampliato l'elenco delle unità autorizzate a utilizzare sistematicamente il NAVS13 includendovi gli organi incaricati dell'esecuzione dei controlli previsti da un contratto collettivo di lavoro di obbligatorietà generale.

Le molteplici audizioni dell'Incaricato da parte delle Commissioni parlamentari durante il processo legislativo hanno permesso di porre la protezione dei dati al centro delle disposizioni legali. L'entrata in vigore di queste nuove norme non è attesa prima della fine del 2021.

1.8 Trasporti

Domande dei cittadini relative ai droni in forte aumento

Nell'anno in rassegna le domande di privati sull'argomento droni hanno registrato un forte aumento. Si tratta sia di proprietari di droni sia di persone disturbate dalle riprese fatte da droni.

I droni sembrano diventare sempre più popolari tra i privati: almeno secondo l'IFPDT, che nell'anno in rassegna ha registrato un forte aumento delle domande di privati su questa tematica. Da un lato si tratta di cittadini che effettuano foto o videoriprese mediante un drone e vorrebbero chiarire i presupposti giuridici (in materia di protezione dei dati) con l'Incaricato e con altre autorità (segnatamente con l'Ufficio federale dell'aviazione civile UFAC). Dall'altro si tratta di privati disturbati da droni che volano nei pressi del loro luogo di lavoro o di domicilio effettuando forse registrazioni audio e video.

Oltre a una consulenza giuridica, i richiedenti desiderano spesso che l'Incaricato prenda una decisione nel loro caso specifico. In simili casi l'IFPDT rammenta che occorre osservare i principi generali della protezione dei dati e che i detentori privati di dati devono disporre di un motivo giustificativo. Per quanto riguarda autorizzazioni o divieti rimanda alle autorità competenti in materia, soprattutto all'UFAC e ai tribunali civili e penali cantonali.

Ulteriori informazioni sulla videosorveglianza con droni nella sfera privata si trovano sulla nostra pagina web.

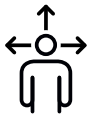
Revisione della legge sul trasporto di viaggiatori: occorre impedire ostacoli discriminatori per i viaggiatori anonimi nei trasporti pubblici

L'IFPDT si è espresso nell'ambito della consultazione degli uffici relativa al messaggio concernente la modifica della legge sul trasporto di viaggiatori (base moderna per i TP).

Dalla consultazione degli uffici si sono svolte numerose sedute con rappresentanti dell'Ufficio federale dei trasporti e dell'Ufficio federale di giustizia in cui si è discusso in particolare in quale misura le imprese di trasporto devono essere soggette alle disposizioni in materia di protezione dei dati per privati o autorità.

L'IFPDT ha rilevato in particolare che, in caso di assoggettamento a disposizioni in vigore per i detentori privati di dati, oltre al consenso, sono disponibili tutti gli altri motivi di giustificazione, come la base legale o un interesse preponderante. Le imprese di trasporto possono appellarsi ad esempio a quest'ultimo se trattano dati in relazione diretta con la conclusione o l'esecuzione di un contratto.

Se il trattamento dei dati è legittimato dal consenso, occorre osservare i criteri relativi alla sua validità giuridica: il consenso deve essere espresso liberamente, dopo debita e trasparente informazione. In caso di dati personali degni di particolare protezione e di profili della personalità, i consensi devono essere espliciti. Inoltre, il trasporto di viaggiatori non può essere vincolato al consenso a un trattamento dei dati per scopi di altra natura. Per trattare dati per ulteriori scopi occorre ottenere separatamente i relativi consensi degli interessati.



Anche dove basta un consenso implicito, occorre un'informazione esaustiva affinché i clienti riconoscano le lesioni della personalità e possano davvero scegliere se optare per l'offerta di raccolta dati o per un'alternativa anonima a condizioni analoghe. Se scelgono la soluzione di raccolta dati, il loro consenso è implicito. L'IFPDT ha inoltre ribadito che le offerte alternative anonime non devono essere collegate a nessun ostacolo finanziario o amministrativo deterrente o discriminante. Dato che in caso di trasferimento completo dei costi supplementari di offerte alternative potrebbe accadere che parti della popolazione verrebbero di fatto escluse, l'IFPDT ha chiesto di integrare la disposizione pertinente nella legge sul trasporto di viaggiatori e di precisare la motivazione nel messaggio.

Per quanto riguarda l'infrastruttura di distribuzione, ossia la piattaforma centrale di ordinazione, al momento non ancora concretizzata, l'IFPDT ha fatto notare i principi generali validi già oggi nonché i requisiti da osservare, secondo la LPD riveduta, nella fase di sviluppo della piattaforma digitale, come ad esempio la protezione dei dati personali sin dalla progettazione e per impostazione predefinita («privacy by design» e «privacy by default»), nonché la protezione dei dati persistenti.

L'IFPDT continuerà a seguire la procedura legislativa e si adopererà affinché i requisiti in materia di protezione dei dati siano osservati.

Utilizzo di dati dei passeggeri aerei nella lotta al terrorismo

Il DFGP sta elaborando un progetto legislativo per utilizzare i dati dei passeggeri rilevati dalle compagnie aeree nella lotta alla criminalità e al terrorismo in Svizzera. L'IFPDT siede nel comitato esterno di esperti del progetto.

Il 12 febbraio 2020 il Consiglio federale si è pronunciato in una decisione di principio a favore dell'utilizzo di dati dei passeggeri aerei (Passenger Name Records, PNR) nella lotta alla criminalità e al terrorismo in Svizzera. A questo scopo il DFGP è stato incaricato di avviare l'introduzione di un sistema PNR nazionale (cfr. 27° rapporto di attività, n. 1.2, pag. 27). Il DFGP deve ora elaborare assieme al DATEC entro la metà del 2021 un avamprogetto di legge sulla raccolta e il trattamento di dati dei passeggeri aerei da parte della Svizzera da porre in consultazione nonché la loro comunicazione a Paesi nei quali la protezione e il trattamento dei dati corrispondono allo standard richiesto nella Direttiva (UE) 2016/681 del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (Direttiva PNR dell'UE). Entro metà 2021, inoltre, il DFGP preparerà assieme al DFAE un mandato per negoziare con l'UE un accordo per lo scambio di informazioni PNR tra i servizi di coordinamento competenti (Passenger Information Unit, PIU) in Svizzera e negli Stati membri dell'UE.

L'IFPDT ha aderito al comitato esterno di esperti del progetto PNR e partecipa alla sua strutturazione dal profilo della protezione dei dati. Nell'allestire un sistema PNR le limitazioni dei diritti fondamentali devono essere unicamente quelle strettamente necessarie a conseguire lo scopo previsto. L'equilibrio tra la garanzia dei diritti fondamentali e le limitazioni indispensabili a garantire la sicurezza pubblica dev'essere mantenuto. Ciò significa in particolare che i dati sono trasmessi mediante il sistema «push», che non permette ad autorità straniere di accedere direttamente ai dati. Come da sua prassi consolidata, l'Incaricato s'impegna inoltre a far sì che venga redatto un elenco dei reati. Ciò adempie il principio della proporzionalità e favorisce la trasparenza.

Lo scudo per la privacy non garantisce agli interessati in Svizzera un adeguato livello di protezione per la comunicazione di dati agli Stati Uniti.

L'IFPDT ha rivalutato la conformità del regime dello scudo per la privacy alla luce dei suoi riesami annuali e della recente giurisprudenza della Corte di giustizia dell'Unione europea (CGUE). È giunto alla conclusione che lo scudo per la privacy non garantisce agli interessati in Svizzera un adeguato livello di protezione ed esorta le aziende svizzere a effettuare nel caso specifico una valutazione dei rischi quando comunicano dati negli Stati Uniti sulla base di garanzie contrattuali.

Già in occasione dei riesami dello scudo Svizzera-USA per la privacy effettuati nel 2018 e 2019 l'IFPDT ha constatato nei suoi rapporti di valutazione che il regime dello scudo per la privacy – nonostante i miglioramenti apportati dalla sua entrata in vigore – non offre agli interessati sufficienti diritti vincolanti in caso di accesso ai dati da parte delle autorità statunitensi (cfr. anche 27° rapporto d'attività, pag. 34 e 26° rapporto d'attività, n. 1.2). Ha criticato in particolare il fatto che, per mancanza di trasparenza, non è possibile valutare l'efficacia del cosiddetto meccanismo del mediatore, inteso a garantire un rimedio giuridico indirettamente vincolante. Non sono provate neppure le competenze decisionali del mediatore nei confronti dei servizi d'informazione statunitensi o la sua effettiva indipendenza. L'IFPDT ha reputato problematiche la mancanza di trasparenza e la conseguente assenza di garanzie in caso di accesso da parte delle autorità statunitensi alla sfera privata di persone in Svizzera.

Il 16 luglio 2020 la CGUE ha pronunciato la sentenza relativa alla causa C311/18 Data Protection Commissioner contro Facebook Ireland Limited e Maximilian Schrems (cosiddetta sentenza Schrems II) che ha dichiarato invalida la decisione di adeguatezza 2016/1250 della Commissione UE concernente le imprese statunitensi certificate ai sensi del regime dello scudo per la privacy. La CGUE chiarisce inoltre che l'impiego di clausole contrattuali modello per gli Stati Uniti e per altri Paesi terzi prive di un'adeguata protezione dei dati necessitano di un esame della loro adeguatezza nel caso specifico e, qualora necessario, di un completamento. La sentenza non è vincolante per la Svizzera. Secondo il RGPD, tuttavia, il diritto in materia di protezione dei dati dell'UE e la giurisprudenza della CGUE su di esso fondata vengono applicati dalle autorità e dai tribunali dell'UE e del SEE anche nei confronti di aziende svizzere se queste trattano dati in modo tale da ricadere nel settore di applicazione del RGPD. Dopo un'analisi approfondita della sentenza della CGUE e della situazione giuridica svizzera, nel suo parere dell'8 settembre 2020 (v. comunicato stampa) l'IFPDT è giunto alla conclusione che, nonostante garantisca anche agli interessati in Svizzera specifici diritti alla protezione dei dati personali, il regime dello scudo per la privacy non prevede un adeguato livello di protezione per la comunicazione di dati dalla Svizzera agli Stati Uniti conformemente alla legge federale sulla protezione dei dati (LPD). Sulla base di quest'analisi fondata sul diritto svizzero, l'IFPDT ha deciso di stralciare dall'elenco degli Stati che garantiscono un livello di protezione adeguato conformemente alla LPD (disponibile in tedesco e francese) l'osservazione secondo cui gli Stati Uniti offrono una «protezione dei dati adeguata a determinate condizioni». L'elenco ha carattere indicativo. Al momento attuale non esiste in Svizzera nessuna giurisprudenza paragonabile alla sentenza della CGUE summenzionata. È fatta salva una valutazione diversa da parte dei tribunali svizzeri.

Le garanzie contrattuali applicate, oltre al regime dello scudo per la privacy, per la comunicazione di dati negli Stati Uniti e in altri Paesi terzi senza decisione di adeguatezza, come ad esempio le clausole contrattuali modello dell'UE utilizzate spesso anche in Svizzera o le cosiddette «Binding Corporate Rules», non riescono a impedire che autorità estere accedano a dati personali se il diritto pubblico dello Stato importatore prevale e consente l'accesso

da parte delle autorità ai dati personali comunicati senza la trasparenza sufficiente e la protezione giuridica indipendente degli interessati.

Nel suo parere dell'8 settembre 2020 succitato, l'IFPDT ha sensibilizzato le cerchie economiche a questo problema e ha prospettato le prime, limitate possibilità di risolverlo come una propria cifratura o la completa anonimizzazione.

L'IFPDT esorta le aziende a effettuare nel caso specifico una valutazione dei rischi quando comunicano dati negli Stati Uniti sulla base di garanzie contrattuali. Soltanto sulla base di una valutazione dei rischi un'azienda è in grado di giudicare se una comunicazione di dati negli Stati Uniti è conforme alle norme sulla protezione dei dati e, se del caso, di provarlo anche in modo plausibile all'IFPDT. Attualmente l'UE elabora nuove clausole contrattuali modello. L'IFPDT segue questi sforzi e si esprimerà a tempo debito in proposito.

1.9 Internazionale

Introduzione

Nell'anno in rassegna la cooperazione internazionale è stata condizionata dalla crisi legata alla pandemia di COVID-19. Infatti non si sono praticamente potute organizzare conferenze in presenza. Gli incontri hanno dovuto essere annullati oppure svolti in videoconferenza, il che ha comportato, almeno all'inizio dell'emergenza, difficoltà tecniche. Venuti meno i tempi di viaggio e i costi, ad alcune videoconferenze ha partecipato un numero più elevato del solito di autorità preposte alla protezione dei dati e di persone per ciascuna autorità. Per contro non è praticamente stato possibile instaurare colloqui e contatti informali, importanti per la cooperazione. La crisi ha evidenziato l'importanza dello scambio a livello internazionale tra le autorità preposte alla protezione dei dati.

La comunicazione di dati all'estero ha continuato ad aumentare, non da ultimo anche a causa della pandemia: ciò riguarda sia la comunicazione diretta di dati personali all'estero sia la registrazione di dati in cloud e server all'estero. Per le persone interessate è spesso difficile valutare quali imprese e autorità all'estero trattino i loro dati. È quindi particolarmente importante adoperarsi per migliorare l'imposizione della protezione dei dati a livello internazionale, promuovere la cooperazione internazionale tra le autorità preposte alla protezione dei dati e impegnarsi a favore della condivisione e di un'interpretazione uniforme delle norme e dei requisiti internazionali.

Se i requisiti sono armonizzati su scala internazionale, alle persone interessate possono essere garantiti gli stessi diritti indipendentemente da dove sono domiciliate. Inoltre, le autorità preposte alla protezione dei dati a livello internazionale devono consigliarsi su come reagire, dal punto di vista tecnico e dell'impostazione pratica della loro attività di consulenza e vigilanza, alle sfide globali inerenti al diritto in materia di protezione dei dati, quali i big data, l'Internet delle cose e l'intelligenza artificiale.

L'IFPDT continua ad essere presente sulla scena internazionale e si impegna nel contesto di diversi organi internazionali. Tra questi citiamo in particolare il Consiglio d'Europa, la Conferenza europea e la Conferenza internazionale delle autorità di protezione dei dati personali, l'Associazione francofona delle Autorità di protezione dei dati e l'OCSE. Ricordiamo inoltre la cooperazione e il coordinamento delle autorità di protezione dei dati degli Stati membri di Schengen e lo scambio con il Comitato europeo per la protezione dei dati (EDPB).

Consiglio d'Europa

Il Comitato consultivo della Convenzione 108 ha tenuto sei sessioni in videoconferenza su diversi temi. Il Comitato consultivo ha adottato linee guida sulla protezione dei dati personali dei bambini nell'ambiente educativo e linee guida sul riconoscimento facciale. Durante la riunione plenaria si è pure proceduto all'elezione dell'Ufficio.

Nei giorni in cui avrebbe dovuto svolgersi la 40ª sessione plenaria del Comitato, differita a causa della crisi sanitaria, l'Ufficio del Comitato della Convenzione 108 e l'Unità protezione dei dati hanno organizzato sessioni in videoconferenza aperte a tutti per presentare i lavori del Comitato a un pubblico più vasto di quello delle delegazioni che partecipano abitualmente alle riunioni di Strasburgo. Dal 1° al 3 luglio 2020 hanno avuto luogo sei sessioni tematiche volte a precisare e chiarire diversi aspetti:

- Sessione 1: Come assicurarsi che i Paesi aderenti alla Convenzione 108+ rispettino le sue richieste? Perché è necessario un meccanismo di controllo e di valutazione e quale meccanismo scegliere?
- Sessione 2: Come affrontare le ultime sfide poste dalla profilazione nell'era dell'intelligenza artificiale?
- Sessione 3: Che cosa implica il diritto alla protezione dei dati personali nel contesto educativo? Che cosa devono fare le scuole e cosa non devono più fare?
- Sessione 4: I programmi d'identità digitale sono sviluppati secondo il principio della protezione dei dati sin dalla loro progettazione («privacy by design»)?
- Sessione 5: Gli specchi delle nostre anime: ricordare le lezioni di Cicerone e affrontare i rischi del riconoscimento facciale.
- Sessione 6: Campagne politiche ed elezioni: perché la protezione dei dati è cruciale.

Il Comitato consultivo ha potuto svolgere la sua 40ª sessione plenaria, inizialmente prevista dal 1° al 3 luglio, mediante videoconferenza dal 18 al 20 novembre 2020. Durante la sessione il Comitato consultivo ha adottato il testo riveduto delle linee guida sulla protezione dei dati personali dei bambini nell'ambiente educativo. Le linee guida stabiliscono i principi fondamentali dei diritti dei bambini nell'ambiente educativo e mirano ad aiutare i legislatori e i decisori politici, ma anche i titolari del trattamento dei dati e l'industria, a rispettare tali diritti. Il Comitato ha pure proceduto all'elezione del proprio Ufficio, eleggendo fra l'altro una rappresentante dell'IFPDT nella persona di Caroline Gloor Scheidegger, responsabile dell'Ambito direzionale Affari internazionali.

Mediante procedura scritta il Comitato della Convenzione 108 ha inoltre adottato le linee guida sul riconoscimento facciale. Le linee direttrici contengono indicazioni per i legislatori e i decisori, tra cui il coinvolgimento necessario delle autorità di controllo. Esse reggono pure l'operato di sviluppatori, fabbricanti e fornitori di servizi, precisando fra l'altro che l'affidabilità degli strumenti utilizzati dipende dall'efficacia dell'algoritmo. Un terzo aspetto delle linee guida riguarda le entità utilizzatrici di tecnologie del riconoscimento facciale, per le quali si stabilisce fra l'altro la responsabilità nel procedere a un'analisi dell'impatto sulla protezione dei dati e nel garantire la protezione dei dati sin dalla progettazione («privacy by design»). Infine, le linee guida precisano che alle persone interessate sono garantiti tutti i diritti quali il diritto d'informazione, il diritto d'accesso, il diritto di essere informati in caso di decisione individuale automatizzata, il diritto d'opposizione e il diritto di rettifica.

Assemblea mondiale per la protezione della vita privata

La 42ª Assemblea mondiale per la protezione della vita privata (AMVP), precedentemente denominata Conferenza internazionale dei commissari alla protezione dei dati e della vita privata, si è tenuta dal 13 al 15 ottobre 2020, per la prima volta online.

La 42ª sessione a porte chiuse dell'Assemblea mondiale per la protezione della vita privata (AMVP) è stata aperta da Elizabeth Denham, commissaria all'informazione del Regno Unito, che ha sottolineato il lavoro effettuato negli ultimi anni dall'AMVP per modernizzare la propria assemblea, definire il suo orientamento strategico e rafforzare le sue capacità al fine di raccogliere le sfide legate alla pandemia di COVID-19 nel 2020.

Quest'anno l'evento era diviso in tre sessioni online, ciascuna delle quali seguita da una discussione. Oltre 100 membri hanno partecipato a questa importante riunione annuale.

La prima giornata della conferenza è stata dedicata in particolare all'esame dei progressi realizzati nel quadro del piano strategico dell'AMVP convenuto in occasione della 41ª Conferenza internazionale dello scorso anno a Tirana, e segnatamente all'esame dei principali obiettivi conseguiti a proposito delle tre priorità strategiche che vi erano state definite, ossia: far progredire il rispetto della vita privata su scala mondiale nell'era digitale, potenziare al massimo la voce e l'influsso dell'AMVP sulla scena internazionale e rafforzare le sue capacità.

La seconda giornata dell'evento è stata incentrata sulle sfide legate alla pandemia di COVID-19. A questo riguardo sono stati sottolineati il ruolo e il contributo essenziali del gruppo di lavoro COVID-19 dell'AMVP. Sono state discusse le attività di quest'ultimo e sono stati presentati i risultati specifici dei suoi lavori, in particolare il compendio delle migliori pratiche in risposta alla pandemia di COVID-19, che affronta ad esempio il tema del tracciamento dei contatti.

Quale primo argomento della terza giornata è stato discusso il futuro della Conferenza. In seguito sono stati comunicati i risultati del voto dei membri sui rapporti dei gruppi di lavoro, sul rapporto del Comitato esecutivo 2020 e sul rapporto della 41ª Conferenza internazionale 2019: tutti i rapporti sono stati adottati.

Il 15 ottobre 2020 sono state adottate cinque risoluzioni:

- Risoluzione sulla tecnologia del riconoscimento facciale;
- Risoluzione sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione delle crisi;
- Risoluzione sulla responsabilizzazione nello sviluppo e nell'impiego dell'intelligenza artificiale;
- Risoluzione sulle sfide legate alla protezione dei dati personali e della vita privata nel contesto della pandemia di COVID-19;
- Risoluzione sulle dichiarazioni congiunte relative alle questioni internazionali emergenti.

OCSE: gruppo di lavoro «Data Governance and Privacy in the Digital Economy»

I lavori di questo gruppo sono proseguiti anche nell'anno in rassegna, anche se la riunione del mese di novembre 2020 si è potuta tenere soltanto in maniera virtuale. A questo proposito segnaliamo due argomenti: innanzitutto la «portabilità dei dati», tema sul quale la Segreteria ha presentato uno stato intermedio in vista di un eventuale rapporto e, in secondo luogo, il rapporto della Segreteria sull'attuazione delle Linee guida dell'OCSE sulla protezione della vita privata e i flussi transfrontalieri di dati di carattere personale.

Brexit: adeguatezza della protezione dei dati

Il Regno Unito permane sulla lista degli Stati la cui legislazione assicura un'adeguata protezione dei dati conformemente alla legge svizzera sulla protezione dei dati. Dal canto suo anche il Regno Unito riconosce la Svizzera quale Paese con una protezione dei dati equivalente.

Come già spiegato nell'ultimo rapporto d'attività (cfr. 27° rapporto, n. 1.9) il 1° febbraio 2020 il Regno Unito è uscito dall'UE (Brexit), dopo qualche ritardo sulla tabella di marcia. Si è quindi posta la questione relativa all'adeguatezza reciproca in materia di protezione dei dati. L'IFPDT ha condotto numerosi colloqui al riguardo con autorità della Confederazione e rappresentanti del Regno Unito. Tali colloqui sono proseguiti a scadenze regolari durante l'anno in rassegna. Parallelamente si sono tenuti colloqui anche con rappresentanti della Commissione europea dato che per parecchio tempo non era stato chiaro se l'UE avrebbe ancora confermato l'adeguatezza del Regno Unito a partire dal 2021. D'altro canto il Regno Unito ha riconosciuto sul piano della legge l'equivalenza di tutti i Paesi che il 31 dicembre 2020 sono a loro volta stati riconosciuti come equivalenti dall'UE.

Il fatto che a fine 2020 la Commissione UE non avesse ancora preso una decisione in merito alla Svizzera significava comunque anche che l'adeguatezza di quest'ultima rimanesse riconosciuta dall'UE e che, di conseguenza, sarebbe stata automaticamente riconosciuta anche secondo il diritto del Regno Unito, verosimilmente per i quattro anni successivi. Questo non comportava però automaticamente un accordo di reciprocità da parte della Svizzera. Tuttavia, siccome durante l'anno in esame il diritto in materia di protezione dei dati del Regno Unito non è stato modificato in misure sostanziale, questo Paese permane nell'elenco degli Stati la cui legislazione assicura una protezione adeguata dei dati secondo l'articolo 6 capoverso 1 LPD. Ci riserviamo tuttavia la possibilità di un riesame, a dipendenza di come evolverà la legislazione del Regno Unito in materia di protezione dei dati.

Gruppo di lavoro sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione delle crisi

In occasione della 42ª Assemblea mondiale per la protezione della vita privata (AMVP), l'IFPDT ha presentato una risoluzione sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione delle crisi. Grazie al sostegno di 15 autorità preposte alla protezione dei dati, la risoluzione è stata adottata all'unanimità.

Questa risoluzione si prefigge di definire la posizione dei membri dell'AMVP su diversi obiettivi formulati nella sua strategia politica, in particolare su quelli che riguardano la progressione della protezione della vita privata su scala mondiale e il rafforzamento delle relazioni con altri organismi e reti internazionali che fanno progredire le questioni legate alla protezione dei dati e della vita privata.

In seguito all'adozione della risoluzione è stato deciso di istituire un gruppo di lavoro sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione delle crisi. Il gruppo di lavoro ha definito due obiettivi principali:

- rispondere alla domanda di cooperazione degli attori pertinenti al fine di sviluppare linee direttrici e scambiare le migliori pratiche in materia di protezione dei dati personali e della vita privata, tenendo conto delle specificità dell'aiuto internazionale allo sviluppo e dell'azione umanitaria internazionale, come pure della necessità di facilitare le loro attività;
- sviluppare una strategia di appello e mobilitazione presso gli attori pertinenti.

Questo gruppo di lavoro, coordinato dall'IFPDT, riunisce autorità preposte alla protezione dei dati del mondo intero, come pure il CICR e l'Organizzazione internazionale per le migrazioni.

Regolamento generale sulla protezione dei dati

Il nuovo Regolamento generale sulla protezione dei dati (RGPD) è entrato in vigore il 25 maggio 2018. A determinate condizioni, il regolamento è pure applicabile al trattamento di dati da parte delle imprese di Paesi terzi. Numerose questioni ancora aperte sono state discusse con le autorità di protezione dei dati dell'Albania, Jersey e Monaco in una riunione in Svizzera.

Il Regolamento generale sulla protezione dei dati (RGPD), adottato il 27 aprile 2016, è direttamente applicabile in tutti gli Stati membri dell'Unione europea (UE) dal 25 maggio 2018. Il suo campo d'applicazione va tuttavia oltre il territorio dell'UE. In effetti, il titolare del trattamento dei dati (o il responsabile del trattamento) è soggetto al RGPD, anche se non è stabilito nell'UE, dal momento che propone beni o servizi a persone che si trovano nell'UE o che osserva il comportamento di tali persone in particolare per analizzare le loro preferenze. Le autorità dei Paesi francofoni europei non membri dell'UE sono confrontate con le stesse sfide. Dopo una prima, proficua riunione a Monaco nel 2018, nel febbraio 2020 l'IFPDT ha organizzato un incontro a Berna allo scopo di permettere alle autorità di scambiarsi opinioni sull'entrata in vigore del RGPD, condividere le esperienze fatte e riunire le domande loro indirizzate al fine di coordinare le risposte.

Poco più di un anno dall'entrata in vigore del RGPD, il Comitato europeo per la protezione dei dati (CEPD), l'organo europeo indipendente che

contribuisce all'applicazione coerente delle regole in materia di protezione dei dati in seno all'UE, ha pubblicato le proprie linee direttrici sul campo d'applicazione del RGPD. Le linee direttrici erano state dapprima poste in consultazione pubblica, alla quale l'IFPDT aveva partecipato in collaborazione con l'autorità monegasca di protezione dei dati (CCIN - Commission de contrôle des informations nominatives) al fine di chiedere il chiarimento di un certo numero di elementi su tale questione della massima importanza per i Paesi terzi integrati nell'area dell'UE. Quest'ultima versione è pure stata analizzata e discussa in occasione dell'incontro. Occorre comunque constatare che diverse questioni restano ancora aperte.

Gruppi di coordinamento della vigilanza sui sistemi d'informazione SIS II, VIS ed Eurodac

Nell'anno in rassegna i gruppi di coordinamento della vigilanza hanno svolto le loro due sedute in videoconferenza. Hanno discusso tra l'altro di come ovviare alla difficoltà di trovare un numero sufficiente di esperti tra le autorità di protezione dei dati per effettuare le valutazioni Schengen.

Anche quest'anno l'IFPDT ha partecipato, quale autorità di vigilanza nazionale, alle sedute dei tre gruppi di coordinamento della vigilanza sui sistemi d'informazione dell'UE SIS II, VIS (IFPDT presidente) ed Eurodac. Le sedute si sono svolte il 17 e 18 giugno 2020 e il 25 e 26 novembre 2020 in videoconferenza. Erano rappresentati il Garante europeo della protezione dei dati (GEPD) e le autorità nazionali di protezione dei dati degli Stati membri.

I gruppi di coordinamento della vigilanza SIS e VIS si sono interrogati tra l'altro sul perché per la valutazione Schengen effettuata dalla Commissione UE in materia di protezione dei dati sia difficile mettere a disposizione un numero sufficiente di esperti tra le diverse autorità di protezione dei dati. Nel gennaio 2021 la Commissione UE, che sta riesaminando la procedura delle valutazioni Schengen, ha organizzato una videoconferenza sull'argomento con le autorità di protezione dei dati degli Stati membri Schengen e con il Garante europeo della protezione dei dati. Lo scambio sulle possibili cause e sulle possibilità di miglioramento è stato costruttivo. Entrambe le parti esamineranno l'opportunità di formare un pool di esperti nella protezione dei dati per le valutazioni Schengen. La Commissione UE introdurrà inoltre, se possibile, una formazione continua per il futuro personale specializzato nelle valutazioni in materia di protezione dei dati. Nella sua seduta del 18 giugno 2020 il gruppo di coordinamento della vigilanza VIS ha confermato per altri due anni la rappresentante dell'Incaricato quale presidente del gruppo di coordinamento.

Principio di trasparenza

2.1 In generale

La pandemia da coronavirus ha avuto effetti anche sull'applicazione del principio di trasparenza nell'Amministrazione federale. I media e la società hanno espresso la forte esigenza di avere informazioni specifiche e trasparenti su documenti riguardanti il coronavirus. Di conseguenza, le singole autorità si sono trovate confrontate a un gran numero di domande di accesso, tra cui domande voluminose e complesse che spesso hanno reso necessario un coordinamento tra gli Uffici o addirittura i Dipartimenti. Nel complesso, è emerso che nei periodi di pandemia l'applicazione del principio di trasparenza può essere un impegno e una sfida. Se da un lato l'Amministrazione, che opera in tempi ristretti, è soggetta ad aspettative elevate e a critiche successive da parte dell'opinione pubblica, dall'altro i richiedenti auspicano un accesso rapido e completo, così da poter capire le azioni dello Stato nella lotta contro la pandemia, in parte basate su competenze in materia di diritto di necessità. Tuttavia, le statistiche dimostrano che, nonostante gli affari ordinari talvolta urgenti durante l'anno pandemico, nella maggior parte dei casi le autorità federali sono riuscite ad attuare con successo il principio di trasparenza nell'Amministrazione.

Dai dati riportati più avanti (cfr. cap. 2.2) si evince inoltre che sono confermate anche per l'anno in esame le tendenze osservate negli ultimi anni, ossia un aumento continuo delle domande di accesso e una quota di casi per lo più costantemente elevata nei quali l'accesso è stato concesso integralmente.

Introdotta dall'Incaricato nel 2017, la primazia delle mediazioni orali è di nuovo risultata efficace nel 2020. Il fatto che a prima vista i numeri sembrino confermarlo soltanto in parte dipende dagli adeguamenti nella procedura di mediazione dovuti alla pandemia. Quando, considerata l'ulteriore diffusione del coronavirus, nella sua seduta del 16 marzo 2020 il Consiglio federale ha introdotto l'obbligo del telelavoro e vietato gli assembramenti di oltre cinque persone, l'Incaricato si è visto costretto, per ragioni di salute pubblica e per tutelare la salute delle parti interessate, a rinunciare alle sedute di mediazione durante la prima diffusione della pandemia (tra marzo e giugno 2020), come pure durante la seconda ondata.

Per i motivi summenzionati, in numerosi casi si sono dovute svolgere procedure di mediazione scritte. Nell'anno di riferimento, tale procedura ha portato, da una parte, a una minore percentuale di soluzioni consensuali e, dall'altra, a tempi di elaborazione più lunghi e a un conseguente ritardo nello sbrigare le procedure. Gli effetti negativi dello svolgimento scritto delle procedure di mediazione sulla durata di elaborazione e sui risultati della procedura sono precisati nel capitolo 2.3.

Il rispetto del termine legale di 30 giorni per svolgere le procedure di mediazione non costituisce una sfida soltanto in tempi di pandemia. L'esperienza insegna che il termine è spesso superato nelle procedure complesse con tre o più parti coinvolte e riguardanti domande di accesso a documenti con informazioni rilevanti ai fini del segreto d'affari o relative alla protezione della personalità di privati.

Ai fini dello svolgimento della procedura, le autorità sono tenute a fornire all'Incaricato i documenti richiesti e, in cambio, questi sottostà al segreto d'ufficio nella stessa misura delle autorità. Di norma le autorità trasmettono la documentazione all'Incaricato senza difficoltà. Non sempre tuttavia la cooperazione risulta ottimale. È esemplare in tal senso un caso riguardante l'obbligo di cooperazione nella procedura di mediazione. In virtù del principio di trasparenza dell'Amministrazione federale sancito dalla legge sulla trasparenza (LTras) non si lascia più alla discrezione dell'Amministrazione decidere se vuole rendere accessibili o meno le informazioni e i documenti ufficiali. Le autorità sono tenute a cooperare nella procedura di mediazione e, per legge, devono trasmettere all'Incaricato tutti i documenti oggetto di una domanda. Nel caso in questione, l'autorità si è rifiutata di trasmettergli i documenti oggetto della controversia, obiettando che non rientravano nel campo di applicazione della legge

sulla trasparenza. Poiché l'autorità, cui incombe l'onere della prova, ha negato a sua discrezione l'applicabilità della legge sulla trasparenza, l'Incaricato si è trovato nell'impossibilità di verificare la qualità dei documenti di cui all'articolo 5 LTras e di valutare la sussistenza di motivi di non entrata nel merito e di eccezione, addotti dalla predetta autorità. Di conseguenza, l'Incaricato si è visto costretto a raccomandare il pieno accesso ai documenti richiesti, in quanto l'autorità che non è disposta a confutare la presunzione giuridica dell'accesso a documenti ufficiali mostrandoli all'autorità di mediazione non può trarre vantaggio dal suo comportamento (v. raccomandazione del 28 gennaio 2021).

Come già in precedenza, si constatano tentativi dell'Amministrazione per limitare ulteriormente il principio della trasparenza introducendo eccezioni in nuove disposizioni legali. È stato il caso nell'anno in rassegna con la legge sulle fideiussioni solidali COVID-19 (v. cap. 2.4).

2.2 Domande di accesso: nuovo aumento nel 2020

Secondo i dati comunicatici dalle autorità federali, se nel 2019 sono pervenute 916 domande di accesso, nell'anno in esame (1° gennaio – 31 dicembre 2020) ne sono pervenute 1193, pari a un aumento del 30 per cento. Sono state conteggiate anche le domande di accesso presentate dal Ministero pubblico della Confederazione (13) e dai Servizi del Parlamento (6).

Uno dei motivi dell'aumento risiede nella marcata necessità di rendere più comprensibile l'azione del Governo nella lotta contro la pandemia da coronavirus. Secondo i dati forniti dalle autorità federali, 308 delle 1193 domande di accesso (26 %) erano connesse all'argomento «coronavirus». Le autorità sono state in grado di rilevare statisticamente le domande di accesso ai documenti riguardanti tale argomento. Dalla statistica, riportata separatamente (v. cap. 3.3), risulta che l'accesso completo è stato concesso in 121 casi (39 %), ossia con minore frequenza rispetto alla statistica complessiva (v. sotto), mentre nel caso dell'accesso negato completamente (risp. 38 e 12 %) si è constatata una quota soltanto leggermente superiore rispetto alla statistica complessiva.

All'aumento del numero di domande di accesso presentate potrebbe anche aver contribuito il fatto che, grazie alle notizie riportate dai media, nel corso degli anni la popolazione ha imparato a conoscere sempre meglio la legge sulla trasparenza e ne sfrutta sempre più attivamente le possibilità. L'Incaricato si aspetta che tale tendenza perdurerà nei prossimi anni.

In 610 casi (51 %), le autorità hanno concesso l'accesso completo (contro, rispettivamente, 542 e 59 % l'anno prima), mentre per 293 domande (25 %) è stato autorizzato un accesso ai documenti parziale o differito. In 108 casi (9 %) l'accesso è stato negato completamente e, secondo le autorità, 35 domande di accesso (3 %) sono state ritirate, 80 domande erano ancora pendenti a fine 2020 e in 67 l'autorità non disponeva dei documenti richiesti. Dal 2015, in oltre il 50 per cento dei casi è stato autorizzato un accesso completo. Per contro, gli accessi negati completamente sono in minoranza e si attestano sul 10 per cento nel corso degli anni.

Rispetto agli anni precedenti si può constatare che, in generale, nell'anno del coronavirus la quota di autorizzazioni di accesso completo è diminuita dell'otto per cento, mentre quella di autorizzazioni di accesso parziale o di differimento di accesso è aumentata del sei per cento. Una spiegazione per tali cambiamenti sta nel fatto che, quanto alle domande di accesso ai documenti riguardanti il coronavirus (circa un quarto del totale), in percentuale le autorità hanno concesso meno spesso un accesso completo, mentre più di frequente l'hanno negato parzialmente, differito o negato completamente.

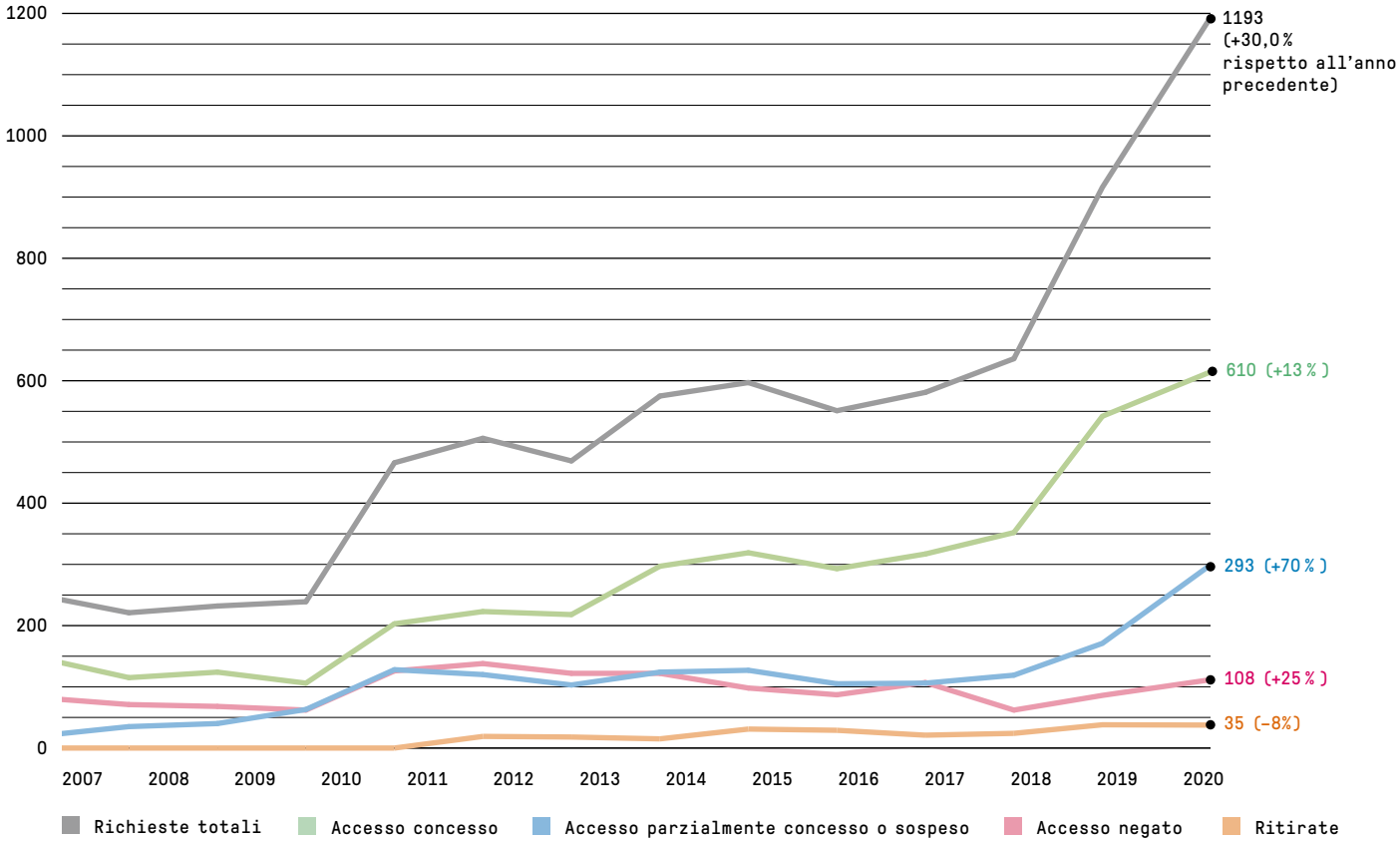
Dipartimenti e Uffici federali

A causa della pandemia da coronavirus, nel 2020 alcune unità amministrative hanno attirato una particolare attenzione dei media e della società. Dati i compiti che svolgono, sono stati soprattutto l'UFSP, il DDPS e il DFF a trovarsi confrontati a un gran numero di domande di accesso. Secondo tali autorità, si trattava in parte di domande molto voluminose e complesse. In un gran numero di casi è stato necessario un intenso coordinamento amministrativo interno tra gli Uffici o i Dipartimenti, ad esempio per i documenti riguardanti l'acquisto di materiale medico. Per ovvie ragioni, il trattamento è risultato più dispendioso rispetto agli anni precedenti.

Per quanto riguarda gli Uffici federali, i dati riportati mostrano che nel 2020, con 181 casi, l'UFSP ha segnalato il maggior numero di domande di accesso, di cui ben 134 riguardavano documenti rilevanti per il coronavirus (v. cap. 3.3). Seguono l'UFSPO con 150, swissmedic con 42 e l'UFAM con 38 domande. Per quanto riguarda i Dipartimenti, sono in testa il DFI (312) e il DDPS (251). Per contro, 13 autorità hanno segnalato di non avere ricevuto alcuna domanda di accesso nell'anno di riferimento. All'Incaricato sono giunte dieci domande di accesso e in otto casi ha concesso l'accesso completo. In un caso non c'era alcun documento pertinente e in un caso la domanda era ancora pendente a fine 2020.

L'importo degli emolumenti riscossi nel 2020 per l'accesso ai documenti ufficiali ammonta a un totale di 15 189 franchi, inferiore così a quello dell'anno precedente (18 185 franchi). Soltanto per due domande di accesso a documenti riguardanti il coronavirus è stato richiesto complessivamente un emolumento di 450 franchi.

Figura 1: valutazione delle domande di accesso – evoluzione dal 2006



Mentre il DFGP e la Cancelleria federale non hanno riscosso alcun emolumento, i sei Dipartimenti restanti hanno fatturato ai richiedenti una parte del tempo impiegato (DFI: 4643 franchi; DEFR: 3786 franchi; DATEC: 3310 franchi; DFF: 1900 franchi; DFAE: 900 franchi; DDPS: 650 franchi). Si noti al riguardo che è stato riscosso un emolumento unicamente per 25 delle 1193 domande di accesso presentate. Rispetto all'anno prima, in cui in 31 casi era stato richiesto un emolumento, ciò rappresenta un calo, sia quanto al numero di casi nei quali è stato riscosso un emolumento, sia quanto all'importo totale degli emolumenti. Queste osservazioni sono degne di nota nel senso che il numero di domande di accesso è (di nuovo) aumentato in modo considerevole. Come già negli anni precedenti, la riscossione di emolumenti rimane un'eccezione: in circa il 98 per cento delle domande di accesso non è stato percepito alcun emolumento. La prassi amministrativa suffraga quindi il principio dell'esenzione dagli emolumenti nell'accesso ai documenti ufficiali proposto dalla Commissione delle istituzioni politiche del Consiglio nazionale (cfr. cap. 2.4, parere dell'IFPDT).

Per quanto riguarda il tempo impiegato per il trattamento delle domande di accesso, l'Incaricato rammenta che le autorità non sono tenute a registrarle e che non esistono prescrizioni applicabili all'intera Amministrazione federale per una registrazione uniforme. I dati fornitigli rispecchiano quindi soltanto in parte le ore di lavoro effettivamente prestate. Secondo questi dati, il tempo impiegato nell'anno di riferimento, ovvero 5010 ore, è aumentato rispetto al 2019 (4375 ore).

L'incremento del numero di domande di accesso (30 %) non ha quindi avuto la stessa incidenza sull'aumento del tempo impiegato (15%). È parimenti aumentato il tempo impiegato comunicato per la preparazione di procedure di mediazione: 569 ore (rispetto alle 473 del 2019).

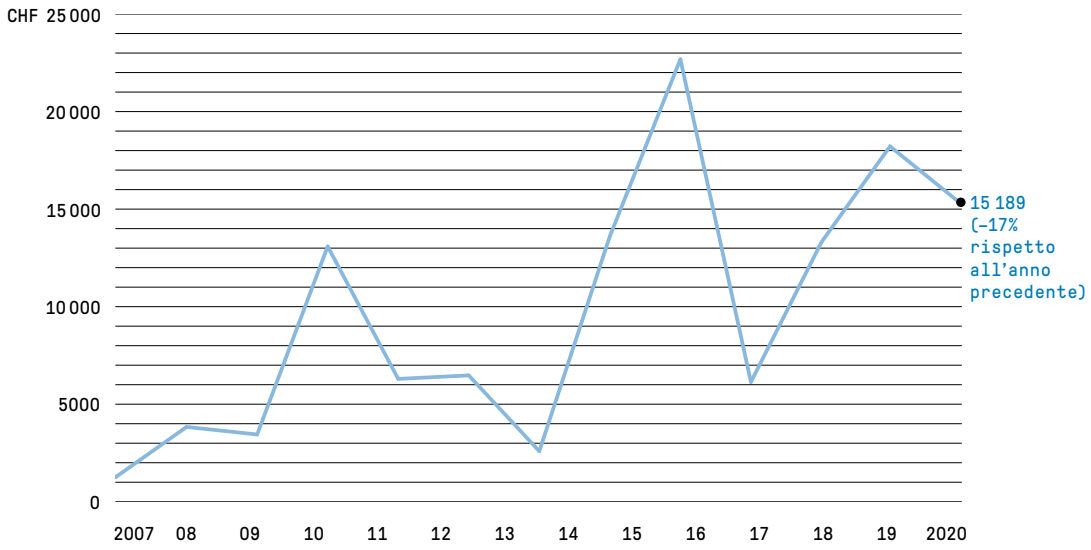
Servizi del Parlamento

I Servizi del Parlamento hanno comunicato di aver ricevuto sei domande di accesso. A parte un caso i Servizi non disponevano del documento richiesto, le altre cinque domande sono state integralmente respinte.

Ministero pubblico della Confederazione

Il Ministero pubblico della Confederazione ha comunicato la ricezione di 13 domande per il 2020. In sei casi la domanda di accesso è stata soddisfatta integralmente, mentre in un caso l'accesso è stato completamente negato. Quanto alle altre richieste, in due casi non erano disponibili documenti ufficiali e quattro casi erano ancora pendenti alla fine dell'anno di riferimento.

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



2.3 Procedure di mediazione – meno richieste di mediazione

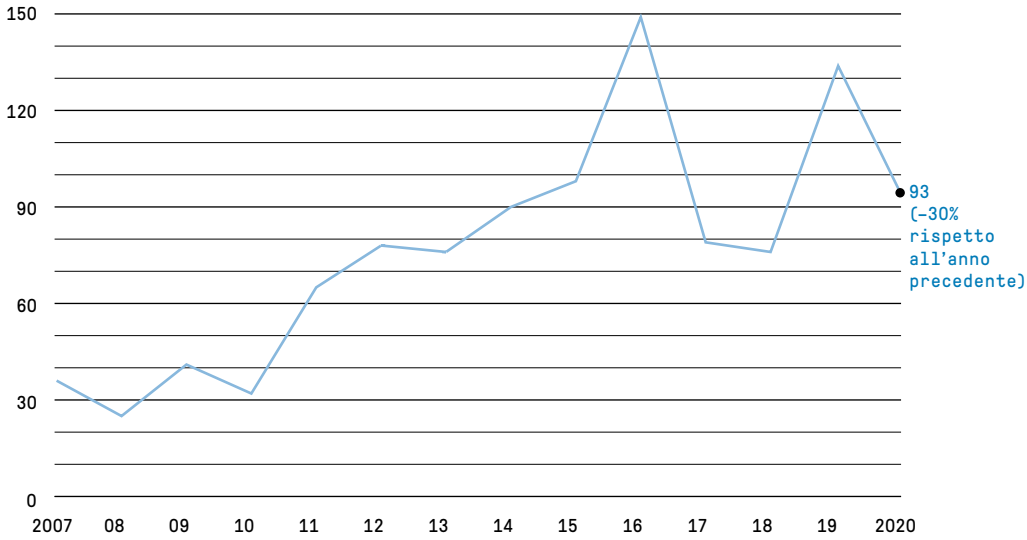
Nel 2020 all'Incaricato sono state presentate 93 richieste di mediazione, un calo del 30 per cento rispetto alle 133 ricevute nel 2019 (di cui 28 procedure riguardavano lo stesso oggetto). La maggior parte è stata presentata da privati (42) e da giornalisti (31). Da tali cifre si può concludere che nei 401 casi in cui l'Amministrazione federale ha integralmente o parzialmente rifiutato l'accesso, per 93 volte o nel 23 per cento dei casi in cui la domanda è stata respinta sul merito è stata presentata una richiesta di mediazione all'Incaricato. Di queste richieste, 24 (26 %) riguardavano documenti ufficiali legati al coronavirus.

Nel 2020 sono state evase 119 richieste di mediazione, di cui 79 pervenute nello stesso anno e 40 in quello precedente. In 40 casi è stato possibile trovare una soluzione consensuale. L'Incaricato ha inoltre emesso 27 raccomandazioni che hanno portato alla conclusione di 55 casi per i quali non è stato possibile raggiungere un accordo.

Tra i casi risolti vanno annoverate anche 11 richieste che non sono state presentate entro il termine previsto, 12 casi in cui non sono stati soddisfatti i requisiti per l'applicazione della legge sulla trasparenza e una richiesta di mediazione che è stata ritirata.

A fine anno otto procedure risultavano sospese in, previa grazie a un'intesa tra le parti.

Figura 3: richieste di mediazione dall'entrata in vigore della LTras



Percentuale di soluzioni consensuali

Lo svolgimento delle sedute di mediazione presenta numerosi vantaggi poiché consente di accelerare la procedura di accesso ai documenti o di creare le basi per un'eventuale collaborazione futura tra i partecipanti.

L'efficacia delle misure introdotte nel 2017 e dello svolgimento delle sedute di mediazione è dimostrata regolarmente dalla proporzione esistente tra le soluzioni consensuali e le raccomandazioni.

Nell'anno in rassegna sono state raggiunte 40 soluzioni consensuali e l'Incaricato ha emesso 27 raccomandazioni per risolvere 55 casi, il che corrisponde al 34 per cento di soluzioni consensuali rispetto alle raccomandazioni, percentuale nettamente inferiore rispetto agli anni precedenti (v. tabella 1).

Come già menzionato nel capitolo 2.1, la pandemia da coronavirus ha fatto sì che nel periodo tra marzo e giugno 2020 in 13 casi si è dovuto rinunciare a svolgere le sedute di mediazione. Una soluzione consensuale può essere raggiunta, di norma, soltanto se si svolge una seduta di mediazione. Nell'anno in esame, nelle 40 sedute di mediazione che si sono potute svolgere è stato così raggiunto un accordo in 24 casi (60 %), il che corrisponde ai valori degli anni precedenti.

Le apparentemente numerose (rispetto agli anni precedenti) procedure di mediazione in cui il delegato ha emesso una raccomandazione sono dovute principalmente a un'anomalia statistica: in due domande di accesso, un numero insolitamente elevato di terzi interessati ha presentato una richiesta di mediazione (in un caso 10 e in un altro 18 terzi interessati). Da queste 28 richieste di mediazione risulta oltre la metà di tutti i casi conclusi con una raccomandazione.

In conclusione, l'Incaricato constata che le udienze di mediazione orali continuano a risultare efficaci per giungere a soluzioni rapide e consensuali. In alcuni casi, alla luce di provvedimenti inerenti alla pandemia da coronavirus, le parti hanno chiesto di sospendere la procedura fino al momento in cui saranno di nuovo possibili mediazioni orali.

L'IFPDT pubblica l'insieme delle raccomandazioni sul proprio sito Internet.

Tabella 1: soluzioni consensuali

2020	**34 %**
2019	61 %
2018	55 %

Durata della procedura di mediazione

La tabella 2 è suddivisa in quattro colonne in base alla durata della procedura. Si noti che questa durata di elaborazione non tiene conto del periodo di tempo durante il quale una procedura viene sospesa previo accordo dei partecipanti. La sospensione della procedura di mediazione si verifica in particolare quando, dopo la seduta, un'autorità desidera riconsiderare la propria posizione o deve consultare i terzi interessati. Se la seduta viene rinviata su richiesta di una parte interessata (p. es. a causa di assenza per vacanze, malattia ecc.), il periodo che intercorre tra il termine previsto inizialmente e il nuovo termine fissato o il conseguente prolungamento della procedura non viene considerato della procedura.

La tabella 2 mostra che il 43 per cento delle procedure di mediazione concluse nel 2020 è stato risolto entro il termine legale di 30 giorni. Nel 30 per cento dei casi la procedura è durata tra 31 e 99 giorni e nel 27 per cento dei casi addirittura più di 100 giorni. Il superamento del termine è stato spesso causato dall'assenza di persone o autorità interessate (vacanze, malattia, spostamenti), dal numero elevato di terzi coinvolti nella procedura o dalla complessità delle questioni giuridiche trattate, a cui nell'anno in rassegna si sono aggiunti impedimenti delle parti nonché del proprio personale dovuti al coronavirus. Queste spiegazioni valgono anche per i 32 casi (di cui dieci procedure, in un caso, e 18 in un altro, in cui le procedure sono state riunite) che hanno superato i 100 giorni di trattamento. A ciò si aggiunge anche il fatto che il rispetto del termine è stato reso ulteriormente difficile a causa di consultazioni all'estero, di molteplici tentativi di mediazione tra i partecipanti e del numero di documenti o persone coinvolte. Occorre notare che le situazioni summenzionate comportano spesso un trattamento particolarmente dispendioso e che in tali casi l'Incaricato può concedere una proroga ragionevole del termine stabilito all'articolo 12ª dell'ordinanza sul principio di trasparenza dell'amministrazione (OTras; RS 152.31). Nell'anno in esame sono state

Tabella 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
entro 30 giorni	11 %	59 %	50 %	57 %	43 %
da 31 a 99 giorni	45 %	37 %	50 %	38 %	30 %
più di 100 giorni	44 %	4 %	0 %	5 %	27 %

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

concesse varie proroghe dei termini nella procedura di mediazione alle autorità fortemente colpite dalla pandemia da coronavirus.

Di norma, il termine legale di 30 giorni per lo svolgimento della procedura di mediazione può essere rispettato se le sedute di mediazione vengono concluse con successo mediante un accordo, ossia senza una richiesta di rinvio da parte degli interessati, entro il termine successivo al ricevimento della domanda. Se non si raggiunge un accordo, l'Incaricato non riesce sempre a trasmettere la propria raccomandazione scritta alle parti entro 30 giorni dal ricevimento della domanda.

Dall'aumento della quota di procedure di mediazione scritte e di raccomandazioni dovuto alla pandemia è scaturito, per l'Incaricato, un carico di lavoro nettamente maggiore. Questo, a sua volta, ha allungato la durata delle procedure e portato a ritardi. Visto il nuovo confinamento all'inizio del 2021, l'Incaricato si aspetta che aumenteranno ancora.

Inoltre, anche nell'anno in rassegna vi sono stati casi in cui i terzi consultati hanno fatto ricorso a una rappresentanza legale sin dalla procedura di accesso e poi di mediazione, il che non favorisce, di norma, una soluzione semplice, pragmatica e rapida.

Numero di casi pendenti

I dati riportati di seguito forniscono informazioni sul numero di casi pendenti alla fine dei rispettivi anni in esame. All'inizio di gennaio del 2021 erano pendenti 17 procedure di mediazione, di cui otto sospese (tre risalenti al 2019, cinque al 2020). Sette casi sono stati conclusi prima della chiusura di redazione del presente rapporto.

Tabella 3: procedure di mediazione pendenti

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 a febbraio 2019 e 2 sospese)

2.4 Procedura legislativa

CORONA

Procedura legislativa ai fini della trasposizione dell'ordinanza sulle fideiussioni solidali COVID-19 nella legge sulle fideiussioni solidali COVID-19

Secondo la legge sulle fideiussioni solidali COVID-19, nell'ambito del programma di fideiussioni della Confederazione devono essere mantenuti segreti l'identità e le coordinate bancarie delle imprese e delle persone, nonché gli importi concessi o negati loro. Durante l'iter legislativo, l'Incaricato si era pronunciato, senza successo, contro tale limitazione del principio di trasparenza.

Il 25 marzo 2020, con l'introduzione di un'ordinanza di necessità con validità limitata, il Consiglio federale ha reso possibile un rapido accesso a finanziamenti transitori per numerose imprese, al fine di garantire la liquidità necessaria alla gestione della crisi causata dalla pandemia. I contenuti di questa ordinanza di necessità sono stati trasposti in una legge federale urgente e di durata limitata approvata dal Parlamento nel dicembre 2020.

Secondo l'articolo 12 capoverso 2 della legge sulle fideiussioni solidali COVID-19 (LFiS-COVID-19), non possono essere comunicati i dati personali e le informazioni delle imprese e delle persone che richiedono un credito e di quelle che lo ricevono, qualora ne contengano l'identità e le coordinate bancarie, nonché gli importi concessi o negati. Secondo il messaggio concernente la LFiS-COVID-19 si tratta di una disposizione speciale ai sensi dell'articolo 4 LTras, con conseguente esclusione di tali informazioni dal campo di applicazione della legge sulla trasparenza, per cui non sono disponibili in seguito a domanda di accesso.

L'Incaricato si era espresso contro l'introduzione di questa disposizione speciale sia nella consultazione sulla LFiS-COVID-19, sia nella successiva consultazione degli uffici concernente il messaggio e il disegno di legge. Ha altresì segnalato gli obiettivi perseguiti dalla legge sulla trasparenza, quali comprendere l'operato dell'Amministrazione o prevenirne la cattiva gestione e la corruzione. Considerato l'impiego di 40 miliardi di franchi di imposte, a giudizio dell'Incaricato non era opportuno il mantenimento incondizionato del segreto sulle informazioni in questione. Se i prestiti concessi generano perdite, queste devono essere coperte dalle imposte. Di fronte alle osservazioni a posteriori formulate nei confronti dell'operato dell'Amministrazione in relazione alle fideiussioni concesse nella navigazione d'alto mare, l'Incaricato si stupisce che il Parlamento abbia sancito nella legge approvata il 19 dicembre 2020 il mantenimento del segreto proposto dal Consiglio federale.

Durante la procedura di consultazione l'Incaricato aveva mostrato, invano, che i legittimi interessi privati rimangono tutelati anche in caso di applicazione della legge sulla trasparenza. Essa garantisce ad esempio esplicitamente la tutela dei segreti d'affari (art. 7 cpv. 1 lett. g LTras) e della sfera privata nonché dei dati personali di persone fisiche e giuridiche (art. 7 cpv. 2 LTras, art. 9 cpv. 2 LTras nonché art. 19 LPD). L'Incaricato ha inoltre spiegato che, secondo la dottrina e la giurisprudenza, il segreto bancario prevale sulla legge sulla trasparenza. Sempre senza successo, nel suo parere l'Incaricato ha segnalato la legge federale sugli aiuti finanziari e le indennità (legge sui sussidi) e la legge federale sugli aiuti finanziari alle organizzazioni che concedono fideiussioni alle piccole e medie imprese. Sebbene entrambe le leggi presentino evidenti analogie con il presente progetto, non prevedono alcuna disposizione speciale ai sensi dell'articolo 4 LTras.

Consultazione degli uffici sulla bozza del parere del Consiglio federale sul rapporto del 15 ottobre 2020 della Commissione delle istituzioni politiche del Consiglio nazionale concernente l'iniziativa parlamentare 16.432 Graf-Litscher. Disciplinamento degli emolumenti. Principio della trasparenza nell'amministrazione federale

La Commissione delle istituzioni politiche del Consiglio nazionale ha elaborato un progetto che prevede di norma la gratuità dell'accesso ai documenti ufficiali e la riscossione di un emolumento soltanto in casi eccezionali. Il Consiglio federale vorrebbe fissare l'importo massimo dell'emolumento nell'ordinanza. L'Incaricato è invece dell'opinione che l'importo massimo vada iscritto direttamente nella legge sulla trasparenza.

L'iniziativa parlamentare 16.432 «Disciplinamento degli emolumenti. Principio della trasparenza nell'amministrazione federale» chiede che le basi legali nella legge sulla trasparenza siano modificate in modo tale da rendere, di norma, gratuito l'accesso ai documenti ufficiali.

La competente Commissione delle istituzioni politiche del Consiglio nazionale (CIP-N) ha quindi adottato un progetto preliminare di modifica della legge sulla trasparenza che, dopo la consultazione, ha rielaborato e sottoposto al Consiglio nazionale. Il progetto mira a introdurre nella legge il principio della gratuità dell'accesso ai documenti ufficiali. Quale unica eccezione un emolumento potrà essere riscosso «se una domanda richiede un trattamento particolarmente dispendioso da parte dell'autorità». Secondo la maggioranza della Commissione, nella legge sulla trasparenza andrebbe fissato un emolumento massimo di 2000 franchi, mentre il Consiglio federale dovrebbe disciplinare i dettagli e il tariffario adeguato all'onere. Una minoranza della Commissione vuole invece lasciare al Consiglio federale il compito di fissare il tetto massimo per l'emolumento.

L'Incaricato ha sostenuto la proposta della maggioranza della Commissione di fissare un importo massimo direttamente nel testo di legge, perché questo livello garantirebbe che la riscossione di emolumenti in via eccezionale non assuma proporzioni tali da finire per diventare un ostacolo all'accesso ai documenti ufficiali. Ora che il Consiglio federale si è espresso contro l'inserimento di un tetto massimo nella legge, spetta al Consiglio nazionale prendere una decisione.

Revisione della legge federale sulla promozione della ricerca e dell'innovazione (LPRI). Consultazioni degli uffici nell'ambito dei lavori preparatori per il messaggio del Consiglio federale

Durante la consultazione relativa alla revisione della LPRI è stato chiesto di inasprire il disciplinamento in materia di comunicazione dei nomi dei relatori e dei periti scientifici nell'ambito della procedura di ricorso. L'Incaricato tuttavia vi si oppone.

Nei ricorsi presentati a causa della mancata concessione di contributi per la ricerca, l'articolo 13 capoverso 4 LPRI prevede che il ricorrente riceva, su richiesta, i nomi dei relatori e dei periti scientifici soltanto previo loro consenso. Nella sua sentenza A-6160/2018 del 4 novembre 2019 inerente a un ricorso in virtù della legge sulla trasparenza (LTras) il Tribunale amministrativo federale (TAF) ha interpretato l'articolo 13 capoverso 4 LPRI nel senso che i nomi menzionati possono essere comunicati a ulteriori persone non coinvolte se i relatori e i periti scientifici interessati hanno dato il loro esplicito consenso. Secondo il TAF, è pur vero che si tratta di una disposizione speciale ai sensi dell'articolo 4 LTras e che pertanto quest'ultima legge non si applica. Sempre secondo il Tribunale, l'articolo 13 capoverso 4 LPRI non costituisce tuttavia un obbligo generale di mantenere il segreto.

Nell'ambito della consultazione relativa alla revisione della LPRI, il Fondo nazionale svizzero (FNS) ha chiesto di limitare il disciplinamento in materia di comunicazione dei nomi

così che soltanto i ricorrenti possano chiedere la comunicazione dei nomi in questione. In seguito, l'Incaricato si è adoperato con successo nei confronti della Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI), competente in materia, affinché tale richiesta non fosse inserita nel progetto.

Nel messaggio del Consiglio federale del 17 febbraio 2021 si è rinunciato alla richiesta limitazione del disciplinamento in materia di comunicazione dei nomi.

Revisione parziale della LAMal concernente misure di contenimento dei costi (pacchetto 2)

L'Ufficio federale della sanità pubblica (UFSP) elabora una revisione parziale della LAMal concernente misure di riduzione dei costi. Tale progetto prevede, tra l'altro, di escludere dal principio di trasparenza tutti i documenti riguardanti i modelli di prezzo dei medicamenti nell'assicurazione malattie. L'Incaricato si oppone a questo proposito.

Nel 27° rapporto d'attività 2019/20 l'Incaricato aveva riferito in merito a una consultazione da avviare, che si è ora svolta nell'anno in esame, su una revisione parziale della legge sull'assicurazione malattie. L'Incaricato si era opposto al progetto dell'UFSP di abrogare il diritto di accesso del pubblico ai documenti relativi alla fissazione dei prezzi dei medicamenti. L'Incaricato ritiene che i prezzi effettivi dei medicamenti rimborsati dall'assicurazione obbligatoria delle cure medico-sanitarie e i documenti che servono a determinare il prezzo debbano rimanere a disposizione del pubblico. Ne risulterebbe altrimenti una prassi poco chiara quanto ai criteri di ammissione nell'elenco delle specialità e dei successivi riesami di tali criteri, nonché al meccanismo di rimborso. Sia per la popolazione, sia per le imprese concorrenti dovrebbe continuare a essere possibile comprendere e controllare pienamente la prassi di approvazione dell'UFSP.
Il risultato della consultazione non è ancora noto al momento della chiusura di redazione.

Nell'anno in rassegna l'Incaricato ha svolto una procedura di mediazione su documenti dell'UFSP relativi alla fissazione dei prezzi dei medicamenti nell'assicurazione malattie obbligatoria. Concretamente, è stato chiesto l'accesso alle informazioni relative ai medicamenti con modelli di prezzo. Non essendo giunti a un accordo tra l'UFSP e il richiedente nella procedura di mediazione, l'Incaricato ha dovuto emanare una raccomandazione scritta (raccomandazione del 6 gennaio 2021). L'UFSP ha motivato il suo rifiuto di fornire i documenti richiesti principalmente sostenendo che senza il mantenimento del segreto non può più essere garantita la sicurezza dell'approvvigionamento di medicamenti innovativi e onerosi. Nella sua raccomandazione l'Incaricato ha osservato, tra l'altro, che a suo parere la vigente legge sulla trasparenza non lascia spazio per procedere previamente alla modifica di legge auspicata dal Consiglio federale. Poiché l'UFSP non è stato in grado di dimostrare la sussistenza di motivi di eccezione secondo la suddetta legge e non ha così potuto confutare la presunzione giuridica dell'accesso alle informazioni richieste, l'Incaricato ha raccomandato il pieno accesso.

Nuova legge federale sulla parte generale della riscossione dei tributi e sul controllo del traffico transfrontaliero di merci e persone da parte dell'Ufficio federale della dogana e della sicurezza dei confini (legge sui compiti d'esecuzione dell'UDSC)

Nell'ultimo trimestre del 2020 l'Amministrazione federale delle dogane (AFD) ha svolto una procedura di consultazione ai fini dell'introduzione di una nuova legge sui compiti d'esecuzione dell'UDSC. Questo avamprogetto non contiene più alcuna limitazione al principio di trasparenza.

Nel 27° rapporto d'attività 2019/2020 l'Incaricato ha riferito in merito alla consultazione degli Uffici per l'apertura della procedura di consultazione su una nuova legge federale sulle dogane e sulla sicurezza dei confini. Il progetto di legge è stato rielaborato dopo la consultazione degli Uffici e riporta ora la denominazione «legge federale sulla parte generale della riscossione dei tributi e sul controllo del traffico transfrontaliero di merci e persone da parte dell'Ufficio federale della dogana e della sicurezza dei confini» (legge sui compiti d'esecuzione dell'UDSC). L'AFD ha tenuto conto delle preoccupazioni dell'Incaricato e ha stralciato le limitazioni al principio di trasparenza previste inizialmente. La procedura di consultazione si è svolta soltanto nell'attuale anno in esame.

L'IFPDT

3.1 Compiti e risorse

CORONA

Pandemia

I progetti di trattamento di dati per lotta all'attuale pandemia, realizzati a breve termine a causa della crisi sanitaria, e la maggiore richiesta di documenti pubblici hanno sollecitato tutto il personale in modo straordinario.

In quanto unità della Confederazione, aggregata sul piano amministrativo alla Cancelleria federale, l'IFPDT ha attuato tutte le prescrizioni del Consiglio federale volte a proteggere i propri collaboratori dalla pandemia. Nell'anno in rassegna il personale dell'IFPDT ha pertanto svolto da casa la maggior parte del lavoro. Gli incontri personali si sono limitati a poche settimane, il che ha reso difficile in particolare l'introduzione dei nuovi collaboratori e la loro assistenza.

Prestazioni e risorse nell'ambito della protezione dei dati

Effettivi del personale

Tra il 2005 e il 2019 l'effettivo del personale per l'esecuzione della legge federale sulla protezione dei dati (LPD) ha conosciuto una fluttuazione di 20–24 posti a tempo pieno. Le oscillazioni si spiegano da un lato con l'entrata in vigore della legge sulla trasparenza (LTras) nel 2006. Visto che i posti previsti a tal fine non sono mai stati autorizzati dal Consiglio federale, la nostra autorità ha dovuto far capo al personale esistente presso l'IFPDT e in parte alle risorse della Cancelleria federale. Dall'altro lato, per motivi di risparmio generali non è stato possibile reclutare tutto il personale destinato ai posti supplementari autorizzati nel contesto dell'adesione all'Accordo di Schengen e Dublino e dell'emanazione di leggi speciali nel settore sanitario.

Nel messaggio concernente la revisione totale della LPD il Consiglio federale aveva prospettato all'IFPDT la creazione di risorse supplementari nella misura di 9–10 posti (FF 2017 6154). Nel frattempo, con la nuova legge sulla protezione dei dati in ambito Schengen (LPDS, RS 235.3) il legislatore federale ha anticipato un aspetto parziale della revisione totale della LPD. Dopo aver posto in vigore la nuova legge al 1° marzo 2019, il Consiglio federale ha assegnato all'IFPDT tre ulteriori posti per l'attuazione dei nuovi compiti e attribuzioni, di modo che dal 2020 l'effettivo del personale ammonta a 27 posti a tempo pieno. Tenuto conto che l'entrata in vigore della LPD riveduta è prevista per il 2022, nella primavera del 2021 l'IFPDT ha proposto al Consiglio federale di autorizzare i rimanenti sei posti a tempo pieno.

In seguito a pensionamenti e altre partenze la struttura d'età dell'autorità è ringiovanita negli ultimi anni, il che sgrava il credito per il personale.

Tabella 4: Posti attribuibili per trattare questioni riguardanti la LPD

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27

Prestazioni

Secondo il nuovo Modello di gestione dell'Amministrazione federale (NMG) i compiti dell'IFPDT in quanto 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, dal 1° aprile 2020 al 31 marzo 2021, le risorse di personale impiegate presso l'IFPDT che potevano essere destinate alla protezione dei dati sono state ripartite in tali gruppi nel modo seguente:

Tabella 5: Servizi protezione dei dati

Consulenza a privati	24,8 %	
Consulenza alla Confederazione	20,1 %	
Collaborazione con i Cantoni	1,8 %	
Collaborazione con autorità estere	11,1 %	
Totale Consulenza		**57,8 %**
Vigilanza	15,0 %	
Certificazione	0,1 %	
Registro delle collezioni di dati	0,4 %	
Totale Vigilanza		**15,0 %**
Informazione	17,0 %	
Formazione / Conferenze	2,4 %	
Totale Informazione		**19,4 %**
Legislazione	7,3 %	
Totale Legislazione		**7,3 %**
Totale Protezione dei dati		**100,0 %**

Consulenza

Come illustrato nel capitolo iniziale «Sfide attuali», nel settore della consulenza l'IFPDT è confrontato a una continua crescita delle richieste derivante dalla necessità di accompagnare grandi progetti digitali. Le risorse di personale impiegate nella consulenza sono aumentate del 7 per cento circa, attestandosi al 57,8 per cento. Secondo il piano di controllo dell'IFPDT per il 2021, l'accompagnamento a titolo di consulenza è in corso per 15 grandi progetti. Sei di questi progetti sono legati alla trasformazione digitale ordinata dal Consiglio federale per l'Amministrazione federale, la quale cerca di recuperare il ritardo nella digitalizzazione lamentato dalla politica e dai media proprio in relazione alla lotta contro la pandemia.

Visto che le risorse dell'IFPDT sono sempre insufficienti per affrontare i rischi giuridici e tecnologici di una digitalizzazione che procede in modo dinamico, anche nel periodo in esame la nostra autorità non ha potuto adempiere l'accresciuta richiesta di accompagnamento di progetti con la dovuta accuratezza e nei tempi auspicati. I tre team dell'ambito direzionale Protezione dei dati hanno risposto ogni mese a circa 60 richieste e segnalazioni di cittadini, inviando agli interessati una lettera standard che li informava sulle vie previste dalla procedura civile. Ciò porta a un'incomprensione sempre più grande poiché, da un lato, il Regolamento generale dell'UE sulla protezione dei dati (RGPD) impone alle proprie autorità di protezione dei dati di dare seguito a tutte le denunce dei cittadini e, dall'altro, la nuova LPD prevede anche per l'IFPDT un obbligo esteso di trattare sotto il profilo materiale singole istanze della popolazione svizzera.

Dato che i big data e l'intelligenza artificiale si stanno imponendo come modello d'affari in tutti i settori e i rischi tecnologici legati alla protezione dei dati continuano ad estendere il campo di vigilanza dell'IFPDT, verosimilmente il numero di grandi progetti pubblici e privati che implicano un trattamento di dati continuerà a crescere, come negli scorsi anni.

Tabella 6: Consulenze svolte nel 2021 per grandi progetti

Diritti fondamentali	5
Finanze	1
Sanità e lavoro	3
Telekommunicazioni	1
Commercio e economia	2
Archivio federale	1
Migrazione	1
Dogna	1
Totale	**15**

Vigilanza

La dinamica delle applicazioni basate su cloud impone un'esecuzione estremamente rapida dei controlli. Questa accelerazione e la necessità, che si rivela sempre più importante, di disporre di una combinazione di conoscenze giuridiche e competenze tecniche escludono interruzioni prolungate nelle procedure di accertamento dei fatti, facendo in modo che i controlli più estesi debbano essere svolti da più collaboratori. L'attuale entità degli effettivi limita considerevolmente la densità dei controlli. Nel 2018 all'attività di vigilanza è stato attribuito più o meno il 12 per cento delle risorse di personale, quota sensibilmente inferiore al 20 per cento della media degli anni precedenti. Negli ultimi periodi in rassegna si è almeno potuto evitare che la quota scendesse sotto il 15 per cento. Secondo il piano di controllo per il 2021, queste risorse dovranno servire a svolgere 13 controlli di vasta portata. Se rapportata al volume dei trattamenti di dati da parte di organi federali e alle circa 12000 grandi e medie imprese commerciali nonché alle circa 100000 fondazioni e associazioni attive in Svizzera, l'attuale densità dei controlli si rivela ancora bassa. Per l'Incaricato rimane dunque difficile far comprendere ai media e alle organizzazioni attive nella protezione dei consumatori le proprie reticenze, imputabili alla limitatezza delle risorse disponibili, ad avviare procedure formali per l'accertamento dei fatti. In vista dell'imminente entrata in vigore della nuova LPD l'aspettativa del pubblico è aumentata. Detto questo, resta solo da sperare che il Consiglio federale conceda all'IFPDT i sei posti richiesti.

Legislazione

Gli adeguamenti del trattamento dei dati personali conseguenti alla trasformazione digitale degli uffici federali risultano leciti soltanto se si fondano su una base legale. Quest'ultima comporta l'introduzione nel diritto federale di tutta una serie di prescrizioni nuove e rivedute sul trattamento dei dati, in merito alle quali l'IFPDT si esprime nell'ambito delle diverse procedure di consultazione. Nonostante il corrispondente onere e la dispendiosa revisione della LPD e della relativa ordinanza, negli ultimi periodi in esame siamo riusciti a stabilizzare l'attività di vigilanza a un livello basso, fra l'altro limitando i pareri dettagliati ai progetti chiave.

Revisione totale della LPD

Con l'imminente entrata in vigore della nuova LPD e dell'ordinanza d'esecuzione, per l'IFPDT si prospettano onerosi lavori preparatori per quanto concerne i nuovi compiti e le nuove competenze come pure l'informazione tempestiva della popolazione e dell'economia. Grazie alla liberazione di tre posti da parte del Consiglio federale, avvenuta in vista dell'entrata in vigore della LPD, è stato possibile portare avanti tali lavori.

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

Nel periodo in rassegna, nell'aprile 2020, la CIP-N ci ha invitati due volte per uno scambio sul tema del coronavirus in relazione a un'applicazione della Swisscom mirata a visualizzare gli assembramenti di persone. Inoltre, a inizio maggio la Commissione ci ha sentiti in merito all'introduzione dell'applicazione di tracciamento di prossimità. Nello stesso periodo la CIP-S ci ha consultati sia sulla revisione della LPD (appianamento delle divergenze) sia sulla revisione parziale della legge sull'AVS in relazione all'utilizzo del numero AVS. Alla fine di maggio la CIP-S ha sentito due volte l'IFPDT sulla modifica urgente della legge sulle epidemie. Prima di essere stati coinvolti, nel luglio 2020, nell'appianamento delle divergenze per la revisione della LPD, la stessa Commissione ci aveva già consultati prima di tale revisione e prima della revisione della legge sull'AVS. Nel luglio 2020 siamo stati invitati dalle sottocommissioni DFGP/CaF delle CdG a presentare il nostro rapporto d'attività annuale.

Nell'anno in rassegna vi sono inoltre state audizioni in merito alla cartella informatizzata del paziente, da parte della CdG-N, e alla petizione della Sessione dei giovani sulla protezione dei dati nel sistema sanitario, da parte della CIP-S.

Infine le CIP di entrambe le Camere ci hanno coinvolti in cinque riunioni e le CSSS di entrambe le Camere in due riunioni, durante le quali si è discusso

delle agevolazioni per le persone vaccinate e di altri temi legati alla pandemia di COVID-19.

Criteri di valutazione

La responsabilità di decidere se e in che misura attribuire all'IFPDT risorse supplementari compete alle autorità politiche, che dispongono di un considerevole margine di manovra nel valutare gli sviluppi attuali e futuri della digitalizzazione e le sue ripercussioni sull'attività della nostra autorità. Il compito principale dell'IFPDT è proteggere la sfera privata e garantire il diritto all'autodeterminazione informativa nella società digitale. L'IFPDT deve poter agire in piena indipendenza.

Ciò richiede un'adeguata e sufficiente dotazione di risorse umane, materiali, tecniche e finanziarie, in modo che l'autorità di vigilanza non debba limitarsi, reagendo semplicemente, a sbrigare l'indispensabile, ma sia in grado di agire di sua iniziativa, in particolare con quella credibilità e quell'intensità che i cittadini possono ragionevolmente aspettarsi per la tutela dei loro diritti fondamentali.

Per quanto riguarda i diversi gruppi di prestazioni, la valutazione delle risorse deve fondarsi sui seguenti obiettivi di efficacia (v. tabella 7 qui sotto):

Prestazioni e risorse nell'ambito della legge sulla trasparenza

Dopo un esperimento pilota durato per tutto il 2017, l'ambito direzionale Principio di trasparenza, che nell'anno in rassegna era dotato di 4,4 posti a tempo pieno, ha adottato una procedura accelerata e sommaria che si caratterizza per l'esecuzione di sedute di mediazione orali. Da allora questa procedura continua a dimostrarsi valida: oltre al fatto che il numero di mediazioni terminate in modo consensuale sia rimasto elevato nel corso degli anni, si è riusciti a fare in modo che i termini di legge non venissero superati, salvo in alcuni casi particolarmente complessi dal punto di vista processuale e materiale.

A seguito della pandemia e delle misure adottate dal Consiglio federale per proteggere la salute pubblica, sia nell'anno in esame che nell'anno in corso non è stato possibile, per diversi mesi, svolgere sul posto le trattative di mediazione. In tali periodi l'Incaricato ha dovuto ricorrere nuovamente alla procedura scritta. Questo ha pregiudicato direttamente la durata del trattamento delle singole procedure e, assieme al numero costantemente elevato di domande di mediazione (complesse e vaste), ha fatto sì che le procedure inevase si accumulassero. L'anno in rassegna ha altresì dimostrato, ancora una volta, che numerose domande di mediazione da trattare in tempi brevi e le assenze di personale causano rapidamente lavoro arretrato, con la conseguenza che diventa ancora più difficile rispettare i termini impartiti dalla legge (v. cap. 2.2).

La tendenza all'aumento di domande di mediazione sembra confermarsi anche per il 2021, di modo che l'accumulo di domande inevase renderà ulteriormente difficile, con le risorse disponibili, trattare i nuovi casi nei termini prescritti.

Tabella 7: Criteri di quantificazione IFPDT

Gruppo di prestazioni	Obiettivi di efficacia
Consulenza	L'IFPDT 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, avvalendosi di strumenti di lavoro adeguati alla realtà digitale.
Vigilanza	L'IFPDT dispiega una densità di controlli credibile.
Informazione	L'IFPDT sensibilizza l'opinione pubblica in modo proattivo sui rischi legati alla tecnologia e alle applicazioni nel contesto della digitalizzazione.
Legislazione	L'IFPDT 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.


OPEN
RIDE

3.2 Comunicazione

Attività di comunicazione dominata dalla pandemia

L'inizio dell'anno in rassegna ha praticamente coinciso con l'arrivo della pandemia di coronavirus in Svizzera. Come prevedibile, l'intero periodo è stato focalizzato su questa problematica e così sarà anche in seguito. L'attività di comunicazione dell'Incaricato è stata orientata all'indicazione e alla diffusione dei rischi rilevanti per la protezione dei dati. Nonostante l'indipendenza di principio dell'Incaricato, in molti casi si è rivelato necessario e opportuno un accordo con le autorità, affinché durante la crisi la popolazione ricevesse informazioni coerenti. Questa esigenza in materia di comunicazione riguardava parimenti, a seconda dei casi, lo scambio con gli incaricati cantonali della protezione dei dati.

Per il resto, pur prescindendo dalle tematiche riguardanti la pandemia, l'accelerazione della digitalizzazione e della globalizzazione della società hanno reso costantemente onnipresenti le questioni in materia di protezione dei dati. L'attività di comunicazione dell'IFPDT si è quindi vista sollecitata, sotto diversi aspetti, a sensibilizzare in modo efficace i giornalisti e l'opinione pubblica in merito alle tematiche urgenti sulla protezione della sfera privata e sul principio di trasparenza nell'Amministrazione.

Al centro figurava infine il dibattito parlamentare riguardante la nuova legge sulla protezione dei dati, seguito in modo continuativo dall'Incaricato e conclusosi nel settembre 2020 con la sua adozione da parte di entrambe le Camere. Non essendo stato presentato il referendum contro la revisione totale della LPD, abbiamo pubblicato sulla nostra pagina web un breve commentario alle nuove disposizioni (cfr. priorità I). Con l'entrata in vigore della legge l'IFPDT sarà investito di nuovi compiti e di maggiori competenze di vigilanza, ciò che comporterà da parte sua una crescente esigenza di comunicazione e una maggiore presenza pubblica. In vista dell'entrata in vigore della nuova legge e della relativa ordinanza, i promemoria, le spiegazioni e le direttive esistenti sono attualmente in fase di rielaborazione.

Sfide e condizioni poste alla comunicazione

Nella seconda metà del 2020 il settore Comunicazione ha potuto ripristinare lo stato originario del suo organico che dispone quindi di 2,4 posti a tempo pieno, ripartiti fra tre persone. L'occupazione dei posti ha fatto sì che anche il plurilinguismo venisse meglio rappresentato. A causa delle risorse limitate, l'Incaricato focalizza la sua attività di comunicazione su tre canali centrali di comunicazione: il (presente) rapporto di attività, il sito web e il contatto diretto con i giornalisti. Twitter viene usato limitatamente mentre, per motivi di protezione dei dati, si rinuncia a ricorrere ad altre piattaforme di media sociali.

Nell'anno in rassegna abbiamo proceduto alla riaggiudicazione del rapporto di attività. In tal modo hanno potuto essere migliorate le condizioni quadro redazionali e concettuali nei limiti esistenti dei costi.

Interesse costantemente elevato dei media

Nell'anno in rassegna il grande interesse dei media ha trovato riscontro nelle numerose prese di posizione dell'Incaricato e nella comunicazione in merito a richieste correnti come pure nei numerosi articoli e contributi apparsi in generale nei formati analogico e digitale sui temi della protezione dei dati e del principio di trasparenza. Già soltanto nel nostro monitoraggio dei media svizzeri e di una scelta di prodotti chiave della stampa internazionale, abbiamo registrato 4000 contributi, vale a dire circa il doppio rispetto all'anno precedente. Questo incremento non può essere una conseguenza dell'avvenuto adeguamento del profilo di ricerca bensì va ricondotto a un notevole incremento in termini di rilevanza: oltre la metà dei contributi riguarda infatti la pandemia di coronavirus.

Parallelamente riscontriamo una forte attività nel web sociale (media sociali e piattaforme online; cfr. cifre chiave sul retro della busta). Si registrano 7320 menzioni riguardanti l'IFPDT, in 1152 delle quali l'Incaricato o un portavoce sono stati direttamente nominati. Oltre la metà di tali menzioni ha avuto luogo su canali all'estero. Un indicatore centrale nel web sociale è costituito dai tassi di coinvolgimento (engagement rate), ossia dal numero di attività quali «mi piace», «inoltra» o «commenta» per contributo. Con un valore di 3,36, il tasso di coinvolgimento è molto alto e riflette un'ampia e attiva rete di collegamenti nelle comunità dei media sociali.

Complessivamente sono state elaborate circa 600 domande dei media, ossia un terzo in più rispetto all'anno

precedente. La maggioranza dei contatti ha avuto luogo con i giornalisti accreditati presso il Centro media di Palazzo federale. I cittadini e le imprese hanno trasmesso lettere per corrispondenza elettronica o postale o utilizzato l'hotline telefonica per esprimere le loro esigenze e domande al nostro personale specializzato. Attraverso questi canali ci sono pervenute circa 4200 richieste.

L'Incaricato ha nuovamente preso parte a circa quaranta eventi organizzati da associazioni, istituti di formazione, autorità o imprese e organizzazioni nell'ambito della digitalizzazione.

CORONA

Informazioni concernenti il coronavirus

Accanto a un'ampia attività di consulenza prestata durante la pandemia, l'Incaricato e i suoi collaboratori specializzati hanno reso pubblica la posizione dell'IFPDT in materia di conformità della protezione dei dati nell'ambito di sfide centrali, segnatamente nei seguenti settori:

- valutazione dei modelli di mobilità sul territorio della Svizzera: accesso da parte dell'UFSP ai dati visualizzati di Swisscom;
- applicazione per il Proximity Tracing: conformità alla protezione dei dati dell'applicazione SwissCovid;
- misure per un'utilizzazione sicura di soluzioni di audio e videoconferenze;
- concetti di protezione contro il coronavirus da parte di operatori privati: trasmissione facoltativa di dati personali;
- liste di ospiti e dati di contatto: nel rilevamento dei dati i gestori devono assicurare la protezione dei dati di contatto; uso facoltativo di applicazioni;
- procedimento contro la piattaforma sulle vaccinazioni Fondazione mievaccinazioni.

Nel quadro della Giornata internazionale della protezione dei dati, tenutasi il 28 gennaio 2021, l'IFPDT e la Conferenza degli incaricati cantonali della protezione dei dati (privatim) hanno ribadito la necessità di proteggere i dati relativi alla sfera privata durante la pandemia. Le autorità in materia di protezione dei dati hanno riaffermato di fronte ai media i diritti alla vita privata e all'autodeterminazione, i quali non dovrebbero rimanere circoscritti all'attuale fase di pandemia. Anche in futuro la popolazione dovrà avere la possibilità di esercitare un diritto di scelta effettivo in materia di tecnologie digitali e ripiegare su alternative anonime.

Pareri, raccomandazioni e pubblicazioni

Nell'anno in esame l'Incaricato ha pubblicato diversi pareri e dichiarazioni riguardanti attuali progetti ed eventi riguardanti tra l'altro i seguenti temi, oltre al coronavirus (cfr. riquadro):

- consulenza riguardante la revisione totale della legge sulla protezione dei dati e le disposizioni della stessa;
- regolamentazione insufficiente del trattamento dei dati nella nuova legge sulla polizia doganale;
- scudo Svizzera-USA per la privacy e scudo UE-USA per la privacy; in particolare sentenza della Corte di giustizia delle Comunità europee (CGCE) concernente le clausole contrattuali standard europee;
- trattamento dei dati relativi a Diem (in precedenza Libra);
- revisione LAMal: IFPDT per la trasparenza nei modelli dei prezzi.

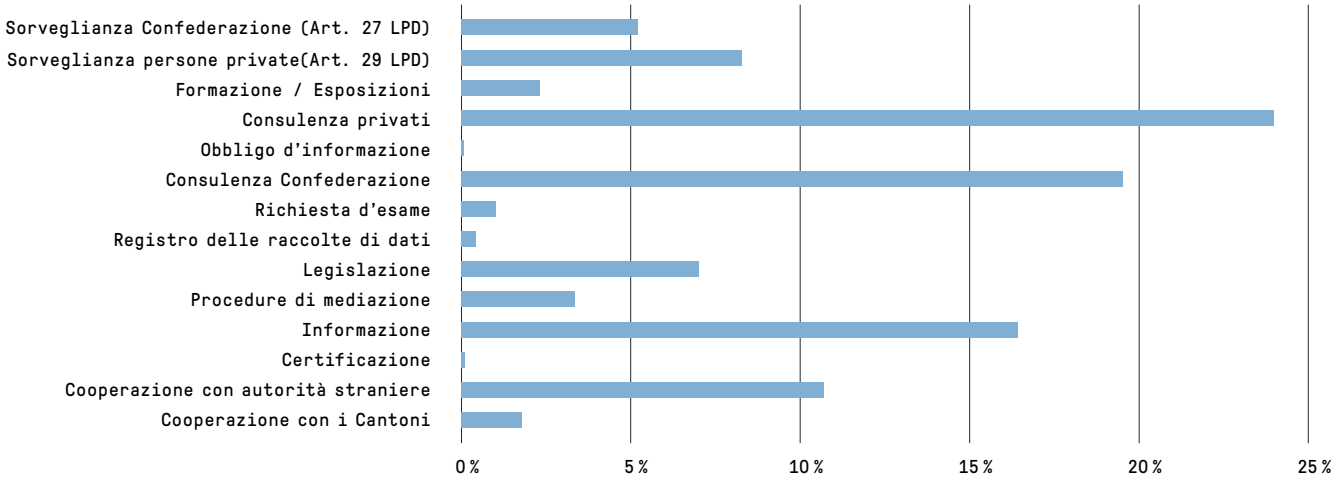
Sul sito web dell'IFPDT abbiamo pubblicato inoltre 26 raccomandazioni concernenti il principio di trasparenza.

Il 30 giugno 2020 è stato pubblicato, secondo l'articolo 30 LPD, il 27° rapporto d'attività 2019/2020. Quest'ultimo è disponibile in quattro lingue nelle versioni stampata ed elettronica.

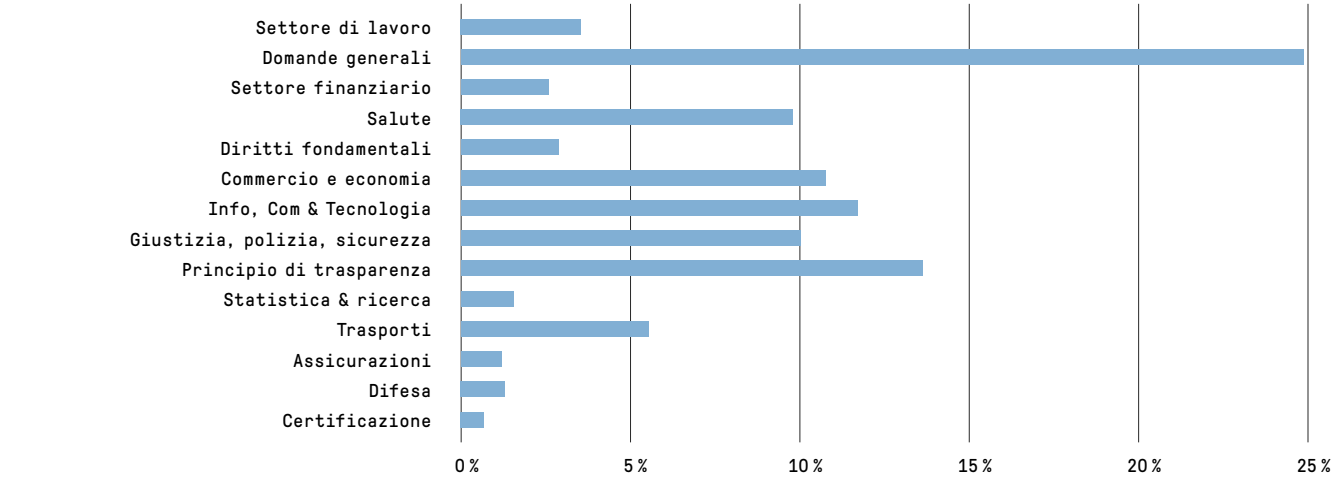
3.3 Statistica

Statistiche sulle attività dell'IFPDT dal 1° aprile 2020 al 31 marzo 2021 (Protezione dei dati)

Carico di lavoro per compiti

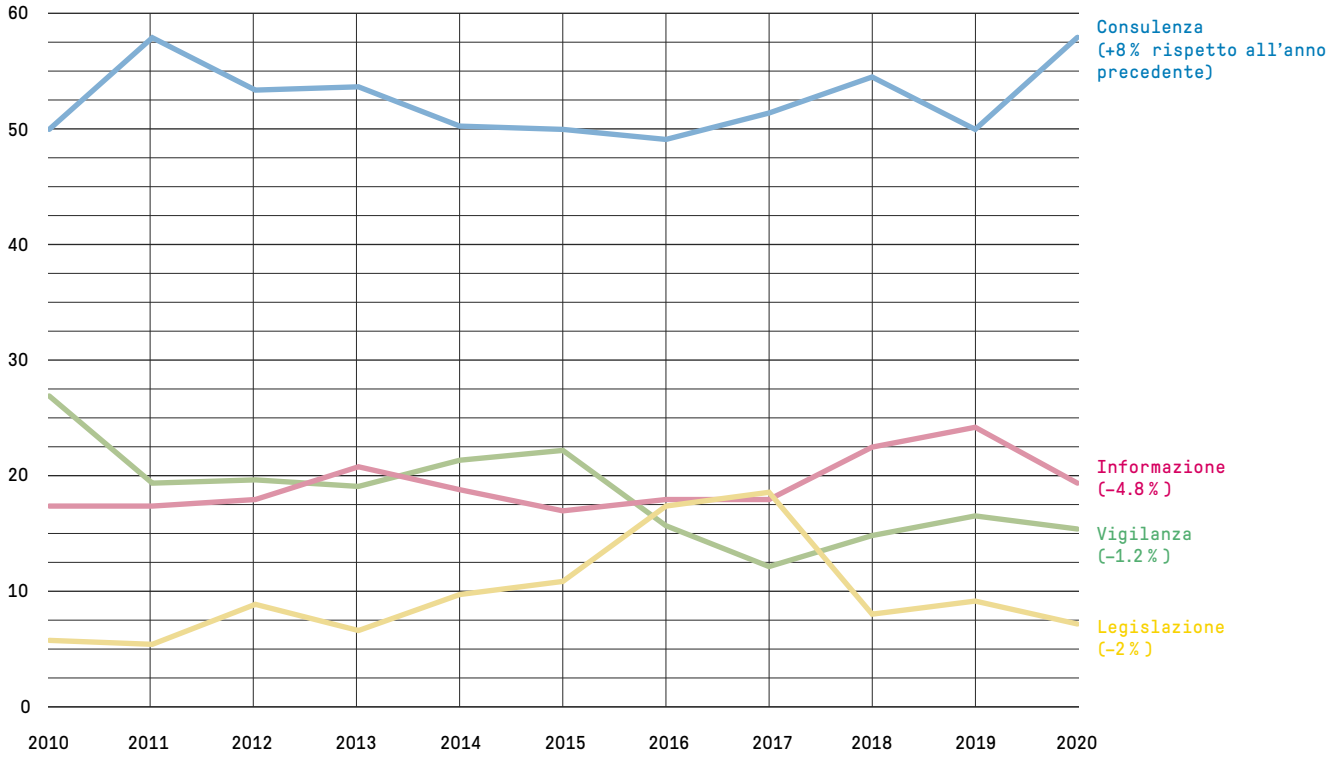


Carico di lavoro per materie



Paragone pluriennale

(in percentuale)



Panoramica delle domande d'accesso dal 1° gennaio al 31 dicembre 2020

Sezione	Numero di domande		Accesso interamente concesso		Accesso interamente negato		Accesso parzialmente concesso o sospeso		Domanda ritirata		Domanda pendente		Nessun documento disponibile	
CaF	31		20		5		4		0		2		0	
DFAE	174		88		14		47		11		4		10	
DFI	312		114		26		100		8		41		23	
DFGP	77		45		11		9		2		3		7	
DDPS	251		184		10		37		5		10		5	
DFF	109		51		13		28		3		6		8	
DEFR	115		49		15		36		3		7		5	
DATEC	105		53		8		32		3		3		6	
MPC	13		6		1		0		0		4		2	
SP	6		0		5		0		0		0		1	
Totale 2020 (%)	1193	(100)	610	(51)	108	(9)	293	(24)	35	(3)	80	(7)	67	(6)
Totale 2019 (%)	916	(100)	542	(62)	86	(11)	171	(21)	38	(6)	43	(5)	36	(4)
Totale 2018 (%)	636	(100)	352	(55)	62	(10)	119	(19)	24	(4)	48	(7)	31	(5)
Totale 2017 (%)	581	(99)	317	(55)	107	(18)	106	(18)	26	(4)	21	(4)	–	
Totale 2016 (%)	551	(99)	293	(53)	87	(16)	105	(19)	33	(6)	29	(5)	–	
Totale 2015 (%)	597	(100)	319	(53)	98	(16)	127	(21)	31	(5)	22	(4)	–	
Totale 2014 (%)	575	(100)	297	(52)	122	(21)	124	(22)	15	(3)	17	(3)	–	
Totale 2013 (%)	469	(100)	218	(46)	122	(26)	103	(22)	18	(4)	8	(2)	–	
Totale 2012 (%)	506	(100)	223	(44)	138	(27)	120	(24)	19	(4)	6	(1)	–	
Totale 2011 (%)	466	(100)	203	(44)	126	(27)	128	(27)	0	(0)	9	(2)	–	

Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2020

	Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	**21**	12	5	3	0	1	0
	IFPDT	**10**	8		1		1	
	Totale	**31**	**20**	**5**	**4**	**0**	**2**	**0**
Dipartimento federale degli affari esteri DFAE	DFAE	**174**	88	14	47	11	4	10
	Totale	**174**	**88**	**14**	**47**	**11**	**4**	**10**
Dipartimento federale dell'interno DFI	SG DFI	**20**	12	0	5	0	3	0
	UFU	**4**	3	0	0	1	0	0
	UFC	**3**	1	0	2	0	0	0
	AFS	**3**	1	0	2	0	0	0
	METEO CH	**1**	1	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	UFSP	**181**	51	22	69	3	26	10
	UST	**7**	4	1	0	0	0	2
	UFAS	**19**	15	0	4	0	0	0
	USAV	**25**	8	3	9	4	0	1
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**42**	15	0	9	0	10	8
	SUVA	**7**	3	0	0	0	2	2
	Totale	**312**	**114**	**26**	**100**	**8**	**41**	**23**
Dipartimento federale di giustizia e polizia DFGP	SG DFGP	**5**	4	0	0	0	0	1
	DFGP	**29**	18	7	2	0	0	2
	FEDPOL	**13**	6	2	2	1	0	2
	METAS	**2**	2	0	0	0	0	0
	SEM	**19**	10	1	5	0	3	0
	Servizio SCPT	**1**	0	1	0	0	0	0
	ISDC	**5**	3	0	0	0	0	2
	IPI	**2**	2	0	0	0	0	0
	CFCG	**0**	0	0	0	0	0	0
	CAF	**0**	0	0	0	0	0	0
	ASR	**1**	0	0	0	1	0	0
	CSI	**0**	0	0	0	0	0	0
	CNPT	**0**	0	0	0	0	0	0
	Totale	**77**	**45**	**11**	**9**	**2**	**3**	**7**

	Sezione	Numero di domande	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	**20**	7	0	10	1	0	2
	Difesa / Esercito	**34**	13	0	9	2	9	1
	SIC	**18**	3	8	3	2	0	2
	armasuisse	**12**	9	0	2	0	1	0
	UFSPO	**150**	147	2	1	0	0	0
	UFPP	**17**	5	0	12	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	UUC	**0**	0	0	0	0	0	0
	Totale	**251**	**184**	**10**	**37**	**5**	**10**	**5**
Dipartimento federale delle finanze DFF	SC DFF	**22**	11	1	9	0	1	0
	ODIC	**1**	0	0	1	0	0	0
	AFF	**10**	1	1	7	1	0	0
	UFPER	**1**	1	0	0	0	0	0
	AFC	**10**	7	0	3	0	0	0
	AFD	**37**	15	7	5	1	3	6
	UFCL	**3**	1	1	1	0	0	0
	UFIT	**4**	2	0	0	1	0	1
	CDF	**8**	3	3	1	0	0	1
	SFI	**3**	0	0	1	0	2	0
	PUBLICA	**0**	0	0	0	0	0	0
	UCC	**10**	10	0	0	0	0	0
	Totale	**109**	**51**	**13**	**28**	**3**	**6**	**8**
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	**9**	6	1	0	1	0	1
	SECO	**35**	16	10	7	1	0	1
	SEFRI	**4**	3	0	0	0	0	1
	UFAG	**14**	3	0	7	0	3	1
	UFAE	**7**	3	0	3	0	0	1
	UFAB	**3**	0	0	3	0	0	0
	SPR	**2**	1	0	1	0	0	0
	COMCO	**18**	11	1	3	1	2	0
	CIVI	**0**	0	0	0	0	0	0
	UFDC	**2**	2	0	0	0	0	0
	FNS	**2**	1	0	0	0	1	0
	IUFFP	**1**	0	0	0	0	1	0
	ETH Rat	**16**	3	3	10	0	0	0
	Innosuisse	**2**	0	0	2	0	0	0
	Totale	**115**	**49**	**15**	**36**	**3**	**7**	**5**

	Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	SG DATEC	**9**	8	0	1	0	0	0
	UFA	**14**	9	0	3	2	0	0
	UFAC	**9**	3	0	2	0	1	3
	UFE	**4**	3	0	0	0	0	1
	USTRA	**9**	7	0	2	0	0	0
	UFCOM	**14**	2	2	10	0	0	0
	UFAM	**38**	17	5	13	1	0	2
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	IFSN	**7**	3	1	1	0	2	0
	PostCom	**1**	1	0	0	0	0	0
	AIRR	**0**	0	0	0	0	0	0
	Totale	**105**	**53**	**8**	**32**	**3**	**3**	**6**
Ministero pubblico della Confederazione MPC	MPC	**13**	6	1	0	0	4	2
	Totale	**13**	**6**	**1**	**0**	**0**	**4**	**2**
Servizi del Parlamento SP	SP	**6**	0	5	0	0	0	1
	Totale	**6**	**0**	**5**	**0**	**0**	**0**	**1**
	Somma totale	**1193**	**610**	**108**	**293**	**35**	**80**	**67**

Domande di accesso 2020 con riferimento a Corona

	Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	**6** (100%)	3 (50%)	3 (50%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IFPDT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**6** (100%)	**3** (50%)	**3** (50%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Dipartimento federale degli affari esteri DFAE	DFAE	**13** (100%)	12 (92%)	1 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**13** (100%)	**12** (92%)	**1** (8%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Dipartimento federale dell'interno DFI	SG DFI	**17** (10%)	11 (6%)	0 (0%)	3 (2%)	0 (0%)	3 (2%)	0 (0%)
	UFU	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METEO CH	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BN	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFSP	**134** (77%)	44 (25%)	16 (9%)	53 (31%)	1 (1%)	11 (6%)	9 (5%)
	UST	**1** (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)
	UFAS	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	USAV	**4** (2%)	3 (2%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	MNS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SWISS MEDIC	**16** (9%)	4 (2%)	0 (0%)	0 (0%)	0 (0%)	9 (5%)	3 (2%)
	SUVA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**174** (100%)	**64** (37%)	**17** (10%)	**56** (32%)	**1** (1%)	**23** (13%)	**13** (7%)
Dipartimento federale delle finanze DFF	SC DFF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ODIC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFF	**9** (36%)	1 (4%)	1 (4%)	6 (24%)	1 (4%)	0 (0%)	0 (0%)
	UFPER	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFC	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFD	**11** (44%)	1 (4%)	5 (20%)	3 (12%)	0 (0%)	0 (0%)	2 (8%)
	UFCL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFIT	**3** (12%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)	0 (0%)	0 (0%)
	CDF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SFI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PUBLICA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UCC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**6** (11%)	**6** (11%)	**9** (16%)	**2** (4%)	**0** (0%)	**2** (4%)

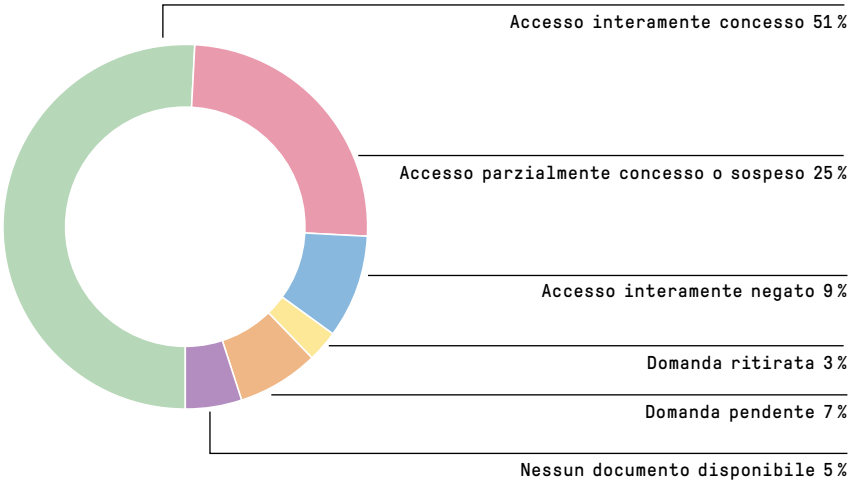
	Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale di giustizia e polizia DFGP	SG DFGP	**1** (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (14%)
	DFGP	**6** (86%)	5 (71%)	1 (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FEDPOL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METAS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SEM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Servizio SCPT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ISDC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IPI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CFCG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CAF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ASR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CSI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CNPT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**7** (100%)	**5** (71%)	**1** (14%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (14%)
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	SG DATEC	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFA	**2** (50%)	1 (25%)	0 (0%)	0 (0%)	1 (25%)	0 (0%)	0 (0%)
	UFAC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	USTRA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFCOM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFAM	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ARE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ComCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IFSN	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PostCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AIRR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**4** (100%)	**3** (75%)	**0** (0%)	**0** (0%)	**1** (25%)	**0** (0%)	**0** (0%)
Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS	SG DDPS	**8** (16%)	1 (2%)	0 (0%)	5 (10%)	0 (0%)	0 (0%)	2 (4%)
	Difesa / Esercito	**23** (46%)	10 (20%)	0 (0%)	3 (6%)	1 (2%)	8 (16%)	1 (2%)
	SIC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	armasuisse	**1** (2%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFSPO	**3** (6%)	3 (6%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFPP	**15** (30%)	3 (6%)	0 (0%)	12 (24%)	0 (0%)	0 (0%)	0 (0%)
	swisstopo	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UUC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**50** (100%)	**18** (36%)	**0** (0%)	**20** (40%)	**1** (2%)	**8** (16%)	**3** (6%)

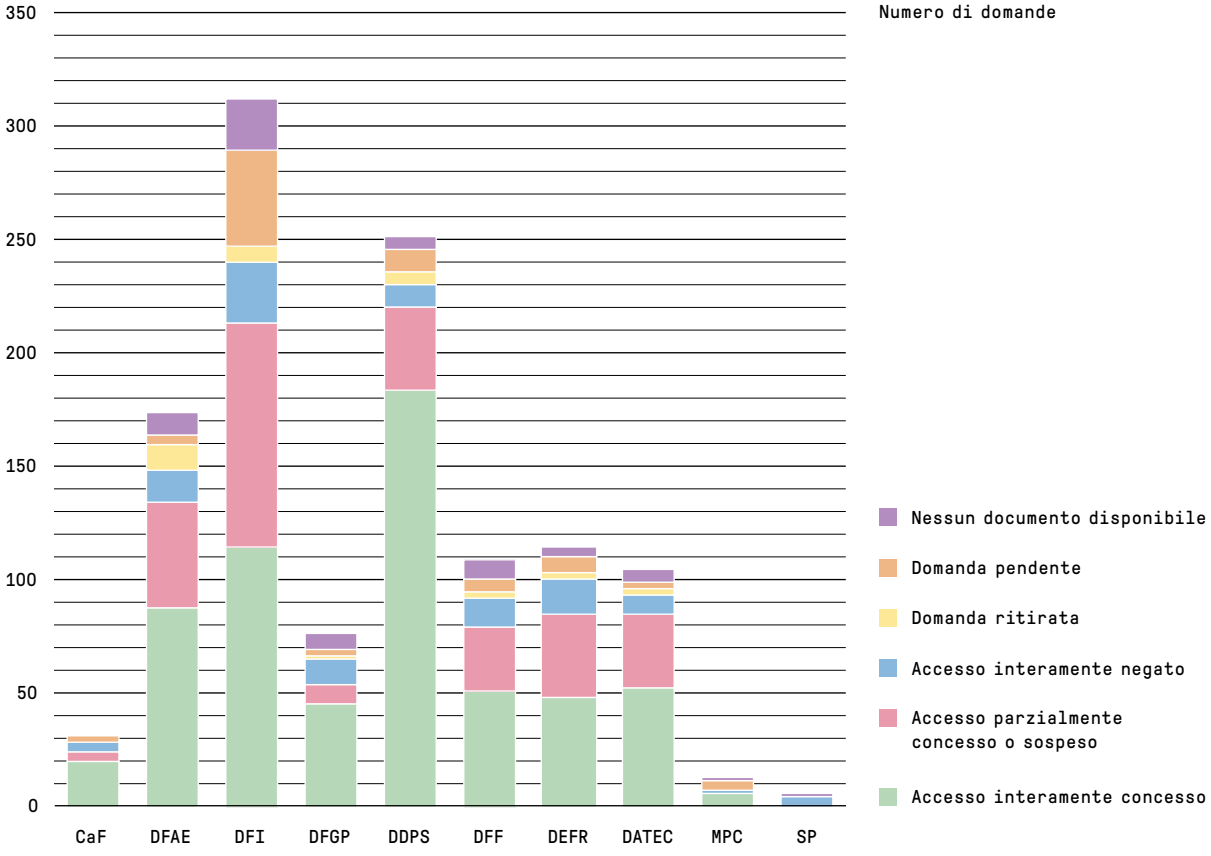
	Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SECO	**14** (56%)	5 (20%)	7 (28%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)
	SEFRI	**1** (4%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFAG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFAE	**5** (20%)	2 (8%)	0 (0%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)
	UFAB	**3** (12%)	0 (0%)	0 (0%)	3 (12%)	0 (0%)	0 (0%)	0 (0%)
	SPR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	COMCO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CIVI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UFDC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FNS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IUFFP	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ETH Rat	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Innosuisse	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Totale	**25** (100%)	**10** (40%)	**7** (28%)	**7** (28%)	**0** (0%)	**0** (0%)	**1** (4%)
Ministero pubblico della Confederazione MPC	MPC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Totale	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Servizi del Parlamento SP	SP	**4** (100%)	0 (0%)	3 (75%)	0 (0%)	0 (0%)	0 (0%)	1 (25%)
	Totale	**4** (100%)	**0** (0%)	**3** (75%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (25%)

Numero di domande di mediazione

Categoria del richiedente	2020
Media	**31**
Privati (o nessuna assegnazione esatta possibile)	**42**
Parti interessati (associazioni, organizzazioni,società ecc.)	**5**
Avvocati	**7**
Aziende	**7**
Università	**1**
Total	**93**

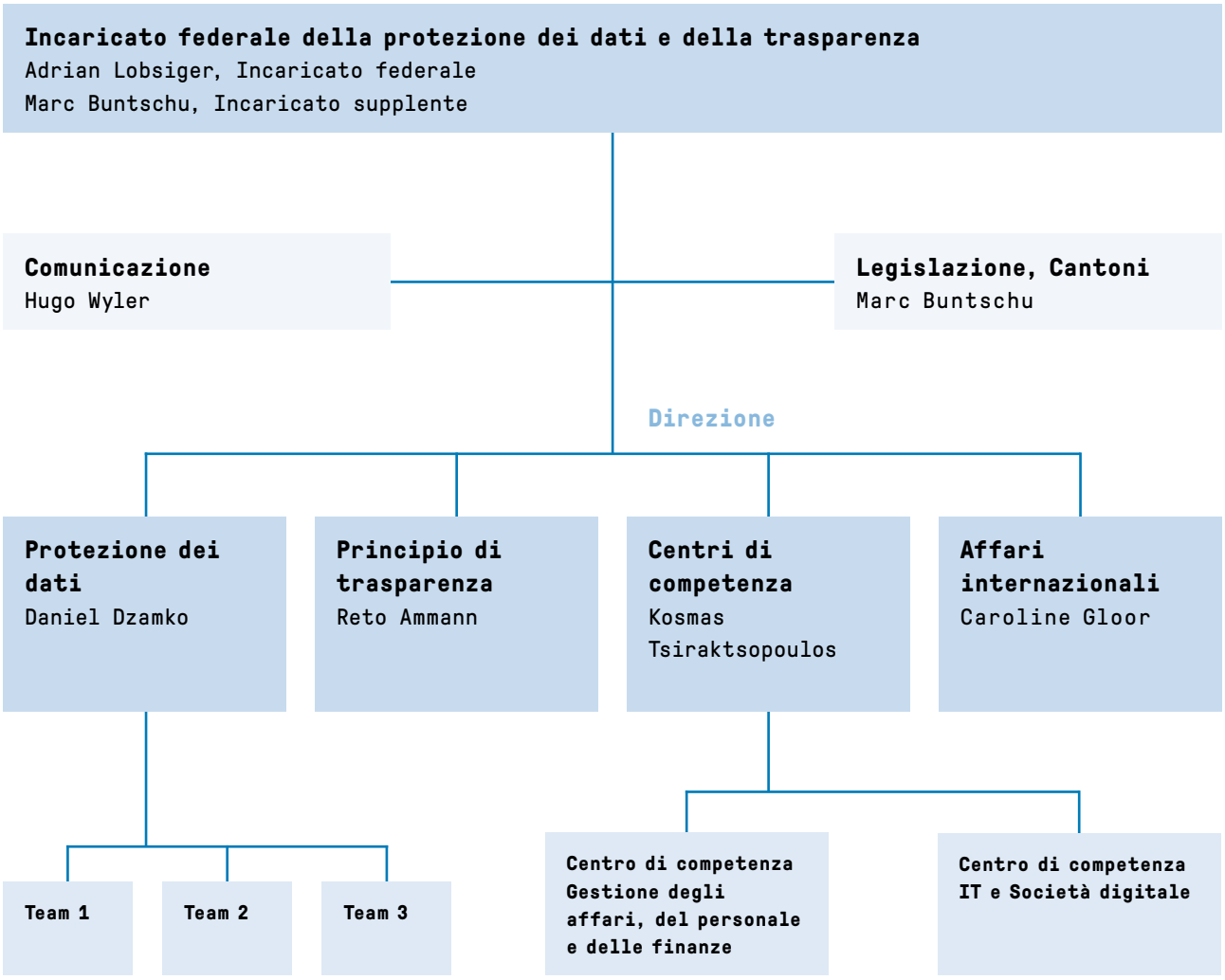
Trattamento delle domande d'accesso dal 1° gennaio al 31 dicembre 2020





3.4 Organizzazione IFPDT (Stato 31 marzo 2021)

Organigramma



Personale dell'IFPDT

Numero di dipendenti	38		
FTE	31.8		
per sesso	Donne	20	53 %
	Uomini	18	47 %
per livello di occupazione	1–89 %	25	63 %
	90–100 %	13	37 %
per lingua	Tedesco	30	79 %
	Francese	7	18 %
	Italiano	1	3 %
per età	20–49 anni	24	63 %
	50–65 anni	14	37 %
Posizioni dirigenziali	Donne	3	33 %
	Uomini	6	67 %

Abbreviazioni

AMVP Assemblea mondiale per la protezione della vita privata

BCR regole aziendali vincolanti (Binding Corporate Rules)

CEPD Comitato europeo per la protezione dei dati

CGUE Corte di giustizia dell'Unione europea

CIP cartella informatizzata del paziente

Convenzione 108+ Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

Datareg registro delle collezioni di dati

GDPR Regolamento generale sulla protezione dei dati

GEPD Garante europeo della protezione dei dati

IA intelligenza artificialie

LCIP legge federale sulla cartella informatizzata del paziente

LEp Legge federale sulla lotta contro le malattie trasmissibili dell'essere umano (Legge sulle epidemie)

LPD Legge federale sulla protezione dei dati

LPDS Legge federale sulla protezione dei dati personali nell'ambito dell'applicazione dell'acquis di Schengen in materia penale

LSIe Legge federale sui servizi d'identificazione elettronica (Legge sull'IE)

LTras Legge federale sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza)

LTV Legge sul trasporto di viaggiatori

NaDB programma di gestione nazionale dei dati

NAVS13 numero AVS a 13 cifre

NCSC Centro nazionale per la cibersicurezza

PNR dati dei passeggeri aerei (Passenger Name Records)

Privatim Conferenza degli incaricati svizzeri per la protezione dei dati

SCC Clausole contrattuali standard

SIC Servizio delle attività informative della Confederazione

TIC tecnologie dell'informazione e della comunicazione

Indice figurativo

Figure

Tabelle

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. 410.028.I

Layout: Ast & Fischer AG, Wabern
Fotografia: Nicolas Stadler
Caratteri: Pressura, Documenta
Stampa: Ast & Fischer AG, Wabern
Carta: PlanoArt®, holzfrei hochweiss

Cifre chiave

Carico protezione dei dati

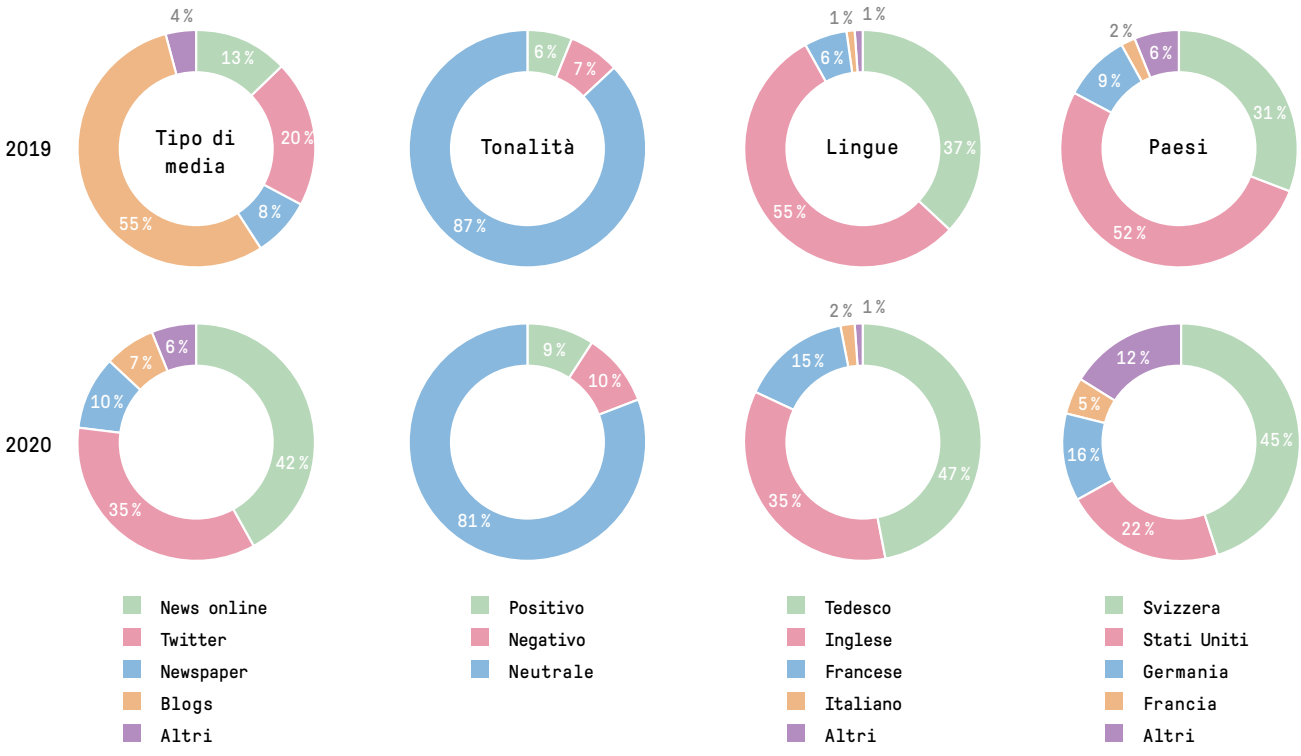
57,8 %	15,0 %	19,4 %	7,3 %
Consulenza	Vigilanza	Informazione	Leglislazione

Domande d'accesso principio di trasparenza (LTras)

51 %	25 %	9 %	3 %	7 %	5 %
interamente concesso	parzialmente concesso o sospeso	interamente negato	ritirata	pendente	nessun documento disponibile

Risonanza mediale del Commissario sul Social Web

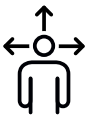
* Numero di tutte le menzioni dell IFPDT (cosiddetti „mentions" in blogs, tweets, news online ecc.)
** Numero di tutte le interazioni (likes, retweets, ecc.)



Preoccupazioni relative alla protezione dei dati

Informazione corretta

Le aziende e gli organi federali forniscono informazioni trasparenti sul loro trattamento dei dati: comprensibili e complete.



Possibilità di scelta

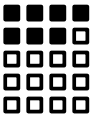
Gli interessati danno il loro consenso e godono di una vera libertà di scelta.

Analisi dei rischi

I possibili rischi per la protezione dei dati sono già stati identificati nel progetto e i loro effetti sono stati minimizzati con misure adeguate.

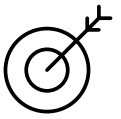
Esattezza dei dati

Il trattamento avviene con i dati corretti.



Proporzionalità

Nessuna raccolta di dati a conservazione, ma solo nella misura necessaria per raggiungere lo scopo. Il trattamento dei dati è limitato nel tempo e nella portata.



Finalità

I dati vengono trattati esclusivamente per le finalità indicate al momento della raccolta, come indicato dalle circostanze o come previsto dalla legge.

Sicurezza dei dati

I responsabili del trattamento garantiscono con misure tecniche e organizzative che i dati personali sono adeguatamente protetti.

Documentazione

Tutti i trattamenti sono documentati e classificati dal responsabile del trattamento.

Responsabilità personale

Gli organi privati e federali sono responsabili dell'adempimento dell'obbligo di rispettare la legislazione in materia di protezione dei dati.

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

E-Mail: info@edoeb.admin.ch
Sito web: www.lincaricato.ch
@derBeauftragte
Telefono: +41 (0)58 462 43 95 (lu – ve, 10 – 12)
Fax: +41 (0)58 465 99 96