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

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

26° Rapporto d'attività 2018/19

Incaricato federale della protezione dei dati e della trasparenza

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapporto d’attività 2018/2019
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 2018 al 31 marzo 2019.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Prefazione

Nelle classifiche sulla competitività digitale del Forum economico mondiale (WEF) e del World Competitiveness Center la Svizzera occupa i primi posti. Affinché il nostro Paese possa mantenere la posizione, il Consiglio federale formula strategie e piani d'azione concepiti per far progredire la digitalizzazione dell'economia e dello Stato.

Ma anche la protezione dei dati offre opportunità per la piazza svizzera dell'innovazione. Con le novità tecniche che garantiscono la tutela della sfera privata e l'autodeterminazione digitale delle persone è pure possibile guadagnare punti.

La gara per la preminenza nell'innovazione non deve però andare a scapito della salvaguardia dei vantaggi già acquisiti per la nostra piazza economica: grazie a un atto lungimirante del Legislatore, nel 1992 – quasi trent'anni fa – la Confederazione si è dotata di una legge sulla protezione dei dati apprezzata a livello internazionale, che permette tutt'ora all'economia svizzera di scambiarsi dati, senza ulteriori oneri legali o restrizioni, con le imprese di importanti nazioni commerciali. E, come tutti sanno, i dati sono un bene ambíto.

La digitalizzazione incide in maniera radicale sulla sfera privata dei circa quattro miliardi di utenti di Internet in tutto il mondo. Di fronte a questo dato di fatto, gli Stati dello Spazio economico europeo hanno potenziato la protezione dei dati per la propria popolazione ponendo in vigore nel maggio 2018 regole unitarie e moderne. Tali regole permettono alle imprese di mantenere lo scambio di dati a livello transfrontaliero, al quale partecipano ora anche imprese giapponesi e – entro i limiti ristretti dell'accordo sullo scudo per la privacy (Privacy Shield) – le imprese statunitensi certificate.

Dalla Svizzera, considerata una piazza formativa, tecnologica ed economica ambiziosa, gli altri Stati si aspettano che continui a partecipare allo scambio di dati incondizionato. Nel messaggio del settembre 2017 sulla revisione totale della legge sulla protezione dei dati il Consiglio federale ha infatti avviato l'iter legislativo parlamentare in questo senso. Da allora la palla è nel campo delle Camere federali, che hanno ora l'opportunità di innalzare il livello di protezione dei dati della nostra popolazione portandolo a un livello comparabile a quello dei nostri vicini europei. Fatto questo lavoro, non solo i nostri cittadini saranno tutelati adeguatamente, ma anche l'accesso dell'economia al libero scambio di dati sarà assicurato.

Adrian Lobsiger
Incaricato federale della protezione dei dati e della trasparenza

Protezione dei dati

Principio di trasparenza

L'IFPDT

Sfide attuali
I Digitalizzazione

Il trattamento di dati personali continua ad essere caratterizzato dallo sviluppo dinamico della tecnologia dell'informazione e della telecomunicazione nell'economia globale, che condiziona sensibilmente la quotidianità della popolazione svizzera nell'ambito del lavoro, del consumo e del tempo libero.

Tecnologia ed economia

Il potenziale tecnico ed economico per le ingerenze nella sfera privata e nei diritti di autodeterminazione della popolazione resta elevato, cosa che l'Incaricato riconduce principalmente ai due sviluppi esposti qui di seguito.

- L'Internet permette di adottare modelli commerciali che attualmente si rivolgono a circa quattro miliardi di utenti in tutto il mondo. Nei mercati dominati dalle aziende tecnologiche americane, quali Google, Amazon e Facebook, per la fornitura di servizi comunicativi e informativi basati su Internet si è imposto una sorta di modello «gratuito». Anziché fatturare i servizi forniti online, gli offerenti chiedono ai clienti di cedere loro i dati d'utente. Gli offerenti trattano questi dati con l'aiuto di algoritmi e dei relativi metodi di analisi per poter inviare ai clienti messaggi pubblicitari in modo mirato. In seguito l'offerente cede a terzi gli spazi pubblicitari mettendoli all'asta. Alcuni offerenti praticano questo modello commerciale con tale successo che miliardi di clienti fruiscono dei loro servizi «gratuiti» su scala globale. Essi possono alimentare i loro algoritmi con flussi tali di dati dei clienti da essere in grado di intensificare ulteriormente l'analisi del comportamento degli utenti realizzando fatturati astronomici sui mercati pubblicitari online, senza tener conto dei crescenti rischi in materia di protezione dei dati cui sono esposti gli utenti per il fatto di ricevere in maniera mirata messaggi commerciali e ideologici. Parallelamente si contraggono le entrate pubblicitarie dei quotidiani e della radio e televisione.
- Dopo che alcune società di telecomunicazione attive in Svizzera hanno annunciato che equipaggeranno la loro infrastruttura di rete per le larghezze di banda della quinta generazione (5G), la tecnica 5G sarà presto realtà: la capacità e la velocità dei flussi di dati mobili aumenteranno ancora enormemente. Sarà dunque ulteriormente accelerata la tendenza, già osservata nel rapporto d'attività precedente, della rapida crescita di apparecchi connessi con sensori che registrano immagini e voci umane, dati di localizzazione e persino funzioni fisiologiche interne nello spazio privato e pubblico e le trasmettono a intelligenze artificiali.

Società e politica dei dati

Nell'anno in rassegna si è ulteriormente acuita la critica dell'opinione pubblica nei confronti dei gestori di piattaforme sociali e offerenti di motori di ricerca che gestiscono su scala globale il menzionato modello commerciale dell'accesso ai dati in cambio di servizi «gratuiti».

Tenuto conto dell'aumento dei dati dei clienti raccolti e della crescente complessità e autonomia delle tecnologie d'analisi, per i gestori criticati diventa sempre più difficile garantire una protezione dei dati sufficiente: se da un lato devono informare i clienti in modo facilmente comprensibile e completo sul trattamento dei loro dati, dall'altro devono anche concedere ai clienti sufficienti possibilità affinché questi ultimi possano accettare o rifiutare scientemente tutti gli aspetti del trattamento. Per poter adempiere a questa responsabilità, gli offerenti devono investire in applicazioni funzionali alla protezione dei dati che conducano i clienti con pochi clic alle necessarie informazioni e opzioni. La tutela della sfera privata e dell'autodeterminazione dei clienti deve quindi essere integrata nei prodotti digitali precocemente e in modo orientato agli utenti.

Gli offerenti che si limitano a proferire dichiarazioni d'intenti in materia regolatoria e a soddisfare meccanicamente le esigenze di protezione giocano con la fiducia dei loro clienti e prima o poi attireranno su di sé l'attenzione della nostra autorità.

Secondo quanto previsto dal regolamento generale sulla protezione dei dati (GDPR) dell'UE, entrato in vigore nel maggio 2017, nell'anno in rassegna le autorità di protezione dei dati degli Stati membri dello SEE hanno inflitto multe elevate alle imprese che non hanno assicurato la trasparenza e l'autodeterminazione. Stando alle prime informazioni di cui dispone l'Incaricato, nel frattempo i procedimenti delle autorità di protezione dei dati di tali Stati hanno coinvolto anche imprese svizzere che trattano dati di abitanti dello SEE. Inoltre, in questi Stati anche le autorità preposte alla concorrenza si occupano in misura crescente del trattamento di dati. Nel periodo in rassegna l'Ufficio federale tedesco dei cartelli (Bundeskartellamt) ha invitato l'azienda Facebook, sulla base della sua posizione classificata come predominante sul mercato, a svincolare le sue condizioni d'utilizzazione da altri servizi del gruppo.

Il futuro dirà se le piattaforme predominanti sul mercato cederanno alla pressione delle autorità di vigilanza e alla critica dell'opinione pubblica o se manterranno il sistema dei servizi «gratuiti». Una valida alternativa dal punto di vista della protezione dei dati sarebbe costituita da modelli commerciali che escludono i clienti paganti dalle valutazioni di dati che generano profili e dagli invii personalizzati di messaggi pubblicitari. Siffatti sistemi di pagamento, che possono essere gestiti sia mediante criptovalute controllate in maniera decentralizzata sia mediante sistemi bancari, sono già diffusi ad esempio in Cina, poiché i gestori locali delle piattaforme riscuotono commissioni sull'esecuzione online dei contratti.

Legislazione

In Svizzera si sta ancora aspettando che la Commissione delle istituzioni politiche del Consiglio nazionale, Camera prioritaria, porti a termine la deliberazione sulla revisione totale della legge federale sulla protezione dei dati (LPD) presentata dal Consiglio federale nel settembre 2017. Dopo che il 12 gennaio 2018 la Commissione aveva scisso in due parti il progetto di revisione totale e in un primo tempo aveva trattato le modifiche necessarie per la ripresa del cosiddetto acquis di Schengen, le Camere federali hanno adottato una nuova legge federale che attua la direttiva (UE) 2016/680, la legge sulla protezione dei dati in ambito Schengen (LPDS). Questa legge speciale, il cui campo d'applicazione è limitato al trattamento dei dati da parte delle autorità federali preposte al perseguimento penale, è entrata in vigore il 1° marzo 2019 ma sarà abrogata con l'entrata in vigore della LPD sottoposta a revisione totale. Ora che questa legge ha investito la nostra autorità di nuovi compiti e competenze in relazione al trattamento particolarmente delicato di dati personali nel settore della polizia, dovremo dare la priorità in particolare al controllo del trattamento di dati da parte dell'Ufficio federale di polizia (fedpol). Al momento della stampa del presente rapporto non si sapeva ancora se il Consiglio federale ci avrebbe assegnato i fondi supplementari sollecitati a questo scopo.

Davanti alla Commissione delle istituzioni politiche del Consiglio nazionale, alle cui deliberazioni sulla LPD è stato invitato a partecipare, l'Incaricato ha sempre sottolineato l'importanza di aumentare a breve il livello di protezione a favore della popolazione svizzera e quindi di portare a termine quanto prima i lavori parlamentari. È tuttavia difficile prevedere la fine delle deliberazioni.

Per quanto determinate cerchie dell'economia possano ritenere sufficienti sia la LPD, risalente al 1992, sia le deboli competenze della nostra autorità, nei suoi contatti con le imprese svizzere di grandi e piccole dimensioni, attive a livello transfrontaliero l'IFPDT incontra una pronunciata disponibilità a investire in una protezione dei dati credibile in ambito aziendale. Queste imprese, direttamente interessate dalla revisione totale della legge, vogliono offrire anche alla loro clientela svizzera una protezione conforme ai nuovi standard europei. Esse sanno anche che nella realtà digitale i progetti di trattamento dei dati possono essere realizzati in funzione dei rischi, e spiegati ai clienti, soltanto se si utilizzano strumenti moderni come la valutazione d'impatto sulla protezione dei dati. E per tutto questo tempo i loro piccoli, medi e grandi concorrenti negli Stati dell'UE e dello SEE sapranno sfruttare il vantaggio concorrenziale che ne deriva.

II Attività di consulenza e controllo

Affinché nella sua funzione di autorità di vigilanza possa garantire che i dati personali vengano trattati con l'intensità ammessa dalla legge e non con quella tecnicamente possibile, l'IFPDT chiede ai responsabili delle applicazioni digitali di ridurre al minimo i rischi elevati in materia di protezione dei dati già nella fase di pianificazione e progetto e di presentare la relativa documentazione all'autorità aziendale e ufficiale di vigilanza sulla protezione dei dati. Nel periodo in rassegna abbiamo pertanto proseguito il monitoraggio di numerosi progetti Big Data di autorità federali e imprese private.

Non da ultimo per ridurre il proprio onere lavorativo, in vista di grandi progetti che implicano rischi elevati in materia di protezione dei dati l'Incaricato continua a insistere sull'impiego responsabile dei moderni strumenti di lavoro quali la valutazione d'impatto sulla protezione dei dati ed eventualmente anche l'istituzione di organi aziendali preposti alla protezione dei dati. Ciononostante nell'anno in esame la quota delle nostre spese complessive per l'accompagnamento consultivo di progetti dell'economia privata è ancora aumentata.

Dopo che nel periodo precedente le spese per i compiti di controllo erano nettamente diminuite, è ora stato possibile riportarle al livello del periodo 2016/17. Tali spese sono tuttavia sempre inferiori al valore medio di diversi periodi precedenti. Visto che la nostra autorità è dotata di mezzi finanziari costantemente limitati, il rialzo delle spese è stato possibile unicamente tagliando altre prestazioni. A proposito del trattamento di dati personali da parte delle applicazioni per consumatori e delle reti sociali, anche nel periodo in rassegna l'Incaricato non è riuscito a soddisfare nella misura auspicata le giustificate aspettative dell'opinione pubblica circa l'adozione di misure in materia di diritto della vigilanza (cfr. n. 3.1 «Compiti e risorse»).

Nell'ambito della consulenza l'IFPDT ha posto un accento particolare in vista del rinnovo del Parlamento federale nell'autunno 2019: nel dicembre 2018 ha pubblicato, assieme alle autorità cantonali per la protezione dei dati, le Linee guida per l'applicazione del diritto in materia di protezione dei dati al trattamento digitale di dati personali in relazione a elezioni e votazioni (www.edoeb.admin.ch/elezioni). Le Linee guida rendono tutti gli attori consapevoli del fatto che i dati personali relativi a opinioni politiche e ideologiche soggiacciono a un livello di protezione superiore rispetto ai dati trattati nel contesto commerciale. Tenuto conto del loro ruolo centrale nello svolgimento delle elezioni federali dell'autunno 2019, i partiti politici sono esortati ad assumere un comportamento esemplare per quanto riguarda la protezione dei dati.

Quanto più tempo la Svizzera impiegherà per sancire esplicitamente tali strumenti nella sua legislazione in materia di protezione dei dati, tanto più spesso le imprese locali – indipendentemente dai loro effettivi investimenti nella protezione dei dati – si vedranno confrontate con domande critiche circa il livello di protezione regolatorio vigente nello Stato in cui hanno la sede.

III Cooperazione nazionale e internazionale

L'IFPDT ha ulteriormente intensificato la cooperazione con gli organi cantonali e comunali preposti alla protezione dei dati, confrontati con gli stessi sviluppi e le stesse tecnologie per il trattamento di dati personali. Per esempio: la valutazione Schengen (cfr. n. 1.2), guida alle elezioni (n. 1.1) o la realizzazione comune della giornata internazionale della protezione dei dati (n. 3.2).

Nuovo diritto europeo in materia di protezione dei dati

Il 25 maggio 2018 è entrato in vigore il GDPR, che in determinate circostanze si applica anche al trattamento di dati da parte di imprese svizzere. Nell'autunno 2017 l'IFPDT ha pubblicato un promemoria, aggiornato costantemente, che illustra in particolare la validità extraterritoriale del nuovo diritto dell'UE (https://www.edoeb.admin.ch/edoeb/it/home.html, Consigli per il GDPR). Continueremo ad aiutare con il massimo impegno le imprese svizzere interessate dall'applicazione del GDPR e ad affermare anche all'estero la nostra presenza quale autorità di vigilanza.

Il prolungato periodo transitorio fino all'entrata in vigore della revisione totale della LPD, sempre pendente in Parlamento (cfr. n. 1.1 e 3.1), continua a rappresentare una sfida per l'IFPDT. Mentre le autorità omologhe degli Stati dello SEE, che dispongono di sufficienti risorse di personale, fanno già da tempo valere le loro nuove competenze d'impartire direttive e di sanzionare (cfr. sopra), nei confronti dell'economia e della maggior parte dell'Amministrazione federale l'Incaricato continua a disporre soltanto della competenza di rilasciare raccomandazioni prevista dalla LPD del 1992. Anche i mezzi finanziari a sua disposizione sono rimasti essenzialmente invariati dal 2005 (cfr. n. 3.1 del presente rapporto). Un ulteriore fattore di complicazione è che la Commissione europea ha avviato la valutazione del livello di protezione dei dati in Svizzera.

In seguito all'entrata in vigore del GDPR l'ex gruppo di lavoro «Articolo 29» delle autorità dell'UE preposte alla protezione dei dati si è ricostituito come Comitato europeo per la protezione dei dati (CEPD). Il compito principale del CEPD consiste nell'assicurare l'applicazione uniforme del GDPR. La richiesta dell'Incaricato di essere ammesso generalmente come osservatore è stata respinta. La nostra partecipazione sarà limitata alle sedute plenarie e unicamente per gli aspetti concernenti l'acquis di Schengen.

Valutazione del livello di protezione

La Commissione europea valuta il livello di protezione dei dati nei paesi terzi. Ha certificato alla Svizzera nel 2000 che il suo livello di protezione dei dati è adeguato. Le imprese dell'UE possono quindi scambiare dati personali con le imprese svizzere senza ulteriori misure. La Commissione sta attualmente riesaminando l'adeguatezza del livello svizzero di protezione dei dati sulla base dei criteri elencati nel GDPR. Ha annunciato che pubblicherà la decisione di adeguatezza sotto forma di relazione nel maggio 2020. La partecipazione della Svizzera alla valutazione è coordinata dall'Ufficio federale di giustizia e sostenuta dall'IFPDT fornendo le informazioni richieste (cfr. n. 1.9).

Nel contesto dell'attuale valutazione, sarebbe vantaggioso per la Svizzera se ciò non fosse più possibile sulla base della DSG del 1992, ma piuttosto sulla base della DSG completamente rivista, che deve ancora essere trattata dalla Commissione del Consiglio nazionale (cfr. cifra I). Sarebbe inoltre opportuno che il Consiglio federale si avvalesse del fatto che la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati personali (Convenzione 108) del Consiglio d'Europa è aperta alla firma dall'ottobre 2018, poiché la Commissione europea ha ripetutamente sottolineato che la ratifica di questa Convenzione modernizzata rappresenta un criterio decisivo per la decisione di adeguatezza.

Swiss-US Privacy Shield

Nell'autunno 2018, nel quadro di una delegazione capeggiata dalla Seco, abbiamo eseguito in quanto autorità di vigilanza la verifica del Swiss-US Privacy Shield, che ha fatto seguito alla seconda verifica dello scudo UE-USA per la privacy a Bruxelles. Seppure il riesame ha dimostrato certi punti deboli, è stato possibile migliorare nel complesso il funzionamento del Privacy Shield dalla sua entrata in vigore.

Gli elettori hanno il diritto di sapere in base a quali insiemi di dati e metodi di trattamento e tecnologie digitali vengono contattati dai partiti o da terzi affini.

IV Misure per accrescere l'efficienza

Per affrontare le sfide prospettate nel rapporto l'Incaricato riafferma il proprio obiettivo strategico, che è quello di assolvere ai suoi compiti di legge nella realtà digitale in modo competente, indipendente e proattivo.

Organizzazione e controllo degli affari dell'autorità

La riorganizzazione dell'autorità, entrata in vigore il 1° aprile 2017, ha dimostrato la sua efficacia. Il programma di consolidamento EFFET, avviato nell'anno in rassegna successivamente alla riorganizzazione e all'inchiesta del personale, è inteso a ottimizzare la collaborazione interna e a rafforzare in tal modo l'efficienza della nostra autorità.

L'anno in rassegna ha registrato anche numerosi avvicendamenti a livello direttivo: dopo 38 anni trascorsi alla Confederazione quale esperto della protezione dei dati, 25 dei quali in qualità di supplente dell'Incaricato, Jean-Philippe Walter è andato in pensione alla fine del gennaio 2019. Gli è succeduto Marc Buntschu, anch'egli francofono, che è diventato il nuovo Incaricato supplente e il capo della Sezione per la cooperazione nazionale e internazionale. Fino al 1° febbraio 2019 Marc Buntschu è stato a capo dell'ambito direzionale Protezione dei dati; da allora questo settore è diretto da Daniel Dzamko, precedentemente attivo nella direzione dell'Amministrazione delle contribuzioni del Cantone di Berna. Nella primavera 2018 Hugo Wyler è stato nominato capo del Settore comunicazione, un ambito che è ora direttamente subordinato all'Incaricato.

L'IFPDT adempie in modo autonomo i compiti legali che gli incombono nella sua qualità di autorità di vigilanza. Beneficia ad ogni modo del sostegno logistico e amministrativo della Cancelleria federale, che fornisce queste prestazioni conformemente agli standard generali della stessa Amministrazione. Un'assistenza in tal senso gli è stata fornita dalla Cancelleria federale anche per quanto riguarda l'introduzione del nuovo sistema di gestione elettronica degli affari Acta Nova, conclusasi con successo nel settembre 2018.

Offerta informativa

L'offerta informativa proposta nel periodo in rassegna è stata migliorata in alcuni suoi aspetti specifici, in particolare per quanto riguarda questo 26° Rapporto d'attività. Lo sviluppo dei contenuti e dei canali di diffusione comporterà invece un impegno più diluito nel tempo, che la nostra autorità dovrà affrontare con risorse limitate (cfr. n. 3.2).

Procedura nell'ambito della legge sulla trasparenza (LTras)

Dopo un esperimento pilota durato un anno, l'IFPDT ha adottato una procedura accelerata e sommaria che si caratterizza per l'esecuzione di udienze di conciliazione orali. Questa procedura continua a dimostrarsi valida: oltre al numero di mediazioni conclusesi in modo consensuale, che resta proporzionalmente elevato, si è riusciti a fare in modo che i termini di legge non venissero superati, salvo in alcuni casi complessi dal punto di vista processuale e materiale, come ad esempio le procedure che implicano questioni particolarmente ardue sul piano giuridico, tecnico o politico a causa dell'ingente mole di documentazione richiesta o qualora sia previsto il coinvolgimento di terzi.

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali

Revisione della legge federale sulla protezione dei dati (LPD)

Non è ancora chiaro quando le Camere federali concluderanno le deliberazioni sulla revisione totale della legge sulla protezione dei dati del 1992.

Il 15 settembre 2017 il Consiglio federale ha trasmesso alle Camere federali il messaggio concernente la revisione totale della legge federale sulla protezione dei dati (17.059). Nel quadro delle deliberazioni sulla revisione della LPD la Commissione delle istituzioni politiche del Consiglio nazionale, quale Camera prioritaria, ha deciso di trattare in una prima fase soltanto le modifiche necessarie per recepire l'acquis di Schengen. Queste disposizioni, circoscritte alle autorità federali di perseguimento penale della Confederazione, nel frattempo sono state approvate dal Parlamento e messe in vigore dal Consiglio federale il 1° marzo 2019 (cfr. LPD Schengen n. 1.2).

La Commissione summenzionata non ha invece ancora terminato le deliberazioni sulla revisione totale delle disposizioni della LPD riguardanti le rimanenti autorità e aziende federali e l'economia privata. Al momento della stampa del presente rapporto non era dunque possibile sapere quando il Consiglio nazionale al completo, quale Camera prioritaria, si occuperà del testo (cfr. cifre I e 1.9).

Linee guida per la protezione dei dati nel contesto di elezioni e votazioni

Nell'anno in rassegna, in collaborazione con le autorità cantonali preposte alla protezione dei dati e con esperti l'IFPDT ha redatto le linee guida per il trattamento dei dati personali in relazione a elezioni e votazioni.

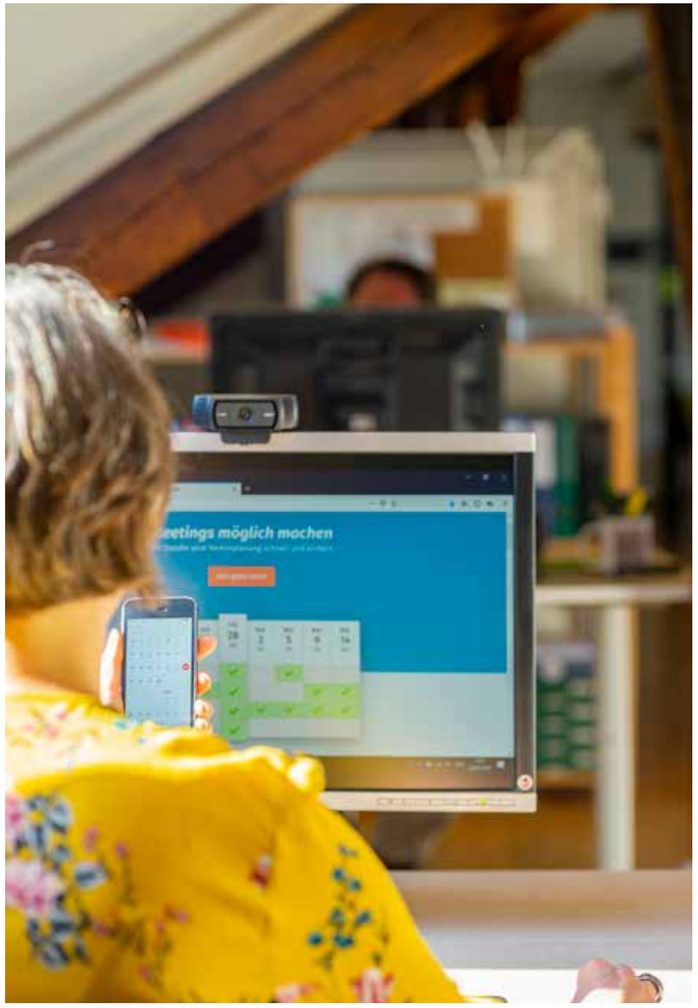
In collaborazione con la Conferenza degli incaricati svizzeri per la protezione dei dati (privatim) e in stretta concertazione con la Cancelleria federale, l'IFPDT ha istituito un gruppo di lavoro con l'obiettivo di sensibilizzare l'opinione pubblica sui rischi sistemici del trattamento dei dati personali in relazione a elezioni e votazioni. Nell'anno in rassegna il gruppo di lavoro, composto oltre che da specialisti di protezione dei dati anche da un politologo, ha consultato diversi esperti. I risultati sono stati recepiti in apposite linee guida, il cui scopo è aiutare i soggetti coinvolti nel processo di formazione dell'opinione politica ad applicare la legge federale sulla protezione dei dati (LPD), risalente al 1992, al trattamento di dati associati a elezioni e votazioni nel dinamico contesto della digitalizzazione.

Raccolta indebita di dati prima di una votazione

Prima della votazione sulla cosiddetta iniziativa per l'autodeterminazione a novembre 2018 un'agenzia, dopo aver ricevuto un mandato, ha raccolto dati personali in modo indebito scaricandoli da un sito. Dopo il nostro intervento ha modificato la sua prassi.

Sul sito internet 25november.ch singole persone potevano registrare fino a dieci numeri di telefonia mobile con nome e cognome di congiunti e amici. Durante il fine settimana della votazione questi ultimi hanno ricevuto sms apparentemente spediti dalla persona che ne aveva registrato i dati mettendoli così a disposizione di terzi. L'IFPDT si è occupato della questione scrivendo all'esercente del sito e chiedendogli di assicurarsi che tutte le persone, i cui numeri di telefonia mobile vengono registrati, siano messe al corrente del fatto che i dati vengono elaborati e a quale scopo indicando chi sia responsabile del loro dossier. Ha precisato che i dati personali possono essere elaborati solo se esiste un consenso giuridicamente valido alla loro raccolta, trasmissione e ad ogni altro trattamento. Inoltre l'esercente deve garantire che i dati personali siano utilizzati solo per inviare sms d'invito a votare e poi cancellati, senza essere conservati per eventuali future campagne di votazione. Sul sito mancava anche una dichiarazione ben visibile e completa sulla protezione dei dati, ma l'esercente ha rapidamente provveduto ad aggiungerla.

Le linee guida invitano questi soggetti a garantire agli aventi diritto di voto la massima trasparenza e la massima autodeterminazione, utilizzando a tal fine opportune applicazioni rispettose della protezione dei dati. Chiunque tratti dati nell'ambito di elezioni e votazioni dovrebbe essere consapevole del fatto che il diritto in materia di protezione dei dati sottopone i dati concernenti opinioni politiche e ideologiche a un livello di protezione più elevato rispetto a dati comparabili in un contesto commerciale. Le linee guida si rivolgono a tutti i soggetti coinvolti nella formazione dell'opinione politica, come partiti e gruppi d'interesse, fornitori di dati e piattaforme di dati, sollecitandoli a rendere i metodi digitali di trattamento riconoscibili e comprensibili per l'elettorato.



Utilizzo sistematico del numero AVS da parte delle autorità

Il Consiglio federale intende promuovere un utilizzo più ampio del numero AVS e il 7 novembre 2018 ha avviato una consultazione sulla modifica della legge concernente l'AVS. La procedura di consultazione si è conclusa il 22 febbraio 2019. Abbiamo colto l'occasione per presentare le nostre osservazioni in via preliminare, le quali sono state incluse nel disegno di legge.
Il disegno posto in consultazione dal Consiglio federale prevede di autorizzare le amministrazioni federali, cantonali e comunali all'utilizzo sistematico del numero AVS quale identificatore unico al di fuori del settore delle assicurazioni sociali.

Accogliamo con favore il fatto che, in seguito alle nostre osservazioni, il disegno di legge del Consiglio federale preveda espressamente che i soggetti che dispongono di banche dati in cui il numero AVS viene utilizzato sistematicamente procedano periodicamente a un'analisi dei rischi, tenendo conto in particolare del pericolo di collegamenti non autorizzati di dati e che sulla base di tale analisi si definiscano e si attuino misure di sicurezza e di protezione dei dati adeguate alla situazione di rischio e conformi allo stato della tecnica.

Accogliamo altresì con favore l'obbligo per i soggetti proposti dal disegno di legge che utilizzano sistematicamente il numero AVS di tenere un registro delle banche dati pertinenti, che funga in particolare da base per le analisi dei rischi da effettuare. Infine, abbiamo sottolineato la necessità di consolidare le misure tecniche e organizzative.

Come l'Ufficio federale delle assicurazioni sociali (UFAS) ha comunicato all'IFPDT, il «Piano di sicurezza per gli identificatori personali», richiesto dal postulato 17.3968 della Commissione degli affari giuridici del Consiglio nazionale entro la fine di quest'anno, sarà integrato nel messaggio nell'ambito dei lavori legislativi relativi all'AVS. Questo piano di sicurezza dovrebbe dimostrare come sia possibile affrontare i rischi correlati all'utilizzo del numero AVS quale numero d'identificazione personale unico e rafforzare la protezione dei dati.

Rimaniamo chiaramente a favore dell'utilizzo di identificatori personali settoriali, giacché si ridurrebbero notevolmente i rischi associati, in particolare l'interconnessione inammissibilie di banche dati e di sistemi informatici separati. In tal senso, dal progetto posto in consultazione si può altresì dedurre che dovrebbe essere possibile continuare a prescrivere identificatori personali settoriali al posto del numero AVS in disposizioni legali speciali per determinati scopi, come ad esempio la cartella informatizzata del paziente.

Valori di riferimento per una politica dei dati della Svizzera

Durante la consultazione degli uffici, l'IFPDT ha avuto modo di esprimere il proprio parere sui valori di riferimento per una politica dei dati in Svizzera. L'IFPDT continua a occuparsi di settori specifici della politica dei dati.
Nel quadro della consultazione degli uffici, l'IFPDT ha segnalato che le disposizioni in materia di protezione dei dati devono essere rispettate non soltanto nel caso degli Open Government Data (OGD) ma anche in tutta una serie di altri settori, tra cui: amministrazione dei dati di base della Confederazione, dati di aziende parastatali e istituti di ricerca, innovazione dei dati in ambito statistico e innovazione mediante dati nei settori della mobilità e della salute. Ha inoltre fatto osservare che con i dati anonimizzati permane sempre il rischio, a seconda della quantità di dati disponibili, che si possa risalire all'identità delle persone interessate, per cui la protezione dei dati va tenuta conto anche in questo caso. L'IFPDT ha poi ribadito che, dalla consultazione degli uffici sulla LPD, si sta adoperando per introdurre un diritto alla portabilità dei dati. Le osservazioni dell'IFPDT sono state recepite.

Attualmente sono in corso a livello federale vari progetti, coordinati dall'UFCOM, sul tema della digitalizzazione e della politica dei dati. L'IFPDT partecipa attivamente ad alcuni di essi, come quello riguardante l'utilizzo dei dati, o al sottogruppo di lavoro sulla disponibilità dei dati.

Comitato consultivo «Trasformazione digitale»

A marzo 2019 l'Incaricato ha partecipato alla sesta seduta del Comitato consultivo «Trasformazione digitale» dei dipartimenti DEFR e DATEC. Lo scopo delle sedute è indicare i risultati concreti e i vantaggi che alcuni campi della trasformazione digitale possono apportare all'economia e alla popolazione. Il progetto «Swiss Data Custodian» è un sistema fiduciario che rappresenta una soluzione per dati che non possono essere resi accessibili al pubblico. Il gestore del «Custodian» riceve dati personali e altri dati grezzi da varie aziende – eventualmente anche da autorità pubbliche –, li sottopone a un'analisi mediante intelligenza artificiale e infine mette a disposizione i risultati anonimizzati per l'utilizzo a valore aggiunto. È attualmente in discussione un'applicazione nei settori della mobilità, della medicina e degli affari umanitari. Tanto nelle sedute preparatorie quanto nella sesta seduta consultiva l'IFPDT ha colto l'occasione per presentare le condizioni quadro previste dalle disposizioni sulla protezione dei dati e le indicazioni di cui è necessario tenere conto. Per il futuro, intende continuare a seguire il progetto.

Collegamenti di dati in ambito statistico

Se, da un lato, i collegamenti permettono di acquisire nuove conoscenze a partire dalle banche dati statistiche, dall'altro possono aumentare significativamente il rischio di reidentificazioni. Per contrastare questo fenomeno, l'Ufficio federale di statistica (UST) ha emanato un apposito regolamento.
L'UST dispone delle basi legali per attuare i cosiddetti «collegamenti». Tali collegamenti di dati provenienti da diverse rilevazioni sono un valido strumento in ambito statistico per acquisire nuove conoscenze a partire dalle banche dati esistenti, osservare gli sviluppi nell'arco di diversi anni o fare previsioni. A tal fine si dotano i singoli set di dati delle varie banche dati di numeri di identificazione, dopodiché si genera un identificatore di collegamento.

In termini di protezione dei dati, ai collegamenti viene associato il rischio di reidentificazione, vale a dire la possibilità di risalire all'identità di determinate persone. I numeri di identificazione e gli identificatori devono quindi essere gestiti internamente in modo tale da escludere tali deduzioni e quindi evitare abusi. L'IFPDT ha chiesto informazioni all'UST sui progetti in corso e previsti riguardanti i collegamenti nonché sulle misure per tutelare i diritti della personalità. Lo scambio ha evidenziato la complessità del tema, che l'IFPDT continuerà a monitorare. Accogliamo con favore il fatto che l'UST abbia emanato e pubblicato un regolamento specifico sui collegamenti.

Tema: prova elettronica dell'identità (eID)

Un'identità elettronica riconosciuta a livello statale mira a garantire l'identità di una persona nelle applicazioni elettroniche. L'IFPDT monitora questo grande progetto digitale in tutte le sue fasi e chiede che venga garantita con assoluta priorità una protezione dei dati sufficiente.

La certezza del diritto e la fiducia sono presupposti fondamentali per la gestione delle transazioni. In tal senso, per diversi processi è essenziale che sia garantita l'identità della controparte. Per il mondo analogico la Confederazione mette a disposizione mezzi di identificazione convenzionali, vale a dire il passaporto svizzero, la carta d'identità e la carta di soggiorno. Con la migrazione dei processi economici nel mondo digitale cambiano i requisiti posti alle possibilità di identificazione. Inoltre, l'identità di una persona fisica deve poter essere comprovata mediante un'identità elettronica (eID) riconosciuta a livello statale.

L'eID rappresenterà uno strumento centrale per accedere online a importanti servizi privati, come l'apertura di un conto bancario, e ad applicazioni di e-government, come l'ordinazione di un estratto del casellario giudiziale. Per questo motivo l'IFPDT ha sempre accompagnato con un atteggiamento favorevolmente critico sia il progetto legislativo per un'eID riconosciuta a livello statale sia l'attuazione concreta del progetto presso SwissSign Group SA (cfr. capitolo La «SwissID» in basso) chiedendo che i requisiti giuridici fondamentali in materia di protezione dei dati siano integrati già nella fase concettuale del progetto.

Il 1º giugno 2018 il Consiglio federale ha adottato il messaggio concernente la legge sui servizi d'identificazione elettronica (Legge sull'eID, LSIE), che disciplina legalmente l'identità riconosciuta a livello statale. Alla fine di marzo il disegno di legge è stato approvato dal Consiglio nazionale con 128 voti contro 48.

Imprese private riconosciute a livello statale come identity provider

Dopo l'audizione dei gruppi interessati da parte della sua Commissione degli affari giuridici, il Consiglio nazionale si è pronunciato contro una soluzione esclusivamente statale, caldeggiando invece una ripartizione dei compiti: le imprese private riconosciute a livello statale – i cosiddetti identity provider (IdP) – sono autorizzate a rilasciare identità elettroniche. Gli IdP vengono riconosciuti dall'Organo direzione informatica della Confederazione (ODIC), il quale esamina inoltre il rispetto dei processi predefiniti e degli standard tecnici da parte degli IdP e, in base a tale esame, concede, proroga o revoca il riconoscimento. Un'interfaccia elettronica gestita dall'Ufficio federale di polizia (fedpol) metterà a disposizione degli IdP dati personali di identificazione, archiviati in registri gestiti e conservati dallo Stato, al solo scopo di identificazione. Da un lato, con la ripartizione dei compiti si assicurano condizioni quadro affidabili e garanti di sicurezza che le istituzioni statali possono applicare nelle procedure di riconoscimento e vigilanza. Dall'altro lato, si lascia che siano le imprese private a occuparsi dell'attuazione tecnica e della commercializzazione di eID.

Consultazione dell'IFPDT come condizione per il riconoscimento

In occasione della consultazione con la Commissione, l'IFPDT ha spiegato che il suo compito è di garantire il massimo livello possibile di protezione dei dati, a prescindere dalla decisione politica a favore di una soluzione interamente o parzialmente statale. L'IFPDT ha chiaramente indicato che il trattamento dei dati da parte degli attori statali deve fondarsi su una base legale sufficiente, chiedendo in proposito miglioramenti specifici della legge sull'eID. Il Consiglio nazionale ha recepito nella legge la consultazione preliminare dell'IFPDT da parte dell'ODIC come presupposto per il riconoscimento degli IdP. In questo contesto l'IFPDT chiederà che gli standard in materia di protezione dei dati, che ha elaborato nel quadro del monitoraggio del progetto SwissSign (cfr. La «SwissID»), fungano da parametro per la valutazione.

L'IFPDT ha inoltre insistito affinché nel messaggio, ritenuto poco chiaro, si precisi che l'utilizzo dell'eID deve essere limitato alle transazioni commerciali che richiedono un'identificazione sicura. Per le numerose operazioni o gli acquisti di servizi in cui ciò non è necessario, non si devono creare nuovi obblighi di identificazione con la legge sull'eID, tanto nelle transazioni commerciali analogiche quanto in quelle elettroniche. Il Consiglio nazionale ha modificato di conseguenza l'articolo sullo scopo della legge.

La «SwissID»

Con una «SwissID» un fornitore privato mette a disposizione del mercato un'identità elettronica. L'IFPDT monitora il progetto riunendosi regolarmente con i responsabili che hanno recepito le sue indicazioni.

Con il suo prodotto «SwissID», SwissSign Group SA – una joint venture di aziende parastatali, società finanziarie, compagnie di assicurazione e casse malati – sta lavorando all'introduzione su diverse piattaforme di un'identità elettronica per le transazioni commerciali online su base privata. Tra i partner contrattuali del servizio online di SwissSign figurano aziende importanti come La Posta Svizzera, Swisscom, Coop e Ringier, e altre continuano ad aggiungersi, come ad esempio le FFS. Diversi Cantoni prevedono di utilizzare «SwissID» per le loro applicazioni di e-government o l'hanno già introdotta.

Per ora «SwissID» si basa ancora su una procedura di login con password, ma in vista dell'entrata in vigore della LSIE (cfr. articolo sull'eID) dovrebbe essere aggiornata come identità elettronica su base privata, affinché gli utenti possano concludere transazioni giuridiche private che richiedono un'identificazione online e acquistare servizi statali online.

Servono maggiori analisi dei rischi in materia di protezione dei dati

Si tratta di un grande progetto digitale, significativo anche in materia di protezione dei dati. L'IFPDT è regolarmente in contatto con i responsabili del progetto, dà loro consigli puntuali e fornisce riscontri sulla documentazione e sulle informazioni che gli vengono sottoposte. SwissSign è consapevole dell'importanza della protezione dei dati nelle sue attività di trattamento degli stessi e ha adottato misure tecniche e organizzative fondamentali a tale scopo. L'IFPDT ha tuttavia fatto osservare la necessità di ampliare le analisi dei rischi associati al progetto per quel che riguarda la protezione dei dati, ritenendo opportuna l'adozione di misure preventive adeguate. Riteniamo inoltre indispensabile la nomina di un responsabile aziendale della protezione dei dati, che controlli costantemente i rischi e le relative misure e possa prendere posizione sulle decisioni aziendali dal punto di vista della protezione dei dati.

I responsabili di progetto di SwissSign concordano con le indicazioni dell'IFPDT e si adopereranno per ampliare le loro analisi e i loro documenti in materia di trattamento dei dati personali. L'azienda ha quindi provveduto a nominare un proprio responsabile della protezione dei dati.

1.2 Giustizia, polizia, sicurezza

Misure di polizia contro il terrorismo

Nell'ambito della seconda consultazione degli uffici sul disegno di legge federale concernente le misure di polizia per la lotta al terrorismo ancora una volta l'IFPDT ha formulato numerose osservazioni. Ha ribadito la sua esigenza di elaborare una legislazione unificata a livello federale. Chiede inoltre di limitare l'accesso alle banche dati della polizia da parte delle autorità preposte alla migrazione.

L'IFPDT ha criticato di nuovo il gran numero di leggi che disciplinano le attività di polizia della Confederazione. Inoltre, i dati di polizia sono trattati in modo confuso in diverse banche dati e in un numero crescente di applicazioni. L'attuale disegno di legge federale sulle misure di polizia per la lotta al terrorismo (MPT) aggrava la situazione. Per questi motivi, l'IFPDT ha ribadito la propria richiesta di elaborare una legislazione unificata a livello federale, così come esiste a livello cantonale. Ha anche ricordato l'importanza di una chiara separazione delle competenze tra il Servizio delle attività informative della Confederazione (SIC) e fedpol.

L'IFPDT ha inoltre messo in dubbio l'utilità per la Segreteria di Stato della migrazione (SEM) di avere accesso ai sistemi d'informazione di cui agli articoli 10, 11, 12 e 14 della legge federale sui sistemi d'informazione di polizia della Confederazione (LSIP). Le basi legali proposte nelle leggi sugli stranieri e sull'asilo riguardano esclusivamente la collaborazione e il coordinamento tra la SEM e fedpol. Queste disposizioni non costituiscono basi giuridiche che conferiscono alla SEM un mandato legale esplicito per individuare atti terroristici e combattere il terrorismo. Inoltre, gli accessi in questione riguardano dati di polizia giudiziaria o relativi ad analisi criminali: si tratta di dati molto sensibili, alcuni peraltro non ancora accertati. L'accesso a dati simili da parte delle autorità di migrazione deve avvenire attraverso l'assistenza amministrativa e non online. In questo modo fedpol potrebbe ridurre la diffusione di tali dati allo stretto necessario.

Da ultimo, l'IFPDT ha anche precisato che la consultazione del sistema di ricerca informatizzato di polizia (RIPOL) non consentirà alla polizia dei trasporti di adempiere il suo mandato legale, che consiste nel controllare l'identità di una persona o nell'identificare una persona. Questo poiché il RIPOL indica se una persona è o meno oggetto di segnalazione. Un accesso di questo tipo al RIPOL richiede, da un lato, la modifica proposta della legge sui sistemi d'informazione della polizia federale e, dall'altro lato, adeguamenti della legge federale sugli organi di sicurezza delle imprese di trasporto pubblico.

Swiss-US Privacy Shield. Necessari alcuni miglioramenti

Nell'autunno 2018 ha avuto luogo a Bruxelles il riesame dello scudo UE-USA per la privacy (EU-US Privacy Shield) e, per la prima volta, anche dello Swiss-US Privacy Shield. Le autorità statunitensi hanno apportato miglioramenti in diversi ambiti che vanno a beneficio anche della Svizzera. Ulteriori sforzi di coordinamento sono invece ancora necessari ad esempio nell'ambito dei dati relativi alle risorse umane.

Nell'anno in rassegna sono stati notificati all'IFPDT due casi concernenti aziende che si sono fatte passare erroneamente come certificate per lo Swiss-US Privacy Shield («false claims»). Entrambi i casi sono stati risolti in collaborazione con il Dipartimento del commercio statunitense (US Department of Commerce, DoC). (cfr. anche il n. 1.4 del Rapporto sul primo riesame annuale dello Swiss-US Privacy Shield). Inoltre, interessati provenienti dalla Svizzera hanno presentato circa dieci reclami fondati presso organi di ricorso indipendenti (Independent Recourse Mechanism, IRM). Per quanto riguarda l'organo di mediazione, che mira a porre rimedio all'accesso a dati personali da parte di autorità, l'IFPDT non è ancora stato confrontato con nessun caso.

La conclusione ovvia è che finora ci si è avvalsi molto poco degli strumenti giuridici messi a disposizione dallo Swiss-US Privacy Shield. Va tuttavia osservato che l'accordo svizzero è in vigore soltanto da aprile 2017 e che prima di presentare un reclamo ufficiale occorre affrontare di regola l'azienda certificata. Si può dunque presumere che sia stato possibile risolvere in questo modo un numero difficilmente quantificabile di violazioni della protezione dei dati.

Primo riesame da parte dell'IFPDT

Il riesame del Privacy Shield riguardava sia gli aspetti commerciali (p. es. controllo e osservanza degli obblighi delle aziende certificate) sia l'accesso da parte delle autorità ai dati relativi alle persone per scopi di sicurezza nazionale. La Svizzera aveva potuto partecipare al precedente riesame dell'EU-US Privacy Shield con lo statuto di osservatore. Argomenti che concernevano sia lo Swiss-US sia l'EU-US Privacy Shield sono stati oggetto di discussione unicamente durante il riesame EU-US. Le esperienze acquisite hanno potuto essere messe a frutto anche per l'accordo svizzero-statunitense.

Dall'entrata in vigore dello Swiss-US Privacy Shield è stato possibile apportare diversi miglioramenti. Per quanto riguarda gli aspetti commerciali, il Dipartimento del commercio degli Stati Uniti è ad esempio sempre più alla ricerca di «false claims». Le autorità statunitensi verificano inoltre a intervalli più regolari che le aziende certificate correttamente non presentino eventuali punti deboli e, in sede di certificazione, sono più severe nel vigilare che non vi siano discrepanze tra i dati nelle rispettive politiche sulla tutela dei dati personali e lo stato effettivo del processo di registrazione.

Per il procedimento arbitrale, che è a disposizione delle persone interessate presso un collegio arbitrale soggetto al diritto americano dopo che sono stati esauriti tutti gli altri rimedi giuridici (IRM) (cfr. 24° Rapporto d'attività 2016/2017, n.1.8.1), è stato possibile nominare già prima del riesame cinque ulteriori arbitri per la Svizzera che completano l'elenco dell'UE.

In vista dell'accesso delle autorità è stato possibile fare progressi a monte del riesame. Il Senato statunitense ha confermato la nomina della presidenza e di due membri dell'Autorità per la tutela della vita privata e delle libertà civili (Privacy and Civil Liberties Oversight Board, PCLOB), cosicché il quorum necessario è raggiunto. Durante il primo anno di Swiss-US Privacy Shield il PCLOB era composto da un unico membro e non era perciò atto a deliberare validamente.

Esiste un potenziale di miglioramento

In diversi ambiti l'IFPDT condivide l'opinione del Comitato europeo per la protezione dei dati (CEPD; European Data Protection Board, EDPB) secondo cui è opportuno apportare ulteriori miglioramenti. Sarebbe necessario, tra l'altro, che le autorità statunitensi verifichino in modo più sostanziale l'ottemperanza di aziende certificate, per esempio l'adeguatezza e la proporzionalità in caso di trasferimento di dati a terzi. Occorre inoltre trovare una soluzione circa l'interpretazione della definizione «dati relativi alle risorse umane» da parte delle autorità statunitensi, da un lato, e dell'IFPDT e di rappresentanti del CEPD, dall'altro. I dati relativi alle risorse umane beneficiano di una protezione ampliata grazie all'accordo Privacy Shield. Secondo l'IFPDT occorre interpretare la definizione in modo più esteso di quanto previsto dal DoC.

In vista dell'accesso delle autorità ai dati personali occorre tra l'altro assicurare che sia nominato un mediatore (ombudsman) che, di fronte alle autorità statunitensi che operano accessi nell'ambito della sicurezza nazionale, disponga della competenza e dell'indipendenza necessarie.

Anche se il riesame ha messo in luce punti deboli, è stato possibile migliorare nel complesso il funzionamento del Privacy Shield dalla sua entrata in vigore.

Circa 2900 aziende statunitensi certificate

Lo Swiss-US Privacy Shield è in vigore dal 2017. Il Privacy Shield consente alle aziende statunitensi di trattare dati personali provenienti dalla Svizzera senza elaborare ulteriori clausole di protezione dei dati. Le aziende possono farsi certificare per il programma presso il Dipartimento del commercio degli Stati Uniti impegnandosi così a garantire un livello di protezione dei dati adeguato secondo il diritto svizzero. Gli interessati hanno a disposizione meccanismi in virtù dei quali possono difendersi da violazioni in materia di protezione dei dati.

Fino a febbraio 2019 si sono certificate per lo Swiss-US Privacy Shield 2883 aziende statunitensi tra cui Facebook, Microsoft (con 27 filiali) e Google.

Per rispettare la procedura di ricorso indipendente (Independent Recourse Mechanism, IRM) le aziende certificate possono scegliere se optare per l'organo di mediazione delle controversie statunitense (Alternative Dispute Resolution body, ADR) o sottoporsi alla vigilanza dell'IFPDT (cfr. Guida allo Swiss-US Privacy Shield).

Un riesame annuale del funzionamento dell'accordo avviene per il tramite della SECO (direzione) e l'IFPDT assieme alle autorità di vigilanza statunitensi.

Divulgazione dei dati dei passeggeri aerei negli Stati membri dell'UE

Diversi Stati membri dell'UE prevedono di richiedere i dati dei passeggeri di voli provenienti dalla Svizzera. Manca però una base legale, che ora deve essere creata a livello di ordinanza.

Nella primavera del 2018 l'Ufficio federale dell'aviazione civile (UFAC), l'Ufficio federale di giustizia (UFG), l'Ufficio federale di polizia (fedpol) e l'IFPDT si sono riuniti per discutere della divulgazione dei dati dei passeggeri aerei (dati PNR, Passenger Name Record) negli Stati membri dell'UE. La seduta si è svolta su iniziativa dell'UFAC, dal momento che le compagnie aeree erano state informate da diversi Stati dell'UE della loro intenzione di richiedere i dati PNR per i voli provenienti dalla Svizzera – in virtù della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio 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). Siccome però l'UE non ha dichiarato tale direttiva rilevante ai fini di Schengen, la Svizzera non è tenuta a recepirla automaticamente.

L'IFPDT ha sottolineato la necessità che la divulgazione dei dati PNR da parte delle compagnie aeree sotto forma di accordo poggi su una base legale. Mentre gli altri uffici federali coinvolti si sono espressi chiaramente a favore di una divulgazione incondizionata dei dati, l'IFPDT ha sostenuto che le compagnie aeree dovrebbero divulgare i dati agli Stati membri in attuazione della direttiva PNR dell'UE solo se sono soddisfatti determinati punti. La Svizzera deve quindi cercare di negoziare e ottenere il più rapidamente possibile un'associazione alla direttiva PNR dell'UE. In tal senso, fedpol prevedeva inizialmente di presentare al Consiglio federale ancora nell'autunno 2018 un progetto relativo, comprensivo del mandato di negoziazione con l'UE. Il progetto, però, è stato rimandato fino a nuovo avviso. Quando l'IFPDT ha saputo del rinvio, ha ribadito agli uffici federali coinvolti la necessità di istituire al più presto una base legale alternativa. All'IFPDT era stato prospettato di creare e prevedere la base legale per la fornitura di dati PNR agli Stati che la richiedono in virtù della direttiva PNR dell'UE mediante una revisione dell'ordinanza sulla navigazione aerea (ONA), per consentire la trasmissione di dati solo a Stati che hanno un livello adeguato di protezione in materia. L'IFPDT monitorerà i lavori legislativi fornendo la propria consulenza.

Sistema di prenotazione di Swiss. Richieste misure contro l'abuso di dati

Swiss International Air Lines adotta diverse misure supplementari per impedire eventuali abusi nel richiamare una prenotazione attraverso il suo sito Internet.

L'IFPDT è stato informato che, inserendo cognome, nome e numero di prenotazione al momento del login sul sito Internet di Swiss, è possibile accedere a diversi dati personali (nome, cognome, data di nascita, sesso, nazionalità, domicilio, numero e periodo di validità del passaporto o della carta d'identità). Di fatto, è molto semplice trovare cognome, nome e numero di prenotazione di altri passeggeri sulle carte d'imbarco che questi hanno lasciato in giro dopo un volo, gettato o pubblicato sui social media. Queste informazioni potrebbero essere lette anche dal codice a barre sulla carta d'imbarco, utilizzando una semplice applicazione per la lettura dei codici a barre. Effettuando il login, si possono visualizzare anche tutte le prenotazioni dei passeggeri interessati e, in parte, anche modificare i dati.

Siccome il contenuto della carta d'imbarco, compreso il codice QR, deve soddisfare determinati standard internazionali, le singole compagnie aeree non possono modificarlo molto facilmente. Tuttavia, queste ultime devono e possono adottare le misure necessarie per garantire che i dati dei passeggeri nel sistema di prenotazione siano adeguatamente protetti da eventuali trattamenti impropri.

In uno scambio tra Swiss e l'IFPDT sono state definite le misure supplementari da adottare per prevenire eventuali abusi. Swiss ha modificato le sue Condizioni generali di trasporto (CGT) per sensibilizzare meglio i propri clienti sulla necessità di proteggere i dati personali visibili sulla carta d'imbarco e memorizzati nel sistema di prenotazione. I clienti ricevono inoltre per e-mail un messaggio di avviso in tal senso anche dopo il check-in automatico. Se il check-in avviene online, è inoltre visualizzato l'indirizzo (e-mail, numero di cellulare) a cui viene inviato il messaggio. Lo scopo è di controllare che la carta d'imbarco sia inviata all'indirizzo corretto o desiderato. In aggiunta, il numero di passaporto, che in determinati casi è visibile quando si richiama la prenotazione nel sistema, deve essere reso parzialmente irriconoscibile. Per accedere alle prenotazioni effettuate non tramite un'agenzia di viaggi o altri terzi ma direttamente sul sito Internet della compagnia aerea, l'IFPDT aveva inoltre proposto che, oltre al nome e al riferimento della prenotazione, si prevedesse l'inserimento di un elemento aggiuntivo, come il numero di cellulare o l'indirizzo e-mail. Le discussioni su questo punto erano ancora in corso alla fine dell'anno in rassegna.

Entrata in vigore della legge sulla protezione dei dati in ambito Schengen

La legge sulla protezione dei dati in ambito Schengen (LPDS) è entrata in vigore il 1° marzo 2019. Oltre a introdurre varie novità rispetto alle competenze attuali dell'IFPDT, la legge gli attribuisce, tra le altre cose, competenze di inchiesta e decisionali per l'applicazione dell'acquis di Schengen per le questioni penali.

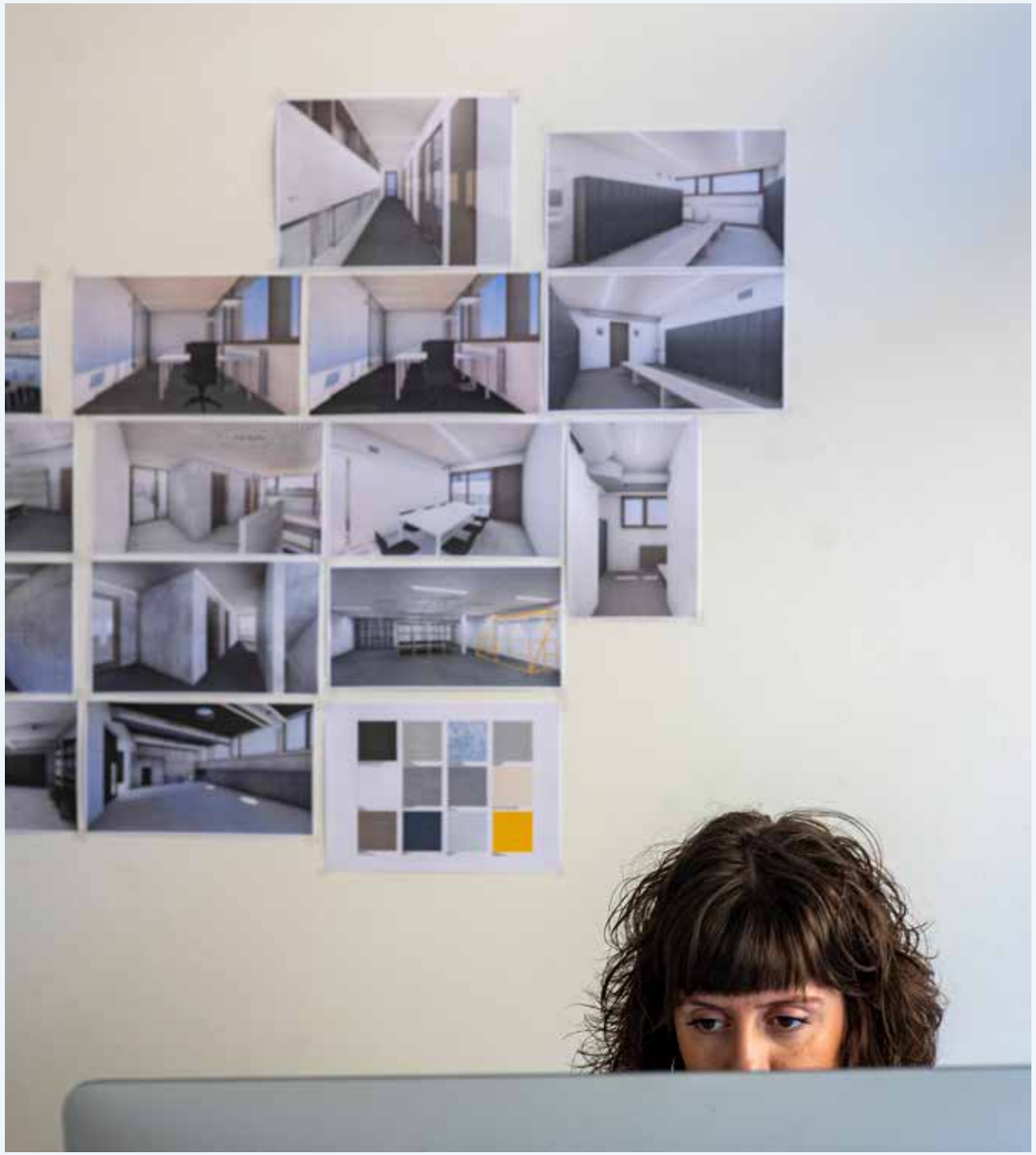
Nell'ambito dei suoi dibattiti sulla revisione della legge sulla protezione dei dati (LPD), il Parlamento aveva deciso di occuparsi in un primo tempo delle modifiche necessarie a recepire l'acquis di Schengen. Su questa base è stata approvata la legge federale sull'applicazione della direttiva (UE) 2016/680, entrata in vigore il 1° marzo 2019. Con questa legge federale non solo viene introdotta la legge sulla protezione dei dati in ambito Schengen (LPDS), ma vengono anche adeguate diverse leggi che, nell'ambito della collaborazione Schengen, si applicano in materia penale.

La LPDS si applica in particolare al trattamento dei dati personali da parte di organi federali in materia penale nell'ambito di applicazione dell'acquis di Schengen. Tra gli organi federali interessati, dunque, figurano non solo l'Ufficio federale di polizia (fedpol), l'Ufficio federale di giustizia (UFG) per quel che riguarda l'assistenza giudiziaria internazionale in materia penale e il Ministero pubblico della Confederazione, ma anche il Tribunale penale federale, il Tribunale federale e i giudici cantonali dei provvedimenti coercitivi, se operano per conto della Confederazione. La LPDS non si applica alle autorità cantonali. Spetta piuttosto ai Cantoni, se necessario, adattare la propria legislazione ai nuovi requisiti dell'UE.

La LPDS presenta principalmente le novità di seguito riportate.

- I dati genetici e biometrici, che permettono di identificare una persona in modo univoco, sono ora presentati come dati personali degni di particolare protezione.
- Il termine «profilazione» subentra all'espressione «profili della personalità», conformemente al diritto europeo. Per profilazione si intende qualsiasi trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare alcuni aspetti personali relativi a una persona fisica. Ciò serve in particolare per analizzare o prevedere aspetti relativi alle prestazioni lavorative, alla situazione economica, alla salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, alla localizzazione o agli spostamenti di tale persona.
- La protezione dei dati mediante la tecnologia e le impostazioni predefinite favorevoli alla protezione dei dati («privacy by design and default») sono sanciti come principi. Per dimostrare il rispetto delle prescrizioni relative alla protezione dei dati, l'organo federale deve prendere le necessarie precauzioni interne e adottare misure conformi a questi due principi.
- La decisione individuale automatizzata è disciplinata esplicitamente. Tale decisione esiste se la valutazione del contenuto dei dati e la decisione basata su di essi non è presa da una persona fisica, cioè se a decidere è la macchina e non l'essere umano.

- Se il trattamento dei dati previsto può comportare un rischio elevato per i diritti fondamentali delle persone interessate, gli organi federali devono effettuare valutazioni d'impatto sulla protezione dei dati e, in determinate circostanze, consultare l'IFPDT.
- Se l'organo federale ha eseguito una valutazione d'impatto sulla protezione dei dati, i risultati devono essere considerati nell'elaborazione delle misure.
- Gli organi federali devono notificare all'IFPDT le violazioni della protezione dei dati.
- L'IFPDT può ora emanare decisioni quale misura amministrativa.



Tema II: Valutazione Schengen della Svizzera – richieste risorse sufficienti per la protezione dei dati

Nel 2018 l'attuazione e l'applicazione dell'acquis di Schengen da parte della Svizzera quale membro associato sono state verificate per la terza volta. Esperti degli altri Stati Schengen e della Commissione europea hanno esaminato principalmente l'applicazione della normativa Schengen sulla protezione dei dati. Alla luce dei risultati, il Consiglio dell'UE ha formulato le proprie raccomandazioni alla Svizzera.

La valutazione, effettuata a intervalli massimi di cinque anni, riguarda tutti i settori della cooperazione Schengen: gestione delle frontiere esterne (aeroporti), ritorno/rimpatrio, sistema d'informazione Schengen SIS II/SIRENE, politica comune in materia di visti, cooperazione in materia di polizia e protezione dei dati.

I lavori di preparazione ed esecuzione della valutazione sono stati coordinati dall'Ufficio federale di giustizia (UFG) in collaborazione con la Direzione degli affari europei (DEA). L'IFPDT ha partecipato attivamente ai lavori della valutazione Schengen nell'ambito della protezione dei dati, collaborando in particolare con l'UFG, l'Ufficio federale di polizia (fedpol), la Segreteria di Stato della migrazione (SEM), il Dipartimento federale degli affari esteri (DFAE) e le autorità cantonali preposte alla protezione dei dati (cfr. testo sul «Gruppo di coordinamento delle autorità svizzere di protezione dei dati nell'ambito di Schengen» nel capitolo 1.9 Internazionale).

La procedura di valutazione della protezione dei dati si è svolta in tre fasi. Durante la prima fase è stato chiesto alla Svizzera di rispondere a circa 200 domande sull'attuazione e l'applicazione della normativa Schengen nonché di presentare le principali modifiche legislative e operative adottate dopo l'ultima valutazione. La seconda fase ha comportato ispezioni locali in Svizzera. Nello specifico, esperti di altri Stati Schengen e dell'UE hanno verificato in loco che la Svizzera attui e applichi correttamente le disposizioni Schengen sulla protezione dei dati. Durante la loro visita, che si è svolta dal 26 febbraio al 2 marzo 2018, hanno focalizzato l'attenzione sulla legislazione in materia di protezione dei dati come pure sulle competenze dell'IFPDT, dell'autorità di protezione dei dati di Lucerna e di altri organi federali (cfr. sopra). In particolare, sono stati esaminati i poteri di sorveglianza, indagine e intervento delle autorità di controllo nonché la loro indipendenza. Sono state analizzate le basi legali e in special modo le competenze di controllo sul SIS II, sul VIS nonché sui servizi che partecipano alla sua gestione. Sono stati inoltre valutati i diritti delle persone coinvolte, la sicurezza dei dati, la cooperazione con le autorità estere e l'informazione pubblica.

Visti i risultati della valutazione, il 7 marzo 2019 il Consiglio dell'UE ha deciso di raccomandare alla Svizzera di eliminare le carenze constatate. Per quel che riguarda l'IFPDT, il Consiglio propone in particolare di controllare più spesso la liceità del trattamento di dati personali in relazione ai sistemi di informazione rilevanti per Schengen. Affinché l'Incaricato sia in grado di svolgere tutti i compiti affidatigli nell'ambito di SIS II e del regolamento VIS, devono essergli messe a disposizione sufficienti risorse finanziarie e di personale. Inoltre deve poter influire concretamente sulla proposta di bilancio per la propria attività e il Parlamento deve essere informato di questa voce nel quadro dei lavori sulla proposta per il bilancio pubblico complessivo. Nelle considerazioni il Consiglio ha apprezzato anche i risultati positivi, come ad esempio la guida sul monitoraggio dell'uso del sistema d'informazione Schengen (SIS) elaborata dal Gruppo di coordinamento Schengen istituito dalle autorità svizzere incaricate della protezione dei dati, la vasta gamma di lettere tipo specifiche per l'esercizio dei diritti degli interessati e le informazioni molto utili sul sito web dell'Incaricato. Entro tre mesi dall'adozione della decisione la Svizzera dovrebbe dunque elaborare un piano d'azione e presentarlo alla Commissione e al Consiglio. La prossima valutazione è prevista nel 2023.

Sistema di ricerca automatica di veicoli e monitoraggio del traffico

Le autorità doganali e di polizia potranno utilizzare i nuovi moduli e le nuove funzionalità del sistema di ricerca automatica di veicoli e monitoraggio del traffico a condizione che tale impiego sia disciplinato da una base legale sufficiente in materia di protezione dei dati.

Da oltre dieci anni l'Amministrazione federale delle dogane (AFD) e le forze di polizia cantonali utilizzano i sistemi di ricerca automatica di veicoli e monitoraggio del traffico (AFV). La Commissione tecnica delle polizie svizzere prevede di sostituire il software (AFV Redesign) e di implementare nuovi moduli e funzionalità. In questo contesto è stata effettuata un'analisi dei requisiti e delle basi legali. L'IFPDT e privatim hanno partecipato a un gruppo di lavoro ad hoc. Gli utenti AFV auspicano di poter utilizzare nuovi moduli e funzionalità. Tali impieghi sono possibili a condizione che vi sia una base giuridica.

È pure necessario che il principio di proporzionalità sia adeguatamente rispettato. L'analisi si basa sul numero di telecamere, la loro ubicazione, l'uso dei dati, la modalità d'impiego dei dati di ricerca, la comunicazione dei dati ecc. Nei Cantoni la verifica avviene di norma durante la consultazione preventiva con l'autorità di protezione dei dati. A livello federale il rispetto del principio di proporzionalità viene verificato durante la consultazione degli uffici su un progetto legislativo.

1.3 Fiscalità e finanza

Comunicazione dei dati personali ad autorità fiscali estere

L'attuazione dei nuovi standard nella lotta mondiale contro la frode fiscale e la sottrazione d'imposta è in fase molto avanzata, ma il livello di protezione dei dati insufficiente in alcuni Stati si sta rivelando problematico. Nell'anno in rassegna abbiamo espresso il nostro parere su diversi progetti dal punto di vista della protezione dei dati.

a) Scambio automatico di informazioni sui conti finanziari (SAI)

Lo standard globale per lo scambio automatico di informazioni sui conti finanziari (SAI) è in vigore in Svizzera dal 1° gennaio 2017 e mira ad aumentare la trasparenza fiscale e ad evitare la sottrazione d'imposta transfrontaliera. Finora oltre 100 Paesi, tra cui la Svizzera, si sono impegnati ad adottare lo standard. Il Consiglio federale intende ora ampliare la rete SAI svizzera con altri 18 Stati partner con i quali lo scambio dovrebbe essere attuato dal 2020/2021. (Informazioni complementari sono disponibili sul sito Internet del DFF.)

Come nelle precedenti consultazioni degli uffici, per quanto concerne l'introduzione del SAI con altri Stati partner l'IFPDT ha ribadito anche nell'anno in corso la necessità di garantire un livello adeguato di protezione dei dati in ognuno di questi Stati. La nostra lista degli Stati contiene una valutazione in tal senso per ogni singolo Paese. A inizio novembre 2018, durante una consultazione degli uffici sull'introduzione del SAI con altri Stati partner a partire dal 2020/21, abbiamo osservato che tutti gli Stati proposti con cui si dovrebbe attuare reciprocamente tale scambio (tra cui Albania, Azerbaigian, Brunei Darussalam ecc.) non hanno un livello adeguato di protezione dei dati (cfr. art. 6 cpv. 1 LPD), il che rende necessario assicurare una protezione dei dati sufficiente mediante garanzie di protezione adeguate (cfr. art. 6 cpv. 2 LPD). In questo contesto il Consiglio federale ha fatto riferimento alla comunicazione basata sull'Accordo multilaterale tra autorità competenti concernente lo scambio automatico di informazioni relative a conti finanziari (Multilateral Competent Authority Agreement, MCAA) e trasmessa il 4 maggio 2017 dalla Svizzera all'Organo di coordinamento, nella quale sono definite le garanzie in materia di protezione dei dati che devono valere anche per i contribuenti degli Stati partner. Secondo l'IFPDT, tuttavia, questa comunicazione non costituisce una garanzia sufficiente ai sensi dell'articolo 6 capoverso 2 LPD (cfr. n. 1.9.1 a del 24° e 25° Rapporto d'attività). L'estensione in programma è quindi problematica dal punto di vista della protezione dei dati.

b) Scambio delle rendicontazioni Paese per Paese di gruppi di imprese multinazionali (SRPP)

Anche quest'anno, nell'ambito di una consultazione degli uffici sull'elenco dei Paesi, l'IFPDT si è pronunciato a favore dell'attivazione dello scambio delle rendicontazioni Paese per Paese (cfr. n. 1.9.1 del 24° e 25° Rapporto d'attività). Ha fatto osservare che gli otto Stati e territori supplementari (tra cui gli Emirati Arabi Uniti, la Serbia e lo Zambia) per i quali è stata prevista di recente l'estensione dell'SRPP, sono classificati con un livello di protezione dei dati insufficiente nell'elenco dei Paesi dell'IFPDT. Quest'ultimo ha quindi ribadito che per Paesi come questi servono garanzie supplementari ai sensi dell'articolo 6 capoverso 2 LPD al fine di assicurare un livello adeguato di protezione dei dati.

c) Attenuazione dell'assistenza amministrativa internazionale in materia fiscale per i dati rubati

Nell'anno in rassegna, nel quadro di una consultazione degli uffici, l'IFPDT si è occupato di nuovo dell'articolo 7 lettera c della legge sull'assistenza amministrativa fiscale (LAAF), che tratta lo scambio di informazioni su domanda di uno Stato estero e disciplina i casi in cui non si entra nel merito di domande di questo genere. Secondo il diritto in vigore non si entra nel merito di una domanda «se viola il principio della buona fede, in particolare se si fonda su informazioni ottenute mediante reati punibili secondo il diritto svizzero». In passato l'IFPDT aveva rilevato al riguardo che, a suo avviso, non importava se lo Stato richiedente avesse ottenuto tali informazioni in modo passivo (ad es. attraverso l'assistenza spontanea) o attivo; in entrambi i casi lo Stato che accetta i dati rubati offertigli agisce illegalmente (cfr. n. 1.9.3 del nostro 23° Rapporto d'attività).

Questa prospettiva coincide con la prassi finora corrente che tuttavia è stata criticata dal Forum globale sulla trasparenza e sullo scambio di informazioni a fini fiscali (Global Forum on Transparency and Exchange of Information for Tax Purposes) perché troppo restrittiva. Una sentenza del Tribunale federale emessa nel frattempo (sentenza 2C_648/2017 del 17 luglio 2018) stabilisce che, in linea di principio, si può entrare nel merito anche di domande fondate su dati di origine delittuosa a condizione che lo Stato richiedente non li abbia acquistati con l'intenzione di utilizzarli poi per una domanda di assistenza amministrativa. Di conseguenza l'articolo 7 lettera c LAAF ora dovrà disciplinare soltanto che non si entra nel merito di una domanda se viola il principio di buona fede. Tenendo conto della decisione del Tribunale federale da rispettare, l'IFPDT ha rinunciato a sollevare obiezioni.

Ricorso contro il DFF nel caso AFC ancora pendente

La raccomandazione emanata dall'IFPDT a fine 2017 concernente l'informazione dei nomi trasmessi apertamente nell'ambito delle procedure di assistenza fiscale internazionale non è stata sostenuta dal Dipartimento federale delle finanze (DFF). L'IFPDT ha presentato ricorso al Tribunale amministrativo federale contro la decisione negativa del DFF.

A fine dicembre 2017 avevamo 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, ma i cui nomi vanno resi noti, ossia non anneriti, all'autorità estera richiedente (cfr. n. 1.9.2 del 25° Rapporto d'attività dell'IFPDT). L'AFC ha respinto questa raccomandazione, per cui l'IFPDT si è avvalso della possibilità prevista dalla legge di sottoporre la questione al dipartimento competente.

Nella sua decisione del 20 settembre 2018, il DFF ha appoggiato l'AFC ritenendo che informare terze persone i cui nomi devono essere resi noti nell'ambito di una procedura di assistenza amministrativa – come raccomandato dall'IFPDT – causerebbe oneri troppo elevati e renderebbe quindi impossibile un'assistenza amministrativa efficace. I diritti degli interessati sarebbero già presi in considerazione, nella misura in cui si trasmettono soltanto i dati strettamente necessari. Il DFF ha pertanto respinto la richiesta dell'IFPDT.

Informazione di terzi possibile con un onere ragionevole

L'IFPDT resta dell'opinione che i terzi debbano avere la possibilità di far giudicare ai tribunali se, nei singoli casi, sia ammissibile rendere noti i loro nomi. Soltanto in questo modo, infatti, si può garantire la tutela dei loro diritti costituzionali. Per poter adire le vie legali, gli interessati devono essere messi al corrente della prevista trasmissione dei loro dati. Inoltre, l'IFPDT parte dal presupposto che si possa contenere l'onere per le informazioni a un livello ragionevole mediante misure tecniche e organizzative adeguate, senza ostacolare un'assistenza amministrativa efficace. Il 5 ottobre 2018 ha quindi presentato ricorso al Tribunale amministrativo federale contro la decisione del DFF. Alla fine dell'anno in esame il caso era ancora pendente.

Raccomandazione dell'IFPDT alla Centrale per le informazioni sui crediti (ZEK)

Le richieste di credito che sono state respinte per motivi che non hanno nulla a che vedere con la solvibilità o la capacità di credito del richiedente devono essere cancellate dalla banca dati immediatamente dopo il rifiuto. L'IFPDT ha emanato una raccomandazione in tal senso all'attenzione della Centrale per le informazioni sui crediti.

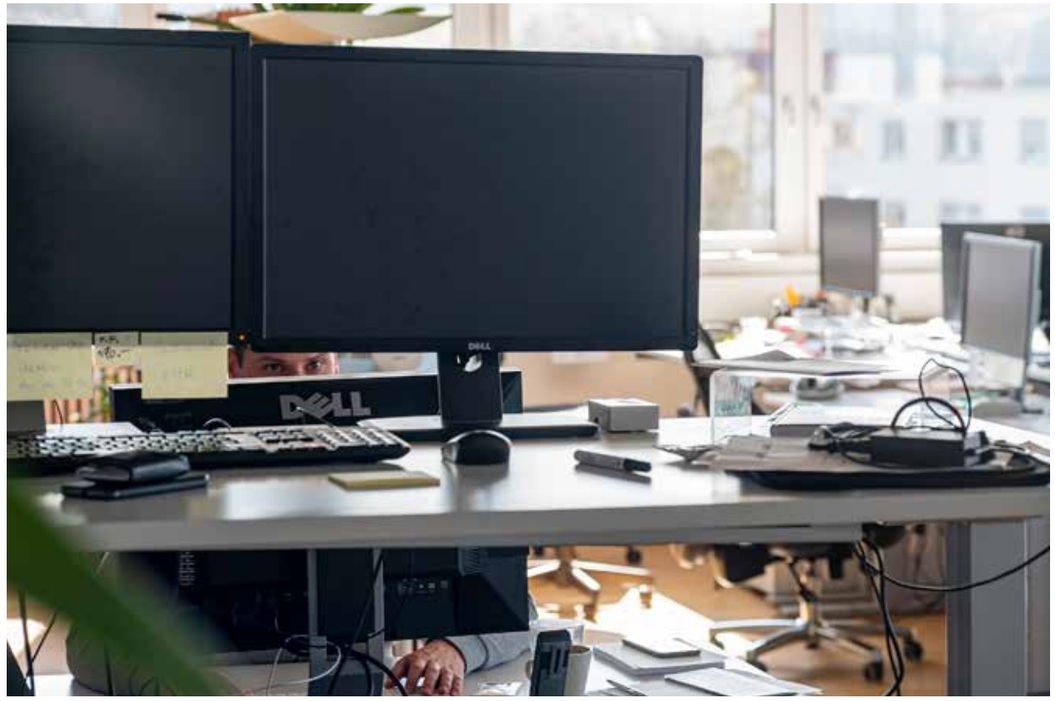
La Centrale per le informazioni sui crediti (ZEK) raccoglie informazioni sulla solvibilità a partire dalle operazioni di credito di persone fisiche e giuridiche e le mette a disposizione dei suoi membri, in particolare delle banche, a pagamento. Nell'anno precedente abbiamo avviato un accertamento dei fatti presso la ZEK (cfr. n. 1.8.12 del 25° Rapporto d'attività dell'IFPDT). Partendo dalle segnalazioni dei cittadini e dagli articoli comparsi sulla stampa, l'IFPDT ha individuato possibili lacune di protezione dei dati nell'elaborazione delle richieste di informazioni, nella rettifica e cancellazione dei dati, nelle misure per evitare interrogazioni improprie come pure nella separazione tecnica e organizzativa delle banche dati della ZEK da quelle della Centrale d'informazione per il credito al consumo (IKO). Quest'ultima ha stipulato con la ZEK un contratto d'uso per il suo sistema informativo.

Nel corso dei nostri accertamenti è tuttavia emerso che, nei settori esaminati, la ZEK agisce nel rispetto della protezione dei dati. Le richieste di informazioni, rettifica e cancellazione sono elaborate correttamente, le misure per impedire interrogazioni improprie soddisfano i requisiti fissati e le banche dati di ZEK e IKO sono separate in modo sufficiente tanto a livello tecnico quanto organizzativo.

Raccomandazione sull'archiviazione impropria dei dati

L'IFPDT ha emesso una raccomandazione unicamente nell'ambito del rifiuto delle richieste di credito e di carte di credito. Ha rilevato che le richieste di credito e di carte di credito che sono state respinte per motivi che non hanno nulla a che fare con la solvibilità o la capacità di credito del richiedente (p. es. esaurimento della quota di credito per un determinato periodo) rimangono memorizzate nella banca dati della ZEK anche dopo il rifiuto della richiesta di credito, sebbene tale informazione sia irrilevante per la valutazione della concessione del credito e quindi per lo scopo perseguito dalla banca dati. Di conseguenza l'IFPDT ha raccomandato che tali registrazioni siano cancellate dalla banca dati della ZEK subito dopo il rifiuto.

La ZEK ha accolto la raccomandazione dell'IFPDT e modificherà in modo opportuno il suo regolamento e la sua banca dati. L'IFPDT ha quindi potuto chiudere la procedura senza ulteriori misure.



1.4 Commercio ed economia

Furto di dati presso Swisscom: caso chiuso senza misure formali

A fine 2017 Swisscom aveva informato l'IFPDT di un furto di dati che aveva riguardato prevalentemente i proprietari privati di numeri di cellulare. L'IFPDT ha potuto chiudere senza raccomandazioni formali la procedura svolta presso Swisscom, finalizzata a esaminare i possibili rischi di danni consequenziali al furto di dati notificato.

A fine dicembre 2017 Swisscom aveva informato l'IFPDT che nell'autunno 2017 si erano verificati accessi non autorizzati ai dati di contatto di circa 800 000 clienti. La fattispecie aveva riguardato prevalentemente gli utenti di cellulare privati e alcuni abbonati alla telefonia fissa. Poco tempo dopo all'IFPDT era stato segnalato un presunto accesso non autorizzato ai dati di un cliente di Swisscom senza che tuttavia vi fosse un nesso causale con il furto di dati notificato (cfr. 25° Rapporto d'attività 2017/18, n. 1.3.1). Tuttavia, dopo la notifica di un accesso abusivo ai dati dei clienti probabilmente correlato al furto di dati presso Swisscom reso pubblico a inizio febbraio 2018, il 9 febbraio 2018 l'IFPDT ha avviato una procedura e chiesto informazioni a Swisscom in relazione al rischio di danni consequenziali (cfr. n. 1.3.2 del 25° Rapporto d'attività 2017/18). Swisscom ha quindi inoltrato la documentazione sui casi sospetti che le sono stati segnalati e sulle misure adottate di volta in volta. In ciascuno dei casi trattati c'era il sospetto che i dati rubati avessero consentito l'accesso illecito ad altri dati dei clienti. Partendo da questa documentazione, l'IFPDT ha verificato se le misure adottate da Swisscom riguardo al furto di dati tutelano a sufficienza le persone interessate o se i casi sospetti notificati comprovano la necessità di misure supplementari.

Anche dopo accertamenti approfonditi, in nessuno dei casi esaminati si è potuto stabilire un nesso con la fuga di dati in questione. Tutti gli episodi sono stati ricondotti a errori tecnici o a manipolazioni errate. Dopo che Swisscom ha adottato misure per correggere gli errori e prevenire episodi analoghi in futuro, l'IFPDT ha potuto chiudere la procedura senza misure formali.

Alla pubblicazione della fuga di dati da parte di Swisscom è seguita una richiesta all'IFPDT di accesso ai documenti del caso, in virtù della legge sulla trasparenza. Previa audizione di Swisscom, l'IFPDT ha deciso di concedere l'accesso ai documenti a eccezione dei dati personali ivi contenuti, emanando una decisione corrispondente. Swisscom ha inoltrato ricorso al Tribunale amministrativo federale contro questa decisione. Alla fine dell'anno in rassegna il caso era ancora pendente.

Furto di dati presso EOS: dati di pazienti salvati inutilmente

EOS ha sostituito il sistema interessato dal furto di dati con uno nuovo, permettendo in questo modo all'IFPDT di concludere l'accertamento dei fatti.

A fine dicembre 2017 l'IFPDT aveva avviato un accertamento dei fatti presso la società di gestione dei crediti EOS Schweiz AG per chiarire gli aspetti relativi alla protezione dei dati del presunto furto di dati, di cui si era parlato anche nei media, che aveva interessato in particolare i pazienti di medici e dentisti svizzeri (cfr. n. 1.8.2 del 25° Rapporto d'attività 2017/18).

Nonostante finora non si siano potute chiarire in modo definitivo le circostanze concrete del presunto furto di dati, dagli accertamenti dell'IFPDT è emerso in particolare che sui server di EOS erano stati memorizzati molti più dati dei pazienti di quelli effettivamente necessari per la fatturazione o il recupero crediti. L'IFPDT ha inoltre appurato che i termini di cancellazione non erano stati rispettati, con conseguente accumulo di una quantità sproporzionata di dati.

Nel quadro dei propri accertamenti, EOS è giunta alla stessa conclusione e nel frattempo ha sostituito il sistema in questione con uno nuovo, eliminando i difetti riscontrati. Pertanto l'IFPDT ha potuto rinunciare all'adozione di misure, chiudendo la procedura senza raccomandazioni formali. Al riguardo rammenta che, per la fatturazione o il recupero crediti, il personale medico deve trasmettere soltanto i dati dei pazienti effettivamente necessari a tale scopo.

Utilizzo dei dati di ricardo.ch all'interno del gruppo Tamedia

Il sito di aste ricardo.ch condivide i dati dei propri utenti all'interno del gruppo Tamedia per motivi di sicurezza e pubblicità mirata. Dall'avvio della procedura formale dell'IFPDT, ricardo.ch ha adeguato la propria dichiarazione sulla protezione dei dati. Esaminiamo se il consenso su cui si basa il gruppo soddisfa i requisiti di legge.

Nel luglio 2017 la piattaforma di aste online ricardo.ch aveva informato i propri utenti della modifica concernente la propria dichiarazione di protezione dei dati, armonizzata con quelle delle società del gruppo Tamedia di cui ricardo.ch fa parte. In particolare, le nuove condizioni di utilizzo avevano lo scopo di permettere uno scambio di dati all'interno del gruppo, segnatamente per consentire una pubblicità mirata, ma anche per prevenire eventuali abusi. In assenza di risposta, si considerava che gli utenti di ricardo.ch avessero accettato la nuova dichiarazione di protezione dei dati e quindi la comunicazione dei loro dati a Tamedia e alle sue società affiliate. In caso di opposizione, l'account veniva automaticamente chiuso o sospeso. Nutrendo dubbi sulla validità del consenso delle persone interessate, abbiamo avviato una procedura formale per verificare il rispetto dei pertinenti requisiti di legge (cfr. n. 1.8.8. del nostro 25° Rapporto d' attività 2017/2018).

Nel frattempo Ricardo ha modificato la propria dichiarazione di protezione dei dati a decorrere dal 25 maggio 2018, contemporaneamente all'entrata in vigore del Regolamento europeo sulla protezione dei dati (GDPR). Gli utenti di Ricardo possono ora opporsi alla condivisione dei dati con il Gruppo Tamedia se ne fanno espressa richiesta. Si presume pertanto che, sebbene l'utente acconsenta al trattamento dei dati ai fini di pubblicità specifica per gruppi target, abbia la possibilità di revocare successivamente il proprio consenso. Abbiamo analizzato le nuove condizioni, per le quali sono stati necessari alcuni chiarimenti. Ora stiamo valutando la situazione su questa nuova base. In particolare, verifichiamo se gli utenti di ricardo.ch sono sufficientemente informati e se è sufficiente la possibilità di opporsi successivamente alla profilazione e all'arricchimento dei dati per scopi pubblicitari mirati (opt-out). La LPD richiede che il consenso – a meno che non vi sia un'altra giustificazione – debba essere dato espressamente quando si elaborano dati personali degni di particolare protezione o profili della personalità. Al momento della conclusione del presente rapporto di attività, l'esame giuridico era ancora in corso.

Accertamento dei fatti concluso presso un produttore di smart TV

La procedura condotta presso un produttore di apparecchi smart TV per chiarire la conformità alla protezione dei dati nel trattamento dei dati degli utenti è stata conclusa senza misure formali.

L'IFPDT ha svolto un accertamento dei fatti presso un produttore di apparecchi smart TV per chiarire quali dati sugli utenti televisivi vengono trattati, in che modo gli utenti sono informati al riguardo e se tale trattamento di dati avviene su base volontaria (cfr. n. 1.3.1 del 25° Rapporto d'attività 2017/18). Da un'analisi approfondita della documentazione inoltrata è emerso che il produttore elabora i dati degli utenti raccolti conformemente alle norme sulla protezione dei dati.

Il produttore di apparecchi tratta i dati degli utenti su base personale soltanto se necessario per motivi tecnici o se richiesto dall'utente per determinate funzioni aggiuntive. Tutti gli altri trattamenti di dati, ad esempio a fini statistici, avvengono senza alcun riferimento personale.

Gli utenti degli apparecchi sono informati delle possibili trasmissioni di dati al produttore e del loro trattamento. Gli utenti hanno modo di impedire completamente tale trasmissione di dati e utilizzare gli apparecchi come televisori convenzionali, vale a dire senza le funzioni smart TV. Utilizzando le funzioni smart TV, il trattamento di determinati dati è necessario per motivi tecnici e l'utente non ha modo di impedirlo né limitarlo. L'utente può invece disattivare i trattamenti di dati che servono a scopo di comfort o per certe funzioni aggiuntive.

Non avendo constatato alcun trattamento di dati improprio da parte del produttore degli apparecchi in questione, l'IFPDT ha chiuso la procedura senza misure formali.

Decathlon – necessaria una migliore informazione sulla raccolta dei dati dei clienti

Nelle sue filiali in Svizzera, il commerciante di articoli sportivi Decathlon ha vincolato la vendita delle merci alla fornitura dei dati dei clienti. L'IFPDT ha pertanto avviato un accertamento dei fatti, in seguito del quale Decathlon ha modificato la controversa procedura.

Nell'anno in rassegna abbiamo avviato un accertamento dei fatti presso Decathlon, dopo aver appreso da articoli di stampa nonché da notifiche di cittadini e organizzazioni dei consumatori che il commerciante di articoli sportivi aveva vincolato la vendita di merci nelle sue filiali in Svizzera alla comunicazione di determinati dati dei clienti.

Una volta avviata la procedura, Decathlon ha informato l'IFPDT che, per poter acquistare merci nei negozi, i clienti dovevano fornire il loro indirizzo e-mail o il numero di telefono. La società ha aggiunto, tuttavia, che da quel momento avrebbe rinunciato a vincolare la vendita di prodotti alla fornitura di questi dati, rilevandoli solo su base volontaria. Siccome con l'adozione di questa misura veniva meno il motivo principale dell'accertamento dei fatti, l'IFPDT ha concentrato la sua azione successiva sul fatto di chiarire se tale volontarietà fosse effettivamente riconoscibile per i clienti.

Ne è emerso che le informazioni di Decathlon al riguardo sono formulate in modo non uniforme e in parte non abbastanza chiaro, dando l'impressione che i dati inizialmente obbligatori continuino a essere tali per l'acquisto degli articoli. L'IFPDT ha quindi presentato a Decathlon proposte per migliorare l'informazione.

1.5 Salute

Progetto di statistica con dati individuali degli assicuratori (BAGSAN)

L'Ufficio federale della sanità pubblica (UFSP) gestisce il progetto di statistica BAGSAN con dati individuali anonimizzati degli assicuratori. L'IFPDT monitora il progetto, che interessa anche la politica.

Dal 2016 l'IFPDT sta seguendo il progetto di statistica BAGSAN dell'UFSP (cfr. 23° Rapporto d'attività, n. 1.6.4). Abbiamo discusso le misure per evitare accessi interni non autorizzati con i responsabili del progetto. Che gli accessi siano documentati mediante registri è un fatto scontato; sarebbero tuttavia auspicabili avvisi automatici, ad esempio quando un collaboratore effettua un numero particolarmente elevato di accessi. Per motivi di protezione della personalità dei collaboratori, verrà ora implementata una soluzione con dati utente pseudonimizzati. In caso di sospetto concreto di abuso, si potrebbe poi procedere a un'analisi nominativa.

Il progetto BAGSAN è oggetto di ulteriori discussioni anche a livello politico. L'obiettivo di un'iniziativa parlamentare del consigliere agli Stati Joachim Eder è di garantire che, in virtù della protezione dei dati, l'UFSP riceva dagli assicuratori solo dati raggruppati che non consentono più di risalire all'identità di singoli individui. La legge federale concernente la vigilanza sull'assicurazione sociale contro le malattie (LVAMal) dovrebbe essere modificata di conseguenza. Nel frattempo, la sottocommissione parlamentare «Fornitura di dati», appositamente istituita, si è occupata del caso e ha elaborato un progetto di revisione per la Commissione della sicurezza sociale e della sanità (CSSS). La CSSS ha posto in consultazione l'avamprogetto con il rapporto esplicativo. Se l'UFSP ricevesse dagli assicuratori malattia solo dati raggruppati, il progetto BAGSAN non sarebbe superato, ma necessiterebbe comunque di modifiche sostanziali. L'IFPDT continuerà a monitorare da vicino il progetto BAGSAN.

Nuovi compiti derivanti dalla cartella informatizzata del paziente

Procedono i lavori di attuazione per la cartella informatizzata del paziente che dovrebbe essere disponibile in tutte le regioni della Svizzera a partire dalla primavera 2020. Per l'IFPDT ciò si tradurrà in nuovi importanti compiti di vigilanza.

Confederazione e Cantoni lavorano a ritmo serrato all'introduzione della cartella informatizzata del paziente (CIP) ai sensi della legge federale sulla cartella informatizzata del paziente (LCIP). Affinché la CIP possa essere proposta alla popolazione di tutte le regioni della Svizzera dalla primavera del 2020, servono fornitori certificati e organizzati secondo il diritto privato – le cosiddette comunità e comunità di riferimento – come disciplinato dalla LCIP. I trattamenti di dati da parte di fornitori di questo genere si attengono anche a speciali disposizioni secondo la LPD, la cui applicazione è soggetta alla vigilanza della nostra autorità. Le comunità sono considerate persone giuridiche private la cui vigilanza rientra nella sfera di competenza della Confederazione (a prescindere dal fatto che i singoli membri delle comunità siano ospedali di diritto pubblico cantonale o di diritto federale privato). La Confederazione gestisce inoltre componenti centrali necessari per il funzionamento della CIP.

Per accedere alla CIP, tanto i pazienti quanto il personale curante hanno bisogno di strumenti di identificazione che consentano un'autenticazione inequivocabile. A tal fine vengono utilizzate identità elettroniche che possono essere memorizzate ad esempio su una chip card o uno smartphone. Gli emittenti di strumenti di identificazione ai sensi della LCIP devono essere certificati. Anche i trattamenti dei dati nel quadro della creazione e della gestione delle identità elettroniche sono disciplinati dalla LPD. Affinché i pazienti abbiano fiducia nella CIP, si devono soddisfare standard elevati per quel che riguarda i requisiti legali e tecnici di protezione dei dati. Su richiesta dei parlamentari, l'IFPDT ha illustrato i suoi compiti nel settore della CIP anche a diverse commissioni delle Camere federali, compiti che deve adempiere rispettando il budget del Consiglio federale senza risorse umane supplementari.

Programma bonus «Helsana+» al banco di prova: successo parziale per l'IFPDT davanti al Tribunale amministrativo federale

Nell'anno in rassegna l'IFPDT ha esaminato attentamente il programma bonus «Helsana+» emettendo una raccomandazione per Helsana Assicurazioni integrative SA, che l'ha respinta. L'IFPDT ha quindi promosso un'azione legale presso il Tribunale amministrativo federale, che è stata parzialmente accolta nel marzo 2019.

Già nel precedente periodo di riferimento, l'IFPDT aveva notato diverse applicazioni sanitarie e programmi bonus delle casse malati, tra cui anche il programma bonus «Helsana+» della cassa malati Helsana, lanciato nel settembre 2017. «Helsana+» è un programma che si prefigge di motivare gli assicurati che vi partecipano ad adottare un comportamento attento alla salute e uno stile di vita attivo. Come ricompensa per le loro attività registrate, i partecipanti ricevono i cosiddetti «punti Plus», che possono convertire in pagamenti in contanti o incassare per offerte e sconti presso le aziende partner di Helsana. Diversamente da offerte equiparabili di altre casse malati, a «Helsana+» possono partecipare anche persone che hanno stipulato solo l'assicurazione di base presso Helsana.

Dopo che abbiamo condotto e completato un accertamento formale dei fatti presso la cassa malati Helsana nell'anno precedente, il 26 aprile 2018 l'IFPDT ha inviato una raccomandazione a Helsana Assicurazioni integrative SA conformemente all'articolo 29 LPD. Nel documento in questione l'IFPDT ha raccomandato anzitutto di interrompere il flusso di dati dall'assicurazione di base all'assicurazione complementare durante il processo di registrazione, ossia di non trattare i dati personali degli assicurati di base al momento della registrazione per il programma bonus. In secondo luogo, l'IFPDT ha chiesto a Helsana Assicurazioni integrative SA di non trattare i dati dei clienti che presso Helsana hanno stipulato soltanto l'assicurazione di base ai fini della valutazione e del pagamento di rimborsi monetari. Secondo l'IFPDT i trattamenti dei dati in questione corrispondono, sul piano economico, a un rimborso successivo di una parte del premio dell'assicurazione di base, il che non è previsto dalla legge.

Dato che Helsana Assicurazioni integrative SA ha respinto la sua raccomandazione, l'IFPDT ha deciso di deferire il caso al Tribunale amministrativo federale di San Gallo, promuovendo un'azione legale il 18 giugno 2018.

La raccolta di dati era illegale per la mancanza di un consenso giuridicamente valido

Nella sentenza del 19 marzo 2019 il Tribunale amministrativo federale ha accolto parzialmente l'azione dell'IFPDT dichiarando che, in mancanza di un consenso giuridicamente valido, la raccolta di dati presso gli assicuratori di base era contraria alla legge. Ha invece giudicato ammissibili gli altri trattamenti di dati nel quadro del programma Helsana+. Il Tribunale amministrativo federale si è espresso per la prima volta in linea di principio sulla questione di quando il trattamento di dati per scopi illeciti contravvenga alla legge sulla protezione dei dati (LPD) giungendo alla conclusione che il trattamento di dati per scopi illeciti è illegale anche ai sensi della LPD solo quando contravviene ad una disposizione che ha come scopo almeno anche la tutela della personalità.

A diritto comparato, il Tribunale rinvia inoltre al regolamento generale sulla protezione dei dati europeo (GDPR), più ampio rispetto sia alla LPD sia al progetto di revisione totale della legge stessa; secondo il regolamento i dati possono essere raccolti solo per scopi legittimi.

Ciò facendo il Tribunale invita l'IFPDT alla prudenza nell'interpretazione dinamica della LPD del 1992 in merito alle applicazioni digitali e rende evidenti i limiti della legge ormai anacronistica. Poiché le disposizioni della legge sull'assicurazione malattie (LAMal) in questione non servono anche a tutelare la personalità, il Tribunale amministrativo federale ha potuto lasciare aperta la questione della conformità del trattamento di dati con la LAMal. Ha però colto l'occasione per precisare che non è evidente una violazione della LAMal, facendo capire di non condividere l'ottica economica dell'IFPDT.

Rischi connessi a una quantità di dati in rapida crescita nella «salute personalizzata»

La digitalizzazione avanzata della medicina e della ricerca sta generando quantità sempre maggiori e più dettagliate di dati sulla salute. Occorre rispettare i principi di protezione dei dati in particolare nei casi in cui tali dati consentono di risalire all'identità di singoli individui.

Nel settore sanitario vengono generate quantità di dati sempre maggiori. Si tratta, ad esempio, di dati clinici provenienti da ospedali, studi medici o biobanche, ma anche di dati raccolti direttamente dalle persone interessate. Questi ultimi provengono, ad esempio, da applicazioni sanitarie, fitness tracker o dispositivi medici come il glucometro. Lo scopo della «salute personalizzata» è di utilizzare questi dati per sviluppare strategie sanitarie sovraordinate, riconoscere precocemente determinati rischi di malattia o ancora per sviluppare trattamenti medici specifici per singoli pazienti o gruppi di pazienti. Per la ricerca medica e per le terapie, il crescente volume di dati si traduce in opportunità, sfide e rischi in termini di protezione dei dati. Una delle sfide consiste nel garantire qualità e affidabilità costanti di tali dati o nell'assicurarne la comparabilità.

Ad esempio, si distinguono rischi per la protezione dei dati a livello di sicurezza tecnica o di cambiamenti nelle finalità di utilizzo difficilmente prevedibili. Non mancano poi le questioni etiche. Per risolvere tutti questi aspetti con un approccio unitario, è stata lanciata l'iniziativa «Swiss Personalized Health Network» (SPHN) sotto la direzione dell'Accademia svizzera delle scienze mediche (ASSM). Lo SPHN è incaricato dalla Confederazione di creare le basi e le infrastrutture per lo scambio di dati sulla salute tra gli istituti di ricerca. L'IFPDT ha partecipato a questi lavori. È importante che nel trattamento di dati sanitari non anonimizzati vi sia trasparenza, sia in termini di scopo del trattamento sia di utilizzo dei rispettivi dati, e che si ottenga in via preliminare il consenso legalmente valido dei pazienti.

1.6 Lavoro

Outsourcing: trattamento di dati personali all'estero

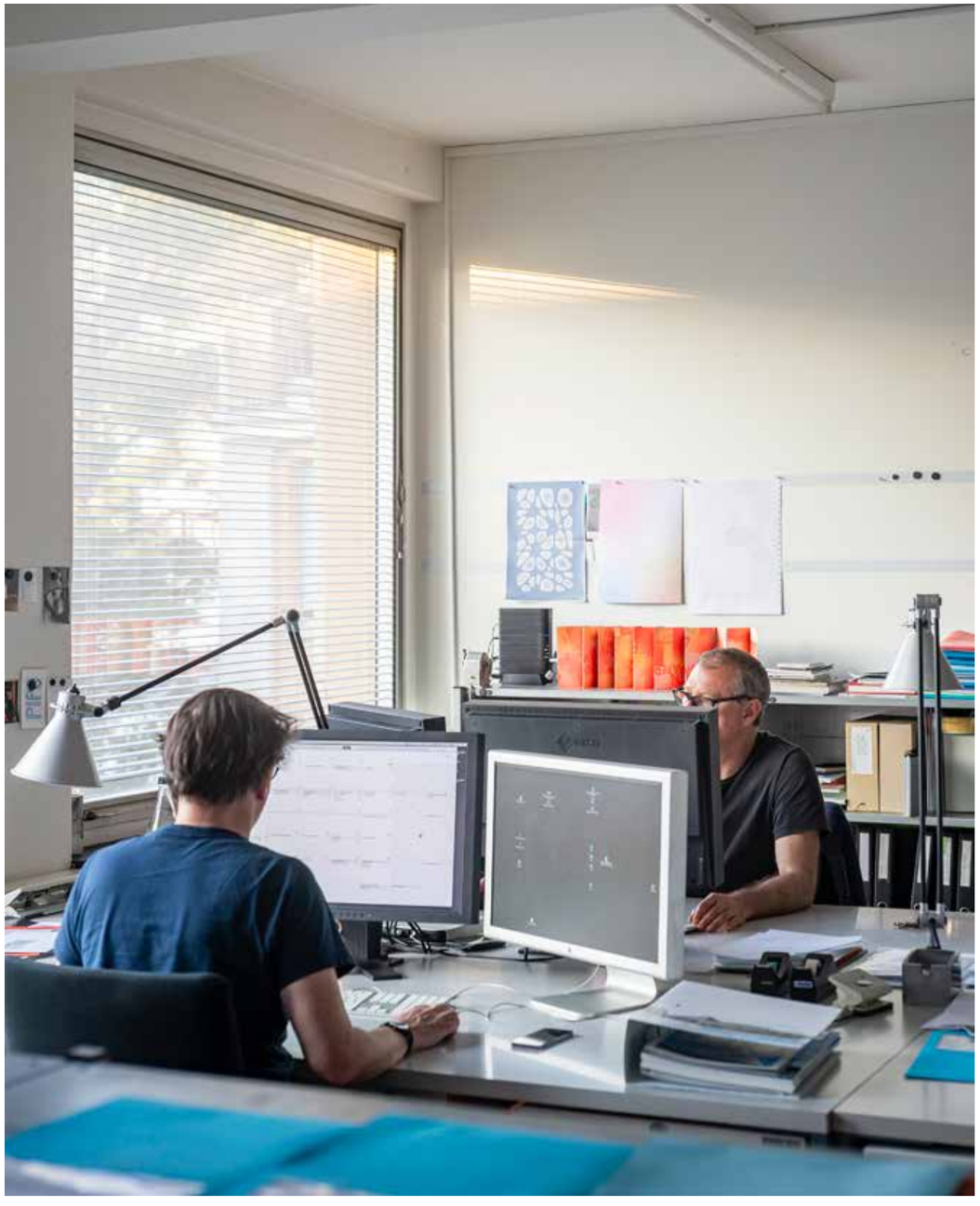
Per motivi di costo od organizzativi, molti datori di lavoro decidono di far trattare i dati personali dei propri collaboratori al di fuori dei confini nazionali. Al riguardo è essenziale informare i collaboratori in modo trasparente e completo. Generalmente, tuttavia, il loro consenso non è necessario e comunque non sarebbe valido.

A fini di razionalizzazione e centralizzazione, si conferma la tendenza dell'economia a conservare ed elaborare i dati personali all'estero. Nell'anno precedente, numerosi collaboratori interessati, ma anche datori di lavoro e responsabili del personale hanno posto domande all'IFPDT sull'ammissibilità e sulle possibilità di strutturazione dell'outsourcing. Vi è un trasferimento di dati all'estero nel momento in cui i dati sono resi accessibili a una società o a un'unità con sede all'estero oppure vengono archiviati in un cloud situato all'estero. L'attenzione si è focalizzata sulle questioni relative all'obbligo d'informazione e al consenso dei collaboratori quando i dati personali sono trattati oltre i confini nazionali. L'IFPDT raccomanda ai datori di lavoro una comunicazione interna esaustiva, sia sul trasferimento di dati all'estero sia sui trattamenti di dati effettivamente eseguiti all'estero e sulle relative finalità. Una comunicazione di questo tipo deve quindi comprendere, ad esempio, indicazioni sul Paese verso cui sono esportati i dati, sulla società che se ne occupa nonché sul tipo di valutazioni effettuate e sul loro scopo. Queste informazioni non vanno confuse con il consenso. Dato che il rapporto di subordinazione nella relazione di lavoro implica regolarmente una mancanza della «volontarietà» rivendicata dall'articolo 4 capoverso 4 LPD, il consenso del collaboratore si rivela generalmente irrilevante sul piano giuridico o inadeguato come motivo giustificativo ai sensi dell'articolo 13 capoverso 1 LPD. Soprattutto nelle società attive a livello globale sembra tuttavia consuetudine chiedere il consenso dei collaboratori nel quadro delle direttive sulla protezione dei dati, le quali di solito si rivelano nulle ai sensi del diritto svizzero sulla protezione dei dati. Spetta al tribunale civile competente decidere nel singolo caso in merito alla legittimità del trasferimento di dati e all'adeguatezza delle informazioni fornite agli interessati.

Procedure di candidatura online e colloqui di assunzione: aspetti da considerare

Durante le procedure di candidatura online del mondo del lavoro digitalizzato sono molto diffuse le analisi automatiche della voce e del comportamento. Dato che potrebbero essere utilizzate per creare profili della personalità dettagliati, occorre osservare un livello di protezione dei dati maggiore.

I colloqui di assunzione si svolgono sempre più spesso online. Candidati e selezionatori si pongono domande sull'ammissibilità e sui requisiti legali delle analisi del comportamento o della voce. Secondo l'articolo 328b CO, nella procedura di candidatura il datore di lavoro è autorizzato a trattare soltanto le informazioni sui candidati necessarie per chiarire la loro idoneità alla posizione o per l'esecuzione del contratto di lavoro. Nell'ambito delle sue consultazioni, l'IFPDT ha fatto osservare che l'elaborazione dei curriculum vitae e di altre informazioni da parte dei responsabili del personale equivale regolarmente all'elaborazione di tratti essenziali della personalità del candidato ovvero di profili della personalità ai sensi dell'articolo 3 lettera d LPD. Ciò vale a maggior ragione quando le registrazioni dei colloqui di assunzione sono sottoposte anche ad analisi del comportamento o della voce.



Le valutazioni devono essere proporzionate e vanno adottate misure adeguate per la sicurezza dei dati. I candidati devono essere informati in anticipo non solo delle valutazioni previste, ma anche della natura e dello scopo dell'utilizzo dei risultati, della durata della loro conservazione nonché del loro diritto di accesso ai dati.

Lotta contro il lavoro nero nel Cantone del Vallese

Su intervento dell'IFPDT, l'associazione ARCC ha disattivato la sua omonima applicazione per smartphone per controlli intensificati sui cantieri vallesani. L'IFPDT esige la cancellazione dei dati già ottenuti con questa modalità.

Per controllare i cantieri sul proprio territorio, diverse commissioni paritetiche del Cantone del Vallese hanno istituito l'Associazione ARCC (Association pour le Renforcement des Contrôles sur les Chantiers). Compito principale dell'associazione è di controllare il rispetto del divieto del lavoro nero e della legge sui lavoratori distaccati. In base alle indicazioni ricevute, abbiamo condotto un accertamento dei fatti presso l'associazione conformemente all'articolo 29 LPD. In questo contesto l'IFPDT ha focalizzato la propria attenzione sull'applicazione per smartphone «ARCC» che permette di inviare notifiche dirette all'associazione.

Tramite l'applicazione vengono trasmesse sia foto, in cui sono visibili la ditta dell'impresa di costruzioni in questione ed eventualmente anche gli operai del cantiere, sia dati su nome e posizione degli utenti dell'applicazione. Nel corso dei nostri accertamenti, l'associazione ha di nuovo disattivato l'applicazione. L'IFPDT è del parere che attualmente non esista una base legale sufficiente per la gestione dell'applicazione e il trattamento dei dati derivanti dal suo utilizzo. Accogliamo quindi con favore la disattivazione e abbiamo chiesto per iscritto all'associazione di distruggere i dati personali già raccolti. Abbiamo inoltre fatto osservare all'associazione che, qualora dovesse continuare a trattare i dati raccolti, dovrà assumersi il rischio di eventuali azioni civili promosse dai diretti interessati.

1.7 Assicurazioni

Nuovo articolo sull'osservazione degli assicurati da parte delle assicurazioni sociali

Le osservazioni segrete sono uno strumento efficace per individuare frodi e abusi nel settore della sicurezza sociale. Dato che rappresentano una massiccia intromissione nella sfera privata, devono essere limitate allo stretto necessario. L'IFPDT accoglie con favore l'obbligo di autorizzazione per l'impiego di strumenti tecnici di localizzazione.

Nel referendum del 25 novembre 2018 l'elettorato ha accettato il nuovo articolo sull'osservazione degli assicurati che prevede sorveglianze segrete nel settore delle assicurazioni sociali. La nuova disposizione dovrebbe entrare in vigore nell'autunno 2019. Coglieremo l'occasione per esprimere a tempo debito il nostro parere sulle disposizioni esecutive ancora pendenti a livello di ordinanza. Particolarmente importanti ai fini della protezione dei dati risultano i requisiti che gli specialisti esterni incaricati dell'osservazione devono avere. Mediante una procedura di selezione e possibilmente anche una procedura di omologazione si tratta di garantire con la massima probabilità che non venga fatto un uso improprio del materiale d'osservazione.

L'IFPDT si aspetta inoltre opportune specifiche a livello di ordinanza o quantomeno istruzioni per l'osservazione di assicurati che si trovino in un posto visibile da un luogo accessibile al pubblico. A fini di proporzionalità occorre assicurarsi che la sfera privata, come l'interno di un'abitazione, rimanga protetta conformemente alla precedente giurisprudenza del Tribunale federale. Accogliamo con favore il fatto che si debba ottenere l'autorizzazione del tribunale per l'impiego di strumenti tecnici di localizzazione. Tale autorizzazione può essere rilasciata soltanto motivando adeguatamente al giudice la necessità di utilizzare tali strumenti nel singolo caso concreto. Senza l'autorizzazione del tribunale, non possono essere utilizzati dispositivi di localizzazione, ad esempio sui veicoli. Le registrazioni video e vocali, invece, possono continuare a essere effettuate senza l'autorizzazione del giudice.

L'IFPDT ritiene importante anche l'obbligo recepito nel nuovo articolo sull'osservazione di informare a posteriori la persona assicurata, qualora l'osservazione non abbia confermato il sospetto di abuso. In tal caso, l'assicuratore deve emettere una disposizione che fornisca informazioni su motivo, tipo e durata dell'osservazione. Gli assicurati possono chiedere l'accesso al materiale d'osservazione e decidere se conservarlo negli atti oppure distruggerlo. L'assicuratore può tuttavia distruggere il materiale d'osservazione solo dopo che la disposizione è passata in giudicato e se l'assicurato non ha dichiarato espressamente che deve rimanere negli atti.

SUVA: maggiore trasparenza nella ricerca con i dati degli assicurati

In collaborazione con l'IFPDT, la SUVA ha migliorato in modo significativo l'informazione degli assicurati sull'utilizzo dei loro dati a fini di ricerca. Sul sito Internet della SUVA gli interessati trovano importanti informazioni sull'utilizzo dei dati degli assicurati per scopi di ricerca e sul diritto di opposizione.

La SUVA utilizza i dati degli assicurati, prevalentemente in collaborazione con terzi, per scopi di ricerca nel settore della medicina del lavoro, assicurativa e di riabilitazione. Nel quadro della nostra consulenza ci siamo adoperati affinché la SUVA fornisca informazioni dettagliate sul sito Internet (rubrica Infortunio – Ricerca medica) in merito al motivo per cui utilizza i dati degli assicurati a scopo di ricerca e agli ambiti in cui li utilizza. L'attività di ricerca della SUVA riguarda principalmente l'apparato locomotore, le malattie professionali, le lesioni cerebrali traumatiche, i dolori cronici, le conseguenze psicologiche di un infortunio e le amputazioni, ma serve anche a migliorare la metodologia delle perizie e la prevenzione. Ora la SUVA fornisce anche informazioni esplicite sul diritto di opposizione di ogni assicurato e su come esercitare facilmente tale diritto.

Pubblicando le relative informazioni sul suo sito Internet, la SUVA può così continuare a fornire un contributo prezioso alla ricerca medica. Al contempo rispetta il principio della riconoscibilità della raccolta e della trasparenza del trattamento dei dati. Per gli assicurati, la partecipazione a progetti di ricerca e la scelta di rendere disponibili dati personali per scopi di ricerca restano volontari e non devono influire in alcun modo sulla cura medica o sulla valutazione di un caso di prestazione. Il personale curante svolge qui un ruolo importante e dovrebbe informare i pazienti del loro diritto di veto sull'uso dei dati personali per scopi di ricerca. Se il paziente comunica alla SUVA il blocco dei propri dati per scopi di ricerca, la SUVA fa un'annotazione perché tale volere sia rispettato.

Sempre nell'ambito di questo progetto, con la nostra consulenza abbiamo fatto in modo che la SUVA rielaborasse le direttive interne, adeguandole ove necessario. Abbiamo attribuito grande importanza al fatto che l'anonimizzazione dei dati personali avvenga quanto prima. Inoltre, se lavorano con dati che non sono stati anonimizzati o pseudonimizzati, i ricercatori devono stipulare accordi di riservatezza specifici con la SUVA. Se utilizzano dati anonimizzati o pseudonimizzati, sono loro vietati anche i trattamenti che potrebbero portare a una reidentificazione delle persone. In particolare, i dati della ricerca non possono essere collegati con dati provenienti da altre fonti. I dati devono altresì essere cancellati al termine del progetto di ricerca e dopo la pubblicazione dei risultati. I ricercatori devono informarne la SUVA per iscritto. Trovano le informazioni pertinenti sul sito Internet della SUVA. La nostra consulenza è terminata, ma spetta alla SUVA garantire che le informazioni e le direttive interne siano sempre conformi ai requisiti della legge sulla protezione dei dati, anche in caso di nuovi metodi di cura e ricerca. In questo contesto, si dovrebbe considerare in modo particolare anche la gestione del materiale genetico o dei risultati di analisi genetiche (p. es. nel settore della medicina altamente specializzata).

1.8 Trasporti

Mobilità multimodale. L'autodeterminazione in materia di informazione è un must

Su incarico del Consiglio federale il DATEC esamina in che modo la Confederazione può promuovere la mobilità multimodale e sfruttarne i potenziali. I viaggiatori devono poter combinare in modo semplice e flessibile le diverse offerte di mobilità su tutti i canali di traffico. L'IFPDT ha monitorato il progetto nell'anno in esame, offrendo consulenza ai fornitori nelle questioni di protezione dei dati e prendendo posizione nell'ambito della consultazione degli uffici.

Grazie alle nuove tecnologie digitali per i viaggiatori dovrebbe essere più semplice informarsi sulla combinazione di diverse offerte di mobilità. Ciò si traduce nel trattamento di notevoli quantità di dati personali. L'IFPDT ha seguito il progetto, che è ancora in fase iniziale, offrendo consulenza ai fornitori di servizi di mobilità multimodale, anche in occasione di diversi incontri. I fornitori sono consapevoli della necessità di garantire l'autodeterminazione in materia di informazione degli interessati nel trattamento dei dati personali nonché di adottare misure concrete a tutela dei diritti della personalità dei soggetti coinvolti. L'IFPDT ha fatto notare in particolare il divieto di ricorrere alla coercizione, sia essa diretta o indiretta, per divulgare i dati personali. Affinché i diretti interessati possano dare il proprio consenso su base volontaria, devono dapprima essere informati in modo trasparente sui trattamenti dei dati che accettano scegliendo uno specifico servizio di mobilità e sulla scelta alternativa disponibile. Qualora il collegamento di dati tecnici, che di per sé non sono assoggettati alla legge sulla protezione dei dati, consenta di risalire all'identità delle persone, si devono rispettare i principi in materia di protezione dei dati.

In aggiunta, l'IFPDT ha segnalato che l'utilizzo dei servizi di mobilità multimodale può generare rapidamente profili di movimento, i quali possono a loro volta generare profili della personalità. In tal caso va osservato il livello di protezione più elevato per dati personali e profili della personalità particolarmente sensibili.

Possibilità di scelta reali e viaggi anonimi per i clienti

Nell'ambito della consultazione degli uffici, l'IFPDT ha inoltre espresso il proprio parere sulla mobilità multimodale, pronunciandosi anche sulla prevista modifica della disposizione della legge sul trasporto di viaggiatori (LTV) relativa al trattamento dei dati da parte delle imprese di trasporto pubblico (TP). Sul piano del trattamento dei dati, con questa modifica le imprese di trasporto pubblico non dovranno più attenersi alle disposizioni in materia valide per gli organi federali, ma saranno assoggettate alle disposizioni in vigore per i privati e, con il consenso dei viaggiatori, potranno trattare i loro dati per determinati scopi. Non essendo d'accordo con la formulazione proposta, l'IFPDT ha sottolineato che, in tal caso, i consensi dei clienti sarebbero significativi solo se volontari, ossia se ottenuti sulla base di possibilità di scelta reali. Nelle biglietterie automatiche, quindi, in alternativa ai modelli previsti, si dovrebbe dare ai clienti la possibilità di viaggiare in modo anonimo alle stesse condizioni, vale a dire su base non discriminatoria, senza rivelare i propri dati personali. Inoltre, il trattamento dei dati personali ai fini dell'amministrazione interventistica richiederebbe in ogni modo una base legale. L'IFPDT accoglie con favore il fatto che le sue osservazioni siano state integrate nell'avamprogetto posto in consultazione.

L'IFPDT continuerà a monitorare il progetto. I rischi in materia di protezione dei dati associati al progetto dovranno essere valutati a tempo debito.

Conformità alla protezione dei dati per le nuove applicazioni di trasporto pubblico

Il settore dei trasporti ci ha informati di diversi progetti, tra cui lo sviluppo ulteriore di varie applicazioni. Al riguardo occorre rivalutare costantemente la conformità alla protezione dei dati. In particolare, si possono raccogliere soltanto i dati strettamente necessari alla fornitura di un servizio.
Anche nell'anno in rassegna l'IFPDT è stato informato da singole imprese di trasporto in merito a progetti di protezione dei dati, tra cui il trattamento di dati in relazione allo sviluppo ulteriore di diverse applicazioni per imprese di trasporto, in particolare le FFS.
Talvolta si è fatto riferimento a dati anonimizzati, sebbene le persone interessate restino identificabili. In casi del genere, nell'informare le persone interessate non si può parlare di dati anonimizzati. L'IFPDT ha fatto notare all'impresa di trasporti che, prima di procedere con altri trattamenti di dati, deve nuovamente chiarire accuratamente la questione dell'anonimizzazione. Nella stessa ottica, ha segnalato alle FFS che, nel trattamento dei dati, si devono rispettare anche i principi di proporzionalità ed economia dei dati. Questo vale anche se si è ottenuto il consenso al trattamento dei dati.

È importante che le imprese di trasporto garantiscano la conformità alla protezione dei dati per ogni progetto. In tal senso, i trattamenti di dati eseguiti o previsti devono essere verificati in modo conseguente e, se necessario, adeguati ai requisiti in materia di protezione dei dati. Nel caso di sviluppo ulteriore di applicazioni, la conformità alla protezione dei dati deve essere costantemente riesaminata.

1.9 Internazionale

Gruppi di coordinamento di controllo dei sistemi d'informazione SIS II, VIS ed Eurodac

Nell'anno in esame i gruppi di controllo si sono riuniti a Bruxelles e hanno espresso il proprio parere in merito alle proposte della Commissione europea sull'interoperabilità tra i sistemi d'informazione dell'UE.
Anche nell'anno in rassegna l'IFPDT, in qualità di autorità nazionale di vigilanza, ha partecipato alle riunioni dei tre gruppi di coordinamento di controllo dei sistemi d'informazione europei SIS II, VIS (presidenza dell'IFPDT) ed Eurodac. Gli incontri si sono svolti a Bruxelles il 12–13 giugno e il 14–15 novembre 2018. Sono rappresentati il Garante europeo della protezione dei dati (GEPD) come pure le autorità nazionali preposte alla protezione dei dati dei 28 Stati membri dell'UE, con la partecipazione dell'Irlanda e del Regno Unito in qualità di osservatori. I gruppi sono integrati dalle autorità nazionali preposte alla protezione dei dati di Svizzera, Liechtenstein, Norvegia e Islanda, dal momento che i rispettivi Paesi partecipano ai sistemi d'informazione.

I gruppi di coordinamento di controllo del SIS e di Eurodac hanno adottato, tra l'altro, i loro rapporti di attività 2016/2017. Inoltre, hanno formulato il proprio parere in merito alle proposte della Commissione europea per un regolamento che dovrà definire il contesto dell'interoperabilità tra sistemi d'informazione dell'UE, sottoponendolo all'attenzione di Parlamento europeo, Consiglio dell'Unione europea e Commissione europea. Da parte sua, il gruppo VIS ha preparato e inviato a questi organismi un parere sulle modifiche proposte dalla Commissione europea riguardo al VIS. (cfr. www.sis2scg.eu, www.visscg.eu, www.eurodacscg.eu)

Attualmente, il segretariato dei tre gruppi di coordinamento di controllo è gestito dal Garante europeo della protezione dei dati. La direzione sarà affidata in futuro al Comitato europeo per la protezione dei dati (CEPD).

Sottogruppo di lavoro «Border, Travel & Law Enforcement»

Nell'anno in rassegna l'IFPDT ha partecipato in qualità di autorità di uno Stato membro Schengen a sette riunioni del sottogruppo di lavoro, incentrate in particolare sull'interoperabilità dei sistemi di informazione su larga scala dell'UE nei settori della migrazione, dell'asilo e della sicurezza, come pure sul futuro dei modelli di sorveglianza dei principali sistemi informatici dell'UE nel settore della giustizia e della politica interna.
Uno dei temi principali affrontati in queste riunioni è stato l'interoperabilità dei sistemi di informazione su larga scala dell'Unione europea (esistenti e futuri) nei settori della migrazione, dell'asilo e della sicurezza. Nel dicembre 2017 la Commissione aveva pubblicato due proposte di regolamento volte a istituire un quadro giuridico per l'interoperabilità dei sistemi di informazione su larga scala dell'Unione europea. Questo nuovo approccio e le nuove componenti introdotte (creazione di un portale di ricerca europeo, di un servizio comune di confronto biometrico e di un archivio comune di dati di identità) hanno ricadute non soltanto sulla protezione dei dati ma anche sulla gestione e la sorveglianza dei sistemi. Sono state sollevate diverse perplessità sul piano della protezione dei dati, come le finalità di una banca dati centralizzata, inclusi i termini e le condizioni d'uso di tale banca.

Sia il Garante europeo sia le autorità nazionali di protezione dei dati chiedono l'istituzione di garanzie reali a salvaguardia dei diritti fondamentali dei cittadini di Paesi terzi (cfr. il parere del Garante europeo del 16 aprile 2018 al seguente link: edps.europa.eu/data-protection [disponibile solo in inglese]).

Durante le varie riunioni si è altresì discusso del futuro dei modelli di sorveglianza dei principali sistemi informatici dell'UE nel settore della giustizia e della polizia. L'idea è di trovare una variante che migliori il meccanismo di sorveglianza dei vari sistemi, ad esempio trasferendo tale sorveglianza a una nuova struttura annessa al Comitato europeo per la protezione dei dati (che è succeduto al Gruppo di lavoro «Articolo 29» e riunisce il Garante europeo e le autorità nazionali di protezione dei dati), cui potrebbero aderire anche Paesi non membri con lo status di osservatori per le questioni che rientrano nell'acquis di Schengen.

Inoltre, sono in fase di elaborazione le linee guida sulla direttiva UE relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità di polizia e delle autorità di perseguimento penale (direttiva UE 2016/680), in particolare in relazione all'articolo 47 e ai poteri delle autorità di sorveglianza.

Gruppo di coordinamento delle autorità svizzere di protezione dei dati nell'ambito di Schengen

Il Gruppo di coordinamento Schengen delle autorità svizzere di protezione dei dati si è riunito due volte nel corso dell'anno in rassegna. L'IFPDT ha informato le autorità cantonali di protezione dei dati in merito ai principali punti trattati nella valutazione Schengen e alle raccomandazioni del Consiglio dell'UE.

A livello svizzero, il coordinamento delle attività legate a Schengen si svolge all'interno del «Gruppo di coordinamento delle autorità svizzere di protezione dei dati nell'ambito dell'attuazione dell'accordo di associazione a Schengen», che riunisce l'IFPDT e le autorità cantonali di protezione dei dati. Il Gruppo consente alle autorità rappresentate di informarsi sugli sviluppi in corso in ambito Schengen, pianificare le attività di controllo e scambiare informazioni. In questo modo, insieme ai nostri omologhi cantonali, coordiniamo le attività di sorveglianza dei trattamenti di dati effettuati in Svizzera nel settore della migrazione, della polizia e della giustizia, in applicazione della cooperazione Schengen.

Il Gruppo di coordinamento delle autorità svizzere di protezione dei dati si è riunito due volte nel corso dell'anno in rassegna. In occasione della prima riunione, l'IFPDT ha informato le autorità cantonali di protezione dei dati in merito ai principali punti discussi durante la valutazione Schengen della Svizzera svoltasi dal 26 febbraio al 2 marzo 2018 (vedi sopra). L'autorità cantonale di protezione dei dati valutata (Lucerna) ha inoltre fornito una panoramica degli elementi che la riguardano in modo particolare, e lo stesso hanno fatto gli altri organi cantonali interessati. Abbiamo inoltre fornito ai nostri omologhi cantonali dettagli dei vari controlli SIS/VIS che abbiamo eseguito nell'anno in rassegna. Da parte loro, i Cantoni hanno presentato i risultati delle loro attività di controllo.

In occasione della seconda riunione l'IFPDT ha fornito ulteriori dettagli sul progetto delle raccomandazioni rivolte alla Svizzera riguardo all'aspetto della protezione dei dati della valutazione Schengen. Abbiamo inoltre informato i colleghi cantonali in merito ai punti principali trattati dai gruppi di coordinamento di controllo SIS/VIS.

Conferenza internazionale degli incaricati della protezione dei dati

La 40ª Conferenza internazionale degli incaricati della protezione dei dati e della vita privata si è incentrata sulla rivoluzione digitale e sul suo impatto sulle nostre società come pure sul modo in cui una nuova etica digitale potrebbe contribuire a garantire il rispetto e la dignità nel nostro mondo dominato dalla tecnologia. È stato costituito un gruppo di lavoro sull'intelligenza artificiale.

La Conferenza, tenutasi a Bruxelles dal 22 al 26 ottobre 2018 sotto l'egida del Garante europeo della protezione dei dati (GEPD) e della Commissione bulgara per la protezione dei dati personali, ha ruotato attorno al tema «Dibattito sugli aspetti etici: dignità e rispetto in una vita dominata dai dati». Infatti, come ha sottolineato Isabelle Falque-Pierrotin, presidente della CNIL e presidente della Conferenza Internazionale, nel suo discorso di apertura, questi temi «hanno assunto una nuova dimensione e si estendono a nuove problematiche, più politiche e più etiche. Si manifestano in un ambiente internazionale che, se non è mai stato tranquillo, ora appare particolarmente controverso. Da un lato non mancano le tensioni, anche su questioni che sono al centro della nostra missione come la localizzazione dei dati, la sicurezza informatica o la sorveglianza di massa e le tecniche dei servizi informativi; dall'altro lato, la tecnologia digitale è un'opportunità unica di sviluppo a livello mondiale, una vera rivoluzione. «Tech for good» o «AI for humanity» sono ormai all'ordine del giorno nelle riunioni dei nostri capi di Stato e di governo e il potenziale di queste tecnologie per trovare soluzioni per l'umanità è immenso».

Dichiarazione sull'etica e sulla protezione dei dati nell'intelligenza artificiale

Per la prima volta la conferenza è stata organizzata congiuntamente da un'istituzione europea e da un'autorità nazionale di protezione dei dati. Ha riunito oltre 1000 partecipanti per discutere delle sfide attuali della tutela della vita privata. Durante la conferenza a porte chiuse, gli incaricati hanno ammesso quattro nuovi membri delle autorità nazionali di protezione dei dati: l'agenzia di accesso all'informazione dell'Argentina, l'autorità bavarese di protezione dei dati, l'autorità di protezione dei dati della Bassa Sassonia e la Commissione per le comunicazioni della Corea. La Conferenza conta ora 123 membri. Si sono tenute le elezioni per eleggere il nuovo presidente, Elisabeth Denham (presidente dell'ICO), che succede a Isabelle Falque-Pierrotin (presidente della CNIL). La prossima conferenza internazionale si terrà a Tirana dal 21 al 25 ottobre 2019.

La sessione a porte chiuse ha adottato un testo storico: la Dichiarazione sull'etica e sulla protezione dei dati nell'intelligenza artificiale. La dichiarazione stabilisce sei principi guida, che costituiscono altrettanti valori fondamentali per la salvaguardia dei diritti umani nello sviluppo dell'intelligenza artificiale. Infine, la Conferenza ha adottato cinque risoluzioni che riguardano i seguenti punti: piattaforme di e-learning, modifica di regole e procedure della conferenza internazionale, tabella di marcia per il futuro della conferenza internazionale, collaborazione tra autorità di protezione dei dati e autorità di protezione dei consumatori e censimento delle conferenze internazionali.

Conferenza europea degli incaricati della protezione dei dati

La Conferenza è stata l'occasione per fare il punto sui problemi legati all'avvio del processo di attuazione del GDPR, che mette a disposizione degli attuali 28 Stati membri dell'Unione europea una legislazione solida e uniforme.
Questa 28ª edizione, intitolata «Data Protection – Better Together», si è svolta a Tirana (Albania) il 3 e 4 maggio 2018. I partecipanti hanno anche discusso dell'aggiornamento della Convenzione 108 del Consiglio d'Europa, che consentirà in particolare di promuovere la cooperazione tra le Parti, dell'integrazione delle norme europee di protezione dei dati negli altri sistemi normativi o ancora del trattamento dei dati personali nell'azione umanitaria. La Conferenza europea ha deciso di prorogare e chiarire il mandato del Gruppo di lavoro sul futuro della Conferenza, di cui l'IFPDT è membro. Il Gruppo di lavoro deve ora elaborare proposte concrete per aggiornare le regole di funzionamento di questo organismo che molto probabilmente sarà chiamato a svolgere un ruolo importante nella collaborazione tra le autorità di protezione dei dati. Infine, la Conferenza ha esaminato una bozza di documento per promuovere e rafforzare la cooperazione e lo scambio di competenze tra gli Stati membri dell'UE e i Paesi terzi nell'ambito del GDPR.

Gruppo di lavoro dell'OCSE sulla sicurezza dell'informazione e la vita privata

Il Gruppo di lavoro sulla sicurezza dell'informazione e la protezione della vita privata dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha dedicato i suoi lavori a diverse raccomandazioni.
Il Gruppo ha esaminato la versione rivista della proposta di Raccomandazione dell'OCSE sulla protezione delle infrastrutture critiche informatizzate (ICI). La proposta evidenzia l'importanza delle linee guida sulla sicurezza per le ICI, fornisce orientamenti sulle politiche nazionali e propone strumenti per migliorare la cooperazione internazionale in materia di protezione delle ICI. Individua la necessità di una maggiore cooperazione internazionale per affrontare i problemi transfrontalieri, data l'importanza di Internet come infrastruttura globale. I delegati hanno discusso su come migliorare i dati destinati all'elaborazione di politiche di sicurezza e protezione della vita privata, in particolare sulla comparabilità dei rapporti di notifica in caso di violazione dei dati. Hanno inoltre esaminato la Raccomandazione del 2012 sulla protezione dei minori su Internet, attualmente in fase di revisione.

Nel 2013 l'OCSE ha adottato le linee guida riviste sulla protezione della vita privata e i flussi transfrontalieri di dati di carattere personale, le quali aggiornano la versione originale del 1980 e prevedono il monitoraggio della loro attuazione nonché un resoconto dopo cinque anni. Pertanto, nella riunione del 13 e 14 novembre il gruppo di lavoro ha esaminato e approvato un processo di revisione di tali linee guida ed è stato incaricato di istituire un gruppo di esperti, di cui l'IFPDT farà parte.

Associazione francofona delle autorità di protezione dei dati (AFAPDP)

L'AFAPDP ha organizzato, tra le altre cose, una tavola rotonda sul tema delle reti sociali e dei processi elettorali con esperti in materia elettorale e rappresentanti dei partiti politici.
L'Associazione francofona delle autorità di protezione dei dati (Association francophone des autorités de protection des données, AFAPDP) si è riunita in conferenza il 18 e 19 ottobre 2018 a Parigi. L'IFPDT è membro dell'associazione sin dalla sua istituzione nel 2007. In questa occasione i membri dell'associazione hanno adottato una risoluzione sulla proprietà dei dati personali, in cui si attira l'attenzione sul fatto che essi sono elementi costitutivi della persona umana; pertanto, all'interno del mondo francofono, quale presupposto per il mantenimento della democrazia e dello Stato di diritto nelle nostre società, è necessario sostenere l'adozione di legislazioni sulla protezione dei dati personali e della vita privata. Tali legislazioni devono consentire agli individui di esercitare pienamente i diritti inalienabili connessi ai loro dati personali, garantendo loro un elevato livello di controllo su di essi. Infine, l'AFAPDP ha proposto una riunione che ha permesso alle varie autorità di condividere le loro esperienze a distanza di cinque mesi dall'entrata in vigore del GDPR.

Il nuovo GDPR. In alcuni casi applicabile anche in Svizzera

Il nuovo Regolamento europeo sulla protezione dei dati (GDPR) è entrato in vigore nell'Unione europea il 25 maggio 2018. In determinate circostanze si applica anche al trattamento dei dati da parte di imprese svizzere. L'IFPDT ha pubblicato un promemoria e ha partecipato a numerose sessioni informative nell'ambito delle sue attività di consulenza e sensibilizzazione.

Adottato il 27 aprile 2016, il Regolamento europeo sulla protezione dei dati (GDPR) è direttamente applicabile in tutti gli Stati membri dell'Unione europea dal 25 maggio 2018. Il suo campo di applicazione, tuttavia, è molto più ampio del solo territorio dell'Unione europea: il titolare del trattamento (o l'incaricato del trattamento), il quale offra beni o servizi a persone all'interno dell'Unione europea ovvero monitori il comportamento di tali persone, in particolare per analizzarne le preferenze, è soggetto ai requisiti del GDPR anche se non risiede nell'Unione. Le nuove norme intendono conferire ai cittadini dell'Unione un maggiore controllo sui loro dati personali, responsabilizzare di più le imprese riducendone al contempo gli oneri di dichiarazione e rafforzare il ruolo delle autorità preposte alla protezione dei dati.

Una delle prime, maggiori difficoltà per un'autorità di protezione dei dati di un Paese terzo come la Svizzera riguarda alcune imprecisioni legate ai concetti di «offrire beni e servizi a persone sul territorio dell'Unione» o «monitorare il comportamento di tali persone». Anticipare e definire i contorni di un testo di cui non siamo né autori né interpreti è azzardato. Tuttavia, dato che questa nuova legge interessa direttamente anche la Svizzera, l'IFPDT ha pubblicato un promemoria che tratta in particolare l'applicazione extraterritoriale del nuovo diritto europeo. Ne consegue che, nel valutare l'assoggettamento al regolamento, occorrerà sempre considerare il caso specifico e in particolare l'intenzione del titolare del trattamento di offrire beni o servizi a persone sul territorio dell'Unione o di monitorarne il comportamento.

Linee guida concernenti il campo di applicazione del GDPR

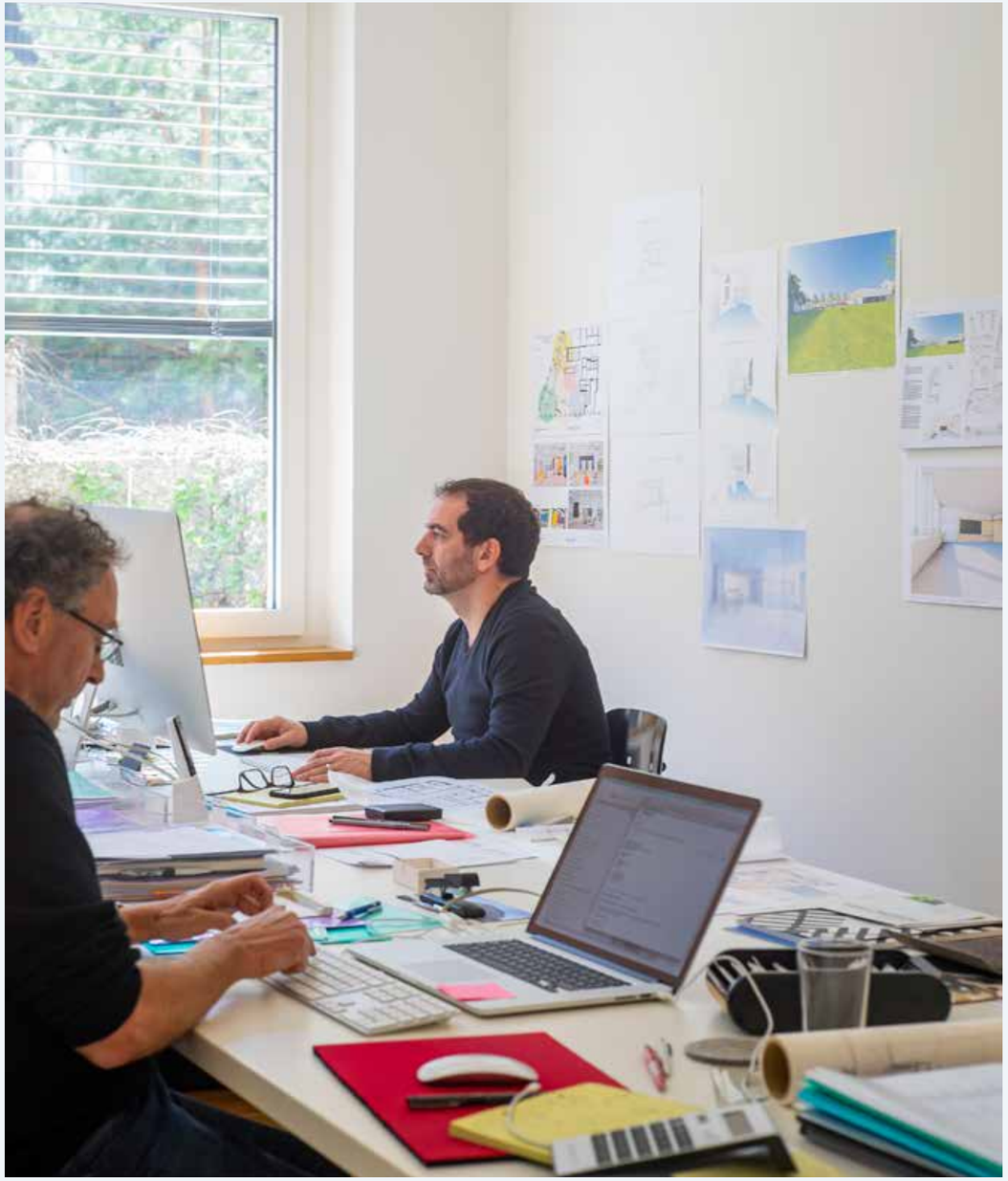
L'IFPDT ha contribuito a numerose sessioni informative su questo tema, sia presso l'Amministrazione federale sia presso privati. Nell'ambito della sua attività di consulenza, ha anche risposto a tutta una serie di quesiti, orali e scritti, posti dai cittadini e dai media.

Siccome le autorità francofone europee al di fuori dell'UE si trovavano ad affrontare le stesse difficoltà, si sono incontrate più volte nel corso dell'anno per condividere le loro esperienze e le domande che vengono loro poste al fine di coordinare le risposte.

Oltre sei mesi dopo l'entrata in vigore del GDPR, il Comitato europeo per la protezione dei dati (CEPD) – ossia l'organismo europeo indipendente che contribuisce all'applicazione coerente delle norme di protezione dei dati nell'Unione europea – ha pubblicato le sue linee guida concernenti il campo di applicazione del GDPR. Le linee sono state oggetto di una consultazione pubblica, cui l'IFPDT ha partecipato in collaborazione con l'autorità monegasca (CCIN), allo scopo di chiedere chiarimenti su una serie di elementi legati a questo tema di grande importanza per i Paesi terzi integrati nel paesaggio dell'Unione.

Valutazione del livello di protezione

La Commissione europea valuta il livello di protezione dei dati nei paesi terzi. Ha certificato alla Svizzera nel 2000 che il suo livello di protezione dei dati è adeguato. Le imprese dell'UE possono quindi scambiare dati personali con le imprese svizzere senza ulteriori misure. La Commissione sta attualmente riesaminando l'adeguatezza del livello svizzero di protezione dei dati sulla base dei criteri elencati nel GDPR. Ha annunciato che pubblicherà la decisione di adeguatezza sotto forma di relazione nel maggio 2020. La partecipazione della Svizzera alla valutazione è coordinata dall'Ufficio federale di giustizia e sostenuta dall'IFPDT fornendo le informazioni richieste (cfr. n. IV).



Consiglio d'Europa. La Svizzera dovrebbe firmare quanto prima la Convenzione riveduta

La Convenzione 108 è stata aggiornata e aperta alla firma. A oggi hanno firmato 22 Stati. La Svizzera, che ha svolto un ruolo di primo piano durante tutta la fase di elaborazione e adozione, non è ancora tra gli Stati firmatari.

I lavori di aggiornamento della Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (Convenzione 108) si sono conclusi il 18 maggio 2018 con l'adozione di un protocollo di modifica (STCE 223) da parte del Comitato dei Ministri del Consiglio d'Europa. La Convenzione aggiornata (Convenzione 108+) è stata aperta alla firma delle Parti il 10 ottobre 2018 ed è stata firmata nel frattempo da 22 Stati. Il Consiglio federale preferisce attendere prima di sottoscrivere il protocollo, dato che non è possibile prevedere quando la revisione totale della LPD giungerà in porto.

La Convenzione 108+ riafferma i principi fondamentali della protezione dei dati, ne consolida alcuni come il principio di proporzionalità, specifica le condizioni di legittimità del trattamento dei dati personali e introduce nuove garanzie e diritti per le persone interessate, ad esempio il diritto di non essere soggetti a decisioni automatizzate, il diritto di essere informati sulla logica sottesa al trattamento, il diritto di opposizione, il diritto di adire l'autorità di protezione dei dati.

La Convenzione introduce anche obblighi per i titolari del trattamento, come la notifica delle violazioni di dati, la messa in conformità, le valutazioni dei rischi, una concezione dei trattamenti atta a prevenire o ridurre al minimo i rischi di violazione dei diritti e delle libertà fondamentali o degli obblighi di trasparenza. Disciplina inoltre i trasferimenti internazionali di dati, precisa ed estende le competenze e i poteri delle autorità di controllo nonché i loro obblighi di cooperazione. Infine, istituisce un meccanismo di monitoraggio e valutazione del rispetto delle disposizioni della Convenzione.

Un aggiornamento necessario che tiene conto della realtà globale e digitale

L'aggiornamento si è reso necessario per tenere conto degli sviluppi tecnologici e giuridici intervenuti dal 1981 e intende essere una risposta credibile ed efficace alla realtà attuale del mondo globalizzato e digitale. Grazie alla sua natura aperta, ha una vocazione universale, un aspetto che è stato preso in considerazione nei lavori di aggiornamento, ed è formulata in termini generali, semplici e senza riferimenti tecnologici. Attualmente la Convenzione conta 53 Parti (47 Stati membri del Consiglio d'Europa e 6 Stati terzi: Capo Verde, Mauritius, Messico, Senegal, Tunisia e Uruguay). Altri tre Stati sono stati invitati ad aderire e altri undici hanno lo status di osservatori nel Comitato consultivo.

Brexit e il trasferimento di dati personali

Dopo il referendum sull'uscita del Regno Unito dall'UE (Brexit) nel giugno 2016, il Governo britannico ha comunicato la decisione di ritirarsi dall'Unione. La relativa procedura si sarebbe dovuta concludere il 29 marzo 2019, ma il termine è stato posposto.

L'Incaricato ha partecipato a numerose sedute con rappresentanti delle autorità federali e del Regno Unito per assicurarsi che la libera circolazione di dati personali tra la Svizzera e il Regno Unito rimanga possibile. Attualmente il Regno Unito è considerato un paese con un livello adeguato di protezione dei dati e l'Incaricato non ha motivo di credere che questo status possa cambiare.

La Convenzione 108+ è considerata un riferimento per un livello adeguato di protezione dei dati

Il protocollo di modifica della Convenzione 108 entrerà in vigore quando tutte le Parti lo avranno accettato o quando, entro un termine di cinque anni, 38 Parti l'avranno accettato. Nell'adottare il testo, il Comitato dei Ministri ha invitato tutte le Parti a fare il possibile per garantire una rapida entrata in vigore. La ratifica della convenzione 108+ è un criterio essenziale affinché l'Unione europea mantenga la validità della decisione di riconoscere l'adeguato livello di protezione dei dati di un Paese terzo. Ciò è particolarmente importante per le piazze economiche e finanziarie di Paesi terzi come la Svizzera, poiché da tale riconoscimento dipende la libera circolazione dei dati tra la Svizzera e l'UE.

Anche in considerazione dello stato di avanzamento della valutazione da parte della Commissione europea (cfr. cifra III), è nell'interesse della Svizzera firmare quanto prima il protocollo di modifica e ratificarlo successivamente. Ciò presuppone che la revisione della legge federale sulla protezione dei dati, attualmente all'esame delle Camere federali, sia effettuata conformemente alle disposizioni della Convenzione 108+, come proposto dal Consiglio federale nel suo messaggio. Anche i Cantoni devono aggiornare rapidamente la loro legislazione.

Il Comitato consultivo della Convenzione 108 (T-PD) ha adottato un progetto di raccomandazione sulla protezione dei dati sanitari. La raccomandazione, che dovrebbe essere adottata dal Comitato dei Ministri nel corso dell'anno e sostituirà la raccomandazione R (97) 5 sulla protezione dei dati medici, permette di tenere conto degli sviluppi tecnologici intervenuti dal 1997 e della Convenzione 108+. Il T-PD ha anche adottato una guida pratica sulla protezione dei dati nel settore della polizia che si rivolge principalmente alle forze di polizia e illustra i principi e le norme in materia di protezione dei dati. Ha adottato anche delle linee guida sulla protezione della vita privata e sui media, elaborate in collaborazione con il Comitato direttivo sui media e la società dell'informazione (CDMSI), nonché una guida ai principi in materia di rispetto della vita privata e di protezione dei dati ai fini del trattamento in relazione all'ICANN (Internet Corporation for Assigned Names and Numbers). Sta inoltre lavorando sulle linee guida concernenti la protezione dei dati e l'intelligenza artificiale come pure sui meccanismi di monitoraggio e valutazione della Convenzione 108+.

Principio di trasparenza

2.1 In generale

Il cambiamento di paradigma perseguito con l'introduzione del principio di trasparenza voluto per rendere l'amministrazione aperta e trasparente continua a consolidarsi: nel complesso l'attuazione della legge sulla trasparenza da parte delle autorità federali va valutata in modo positivo. Lo dimostra soprattutto il fatto che il numero degli accessi completi concessi corrisponde al crescente numero delle domande, mentre la percentuale degli accessi completi negati continua a ridursi col passare degli anni (cfr. n. 2.2 di seguito).

Apprezziamo anche che la legge sulla trasparenza influisca positivamente sulla politica attiva di informazione delle autorità federali: in seguito a domande di accesso e di mediazione, l'Ispettorato federale della sicurezza nucleare (IFSN) pubblica ormai ogni mese l'andamento dei valori di emissione delle centrali nucleari svizzere (i cosiddetti dati ANPA-EMI) e l'Ufficio federale dell'energia (UFE) ogni anno i risultati dell'attuazione delle prescrizioni in materia di emissioni di CO2 per le automobili. Ai fini di una migliore trasparenza, armasuisse pubblica anch'essa un registro delle compensazioni (registro offset) e la Revisione interna DDPS i propri rapporti di verifica.

Il progetto pilota su una procedura di mediazione accelerata si è dimostrato valido ed è dunque passato all'esercizio regolare; ciò ha permesso di ottenere anche durante l'anno in rassegna risultati positivi per quel che riguarda la durata della procedura e la percentuale di intese.

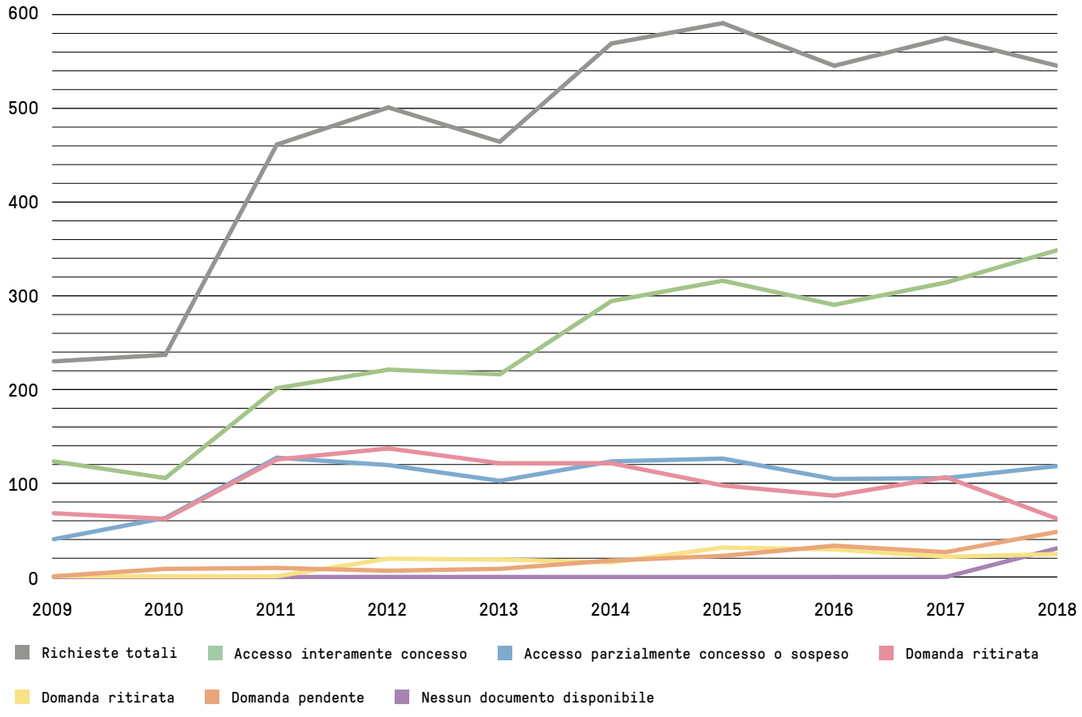
Le procedure con tre o più parti coinvolte si sono rivelate una sfida per tutti gli interessati. Vi rientrano procedure concernenti rapporti su inchieste amministrative o disciplinari, documenti che eventualmente contengono segreti commerciali di imprenditori o che riguardano la tutela della personalità di privati e collaboratori amministrativi. Queste procedure di mediazione sono spesso caratterizzate da complessi accertamenti con i terzi interessati, anche a causa della tendenza di questi ultimi a coinvolgere sempre più spesso avvocati già nella fase di procedura d'accesso e di mediazione. Ne consegue una codificazione di queste fasi procedurali, di per sé informali, e un ritardo dell'autorizzazione di accesso ai richiedenti. Questo sviluppo è chiaramente in contraddizione con l'intenzione del legislatore di allestire una procedura di accesso e mediazione lineare e rapida. Al fine di chiarire le questioni giuridiche ha infatti previsto la procedura amministrativa ordinaria, ossia una decisione delle autorità seguita dalla possibilità di interporre ricorso al Tribunale amministrativo federale.

2.2 Domande di accesso: crescita costante

Secondo i dati fornitici per il 2018, sono state presentate alle autorità federali 636 domande di accesso (contro le 581 del 2017), pari a un aumento del 9,5 per cento. Se si includono anche il Ministero pubblico della Confederazione (8) e i Servizi del Parlamento (3), la cifra sale a 647.

Le autorità hanno accordato l'accesso completo in 352 casi, pari al 55 per cento (contro i 317 del 2017, pari al 55 % del totale), mentre in 119 casi (19 %) i richiedenti hanno ricevuto solo un accesso parziale ai documenti (contro i 106 del 2017, pari al 18 %). In 62 casi (10 %) l'accesso è stato completamente negato (contro i 107 del 2017, pari al 18 %). Inoltre, le autorità hanno comunicato che 24 domande di accesso (4 %) sono state ritirate (contro le 26 del 2017, pari al 4 %), che 48 domande (8 %) erano ancora pendenti alla fine del 2018 (contro le 21 del 2017, pari al 4 %) e che in 31 casi (5 %) non esistevano documenti ufficiali.

Nel complesso l'Incaricato osserva che, dopo un forte aumento del numero di domande di accesso nel 2011, da allora questa cifra è aumentata in modo costante. Rispetto all'anno precedente, tuttavia, l'aumento nel 2018 è stato ancora maggiore, superando per la prima volta le 600 domande. Per quanto riguarda la prassi delle autorità in materia di elaborazione delle domande di accesso, le cifre sono generalmente stabili rispetto agli anni precedenti. Dal 2015, infatti, l'Incaricato osserva una stabilizzazione del numero di domande con accesso completo, che supera il 50 per cento. Per contro, il numero di domande cui l'accesso è stato completamente negato ha continuato a diminuire dal 2015. La nuova distinzione statistica introdotta nel 2018 tra rifiuto di accesso e assenza di documenti ufficiali potrebbe, tra l'altro, spiegare questa diminuzione.

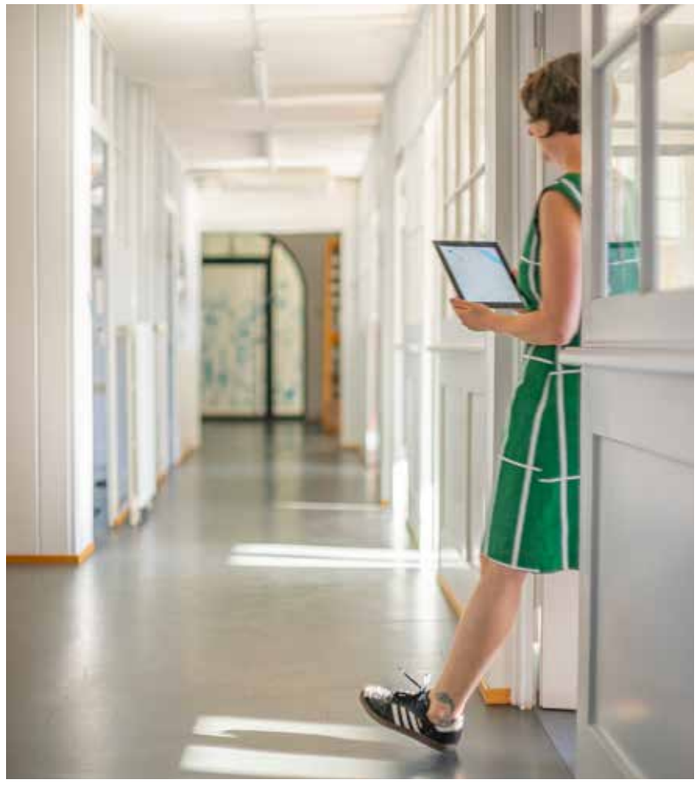


Dipartimenti e uffici federali

Per quanto riguarda i dati comunicati dagli uffici all'Incaricato, quest'ultimo osserva che nel 2018 l'UFSP ha ricevuto il maggior numero di domande di accesso (42), seguito dall'UFT (27) e da Swissmedic (24). I dipartimenti che hanno ricevuto il maggior numero di domande sono stati il DFAE (156) e il DFI (112). Al contrario, 16 autorità ci hanno informato di non aver ricevuto nessuna domanda di accesso nel 2018. Nello stesso periodo l'Incaricato si è visto recapitare sette domande, cui ha accordato l'accesso completo in quattro casi e parziale in un caso; un caso risulta ancora pendente, mentre nell'ultimo caso il documento richiesto non esisteva.

Nel 2018 soltanto 17 domande di accesso hanno comportato la riscossione di un emolumento, pari al 2,62 per cento (contro l'1,89 % del 2017). Va osservato che solo otto autorità hanno applicato emolumenti. Il totale degli emolumenti riscossi per l'accesso ai documenti ammonta a 13 358 franchi svizzeri. Si tratta di un importo superiore a quello del 2017 (6160 franchi), ma sempre in linea con lo standard rispetto agli anni precedenti (2016: 22 700 franchi, 2015: 13 663 franchi). Come negli anni precedenti, la riscossione di emolumenti è stata un'eccezione, poiché in quasi il 98 per cento dei casi non ne è stato applicato alcuno. Mentre la Cancelleria federale, il DFGP, il DFAE e il DFF non hanno riscosso emolumenti, gli altri quattro dipartimenti hanno addebitato ai richiedenti le proprie ore di lavoro in una minoranza di casi. La maggior parte degli importi è stata fatturata dal DFI (10 900 franchi per otto domande) e dal DATEC (1300 franchi per tre domande).

Per quanto riguarda la contabilizzazione delle ore di lavoro dedicate all'elaborazione delle domande, l'Incaricato sottolinea ancora una volta che le autorità non sono tenute a registrarle e che non esiste una direttiva di registrazione uniforme per tutta l'Amministrazione federale. Le informazioni gli vengono fornite su base volontaria e riflettono solo in parte le ore di lavoro effettivamente impiegate nell'elaborazione delle domande. Secondo questi dati, le ore di lavoro comunicate quest'anno sono aumentate del 63 per cento rispetto all'anno precedente (2018: 4827 ore; 2017: 2968 ore). Tale aumento è correlato a un numero di domande di accesso più elevato rispetto agli anni precedenti. Per quanto riguarda le ore di lavoro investite nella preparazione delle sessioni di mediazione, si è riscontrata una netta diminuzione rispetto agli anni precedenti (2018: 672 ore; 2017: 914 ore; 2016: 857 ore). Le ore di lavoro dedicate alla preparazione di una decisione o a un'eventuale procedura di ricorso spesso non sono state contabilizzate o comunicate all'Incaricato.



Servizi del Parlamento

I Servizi del Parlamento ci hanno comunicato di aver ricevuto tre domande di accesso nel 2018. L'accesso è stato completamente negato in due casi mentre per il caso restante non esistevano documenti ufficiali.

Ministero pubblico della Confederazione

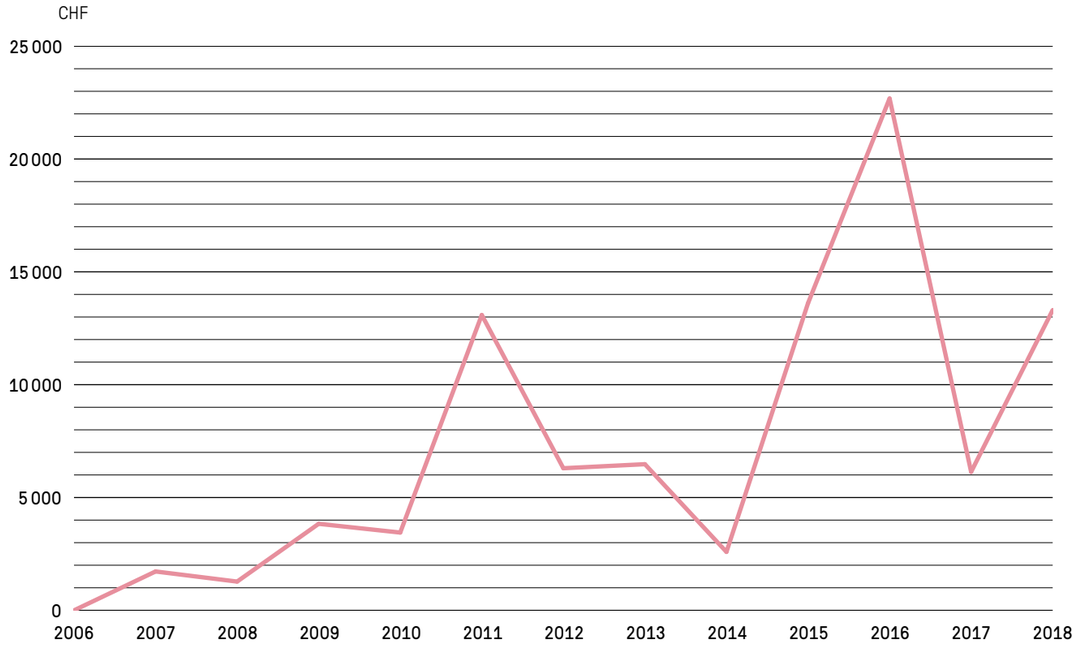
Il Ministero pubblico della Confederazione ci ha comunicato di avere ricevuto otto domande per le quali l'accesso è stato completamente accordato tre volte e negato due volte. Per i casi restanti, due domande sono ancora pendenti e per uno non esistevano documenti ufficiali.

Domande di mediazione

Nel 2018 sono state presentate all'Incaricato 76 domande di mediazione, tre in meno rispetto al 2017 (79). A differenza degli anni precedenti, i privati (26) e i media (24) hanno presentato un numero di domande simile.

Queste cifre mostrano che in 212 casi l'Amministrazione federale ha negato completamente (62) o parzialmente (119) l'accesso o non ha potuto accordarlo per mancanza di documenti (31). Si tratta di dati da mettere in relazione con le 76 domande di mediazione pervenute all'Incaricato.
Nell'anno in rassegna il 36 per cento delle domande di accesso non soddisfatte è stato oggetto di una domanda di mediazione (contro il 37 % nel 2017).

Nell'anno in esame sono state concluse complessivamente 64 procedure di mediazione. Di queste, 61 domande sono state presentate nell'anno in esame e tre nel 2017. In 26 casi è stato raggiunto un accordo tra le parti interessate. In 22 casi, in cui non è stato possibile trovare una soluzione amichevole, abbiamo formulato raccomandazioni. Tre domande sono state ritirate e in sei casi le condizioni per l'applicazione della legge della trasparenza non erano soddisfatte. In altri sei casi, la domanda di mediazione non è stata presentata in tempo.



2.3 Procedura di mediazione: alta percentuale di soluzioni consensuali

Come indicato nel precedente rapporto d'attività, nel 2017 era stato condotto un test pilota per accelerare le procedure di mediazione. In questo contesto, la maggior parte delle domande era stata trattata tramite mediazione orale alla presenza delle persone e delle autorità interessate. In caso di mancato accordo durante la sessione di mediazione, alle parti veniva inviata una raccomandazione scritta con una motivazione sintetica. Considerato il successo ottenuto dalle misure adottate, il nuovo metodo è stato integrato nella gestione ordinaria delle procedure. I dati raccolti nel 2018 sono presentati di seguito a fini comparativi e valutativi. La suddivisione dei capitoli riprende quindi i tre obiettivi del test pilota del 2017.

Tempo di elaborazione

Nella tabella 1 le procedure di mediazione sono state dapprima classificate in una delle seguenti categorie a seconda del tempo che si è reso necessario per risolverle: termine legale di 30 giorni rispettato, tempo di elaborazione da 31 a 99 giorni, tempo di elaborazione oltre 100 giorni. I tempi medi di elaborazione delle domande di mediazione ricevute negli anni dal 2014 al 2016 e poi nel 2017 e 2018 sono stati successivamente integrati come percentuali nelle varie categorie di cui sopra.

Grazie al test pilota i termini sono stati ridotti e la tendenza è stata confermata dai dati raccolti per l'esercizio 2018. Il termine di 30 giorni è stato rispettato per 32 delle 64 procedure di mediazione, pari al 50 per cento delle domande risolte. Inoltre, nessun caso ha richiesto più di 100 giorni di elaborazione.

Il superamento del termine di 30 giorni è stato spesso dovuto all'assenza delle persone o delle autorità interessate (vacanze, malattia, spostamenti), a un numero considerevole di terzi coinvolti nella procedura o alla trattazione di questioni giuridiche complesse. Va aggiunto che le situazioni summenzionate comportano spesso un trattamento particolarmente dispendioso e che, in questo caso, l'Incaricato può concedere una proroga ragionevole del termine prescritto conformemente all'articolo 12a dell'ordinanza sul principio di trasparenza dell'amministrazione (OTras; RS 152.31). Tuttavia, l'Incaricato osserva che il tempo di elaborazione di 30 giorni rimane stabile rispetto al 2017.

Tabella 1: tempo di elaborazione delle procedure di mediazione

Tempo di elaborazione in giorni	Periodo 2014–2016*	Fase pilota 2017	Periodo 2018
entro 30 giorni	11%	59%	50%
da 31 a 99 giorni	45%	37%	50%
più di 100 giorni	44%	4%	0%

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

Percentuale di soluzioni consensuali

Per misurare gli effetti dell'integrazione del test pilota nella gestione ordinaria, sono stati analizzati tre periodi. Il primo riguarda il periodo dal 2013 al 2016, il secondo il 2017, anno di avvio del test pilota, e il terzo il 2018, anno in cui il test è stato concretizzato.

Tabella 2: rapporto tra raccomandazioni e soluzioni consensuali

2013–2016	40%
2017	60%
2018	55%

L'Incaricato osserva che l'aumento della percentuale di soluzioni consensuali rispetto alle raccomandazioni è rimasto stabile e che dunque gli effetti positivi del test pilota del 2017 sono proseguiti nel 2018. L'implementazione del test pilota ha portato a un aumento significativo delle soluzioni consensuali rispetto agli anni precedenti.

A titolo di informazione, tutte le raccomandazioni emesse durante l'anno in rassegna sono disponibili sul sito Internet dell'Incaricato.

Numero di casi pendenti

Tabella 3: procedure di mediazione pendenti

Fine 2016	33
Fine 2017	3
Fine 2018	15 (di cui 13 chiuse nel febbraio 2019 e 2 sospese)

Nel 2017, a seguito dell'introduzione del test pilota, solo tre procedure risultavano pendenti a fine anno (33 nel 2016). Per il 2018, 15 casi erano ancora pendenti, precisando che dieci domande di mediazione sono state depositate a dicembre. È opportuno osservare che nel febbraio 2019, 13 di queste procedure sono state chiuse e due sospese. La sospensione della procedura di mediazione interviene quando un'autorità desidera riesaminare la propria posizione o quando deve consultare terzi coinvolti.

Sebbene il numero di procedure pendenti sia aumentato rispetto alla fine del 2017, l'Incaricato osserva che non si tratta di un calo di efficienza, ma di una coincidenza statistica. Infatti, molte domande di mediazione sono state presentate a dicembre. La diminuzione dei casi pendenti rimane quindi evidente rispetto agli anni precedenti.

2.4 Consultazione degli uffici e altri pareri

Revisione totale della legge federale sugli acquisti pubblici

Il Parlamento ha discusso una revisione completa della legge federale sugli acquisti pubblici. La proposta del Consiglio federale di abolire del tutto il principio di trasparenza negli acquisti pubblici è stata respinta. L'Incaricato ha espresso la sua ferma opposizione a questo progetto sia all'interno della commissione competente sia nei media.

I bandi di concorso e le aggiudicazioni della Confederazione sono pubblicati sulla piattaforma per le commesse pubbliche simap.ch. Durante la procedura di aggiudicazione non vi è alcun diritto di consultare la documentazione relativa agli appalti. Conformemente alla legge sulla trasparenza, i documenti possono essere consultati su richiesta solo al termine della procedura (cfr. anche 24° Rapporto d'attività 2016/2017, n. 2.3.2).

Il Parlamento ha discusso il progetto nel corso del 2018, respingendo la regolamentazione speciale prevista. Fatti salvi i contenuti rilevanti ai fini della concorrenza, i documenti di appalto restano assoggettati alla legge sulla trasparenza e quindi in linea di principio accessibili. Le imprese, i media e la popolazione possono così continuare a controllare in che modo le autorità gestiscono il denaro dei contribuenti per l'acquisto di beni e servizi. Inoltre, con l'attuazione della mozione parlamentare 14.3045 sarà introdotta nell'ordinanza sugli acquisti pubblici una norma che prevede che tutti gli acquisti con un volume contrattuale da 50 000 franchi siano pubblicati almeno una volta all'anno. Complessivamente, la revisione consoliderà la trasparenza.

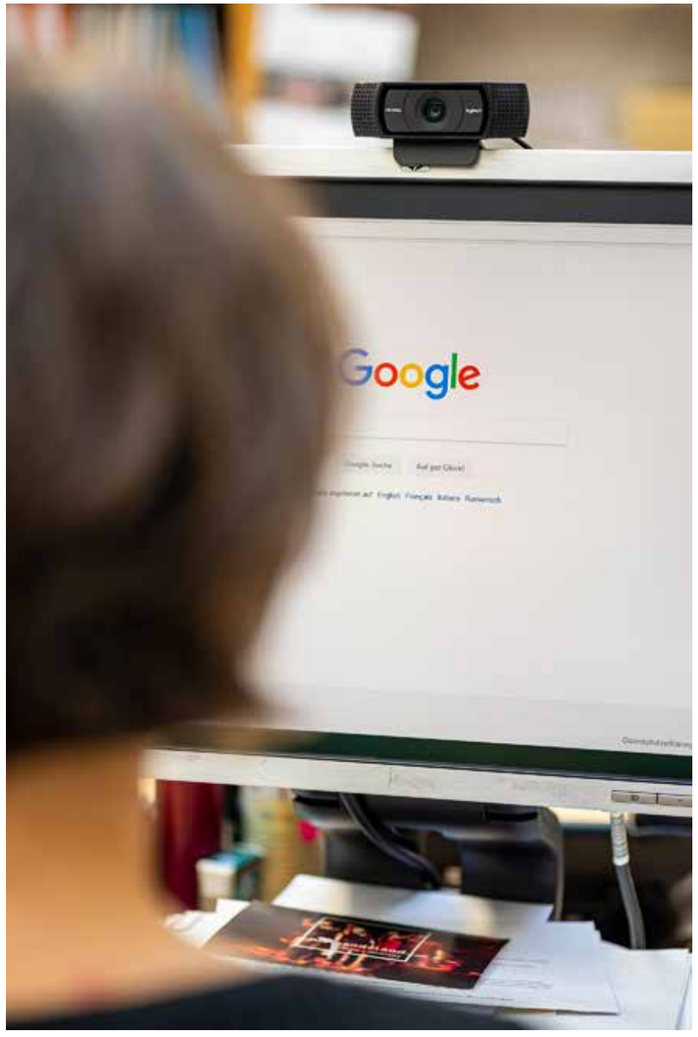
Il progetto è attualmente nella fase parlamentare di eliminazione delle divergenze, che non contempla tuttavia le disposizioni in materia di trasparenza.

Consultazione degli uffici sull'approvazione delle strutture tariffali nell'assicurazione malattie

L'Ufficio federale della sanità pubblica (UFSP) voleva introdurre una deroga al diritto di accesso ai documenti delle due procedure di consultazione degli uffici concernenti le approvazioni delle tariffe. L'Incaricato si è pronunciato contro questa proposta, con esito positivo.

Il Consiglio federale approva regolarmente le strutture tariffali nel settore delle cure ospedaliere stazionarie. Nell'anno in rassegna l'UFSP ha presentato al Consiglio federale due domande di approvazione per il settore psichiatrico. In queste domande l'UFSP ha proposto che tutte le basi di calcolo delle strutture tariffali considerate e sottoposte alla consultazione degli uffici, dopo l'approvazione del Consiglio federale venissero escluse dal diritto di accesso secondo la legge sulla trasparenza, in modo da tutelare i segreti commerciali dei soggetti coinvolti. Quale argomentazione l'UFSP ha richiamato una disposizione della legge sulla trasparenza secondo cui, in via eccezionale, i «documenti ufficiali della procedura di consultazione degli Uffici» non vengono resi accessibili nemmeno dopo la decisione del Consiglio federale.

Nel corso delle consultazioni abbiamo proposto ogni volta di rinunciare a questa regolamentazione, in quanto i documenti in questione erano stati allestiti e inoltrati all'UFSP prima dell'inizio della procedura di consultazione degli uffici e non potevano quindi in alcun modo essere considerati «documenti ufficiali della procedura di consultazione degli Uffici». Pertanto, nella fattispecie, le condizioni per un'esclusione definitiva dalla legge sulla trasparenza non erano soddisfatte. A ciò si aggiunge il fatto che la legge sulla trasparenza contempla già una disposizione specifica per la protezione dei segreti commerciali delle imprese. L'UFSP ha pertanto rinunciato alla regolamentazione speciale.



L'IFPDT

3.1 Compiti e risorse

Prestazioni e risorse nell'ambito della protezione dei dati

Effettivo del personale

Dal 2005 il numero di collaboratori impiegati per l'esecuzione della legge federale sulla protezione dei dati (LPD) ha oscillato fra le 20 e le 24 unità. La fluttuazione si spiega da un lato con l'entrata in vigore nel 2006 della legge sulla trasparenza (LTras). La creazione dei posti destinati all'assolvimento dei nuovi compiti non è mai stata autorizzata dal Consiglio federale e la nostra autorità ha quindi dovuto far capo a personale già impiegato presso l'IFPDT e, in parte, anche a risorse della Cancelleria federale. D'altro canto, l'introduzione di misure generali di risparmio non ha reso possibile la piena occupazione dei posti supplementari accordati nell'ambito dell'adesione agli accordi di Schengen e Dublino, oltre che attraverso l'emanazione di leggi speciali nel settore sanitario.

Nel suo messaggio concernente la revisione totale della LPD, il Consiglio federale ha prospettato all'IFPDT la possibilità di creare di dieci posti supplementari (FF 2017 6154). La revisione totale della legge prevede tuttavia un iter parlamentare la cui conclusione è al momento difficile da prevedere (cfr. cifra I del presente rapporto): per questa ragione è impossibile dire se e quando sarà possibile creare nuovi impieghi. Dopo che un aspetto parziale della revisione totale è stato anticipato con l'entrata in vigore il 1° marzo 2019 della nuova legge federale che attua la direttiva di Schengen (UE) 2016/680, la nostra autorità è chiamata ad assumersi ulteriori compiti e competenze per quanto riguarda il trattamento particolarmente sensibile di dati personali nel settore della polizia (cfr. n. 1.2). Al momento della pubblicazione del presente rapporto non era ancora stato deciso se il Consiglio federale avrebbe accordato le necessarie risorse supplementari richieste dall'IFPDT.

Tabella 4: Posti attribuibili per trattare questioni riguardanti la LPD

2005	22
2010	23
2018	24
2019	24

Ciò ha fatto sì, fra l'altro, che la Svizzera, in seguito all'ultima valutazione dell'UE, è confrontata con la necessità che l'autorità di controllo della protezione dei dati della Confederazione controlli più spesso il trattamento dei dati personali nelle banche dati rilevanti ai fini di Schengen e disponga di risorse sufficienti a tal fine.

Prestazioni

In base al Nuovo modello di gestione dell'Amministrazione federale (NMG), i compiti che incombono all'IFPDT, nella sua veste di autorità di protezione dei dati responsabile per gli organi federali e l'economia privata, sono attribuiti ai quattro gruppi di prestazioni Consulenza, Vigilanza, Informazione e Legislazione. Nel periodo compreso tra il 1° aprile 2018 e il 31 marzo 2019 le risorse umane attribuite all'IFPDT per la protezione dei dati sono state ripartite come segue:

Tabella 5: Servizi protezione dei dati

Consulenza a privati	21,1%	
Consulenza alla Confederazione	21,3%	
Collaborazione con i Cantoni	2,1%	
Collaborazione con autorità estere	9,8%	
Totale Consulenza		**54,3%**
Vigilanza	14,1%	
Certificazione	0,2%	
Registro delle collezioni di dati	0,7%	
Totale Vigilanza		**15,0%**
Informazione	17,6%	
Formazione / Conferenze	5,0%	
Totale Informazione		**22,6%**
Legislazione	8,1%	
Totale Legislazione		**8,1%**
Totale Protezione dei dati		**100,0%**

Consulenza

Come illustrato nel capitolo «Sfide attuali», l'IFPDT è confrontato a una continua crescita delle richieste nel settore della consulenza derivante dalla necessità di monitorare progetti sempre più grandi e complessi. Nel periodo in rassegna, la quota delle risorse di personale attribuite a questo settore è cresciuta ulteriormente, attestandosi al 53,9 per cento. Secondo il piano di controllo dell'IFPDT per il 2019, l'accompagnamento in materia di consulenza è in corso per undici grandi progetti.

Tabella 6: Consulenze svolte nel 2018 per grandi progetti

Trasporti	2
Finanze	1
Sanità e lavoro	3
Sicurezza	2
Telecomunicazioni / Internet delle cose	3

In considerazione del fatto che le risorse dell'IFPDT non sono ancora state adeguate né agli aumentati rischi tecnologici di reidentificazione e di fughe indebite di dati né alle altre sfide poste dalla digitalizzazione, l'autorità non è tuttora in grado di far fronte con la dovuta efficacia e il tempo necessario all'accresciuta richiesta di monitoraggio di progetti. Nel periodo in rassegna i tre team dell'ambito direzionale Protezione dei dati hanno risposto a circa ottanta richieste e denunce di cittadini, inviando agli interessati una lettera standard che li informa sulle vie previste dalla procedura civile al mese. La nostra autorità è stata inoltre costretta a sopprimere altre voci dal gruppo di prestazioni Consulenza, come la collaborazione internazionale. In settori sempre più numerosi i Big Data e l'intelligenza artificiale si stanno imponendo come modelli economici, mentre i rischi tecnologici legati alla protezione dei dati continuano ad estendere il campo di vigilanza dell'IFPDT: tutto ciò fa supporre che il numero dei grandi progetti pubblici e privati che implicano un trattamento di dati continuerà a crescere, come peraltro è già stato rilevato negli scorsi anni.

Vigilanza

La dinamica delle applicazioni basate su cloud impone un'esecuzione estremamente rapida dei controlli. Questa accelerazione e la necessità, viepiù inderogabile, 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 di maggiore portata debbano essere svolti da numerosi collaboratori. Come già osservato a più riprese, l'attuale entità degli effettivi limita considerevolmente la densità dei controlli. Nel 2018 all'attività di vigilanza è stato attribuito il 12 per cento circa delle risorse, quota che risulta di ben 20 punti al di sotto dei valori medi del passato. Nel periodo oggetto del presente rapporto è stato possibile far risalire tale quota attorno al 15 per cento, livello che corrisponde a quello del 2016/17. Secondo il piano di controllo per il 2019, queste risorse dovranno servire a svolgere ancora dodici controlli di vasta portata. La cifra, se rapportata alle 12 000 grandi e medie imprese attive in Svizzera, dimostra come la densità dei controlli continui a restare 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.

Legislazione

L'evoluzione tecnologica, che il Consiglio federale definisce «rapidissima» nell'introduzione al suo messaggio concernente la revisione totale della LPD (FF 2017 5941), si ripercuote anche sul trattamento dei dati personali effettuato dagli organi federali, il quale risulta lecito soltanto se si fonda su una base legale. Questa comporta l'introduzione nel diritto federale di tutta una serie di nuove prescrizioni in materia, in merito alle quali l'IFPDT è tenuto a esprimersi nell'ambito delle diverse procedure di consultazione. Negli ultimi dieci anni l'onere in questo settore è sensibilmente aumentato, andando ulteriormente a scapito della densità dei controlli. È pur vero che nel periodo di cui fa stato il rapporto siamo riusciti a interrompere questa tendenza, ma gli scarsi mezzi a nostra disposizione ci obbligano sempre più a dedicare, in sede di consultazione, una cura poco più che sommaria alla motivazione dei pareri, oltre che a decurtare le nostre prestazioni in altri ambiti di attività.

Revisione totale della LPD

Come già spiegato, i moderni strumenti di lavoro – quali la stima dei rischi legati alla protezione dei dati – fanno ormai parte della realtà digitale. Per la nostra autorità essi sono diventati infatti strumenti di uso comune anche nella gestione di grandi progetti digitali (cfr. tabella qui sopra). Per consolidare questi strumenti di lavoro dal punto di vista della certezza del diritto, e quindi la relativa attività di vigilanza svolta dall'IFPDT, è indispensabile che essi non soltanto vengano iscritti nel GDPR, ma anche integrati nel diritto svizzero in materia di protezione dei dati, come prevede d'altronde il Consiglio federale nel suo progetto di revisione totale della LPD. Dato che al momento non è possibile prevedere quando potranno essere creati i nuovi impieghi prospettati nel messaggio, la nostra autorità deve utilizzare i nuovi strumenti di lavoro nel modo più pragmatico possibile, facendo capo al personale di cui dispone.

Visite di servizio e audizioni delle Commissioni della gestione

In occasione della visita di servizio della sottocommissione DFGP/CaF della Commissione della gestione del Consiglio degli Stati nel 2018, abbiamo presentato i risultati del progetto pilota «Accelerazione delle procedure di conciliazione». Infine, l'11 aprile 2019, nel corso di un'audizione abbiamo potuto informare la sottocommissione sul successo del trasferimento del progetto pilota al normale funzionamento.

Criteri di quantificazione

La responsabilità di decidere se attribuire all'IFPDT risorse supplementari in considerazione dei compiti aggiunti nell'anno in esame e dei risultati dell'ultima valutazione Schengen compete alle autorità politiche, le quali dispongono di un considerevole margine di manovra per 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 degli individui e garantire il diritto all'autodeterminazione informazionale 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 a reagire semplicemente alle circostanze, ma possa agire con spirito d'iniziativa, e in particolare con quella credibilità e quell'intensità che i cittadini hanno ragionevolmente il diritto di attendersi per la tutela dei loro diritti fondamentali.

Per quanto riguarda i diversi gruppi di prestazioni, la quantificazione delle risorse deve fondarsi sugli obiettivi seguenti:

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.

Prestazioni e risorse nell'ambito della legge sulla trasparenza

Dopo un esperimento pilota durato un anno l'unità LTras, che continua ad essere dotata di 3,6 impieghi a tempo pieno, ha adottato una procedura accelerata e sommaria che si caratterizza per l'esecuzione di udienze di conciliazione orali. Questa procedura continua a dimostrarsi valida: oltre al numero proporzionalmente elevato di mediazioni conclusesi in modo consensuale, 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. Un aumento del numero delle richieste di mediazione, la necessità di occuparsi di più richieste in tempi brevi ed eventuali assenze a livello di personale possono però comportare il rapido accumularsi di ritardi.

3.2 Comunicazione

Intensa attività di sensibilizzazione e grande interesse dei media

L'IFPDT mira a sensibilizzare in modo tangibile l'opinione pubblica sulle questioni legate alla protezione dei dati e al principio di trasparenza. Le forme di dialogo con la popolazione vanno ulteriormente rafforzate. Il sito Internet rimane il principale mezzo di comunicazione con circa 2000 visualizzazioni al giorno.

Nell'anno in esame si è riconfermato il crescente interesse del pubblico per il lavoro svolto dall'IFPDT. L'interesse dei media ha fatto sì che si moltiplicassero le dichiarazioni dell'Incaricato, del suo supplente e del servizio stampa. Nei media osservati dall'IFPDT sono apparsi circa 3000 articoli prevalentemente su questioni relative alla protezione dei dati, ma anche sul principio di trasparenza nell'Amministrazione. In totale, abbiamo trattato oltre 400 richieste di informazione da parte dei media. I cittadini e le aziende hanno contattato i nostri esperti per posta elettronica, per posta o mediante la nostra hotline telefonica circa 3500 volte per esprimere preoccupazioni o porre domande. Questo dato è però solo indicativo, poiché nell'anno in esame abbiamo sostituito il sistema di gestione elettronica degli affari.

L'Incaricato ha anche partecipato in qualità di oratore o di animatore di tavole rotonde a una quarantina di eventi organizzati da associazioni, istituti di formazione, autorità, imprese e organizzazioni nel campo della digitalizzazione. Ha anche partecipato alla live chat della serata a tema Dataland andata in onda sulla SRF il 21 novembre 2018. L'IFPDT ha inoltre preso parte alla seconda Giornata Digitale Svizzera e prima dell'evento ha pubblicato un video in cui invitava l'economia a investire in tecnologie rispettose della protezione dei dati nell'ambito dei suoi progetti digitali.

Le autorità preposte alla protezione dei dati di Confederazione e Cantoni hanno partecipato assieme alla Giornata internazionale della protezione dei dati

Dal 2007 la Giornata internazionale della protezione dei dati viene organizzata ogni anno il 28 gennaio, su iniziativa del Consiglio d'Europa. Il suo scopo è quello di rafforzare la consapevolezza dei cittadini sulla tutela della sfera privata e sul diritto all'autodeterminazione informativa e di indurre un cambiamento duraturo del comportamento nei confronti delle nuove tecnologie.

In occasione di una conferenza stampa tenutasi a Berna, l'IFPDT e le autorità cantonali preposte alla protezione dei dati hanno informato congiuntamente i media sugli aspetti della protezione dei dati nell'ambito delle elezioni e sui rischi per la protezione dei dati derivanti da un utilizzo sistematico del numero AVS. Abbiamo inoltre sensibilizzato l'opinione pubblica sull'imminente entrata in vigore della legge sulla protezione dei dati in ambito Schengen e sulla necessità di rafforzare la vigilanza sulla polizia da parte di Confederazione e Cantoni in materia di protezione dei dati.

Pubblicate varie linee guida e raccomandazioni

Nell'anno in esame l'Incaricato ha pubblicato vari documenti più completi.

- Ad esempio, abbiamo pubblicato una guida al regolamento generale sulla protezione dei dati (GDPR) dell'UE prima della sua entrata in vigore il 25 maggio 2018. Alla fine del 2018 sono state pubblicate anche le prime linee guida sul GDPR da parte delle autorità dell'UE, che l'IFPDT ha condiviso su Twitter.
- Per sensibilizzare i bambini e i giovani all'uso sicuro dei nuovi media, all'inizio di agosto 2018 abbiamo rinnovato, con il sostegno dell'Ufficio federale delle assicurazioni sociali (UFAS), tutto il nostro materiale didattico. È destinato agli insegnanti di alunni dai 13 ai 19 anni ed è disponibile nelle tre lingue nazionali sul nostro sito Internet.
- In collaborazione con la Conferenza degli Incaricati svizzeri per la protezione dei dati (Privatim), nel dicembre 2018 abbiamo pubblicato una guida alle elezioni e alle votazioni in tedesco, francese, italiano e inglese.
- Nel gennaio 2019 abbiamo pubblicato spiegazioni concernenti la legge sulla protezione dei dati in ambito Schengen prima della sua entrata in vigore il 1° marzo 2019.
- Sul nostro sito Internet abbiamo pubblicato 18 raccomandazioni sul principio di trasparenza e due sulla protezione dei dati. Abbiamo anche aggiornato varie schede informative e linee guida come ad esempio quelle sulle dashcam e sulla comunicazione dei dati all'estero.

Grazie alla piattaforma interattiva Think Data, collegata al nostro sito Internet, siamo riusciti a sensibilizzare un pubblico più ampio sulla protezione dei dati e su una maggiore trasparenza. Con l'ausilio di scenari concreti, sulla piattaforma vengono formulate raccomandazioni sulla protezione dei dati. Think Data è il progetto di un gruppo di lavoro interdisciplinare (think services) che l'IFPDT continua a sostenere dopo averne in passato fatto parte.

Per la prima volta il rapporto d'attività viene pubblicato integralmente anche in italiano e in inglese. Ne abbiamo pure migliorato la leggibilità, concentrandoci sul layout e sul testo. Per compiere un passo verso l'editoria digitale, il rapporto è stato pubblicato per la prima volta anche come e-paper.

Il sito Internet rimane ancora il nostro canale di comunicazione più importante

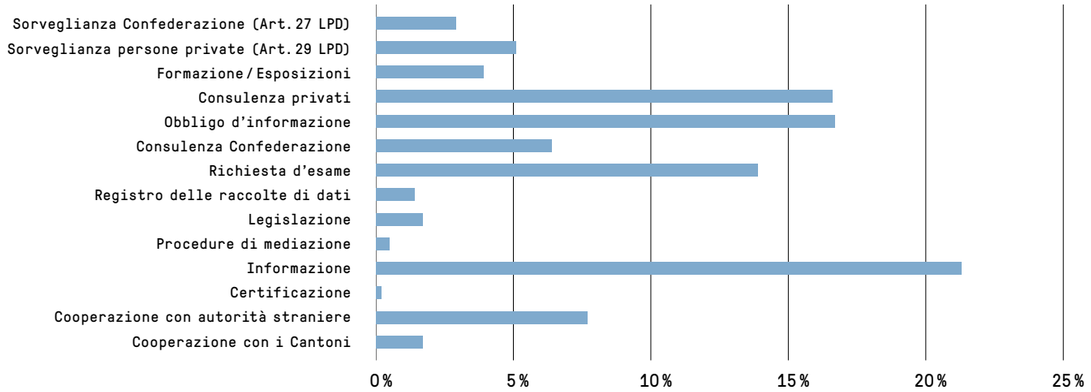
Il sito Internet è il canale di comunicazione principale dell'IFPDT. Contiamo 480 000 visitatori all'anno ossia circa 2000 per giorno lavorativo. Due visitatori su cinque provengono dall'estero – soprattutto da Paesi europei, ma anche da Oltreoceano o dall'Asia. I contenuti sono generalmente disponibili in tedesco, francese e italiano, mentre i contenuti rilevanti per gli utenti stranieri sono disponibili anche in inglese. Si prevede di migliorare il sito Internet a tappe: dovrebbe diventare più semplice con un migliore layout e offrire agli utenti un maggior numero di format di dialogo.

Su @derBeauftragte comunichiamo anche tramite il microblog Twitter. L'obiettivo è quello di consentire ai nostri follower di accedere in modo facile e rapido alle informazioni rilevanti e di far parte della comunità interessata alla protezione dei dati. Per mancanza di risorse e anche per altre ragioni, abbiamo rinunciato all'uso di altre piattaforme di social media.

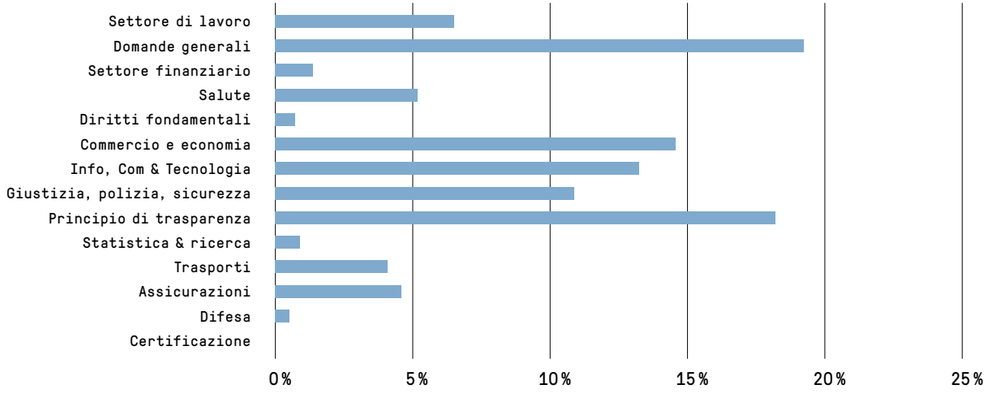
3.3 **Statistica**

Statistiche sulle attività dell'IFPDT dal 1° aprile 2018 al 31 marzo 2019 (Protezione dei dati)

Carico di lavoro per compiti

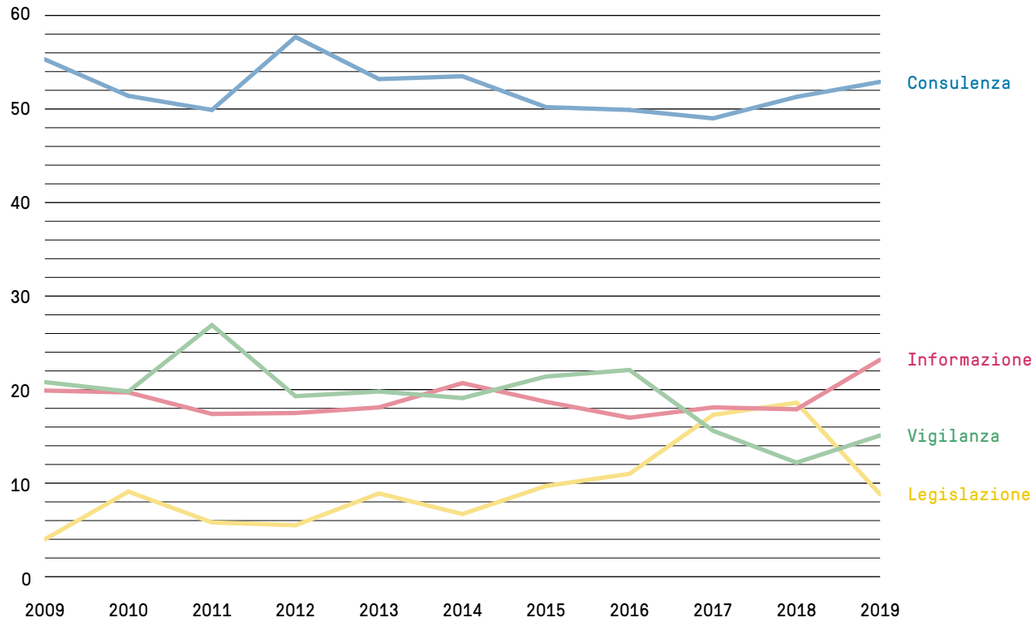


Carico di lavoro per materie



Paragone pluriennale

(in percentuale)



Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2018

	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	**18**	9	4	4	0	0	1
	IFPDT	**7**	4	0	1	0	1	1
	Totale	**25**	**13**	**4**	**5**	**0**	**1**	**2**
Dipartimento federale degli affari esteri DFAE	DFAE	**156**	107	2	28	6	8	5
	Totale	**156**	**107**	**2**	**28**	**6**	**8**	**5**
Dipartimento federale dell'interno DFI	SG DFI	**0**	0	0	0	0	0	0
	UFU	**2**	0	1	1	0	0	0
	UFC	**7**	2	1	3	1	0	0
	AFS	**6**	6	0	0	0	0	0
	METEO CH	**0**	0	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	UFSP	**42**	15	4	11	2	10	0
	UST	**5**	1	3	1	0	0	0
	UFAS	**11**	7	0	1	1	1	1
	USAV	**15**	8	1	4	0	1	1
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**24**	9	2	3	2	8	0
	SUVA	**0**	0	0	0	0	0	0
	Totale	**112**	**48**	**12**	**24**	**6**	**20**	**2**
Dipartimento federale delle finanze DFF	SG DFF	**23**	12	7	2	0	0	2
	ODIC	**3**	1	0	2	0	0	0
	AFF	**0**	0	0	0	0	0	0
	UFPER	**1**	1	0	0	0	0	0
	AFC	**7**	3	2	0	0	1	1
	AFD	**6**	3	1	0	1	1	0
	UFCL	**6**	5	0	0	0	1	0
	UFIT	**0**	0	0	0	0	0	0
	CDF	**19**	5	7	3	0	0	4
	SFI	**0**	0	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	UCC	**3**	2	0	1	0	0	0
	Totale	**68**	**32**	**17**	**8**	**1**	**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 di giustizia e polizia DFGP	SG DFGP	**5**	3	0	0	0	0	2
	DFGP	**3**	3	0	0	0	0	0
	FEDPOL	**4**	3	1	0	0	0	0
	METAS	**2**	2	0	0	0	0	0
	SEM	**13**	7	1	2	0	1	2
	Servizio SCPT	**1**	1	0	0	0	0	0
	ISDC	**1**	1	0	0	0	0	0
	IPI	**0**	0	0	0	0	0	0
	CFCG	**1**	1	0	0	0	0	0
	CAF	**2**	1	1	0	0	0	0
	ASR	**0**	0	0	0	0	0	0
	CSI	**1**	1	0	0	0	0	0
	CNPT	**0**	0	0	0	0	0	0
	Totale	**33**	**23**	**3**	**2**	**0**	**1**	**4**
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	SG DATEC	**5**	4	1	0	0	0	0
	UFA	**27**	10	0	15	2	0	0
	UFAC	**6**	2	0	3	0	0	1
	UFE	**12**	11	1	0	0	0	0
	USTRA	**6**	5	0	0	0	1	0
	UFCOM	**10**	4	0	3	0	0	3
	UFAM	**10**	3	0	1	0	3	3
	ARE	**3**	1	1	0	0	0	1
	ComCom	**1**	0	0	1	0	0	0
	IFSN	**20**	10	1	2	6	1	0
	PostCom	**3**	3	0	0	0	0	0
	AIRR	**2**	2	0	0	0	0	0
	Totale	**105**	**55**	**4**	**25**	**8**	**5**	**8**

Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2018

	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	**6**	5	0	1	0	0	0
	Difesa / Esertico	**14**	6	0	4	1	3	0
	SIC	**9**	2	2	2	1	2	0
	armasuisse	**6**	4	0	0	0	2	0
	UFSPO	**4**	3	0	0	0	1	0
	UFPP	**2**	2	0	0	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	UUC	**0**	0	0	0	0	0	0
	Totale	**41**	**22**	**2**	**7**	**2**	**8**	**0**
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	**6**	3	2	1	0	0	0
	SECO	**12**	4	3	4	0	0	1
	SEFRI	**11**	8	3	0	0	0	0
	UFAG	**17**	4	3	6	1	1	2
	UFAE	**2**	1	0	1	0	0	0
	UFAB	**0**	0	0	0	0	0	0
	SPR	**6**	5	0	1	0	0	0
	COMCO	**20**	12	4	4	0	0	0
	CIVI	**2**	2	0	0	0	0	0
	UFDC	**1**	1	0	0	0	0	0
	FNS	**1**	0	1	0	0	0	0
	IUFFP	**2**	2	0	0	0	0	0
	Consiglio dei PF	**16**	10	2	3	0	1	0
	Innosuisse	**0**	0	0	0	0	0	0
	Totale	**96**	**52**	**18**	**20**	**1**	**2**	**3**
Ministero pubblico della Confederazione MPC	MPC	**8**	3	2	0	0	2	1
	Totale	**8**	**3**	**2**	**0**	**0**	**2**	**1**
Servizi del Parlamento SP	SP	**3**	0	2	0	0	0	1
	Total	**3**	**0**	**2**	**0**	**0**	**0**	**1**

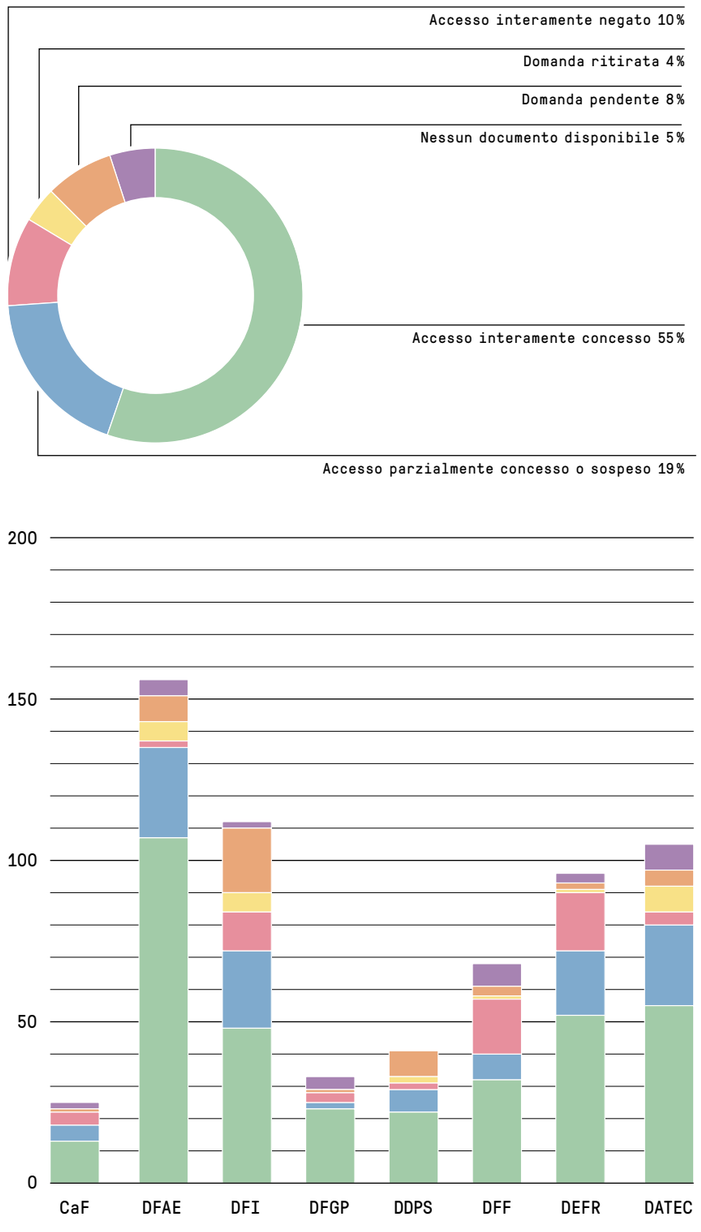
Panoramica delle domande d'accesso dei Dipartimenti e della Cancelleria federale

Dipartimento	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
CaF	**25**	**13**	**4**	**5**	**0**	**1**	**2**
DFAE	**156**	**107**	**2**	**28**	**6**	**8**	**5**
DFI	**112**	**48**	**12**	**24**	**6**	**20**	**2**
DFF	**68**	**32**	**17**	**8**	**1**	**3**	**7**
DFGP	**33**	**23**	**3**	**2**	**0**	**1**	**4**
DATEC	**105**	**55**	**4**	**25**	**8**	**5**	**8**
DDPS	**41**	**22**	**2**	**7**	**2**	**8**	**0**
DEFR	**96**	**52**	**18**	**20**	**1**	**2**	**3**
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)	–
Totale 2010 (%)	**239** (100)	**106** (44)	**62** (26)	**63** (26)	**0** (0)	**8** (3)	–
Totale 2009 (%)	**232** (100)	**124** (53)	**68** (29)	**40** (17)	**0** (0)	–	–

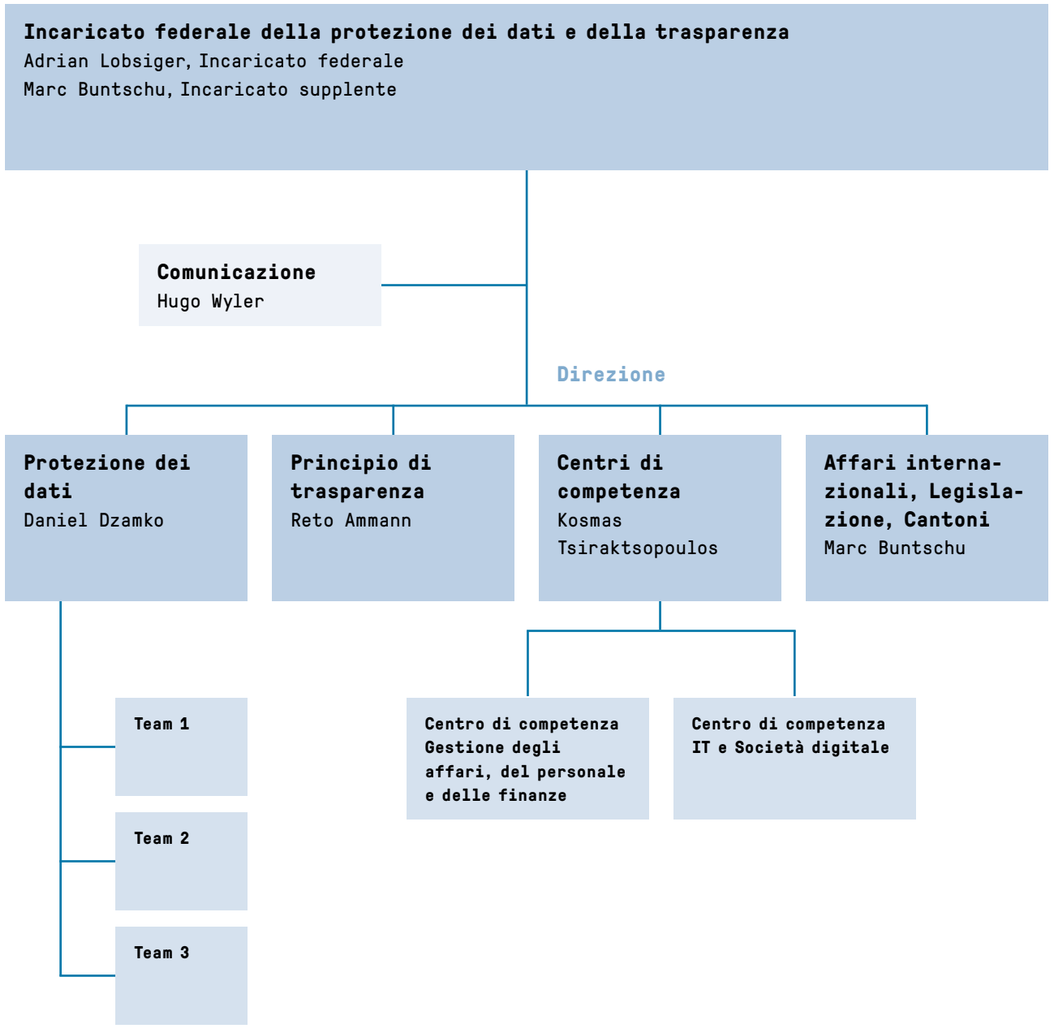
Numero di domande di mediazione

Categoria del richiedente	2018
Media	**24**
Privati (o nessuna assegnazione esatta possibile)	**26**
Parti interessati (associazioni, organizzazioni, società ecc.)	**9**
Avvocati	**4**
Aziende	**13**
Total	**76**

Trattamento delle domande d'accesso



3.4 Organizzazione IFPDT (Stato 31 marzo 2019)



Abbreviazioni

ADR Alternative Dispute Resolution body (organo di mediazione delle controversie statunitense)

AFAPDP Associazione francofona delle autorité di protezione dei dati

CEPD Comitato europeo per la protezione dei dati (EDPB, European Data Protection Board)

CEPD Controllore europeo della protezione dei dati (EDPS, European Data Protection Supervisor)

CIP Commissione delle istituzioni politiche

CNIL Commission Nationale de l'Informatique et des Libertés (Autorità francese di protezione die dati)

DoC Dipartimento del commercio statunitense

Eurodac Banca di dati biometrici dell'UE nel diritto d'asile

GDPR Regolamento europeo sulla protezione dei dati

IRM Independent Recourse Mechanism (organi di ricorso indipendenti)

LAAF Legge sull'assistenza amministrativa fiscale

LAIn Legge federale sulle attività informative

LPD Legge federale sulla protezione die dati

LPDS Legge sulla protezione dei dati in ambito Schengen [RS 235.3]

LSIE Legge federale sui servizi d'identificazione elettronica

LSIP Legge federale sui sistemi d'informazione di polizia della Confederazione

LTras Legge federale sulla trasparenza

MPT Legge federale sulle misure di polizia per la lotta al terrorismo

OCSE Organizzazione per la cooperazione e lo sviluppo economico

OTras Ordinanza sul principio di trasparenza dell'amministrazione

PCLOB Privacy and Civil Liberties Oversight Board (organo per la tutela della vita privata e delle libertà civili)

Privatim Conferenza degli incaricati svizzeri per la protezione dei dati (autorità cantonali)

RIPOL Sistema di ricerca informatizzato di polizia

SAI Scambio automatico di informazioni sui conti finanziari

SIC Servizio delle attività informative della Confederazione

SIS Sistema d'informazione Schengen

VIS Sistema d'informazione visti

Indice figurativo

Tabelle

Immagini

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. 410.026.i

Layout: Duplex Design GmbH, Basel
Fotografia: Maya Valentin
Caratteri: Pressura, Documenta
Stampa: Ast & Fischer AG, Wabern
Carta: PlanoArt®, senza legno, bianco brillante

Cifre chiave

Carico protezione dei dati

8,1 % Legislazione

22,6 % Informazione

15 % Vigilanza

54,3 % Consulenza

Domande d'accesso (LTras) principio di trasparenza

55 % interamente concesso

19 % parzialmente concesso o sospeso

10 % interamente negato

4 % ritirata

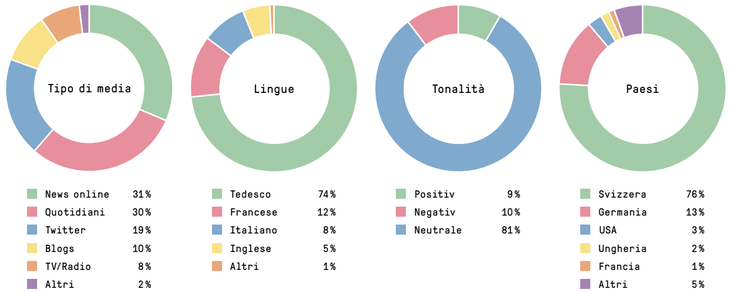
8 % pendente

5 % nessun documento disponibile

Risonanza mediale

526 Contribuzioni esaminate

4925 Dedizione (Engagement)*



*Numero di tutte le interazioni delle contribuzioni esaminate (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.