

30° Rapporto d'attività 2022/23

Incaricato federale della protezione
dei dati e della trasparenza



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapporto d'attività 2022/2023

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).

In materia di protezione dei dati il presente rapporto riguarda il periodo dal 1° aprile 2022 al 31 marzo 2023.

In materia di trasparenza copre il periodo dal 1° gennaio al 31 dicembre 2022.





Premessa

La prima legge sulla protezione dei dati è entrata in vigore il 1° luglio 1993. Già nel messaggio del 23 marzo 1988 il Consiglio federale aveva sottolineato la necessità di un intervento normativo alla luce «dell'impiego dell'informatica e delle moderne tecnologie delle telecomunicazioni in quasi tutti i settori della vita e dell'enorme intensificazione del trattamento e della diffusione dei dati personali in seno alla società, all'economia e allo Stato».

A distanza di trent'anni, la digitalizzazione ha pervaso la nostra quotidianità superando ogni previsione. Il cellulare intelligente (smartphone) e soprattutto Internet, strumenti attraverso cui l'odierna società digitale gestisce praticamente ogni aspetto del proprio vivere quotidiano – dalle operazioni bancarie agli incontri –, hanno moltiplicato in modo esponenziale il volume delle informazioni personali scambiate e l'intensità con cui sono trattate.

Il 1° settembre 2023 entrerà in vigore la nuova legge sulla protezione dei dati adottata il 25 settembre 2020. Frutto di una revisione totale, fornisce agli ambienti economici, all'Amministrazione federale e alle unità della Confederazione preposte alla vigilanza sulla protezione dei dati strumenti nuovi per rispondere con soluzioni al passo con i tempi alle legittime aspettative della popolazione, la quale auspica una protezione della sfera privata solida e rivendica il diritto all'autodeterminazione informativa.

I lavori tesi a garantire il passaggio alle nuove norme procedono a pieno ritmo, secondo la tabella di marcia (vedi il nostro tema prioritario).

Adrian Lobsiger

Incaricato federale della protezione dei dati e della trasparenza



Berna, 31 marzo 2023

Sfide attuali 6

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali 14

- Strategia cloud della Confederazione: Ambizioso progetto cloud della Cancelleria federale
- Gestione di dati a livello nazionale: Progetto «SpiGes» dell'UST
- Certificazione: Nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD)
- Elezioni e votazioni: Aggiornamento delle linee guida
- Identità elettronica, ID-E: Principio della «self-sovereign identity»
- Portale online della Posta: Accesso possibile solo con SwissID
- Strategia «Svizzera digitale»: Progetto licenza di condurre digitale

Tema prioritario 20

30 anni di protezione dei dati in Svizzera

1.2 Giustizia, polizia, sicurezza 26

- UDSC: Legge sulle dogane
- Statuto di protezione S: Applicazione «RegisterMe»
- Mitto AG: Inchiesta preliminare su un possibile abuso dell'accesso al sistema di segnalazione

1.3 Commercio ed economia 30

- Comunicazione di dati ad autorità fiscali estere: Il Tribunale federale si pronuncia negativamente in merito al diritto all'informazione di terzi nell'ambito dell'assistenza amministrativa internazionale in materia fiscale.
- Tecnologie di tracciamento: Verifica di una possibile violazione della personalità nei confronti della popolazione svizzera da parte di Oracle
- Postfinance: Rinuncia alla pubblicazione del conto
- Informazioni sulla solvibilità: Registros nella banca dati sulla base della «famiglia di cattivi pagatori»
- Ciberattacco: Inchiesta preliminare presso Infopro SA e Fiducial Winbiz SA
- Operatore di servizi voice: La falla di sicurezza è stata eliminata tempestivamente
- App di incontri: Analisi del trattamento dei dati
- Corse virtuali: Miglioramento della protezione dei dati presso un fornitore di servizi nell'ambito delle corse virtuali

1.4 Salute 37

- Registro nazionale di donazione di organi: Scarsa sicurezza dell'autenticazione online
- Registri online: Rischi di protezione dei dati nel registro delle protesi mammarie
- Vulnerabilità nella sicurezza dei dati: Procedura di accertamento dei fatti sulla banca dati dei centri di test COVID-19 privati
- Piattaforma online: Progetto di salvataggio dei dati «lemievaccinazioni.ch»
- Cartella informatizzata del paziente: Nuovi sviluppi
- Fatturazione elettronica: Obbligo legale di trasmettere una copia della fattura medica
- Fatturazione elettronica: Progetto per la trasmissione delle fatture elettroniche nell'assicurazione obbligatoria delle cure medico-sanitarie

1.5 Lavoro 47

- Personale federale: Conservazione dei dossier presso l'UST

1.6 Trasporti 48

- FFS: Sistema di misurazione della frequenza dei clienti nelle stazioni

1.7 Internazionale 50

- Europa: Consiglio d'Europa
- Europa: Conferenza europea delle autorità di protezione dei dati a Dubrovnik
- Europa: European Case Handling Workshop
- Internazionale: Assemblea mondiale per la protezione della vita privata
- AMVP: Gruppo di lavoro per l'azione umanitaria
- AFAPDP: Associazione francofona delle Autorità di protezione dei dati
- Bilaterale: Accolta di una delegazione tunisina
- Cooperazione internazionale: Privacy Symposium a Venezia
- Schengen: BTLE ed EDPB
- Schengen: Gruppi di coordinamento di controllo dei sistemi d'informazione SIS II, VIS ed Eurodac
- Schengen: Gruppo di coordinamento Schengen delle autorità svizzere di protezione dei dati
- Schengen: Attività in ambito Schengen a livello nazionale

Principio di trasparenza

2.1 In generale.....	62
2.2 Domande di accesso. Lieve calo nel 2022.....	64
2.3 Procedure di mediazione: leggero calo delle domande di mediazione.....	68
– Percentuale di soluzioni consensuali	
– Durata delle procedure di mediazione	
– Numero di casi pendenti	
2.4 Procedura legislativa.....	72
– Cibersicurezza: Modifica della legge sulla sicurezza delle informazioni (LSIn)	
– Settore dell'energia elettrica: Avamprogetto della legge federale concernente un piano di salvataggio per il settore dell'energia elettrica	
– Legge sull'archiviazione: Necessità di una revisione della legge federale sull'archiviazione	
– Finanze: Entrata in vigore della legge sul riciclaggio di denaro e della relativa ordinanza	
– Legge sui prodotti del tabacco: Revisione parziale della legge federale sui prodotti del tabacco e sulle sigarette elettroniche (LPTab)	
– Economia: Nuova legge federale sulla verifica degli investimenti esteri	
2.5 Riserve di disposizioni speciali ai sensi dell'articolo 4 LTras.....	80

L'IFPDT

3.1 Compiti e risorse.....	85
– Prestazioni e risorse nell'ambito della protezione dei dati	
– Prestazioni e risorse nell'ambito della legge sulla trasparenza	
– Partecipazione a deliberazioni delle commissioni e audizioni da parte di commissioni parlamentari	
3.2 Comunicazione.....	88
– Cifre	
– Temi prioritari	
– Trasmissione e commercio di dati	
– Nuovo sito Internet	
3.3 Statistiche.....	90
– Statistiche sulle attività dell'IFPDT dal 1° aprile 2022 al 31 marzo 2023 (Protezione dei dati)	
– Panoramica delle domande d'accesso dal 1° gennaio al 31 dicembre 2022	
– Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2022	
– Domande d'accesso 2022 con riferimento a Corona	
– Numero di domande di mediazione secondo la categoria di richiedenti	
– Trattamento delle domande d'accesso dal 1° gennaio al 31 dicembre 2022	
3.4 Organizzazione IFPDT.....	100
– Organigramma	
– Personale dell'IFPDT	

Abbreviazioni.....	102
--------------------	-----

Elenco delle illustrazioni.....	103
---------------------------------	-----

Impressum.....	104
----------------	-----

Nel pieghevole

- Cifre chiave
- Preoccupazioni relative alla protezione dei dati

Sfide attuali

I Digitalizzazione

Responsabilità digitale e protezione dei dati

La trasformazione digitale è un fenomeno che riguarda l'intera società e solleva importanti quesiti che toccano da vicino non soltanto le autorità, le imprese e gli utenti finali ma anche la collettività. Anziché aderire ciecamente allo sviluppo tecnologico, dobbiamo invece sfruttare le opportunità offerte dall'analisi dei processi per garantire che le tecnologie digitali siano utilizzate in modo responsabile a beneficio della popolazione.

In tale contesto, assume un'importanza fondamentale la responsabilità digitale, un concetto dalle molteplici sfaccettature e che presenta implicazioni di natura tecnico-finanziaria, giuridica, ecologica, sociale ed etica. Alla luce dei nuovi rischi derivanti dal potenziale sviluppo della digitalizzazione a cui sono esposti anche i titolari del trattamento dei dati, l'IFDPT ritiene che la responsabilità digitale debba

ormai essere considerata come parte integrante del buon governo. Il rispetto degli obblighi derivanti dalla legislazione sulla protezione dei dati, il cui scopo è quello di proteggere i diritti della personalità nel trattamento di dati personali, rientra dunque nell'ambito della responsabilità digitale.

Con la revisione della legge federale sulla protezione dei dati (LPD) i titolari del trattamento sono ora obbligati ad adottare un approccio proattivo nei trattamenti automatizzati e nella digitalizzazione (cfr. Tema prioritario). La nuova normativa offre loro strumenti per effettuare analisi globali e specifiche del trattamento di dati nonché tecnologie per assicurare trasparenza, fiducia

e credibilità nei confronti delle persone interessate. Sebbene non sia possibile escludere totalmente qualsiasi rischio nel trattamento di dati personali, i titolari del trattamento possono servirsi di tali strumenti per individuare e limitare i rischi residui nonché gestirli con autonomia assicurando la protezione della sfera privata e il diritto all'autodeterminazione informativa dei diretti interessati.

L'adozione di un approccio proattivo assume un ruolo decisivo anche per quanto attiene agli aspetti tecnici della sicurezza. Occorre infatti contrastare gli attacchi informatici con misure lungimiranti. I casi tristemente noti delle piattaforme *lemievaccinazioni.ch* o *Swisstransplant* (cfr. n. 1.4) sono la prova del fatto che le norme e gli strumenti introdotti con la nuova legge sono essenziali per la salvaguardia dei diritti fondamentali e la responsabilità digitale.

«Nel suo ruolo di autorità di vigilanza per la protezione dei dati, l'IFDPT non rilascia autorizzazioni.»

Consulenza in materia di vigilanza e gestione di progetti con un approccio basato sui rischi

Il significato concreto di responsabilità digitale quale responsabilità individuale delle imprese appare evidente nei servizi di consulenza forniti dall'IFPDT quale autorità di vigilanza ai responsabili di progetti digitali appartenenti al settore dell'economia. La legislazione svizzera sulla protezione dei dati consente infatti il trattamento di dati personali da parte di privati senza che questi debbano richiedere un'autorizzazione ufficiale.

Nel suo ruolo di autorità di vigilanza per la protezione dei dati, l'IFPDT non rilascia dunque alcuna autorizzazione. Nell'ambito dei suoi servizi di consulenza, l'IFPDT vigila sull'applicazione delle disposizioni sulla protezione dei dati. La gestione dei progetti rimane pertanto di esclusiva competenza dei responsabili di progetto. Da parte sua, l'IFPDT si adopera per sensibilizzare questi ultimi agli aspetti legati alla loro responsabilità digitale, che in alcune circostanze possono anche prescindere dalle disposizioni sulla protezione dei dati: si pensi ad esempio alle implicazioni psicologiche dei sensori digitali impiegati da imprese private negli ambienti di lavoro, negli esercizi commerciali o nelle aree di incontro. La presenza di questi sensori può infatti indurre le persone a modificare la propria condotta, limitandone fortemente

la libertà di autodeterminazione (cosiddetto effetto dissuasivo, o «chilling effect»). Questa sorta di autocensura può essere causata, oltre che dalla quantità di sensori utilizzati, anche dalle finalità poco chiare per le quali sono raccolti i dati tramite tali sensori. Il grado di cautela che dovrebbero assumere i responsabili di progetto nell'impiegare i sensori digitali tenendo conto del «chilling effect» e del principio di proporzionalità in materia di protezione dei dati è in primis una questione di strategia aziendale e dunque di auto-responsabilità digitale (cfr. n. 1.6 «Trasporti»).

«Il cosiddetto «chilling effect» può indurre le persone a modificare la propria condotta, limitandone fortemente la libertà di autodeterminazione.»

Tuttavia, la nuova LPD pone anche dei limiti alla responsabilità individuale delle imprese, che l'Incaricato farà rispettare rafforzando la sua attività di vigilanza. Se durante la fase di pianificazione i responsabili di progetto individuano un rischio potenzialmente elevato connesso al trattamento previsto, la nuova normativa obbliga questi ultimi a effettuare previamente la cosiddetta valutazione d'impatto sulla protezione dei dati (VIPD) allo scopo di valutare più dettagliatamente tale rischio e a prevedere provvedimenti adeguati.

Tuttavia, anche qualora dall'esame della VIPD emerga che, nonostante i provvedimenti previsti dal titolare, il trattamento previsto comporta un rischio elevato, la nuova LPD non

esclude che i dati possano essere comunque trattati. Cionondimeno, la normativa esige che i titolari del trattamento chiedano il parere dell'IFPDT e gli sottopongano la VIPD.

L'IFPDT verifica quindi se la VIPD che gli è stata sottoposta descrive i rischi individuati in modo chiaro, comprensibile e completo e se lo scopo del trattamento è conforme alla legislazione sulla protezione dei dati tenendo conto dei rischi, ovvero se l'entità del trattamento previsto può essere considerato ragionevole per il diretto interessato e dunque nel complesso proporzionale. L'IFPDT comunica entro due mesi al titolare del trattamento le sue obiezioni contro il trattamento previsto e propone eventuali provvedimenti. Tali obiezioni possono riguardare sia le modalità di esecuzione della VIPD sia il trattamento previsto. Il primo caso si verifica se il titolare del trattamento non valuta i rischi imminenti in modo adeguato e trasparente. Il parere dell'IFPDT non implica l'autorizzazione di un progetto specifico.

Se il titolare si rifiuta di accogliere le obiezioni e le proposte sostanziali da parte dell'IFPDT, quest'ultimo può intervenire conformemente al diritto

in materia di vigilanza aprendo un'istruzione oppure ordinando di adeguare il trattamento in base alle proposte presentate, se non addirittura vietando del tutto il trattamento a tempo debito. L'intervento formale dell'IFPDT si rende opportuno se il titolare del trattamento non può esigere che le persone interessate accettino un rischio in base alla probabilità che questo si verifichi e alla gravità della violazione dei diritti della personalità e dunque il trattamento previsto risulta inammissibile ai sensi del diritto in materia di protezione dei dati. Questa ipotesi si realizza ad esempio se il trattamento di dati correlato a un rischio residuo elevato viola i principi concernenti la protezione dei dati secondo l'articolo 6 nLPD (p. es. la proporzionalità) o le esigenze concernenti la sicurezza dei dati secondo l'articolo 8 nLPD.

«La nuova LPD pone dei limiti all'auto-responsabilità digitale, che l'Incaricato farà rispettare rafforzando la sua attività di vigilanza.»

II Aumento delle deroghe alla LTras fondate su leggi speciali e sul diritto di necessità

Nell'ordinanza di necessità del 16 marzo 2023 concernente mutui supplementari a sostegno della liquidità e la concessione da parte della Confederazione di garanzie in caso di dissesto per mutui a sostegno della liquidità erogati dalla Banca nazionale svizzera a banche di rilevanza sistemica, il Consiglio federale ha fra l'altro decretato che l'accesso ai documenti ufficiali in virtù della legge sulla trasparenza è escluso. L'esclusione, per il tramite di un'ordinanza di necessità, dei diritti di accesso garantiti ai cittadini dalla legge sulla trasparenza solleva questioni giuridiche di fondo.

Poco dopo la fase pandemica caratterizzata da decisioni fondate sul diritto di necessità e il piano di salvataggio per le aziende elettriche, il Consiglio federale, emanando l'ordinanza del 16 marzo 2023, ha nuovamente escluso dalla legge sulla trasparenza una serie di attività che ha trasferito all'Amministrazione tramite il diritto di necessità. Entrambi i casi possono comportare l'impiego di denaro pubblico nell'ordine di miliardi di franchi.

Il modo di procedere del Consiglio federale solleva questioni giuridiche di fondo: dai motivi adottati per l'emanazione del diritto di necessità a sostegno del settore elettrico e di quello finanziario, fondandosi direttamente sulla Costituzione federale, in nessuno dei casi citati è possibile dedurre l'esigenza, stando alle informazioni attualmente in possesso dell'IFPDT, di escludere anche il diritto dei cittadini di conoscere l'azione condotta dall'amministrazione nell'ambito del diritto di necessità. Se non risulta indispensabile limitare i diritti dei cittadini derivanti dalla legge sulla trasparenza tramite il diritto di necessità, ci si può chiedere

da quale base legale il Consiglio federale fonda il diritto di abrogare una legge federale mediante ordinanza.

Se la legge sulla trasparenza avesse conservato la sua validità, in entrambi i casi l'Amministrazione federale avrebbe avuto la possibilità di limitare l'accesso ai documenti ufficiali appellandosi alla protezione di interessi pubblici o privati contemplati dalla legge o perlomeno di differire l'accesso fintanto che l'Assemblea federale non avesse deliberato, nell'ambito del processo legislativo ordinario, l'esclusione della trasparenza dell'Amministrazione e, in caso di decisione in tal senso, l'avesse iscritta in una legge formale.

In considerazione del numero crescente di esclusioni dalla LTras in base a leggi speciali, il Commissario ha deciso di pubblicare, a partire da questo rapporto, una tabella che mostra il numero attuale di tali esclusioni. (cfr. n. 2.5).

«L'esclusione, per il tramite di un'ordinanza di necessità, dei diritti di accesso garantiti ai cittadini dalla legge sulla trasparenza solleva questioni giuridiche di fondo.»

III Cooperazione nazionale ed internazionale

Rafforzare la collaborazione con i Cantoni

Nell'ambito della trasformazione digitale il trattamento dei dati personali diventa sempre più complesso: si mescolano molteplici attori pubblici e privati e aumenta il trattamento dei dati a cascata da parte di terzi. L'attualità conferma questo fenomeno quando riporta di ciberattacchi e violazioni della sicurezza dei dati, come per esempio nel caso di Infopro e Winbiz (cfr. n. 1.3).

Al fine di garantire una vigilanza efficace e integrale, soprattutto in considerazione dei punti attinenti alla legislazione federale e cantonale in

materia di protezione dei dati, si intensifica la collaborazione. Ciò vale in particolare nel caso in cui gli enti pubblici cantonali o comunali si avvalgono di persone private per trattare i dati oppure quando gli enti privati o pubblici intervengono in virtù del diritto privato o in qualità di autorità pubbliche oppure ancora laddove sono in vigore disposizioni cantonali che consentono di applicare la legge federale sulla protezione dei dati.

L'IFPDT ne ha fatto peraltro uno dei punti della propria strategia per il 2023, ovvero il rafforzamento della collaborazione in materia di trasparenza e protezione dei dati con i propri omologhi cantonali e comunali, per affrontare insieme la trasformazione digitale, nel rispetto delle competenze e dell'indipendenza di ciascuno.

In vista delle elezioni federali del 2023 l'IFPDT e l'ufficio della Conferenza degli incaricati svizzeri per la

protezione dei dati (privatim) hanno aggiornato la loro guida al trattamento digitale dei dati personali nel contesto delle elezioni e delle votazioni in Svizzera (cfr. n. 1.1).

Inoltre, le autorità di protezione dei dati continueranno a dedicarsi al tema del cloud, in particolare al trasferimento nel cloud di banche dati, applicazioni e processi informatici «on-premise». A tal riguardo, l'IFPDT segue attentamente gli sviluppi all'interno dell'Unione europea e si confronta anche con le varie parti interessate.

«Le autorità per la protezione dei dati della Confederazione, dei Cantoni e delle Comuni intendono intensificare la loro collaborazione.»

Consiglio d'Europa

Il Comitato consultivo della Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (Convenzione 108) è aperto anche agli Stati che non sono membri del Consiglio d'Europa. In seguito all'espulsione straordinaria della Russia dal Consiglio d'Europa, il Comitato consultivo si è dovuto occupare della questione legata alle future condizioni di adesione per eventuali casi analoghi (cfr. n. 1.7). Una partecipazione attiva nel Comitato è un presupposto fondamentale, in particolare nell'ottica della Convenzione 108 modernizzata (la cosiddetta Convenzione 108+), considerata uno strumento importante che costituisce un ponte tra le diverse regioni del mondo e i vari quadri normativi dei singoli Paesi. L'IFPDT continua a impegnarsi attivamente in seno al Comitato.

Cooperazione internazionale

La questione della trasmissione di dati personali in un Paese privo di un livello adeguato di protezione solleva in diversi Stati interrogativi analoghi riguardo alla protezione dei dati. In tale contesto, l'IFPDT segue in particolare l'evoluzione in atto nell'UE e negli Stati membri dell'UE e dello SEE, specialmente anche in relazione ai colloqui che l'UE conduce al riguardo con gli Stati Uniti.

Valutazione del livello di protezione dei dati

Il nostro Paese è ancora in attesa che l'UE riconosca alla legislazione svizzera in materia di protezione dei dati un livello di protezione adeguato ai sensi del regolamento europeo sulla protezione dei dati (GDPR), in vigore dal 2018. Nel frattempo, continua a rimanere valida la decisione di adeguatezza emanata nel 2000 sulla base della precedente direttiva 95/46/CE sulla tutela dei dati personali, sostituita in seguito dal GDPR. Presumibilmente la Commissione europea pubblicherà simultaneamente i rapporti sull'adeguatezza di tutti gli Stati già ritenuti adeguati ancora prima dell'entrata in vigore del GDPR (Andorra, Argentina, Canada [organizzazioni commerciali], Isole Faroe, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Uruguay). Si auspica che la nuova decisione di adeguatezza riguardo alla Svizzera venga emanata nel corso del 2023.

«Si spera che la Commissione europea prenda la nuova decisione di adeguatezza per la Svizzera nel corso dell'anno 2023.»

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali

STRATEGIA CLOUD DELLA CONFEDERAZIONE

Ambizioso progetto cloud della Cancelleria federale

Nell'anno in rassegna l'IFPDT si è occupato di questioni legate all'attuazione della strategia cloud dell'Amministrazione federale. Oltre a partecipare a diverse consultazioni degli uffici, ha fornito consulenza alla Cancelleria federale nell'ambito del progetto CEBA («Cloud-Enabling Bureau Automation», burotica nei cloud). Il settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale ha sottoposto all'IFPDT, nell'ambito di una consultazione degli uffici, i principi del cloud, che costituiscono parte integrante della strategia cloud dell'Amministrazione federale e che dovrebbero fungere per le singole unità amministrative da raccomandazioni per l'acquisto di applicazioni cloud.

L'IFPDT ha chiesto tra l'altro che le raccomandazioni del TDT vengano considerate come norme minime vincolanti, passibili di ampliamenti da parte dei dipartimenti ma non di allentamenti. L'Incaricato ha inoltre constatato che i principi erano fortemente improntati sulla sicurezza delle informazioni e pertanto non tenevano in debito conto la protezione dei dati. Essi, ad esempio,

si basavano in particolare sulla distinzione tra dati personali degni di particolare protezione e altre tipologie di dati personali, distinzione che secondo l'IFPDT rappresenta un criterio limitatamente idoneo a valutare i rischi per la personalità e i diritti fondamentali delle persone interessate, tanto più che anche la combinazione di dati personali che non sono degni di particolare protezione può comportare rischi di trattamento elevati. Possono emergere rischi elevati in particolare durante l'utilizzo di nuove tecnologie o in relazione alla modalità, all'entità, alle circostanze e alla finalità del trattamento.



Questi fattori sono spesso presenti nel caso delle esternalizzazioni di cloud. L'IFPDT si è quindi adoperato affinché per i principi del cloud sia prevista una valutazione d'impatto sulla protezione dei dati, qualora vengano trattati dati personali nel cloud.

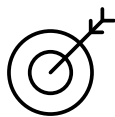
Il settore TDT ha coinvolto l'IFPDT nei suoi lavori preliminari concernenti l'introduzione di Microsoft 365, in particolare sottoponendogli le bozze di un'analisi delle basi legali e del piano SIPD. Nei suoi pareri al riguardo l'Incaricato ha osservato che dal suo punto di vista non è dato sapere fino a quando sarà tecnicamente praticabile la soluzione tuttora prevista nel progetto del settore TDT di far funzionare determinate applicazioni nei propri centri federali anziché nel cloud del gruppo statunitense Microsoft. Alla luce di tale

incertezza, l'Incaricato ha chiesto di presentare alternative migliori sotto il profilo della protezione dei dati rispetto a Microsoft 365. In merito all'analisi delle basi legali ha chiesto di verificare in modo più approfondito se esiste una base legale sufficiente per il trattamento di dati personali nel cloud gestito dal gruppo statunitense e se il rispetto del principio di proporzionalità resta garantito. Per quanto riguarda l'esclusione dei dati personali degni di particolare protezione da parte degli utenti, l'Incaricato ritiene che vi siano ancora questioni aperte circa la finalità e la fattibilità pratica. L'IFPDT ha chiesto infine al TDT di allestire una valutazione completa d'impatto sulla protezione dei dati che evidenzi in modo chiaro i rischi della migrazione nel cloud. A tal proposito l'IFPDT ha ritenuto indispensabile fare analizzare in modo approfondito la problematica del possibile accesso da parte delle autorità di sicurezza statunitensi ai dati personali trattati dall'Amministrazione federale nel cloud di Microsoft.

Progetto «SpiGes» dell'UST

Nell'anno in rassegna l'UST ha sottoposto all'IFPDT un rapporto sullo stato di avanzamento del progetto inerente all'utilizzo multiplo dei dati relativi alle degenze ospedaliere in regime stazionario (SpiGes). L'IFPDT ha richiamato l'attenzione sui rischi dal punto di vista della protezione dei dati legati a questo sottoprogetto del programma «Gestione dei dati a livello nazionale» (NaDB) e ha chiesto l'elaborazione di misure di sicurezza adeguate in caso di attuazione concreta.

Il programma «Gestione dei dati a livello nazionale» (NaDB), avviato a ottobre 2019 sotto la guida dell'UST, mira a consentire l'utilizzo multiplo dei dati e ad agevolare lo scambio dei dati tra le autorità. Uno dei progetti pilota condotti nell'ambito del programma NaDB riguarda l'utilizzo multiplo dei dati nel settore ospedaliero stazionario (progetto SpiGes). I dati relativi alle degenze ospedaliere stazionarie saranno rac-



colti una sola volta utilizzando la piattaforma di interoperabilità dell'UST secondo il principio «once-only» e in seguito potranno essere utilizzati per scopi sia amministrativi sia statistici (cfr. anche 29° rapporto, n. 1.1).

Un rischio specifico che può emergere nel contesto dell'utilizzo multiplo dei dati e che è stato segnalato in modo esplicito dall'IFPDT riguarda la violazione del principio della finalità. Per prevenire tale rischio occorre distinguere chiaramente il trattamento dei

dati per fini statistici da quello finalizzato ad altri scopi (ad es. amministrativi). Va inoltre prestata un'attenzione particolare ai soggetti con doppie funzioni (ad es. ospedali e compagnie d'assicurazione che possono essere sia fornitori di dati sia fruitori di dati). Si rivela quindi indispensabile separare chiaramente a livello organizzativo e informatico le categorie di dati trattate definendo differenti limitazioni d'accesso per ciascuna categoria.

In quest'ottica e in considerazione dell'entità del progetto e del rischio elevato legato al trattamento su vasta scala di dati personali degni di particolare protezione, l'IFPDT ha fatto presente all'UST la necessità di effettuare analisi dei rischi per valutare i rischi specifici relativi alla protezione dei dati ed elaborare misure da adottare per farvi fronte, come previsto nello specifico anche dalla nuova legge sulla protezione dei dati in vigore da settembre 2023 (art. 22 nLPD, Valutazione d'impatto sulla protezione dei dati).

Nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD)

Nell'anno in rassegna l'IFPDT ha fornito consulenza all'Ufficio federale di giustizia durante i lavori legislativi concernenti la nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD).

Per il riconoscimento di procedure di certificazione e l'introduzione di un marchio di qualità inerente alla protezione dei dati, il Consiglio federale ha emanato la nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD) del 31 agosto 2022, che entrerà in vigore il 1° settembre 2023 contestualmente alla nuova LPD.

L'IFPDT ha fornito supporto all'Ufficio federale di giustizia nell'elaborazione dell'OCPD dal punto di vista giuridico e informatico-tecnico, in collaborazione con il Servizio di accreditamento svizzero SAS. Attualmente l'Incaricato sta inoltre elaborando direttive specifiche sui requisiti minimi che un sistema di gestione deve adempiere nonché direttive sui criteri in materia di protezione dei dati in base ai quali deve avvenire il controllo di prodotti, servizi e processi.

Per il trattamento dei dati nel contesto di sistemi, prodotti o servizi certificati, il titolare del trattamento non è tenuto a procedere a una valutazione d'impatto sulla protezione dei dati, nemmeno in caso di rischio elevato per la personalità. Una certificazione offre inoltre ai produttori e ai titolari del trattamento la possibilità di comprovare che operano in conformità alla



legge sulla protezione dei dati. Dall'ottica dell'IFPDT, lo strumento delle certificazioni può rafforzare la protezione dei dati in Svizzera. La certificazione promuove in particolare la trasparenza, dal momento che l'analisi delle operazioni di trattamento dei dati, che diventano sempre più complesse, avviene ad opera di un organo indipendente.



La certificazione di sistemi di gestione va ben oltre le possibilità offerte da una certificazione in materia dei dati europea, che riguarda unicamente prodotti, servizi e processi. Le certificazioni estere conformi ai requisiti della legislazione svizzera vengono riconosciute previa consultazione del Servizio di accreditamento svizzero SAS. L'IFPDT riconosce anche gli organismi di certificazione esteri, sempre dopo aver consultato il SAS, purché garantiscano l'adempimento dei requisiti previsti in Svizzera.

ELEZIONI E VOTAZIONI

Aggiornamento delle linee guida

In accordo con la Conferenza degli incaricati svizzeri della protezione dei dati (privatim) e la Cancelleria federale, l'IFPDT ha aggiornato le linee guida per le elezioni e le votazioni, in particolare in vista delle elezioni federali per il rinnovo del Parlamento previste in autunno 2023. Le linee guida sono state pubblicate nel dicembre 2022 sul sito Internet dell'IFPDT. La versione aggiornata pone l'accento in particolare sull'enorme importanza del principio di trasparenza per la protezione dei dati nel contesto delle elezioni e delle votazioni.

Le linee guida sono state redatte per la prima volta nell'anno di attività 2018/2019 in collaborazione con la Conferenza degli incaricati svizzeri della protezione dei dati (privatim), in stretto accordo con la Cancelleria federale e un gruppo di lavoro (cfr. 26° rapporto, n. 1.1) e da allora vengono aggiornate regolarmente (cfr. 27° rapporto, n. 1.1). Nel presente periodo in esame le linee guida sono state rese nello specifico più comprensibili e sono state integrate le domande di controllo formulate nell'anno in rassegna 2019/2020 concernenti l'osservanza dei principi sanciti dalla legislazione in materia di protezione dei dati per i siti Internet.

IDENTITÀ ELETTRONICA, ID-E

Principio della «self-sovereign identity»

L'IFPDT ha espresso le sue considerazioni nell'ambito della consultazione degli uffici relativa al progetto della nuova legge sull'Id-e. Il disegno di legge è atteso per l'estate 2023.

Respingendo il primo disegno di legge sui servizi di identificazione elettronica nel 2021 la popolazione svizzera ha chiesto una nuova soluzione per un'identità elettronica riconosciuta dallo Stato (cfr. 29° rapporto, n. 1.1). Nell'anno in rassegna il Dipartimento federale di giustizia e polizia (DFGP) ha sottoposto alla consultazione degli uffici l'avamprogetto della nuova legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull'Id-e). Il progetto si basa sul concetto della self-sovereign identity, in virtù del quale gli utenti avrebbero il massimo controllo sui propri dati.

Possono richiedere allo Stato una prova elettronica dell'identità (Id-e) tutte le persone titolari di un documento d'identità rilasciato dalle autorità svizzere. La Confederazione allestisce e gestisce a tale scopo un'infrastruttura di fiducia statale che permette, da un lato, di verificare l'autenticità dell'Id-e e, dall'altro, consente ad altri soggetti, pubblici e privati, di emettere e controllare ulteriori mezzi di autenticazione elettronici. Il progetto di legge disciplina in una prima parte l'Id-e statale e in una seconda l'infrastruttura di fiducia e gli altri mezzi di autenticazione elettronici, ma non definisce i dettagli relativi alla procedura di emissione di un'Id-e.

L'IFPDT si è espresso in merito al progetto, avanzando con successo diverse richieste. Ad esempio, l'Incariato ha contribuito all'elaborazione di disposizioni che pongono limiti al trattamento di metadati che emergono in fase di utilizzo e alla raccolta di dati

tramite interfacce necessarie all'emissione dell'Id-e. Il progetto prevede inoltre, come richiesto dall'IFPDT, che servizi di contatto cantonali forniscano assistenza agli utenti durante l'utilizzo della nuova Id-e. Per l'IFPDT è inoltre importante che nel messaggio concernente il progetto si precisi che l'Id-e non deve essere per i cittadini un mezzo di identificazione generale da utilizzare in Internet. L'IFPDT ha infine chiesto di prevedere obblighi di revoca per i soggetti che utilizzano l'infrastruttura di fiducia per emettere ulteriori mezzi di autenticazione elettronica.

L'IFPDT ritiene problematico l'opzione, continuamente proposta, di un registro pubblico che preveda il versamento di un emolumento: secondo tale impostazione gli emittenti di un'Id-e dovrebbero inserire autonomamente i loro dati nel registro senza che la loro identità sia stata precedentemente verificata. L'IFPDT ha richiamato l'attenzione sul rischio, a ciò correlato, che emittenti con un'identità fittizia potrebbero abusare dell'infrastruttura di fiducia. Secondo l'IFPDT, la Confederazione dovrebbe adottare provvedimenti per impedire un utilizzo abusivo dell'infrastruttura da essa gestita. Pertanto abbiamo chiesto che questi rischi vengano indicati nel messaggio da presentare al Consiglio federale. Abbiamo inoltre fatto presente che, in assenza di

un controllo preliminare dell'identità, sarebbe importante la presenza di un sistema di conferma degli identificativi inseriti nel registro di base. Esisterebbe infatti la possibilità di associare gli identificativi già iscritti nel registro di base a un'organizzazione, un ente o un cittadino privato esistente nel mondo reale.



Il DFGP ha annunciato, dopo l'esito della consultazione, di voler chiarire in modo ancora più approfondito vari punti come la cerchia degli aventi diritto a un'Id-e, la procedura di emissione, aspetti concernenti la protezione dei dati, la convivialità (tra cui l'accessibilità) e i servizi cantonali di supporto agli utenti. L'IFPDT continuerà a seguire gli sviluppi del progetto e a esprimere le proprie considerazioni legate alla protezione dei dati. Il disegno di legge sarà presentato al Consiglio federale nell'estate 2023.

Accesso possibile solo con SwissID

Nell'anno in rassegna la Posta ha effettuato una migrazione del Login clienti Posta sul proprio sito Internet, cosicché da dicembre 2022 è possibile accedere ai servizi online dell'azienda solo con SwissID. L'IFPDT ne è stato informato in via preliminare e ha richiamato l'attenzione sui requisiti previsti dalla legislazione in materia di protezione dei dati. Quando la Posta ha invitato gli utenti dei servizi online a creare uno SwissID, abbiamo ricevuto numerose domande da parte dei cittadini riguardo alla procedura della Posta.

L'esternalizzazione del login e del relativo trattamento dei dati all'azienda privata SwissSign non deve andare a scapito della sfera privata dei clienti della Posta né compromettere la loro autodeterminazione informativa.

L'IFPDT ha comunicato quindi alla Posta che la trasmissione della funzione di login a SwissSign è soggetta alle prescrizioni relative al trattamento dei dati da parte di terzi (art. 10a LPD). Pertanto la Posta, in veste di mandante, rimane responsabile nei

confronti dei propri clienti del trattamento dei dati ad opera di SwissSign per quanto riguarda il login al sito



Internet della Posta stessa. Quest'ultima si è dovuta assicurare mediante convenzione che l'azienda SwissSign garantisca la sicurezza dei dati e tratti i dati raccolti presso i clienti della Posta esclusivamente per le finalità del login.

Dopo che la Posta ha assicurato di riconoscere e osservare, durante la migrazione del login, i requisiti relativi al trattamento dei dati da parte di terzi previsti dalla LPD, l'IFPDT ha rinunciato ad avviare una procedura di sorveglianza.

Progetto licenza di condurre digitale

L'Ufficio federale delle strade (USTRA), l'Associazione dei servizi della circolazione (asa) e l'Ufficio federale di giustizia (UFG) hanno presentato il progetto licenza di condurre digitale. Questo progetto dell'USTRA è parte integrante dell'attuazione della strategia «Svizzera digitale».

L'USTRA prevede di introdurre a tappe, e fondandosi sulle norme in materia di circolazione stradale, una licenza per allievo conducente, una licenza di condurre e una licenza di circolazione in forma digitale. Questi nuovi documenti dovranno essere riconosciuti a livello internazionale e poter essere verificabili dagli organi di controllo della polizia. Il rilascio delle licenze digitali è di competenza dei Cantoni, i quali devono attenersi ai requisiti posti dall'USTRA in relazione alla forma, al contenuto e alla veste grafica.

Già oggi i dati delle licenze sono registrati nel sistema d'informazione sull'ammissione alla circolazione (SIAC), che l'USTRA gestisce in collaborazione con i Cantoni e di cui i Cantoni si avvalgono per svolgere i compiti conferiti loro dalla legge.

Sulla base delle informazioni ricevute, l'IFPDT ritiene possibile un'attuazione del progetto conforme alle esigenze in materia di protezione dei dati.

30 anni di protezione dei dati in Svizzera

La legge federale del 1992

Il 1° luglio 1993 entrò in vigore la prima legge federale sulla protezione dei dati, adottata dall'Assemblea federale il 19 giugno 1992.

Già nel suo messaggio del 23 marzo 1988 il Consiglio federale aveva motivato la necessità di intervenire a livello legislativo adducendo «l'impiego dell'informatica e delle moderne tecnologie delle telecomunicazioni in quasi tutti i settori della vita e l'enorme intensificazione del trattamento e della diffusione dei dati personali in seno alla società, all'economia e allo Stato». A distanza di 30 anni la nostra vita quotidiana si svolge in una realtà digitale che all'epoca il legislatore non avrebbe potuto prevedere. Ciononostante, i principi in merito al trattamento dei dati personali codificati dal legislatore di allora si sono dimostrati lungimiranti. Anche la nuova legge del 25 settembre 2020 sulla protezione dei dati, che entrerà in vigore il 1° settembre 2023, si basa su questi principi: trasparenza, proporzionalità e conformità allo scopo rimangono i pilastri centrali su cui si basa il trattamento dei dati personali secondo il nuovo diritto.

Sebbene la nostra vita quotidiana nel frattempo sia stata fortemente trasformata da Internet e dagli smartphone, molte tematiche nel settore della protezione dei dati non

hanno perso nulla della loro attualità: già nel primo rapporto d'attività ci occupavamo del trattamento dei dati da parte della polizia nel contesto della «lotta al crimine organizzato» o della «sorveglianza delle frontiere tramite videocamere». E anche la «sorveglianza telefonica/osservazione a fini di perseguimento penale» era già allora un tema d'interesse. Eppure all'epoca il telefono, la videocamera, la televisione, la biblioteca e il computer non si portavano in tasca.

La costante connessione a Internet che permette alla moderna società digitale di compiere innumerevoli faccende quotidiane, dalle operazioni bancarie agli incontri online, ha aumentato esponenzialmente la portata e l'intensità con la quale vengono trattate le informazioni personali. Tuttavia la missione dell'autorità indipendente della Confederazione preposta alla vigilanza della protezione dei dati rimane la stessa: porre i diritti fondamentali e la personalità delle persone al di sopra dell'applicazione indiscriminata delle possibilità offerte dalla tecnologia. Una sfida che l'attuale Incaricato accetta, seguendo l'esempio dei suoi predecessori Odilo Guntern e Hanspeter Thür che hanno contraddistinto i primi 23 anni dell'autorità di vigilanza sulla protezione dei dati della Confederazione, e che considera una «mission possible» nonostante la dinamica dei progressi tecnologici.

Vecchia o nuova legge: quale si applica?

Alcuni procedimenti non si sono potuti concludere nell'anno di riferimento. È importante sapere che, in base alla disposizione transitoria di cui all'art. 70 nDSG, questi saranno valutati in base alla legge attualmente in vigore, anche se non saranno conclusi fino all'entrata in vigore della nuova legge sulla protezione dei dati il 1° settembre 2023. Ciò vale in particolare per l'accertamento dei fatti che l'IFPDT ha avviato nella primavera del 2021 in merito al trattamento dei dati di un negozio online svizzero e per quello relativo al trattamento dei dati della piattaforma d'asta Ricardo AG e TX Group AG, entrambi ancora in corso (cfr. 29° TB, n. 1.3).

La nuova legge sulla protezione dei dati

Con la revisione totale della legge federale sulla protezione dei dati nel 2020 il legislatore ha messo a disposizione dei responsabili e della vigilanza della protezione dei dati nuovi strumenti che rispondono alle legittime attese della popolazione a una protezione solida e legalitaria della personalità. L'IFPDT intensificherà quindi la sua attività di vigilanza.

Ruolo dell'IFPDT

La nuova legge sulla protezione dei dati entra in vigore il 1° settembre 2023. Le novità non riguarderanno solo i titolari del trattamento e le persone interessate, bensì anche i compiti e le competenze dell'IFPDT, che intensificherà quindi le attività di vigilanza e aumenterà il numero di indagini.

Novità dal punto di vista istituzionale

In futuro il capo dell'IFPDT, ovvero l'Incaricato, sarà eletto dal Parlamento. Finora l'elezione avveniva ad opera del Consiglio federale e l'Assemblea federale si limitava a confermarla. La nuova disposizione rafforza l'indipendenza dell'ufficio dall'Esecutivo e la relativa legittimazione democratica. L'Incaricato assume il proprio personale e dispone di un proprio preventivo: il Consiglio federale inoltra il progetto di preventivo all'Assemblea federale senza modifiche.

Come in passato, sul piano amministrativo l'IFPDT rimane un'autorità aggregata alla Cancelleria federale e la comunicazione tra il Consiglio federale e l'IFPDT avviene per il tramite del cancelliere della Confederazione. In virtù di un accordo di prestazioni, la Cancelleria federale fornisce

per conto dell'IFPDT una serie di prestazioni nell'ambito dell'amministrazione del personale, delle finanze e della burocratica.

Ora il Consiglio federale constaterà se la legislazione di uno Stato terzo garantisce una protezione adeguata dei dati e se i dati potranno essere quindi comunicati dalla Svizzera all'estero senza ulteriori misure. L'elenco figura come allegato nell'ordinanza sulla protezione dei dati.

Nuovi compiti dell'IFPDT

Se il trattamento previsto dei dati personali può comportare un rischio elevato per la personalità o i diritti fondamentali, il titolare del trattamento, privato o presso un'autorità, deve effettuare una valutazione d'impatto sulla protezione dei dati (VIPD). Se da quest'ultima emerge che, nonostante provvedimenti appropriati, il trattamento previsto comporta ancora un rischio elevato per la personalità o i diritti fondamentali delle persone interessate, il titolare del trattamento deve rivolgersi all'IFPDT prima di procedere al trattamento dei dati. L'IFPDT verifica la valutazione d'impatto sulla protezione dei dati e comunica al titolare del trattamento entro due mesi eventuali obiezioni. Il parere dell'IFPDT non rappresenta alcuna «autorizzazione» al trattamento dei dati previsto. Non è impugnabile, ma è soggetto a pagamento.

La legge riveduta attribuisce nuovi compiti all'IFPDT. Le associazioni professionali, di settore ed economiche possono elaborare propri codici di condotta e sottoporli all'IFPDT affinché si esprima al riguardo. I pareri vengono pubblicati dall'IFPDT, il quale pubblica inoltre un elenco delle clausole tipo di protezione dei dati da esso approvate, stabilite o riconosciute. L'IFPDT può ora riscuotere emolumenti per i pareri espressi in merito a un codice di condotta nonché per l'approvazione di clausole tipo di protezione dei dati e di norme interne d'impresa vincolanti sulla protezione dei dati.

«L'IFPDT intensificherà le sue attività di vigilanza e aumenterà progressivamente il numero di indagini.»

Il titolare del trattamento deve ora notificare all'IFPDT ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. L'IFPDT mette a disposizione un apposito portale di notifica sul proprio sito Internet.

Inchieste

L'IFPDT, in qualità di organo di vigilanza, deve garantire che organi federali e privati rispettino le disposizioni federali in materia di protezione dei dati, in particolare la LPD. Se sussistono indizi sufficienti per supporre che un trattamento dei dati possa violare le disposizioni sulla protezione dei dati, l'IFPDT apre un'inchiesta, salvo nel caso in cui la violazione sia di lieve entità. Nell'ambito dell'inchiesta l'IFPDT definisce le modalità con cui un organo federale oppure un privato o un'azienda privata trattano i dati personali che si riferiscono a una persona fisica. Successivamente, sulla base dei fatti constatati, valuta se sussiste realmente una violazione delle disposizioni federali in materia di protezione dei dati.

Con l'entrata in vigore della legge sulla protezione dei dati riveduta la Svizzera sarà chiamata alla ratifica della Convenzione 108+ del Consiglio d'Europa, uno strumento multilaterale vincolante in materia di protezione dei dati che risale al 1981 e che ora è stato modernizzato e adeguato alle sfide dell'era digitale. Per soddisfare i requisiti della Convenzione 108+, il legislatore ha esteso le competenze dell'IFPDT in materia di indagine. Mentre finora, in caso di trattamento dei dati da parte di privati, l'Incaricato poteva avviare un accertamento dei fatti solo se le modalità di trattamento erano tali da violare la personalità di un numero elevato di persone (errore di sistema), con il nuovo diritto tale soglia non esiste più.

L'Incaricato intensificherà quindi le sue attività di vigilanza a partire dall'entrata in vigore della nuova legge e aumenterà gradualmente il numero di indagini formali. L'autorità è stata dotata di risorse di personale aggiuntive per l'esecuzione della nuova legge. L'IFPDT ha potuto completare con successo le assunzioni corrispondenti nella primavera del 2023.

Inchieste preliminari informali

Durante l'attività di vigilanza in corso possono emergere elementi che fanno presupporre possibili violazioni della protezione dei dati oppure possono giungere all'IFPDT segnalazioni al riguardo da parte di persone interessate o terzi, come società di media o organizzazioni di tutela dei consumatori. In presenza di prime avvisaglie o segnalazioni di una violazione delle disposizioni in materia di protezione dei dati, l'IFPDT verifica, inizialmente nel contesto di accertamenti iniziali, la propria competenza, se sussistono indizi sufficienti per una violazione e se quest'ultima è di grande o lieve entità.

L'IFPDT ha inoltre la possibilità di invitare il titolare del trattamento a rispondere su base volontaria, inizialmente in modo informale, ad alcune domande, ad es. qualora le sue competenze non siano chiare o ritiene probabile che in seguito al colloquio con il titolare del trattamento possa essere superfluo avviare un'inchiesta. Quest'ultima possibilità si verifica in particolare quando il titolare del trattamento riesce a confutare rapidamente i primi indizi di violazione oppure adotta spontaneamente e in tempo utile provvedimenti per garantire il rispetto delle disposizioni in materia di protezione dei dati.

Procedura d'inchiesta formale

In base al diritto vigente, l'IFPDT accerta i fatti e verifica se sussista una violazione delle disposizioni in materia di protezione dei dati nell'ambito di un accertamento dei fatti, il quale si conclude eventualmente con una raccomandazione giuridicamente non applicabile di modificare o sospendere un determinato trattamento dei dati. Ai sensi del nuovo diritto la procedura d'inchiesta si basa sulla legge federale sulla

procedura amministrativa (PA). Se nel corso della procedura l'IFPDT constata una violazione delle disposizioni in materia di protezione dei dati, esso ha la competenza di emanare una decisione applicabile dal punto di vista del diritto in conformità con l'articolo 5 PA, che il titolare del trattamento può impugnare dinanzi al Tribunale amministrativo federale se non intende accettarla. L'IFPDT può ordinare di adeguare, sospendere o cessare un trattamento dei dati o di cancellare i dati personali.

Assistenza amministrativa

La legge riveduta prevede due disposizioni specifiche riguardanti la collaborazione tra l'IFPDT e le autorità svizzere ed estere. Le autorità svizzere sono tenute a fornire assistenza amministrativa all'IFPDT, mentre l'obbligo dell'Incaricato in tal senso si limita alle autorità svizzere incaricate della protezione dei dati, alle autorità di perseguimento penale in relazione alle relative denunce nonché alle autorità federali e agli organi di polizia coinvolti per l'esecuzione dei suoi provvedimenti.

L'assistenza amministrativa dell'IFPDT nei confronti delle autorità estere si estende a quelle incaricate della protezione dei dati. Sono oggetto di scambio le informazioni e i dati personali necessari all'autorità per l'adempimento dei propri compiti legali. Deve essere soddisfatta tutta una serie di requisiti, come ad esempio la reciprocità, la salvaguardia del segreto e l'utilizzo delle informazioni solo per la procedura in questione.

Regolamentazione degli emolumenti

In base al nuovo diritto, l'IFPDT riscuoterà dai titolari del trattamento privati emolumenti per una serie di compiti. Oltre che per le attività a pagamento menzionate in precedenza (parere in merito a un codice di condotta e a valutazioni d'impatto sulla protezione dei dati, approvazione di clausole tipo di protezione dei dati e di norme interne d'impresa vincolanti), l'IFPDT riscuoterà emolumenti anche nell'ambito delle procedure d'inchiesta. In futuro saranno

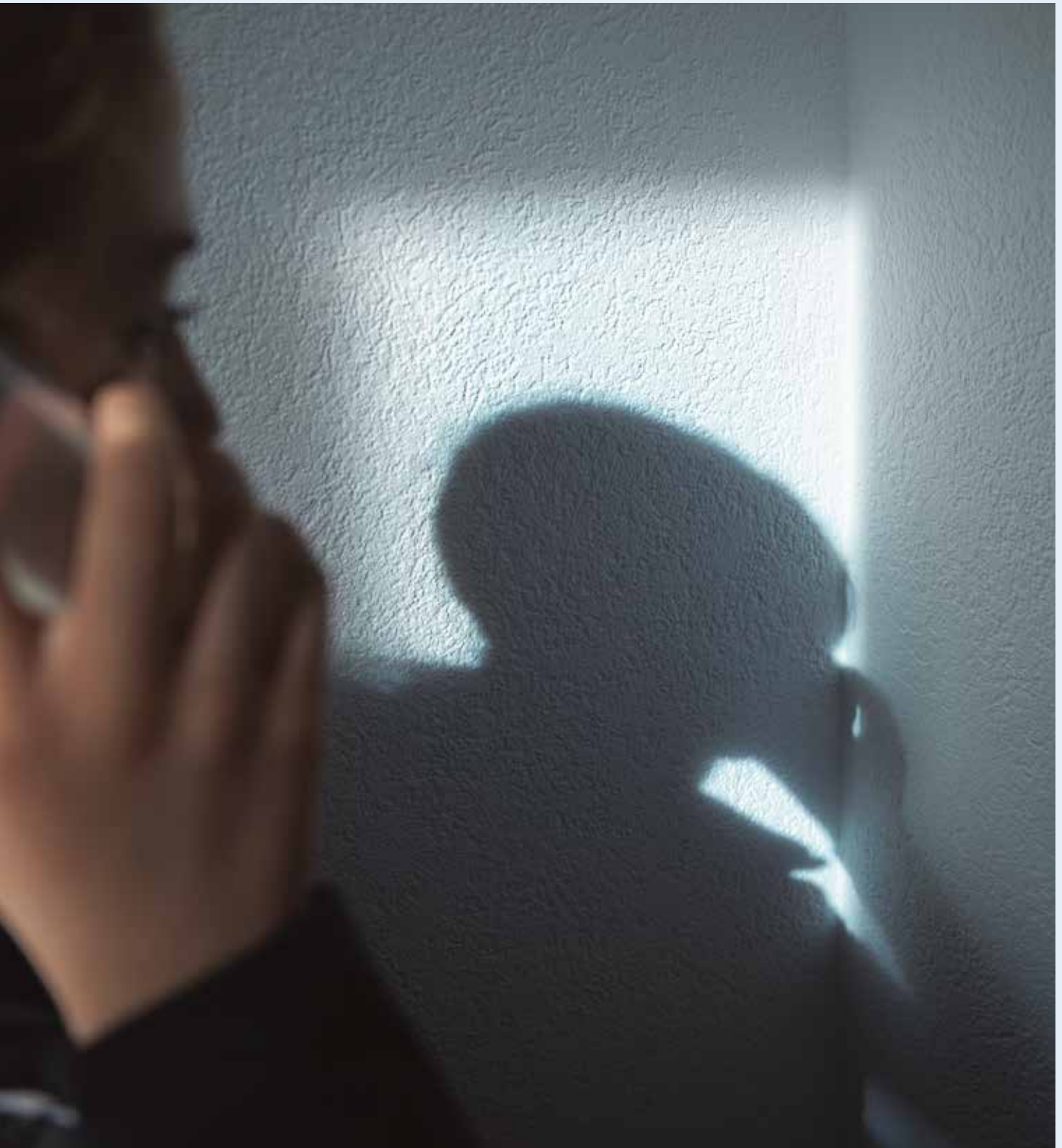
soggette a pagamento anche le consulenze su questioni inerenti alla protezione dei dati fornite a privati. L'importo degli emolumenti varia in base al tempo richiesto. A seconda della funzione del personale competente, si applica una tariffa oraria compresa tra 150 e 250 franchi. Se una prestazione richiede un onere straordinario o si rivela particolarmente complessa o urgente, possono essere applicati supplementi. Viene riscosso un supplemento anche quando una prestazione viene riutilizzata per finalità commerciali. L'IFPDT può rinunciare alla riscossione di emolumenti in caso di prestazioni di interesse pubblico o che richiedono poco tempo.

Diritto penale

Come in precedenza, anche in base al nuovo diritto l'IFPDT non ha alcuna competenza sanzionatoria, a differenza delle autorità di vigilanza dell'Unione europea. Nella LPD sono state invece ampliate le disposizioni in materia di diritto penale accessorio. Sono punibili il mancato rispetto intenzionale degli obblighi di informare, di concedere l'accesso e di notifica nonché la violazione intenzionale degli obblighi di diligenza, in particolare per quanto riguarda la comunicazione di dati personali all'estero, il trattamento da parte di un responsabile e la sicurezza dei dati. Vengono punite con una multa pari a un massimo di 250 000 franchi le persone fisiche che si rendono responsabili della violazione. L'importo massimo della multa per le persone giuridiche, previsto unicamente in via sussidiaria, è pari a 50 000 franchi.

In occasione delle deliberazioni parlamentari sulla nuova LPD, il Consiglio federale ha preso in considerazione di valutare l'introduzione di sanzioni di diritto penale amministrativo contro le aziende inadempienti in vista dell'emanazione di una nuova legge federale.

«L'IFPDT può ora decidere la cessazione di un trattamento di dati o la cancellazione di dati personali.»



Consultazione dell'UFG in relazione alle direttive interne all'Amministrazione concernenti la valutazione d'impatto sulla protezione dei dati

In seguito alla revisione totale della legge sulla protezione dei dati (nLPD), i servizi responsabili dell'Amministrazione federale devono eseguire una cosiddetta valutazione d'impatto sulla protezione dei dati (VIPD) nei casi in cui il trattamento dei dati possa comportare un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. L'IFPDT presta consulenza all'Ufficio federale di giustizia (UFG) in merito alle direttive e agli strumenti a supporto degli organi federali.

Durante la pianificazione di progetti nell'ambito della trasformazione digitale dell'Amministrazione federale, i servizi responsabili devono valutare i potenziali rischi per la personalità o i diritti fondamentali delle persone interessate. Se da questa prima analisi risulta che il previsto trattamento di dati personali presenta rischi elevati, gli organi federali responsabili devono elaborare una valutazione d'impatto sulla protezione dei dati in cui illustrano i rischi e i provvedimenti per ridurli.

L'IFPDT ha assistito l'UFG nella formulazione di direttive e strumenti volti ad agevolare i lavori dei servizi federali responsabili in questo ambito. Si è detto contrario che, sia per quanto concerne l'esame preliminare volto ad accertare la necessità di effettuare una VIPD che l'esecuzione vera e propria della VIPD, ci si avvalga unicamente di liste di controllo predefinite e strumenti ausiliari (supportati dall'informatica). Ciò che una VIPD richiede è invece una valutazione ponderata dei rischi globali tenendo conto di tutte le circostanze nel caso concreto. Sulla base delle esperienze pratiche con le valutazioni dei rischi condotte dall'Amministrazione federale conformemente alla vigente legge sulla protezione dei dati in ambito Schengen, l'IFPDT si è impegnato affinché, nei casi di trattamento di dati già in corso, i servizi dall'Amministrazione responsabili debbano indicare nella VIPD le divergenze sostanziali rispetto a quanto previsto dalle direttive. Questo raffronto deve comprendere sia gli aspetti sistemici (portata, intensità e durata del trattamento e cerchie autorizzate all'accesso) sia gli aspetti tecnici in materia di sicurezza in relazione al trattamento dei dati.

Tre nuovi portali online

Prima che entri in vigore la nuova legge sulla protezione dei dati l'IFPDT introdurrà nuovi portali di notifica. A quello riservato agli organi federali per la notifica dei registri delle attività di trattamento faranno seguito altri due portali: uno per la notifica dei consulenti per la protezione dei dati e un altro per la notifica delle violazioni della sicurezza dei dati.

L'IFPDT ha avviato nel 2021 un progetto relativo all'implementazione di tre portali di notifica.

Con l'introduzione del nuovo registro delle attività di trattamento degli organi federali previsto dall'articolo 12 nLPD (DataReg), che sostituisce l'attuale soluzione per la notifica delle collezioni di dati da parte di privati e autorità (WebDataReg), a novembre 2022 siamo riusciti già a implementare il primo portale di notifica. Il portale DataReg, interamente riprogettato, è concepito per la notifica e la pubblicazione delle iscrizioni nel registro da parte degli organi federali e ageverà questi ultimi nella gestione dei registri. L'attuale WebDataReg, dove vengono pubblicate anche le notifiche delle collezioni di dati delle aziende private, cesserà di funzionare il 1° settembre 2023. Secondo il nuovo diritto, i privati non saranno più soggetti all'obbligo di notifica.

Il portale di notifica dei consulenti per la protezione dei dati serve alla trasmissione dei dati di contatto dei consulenti nominati.

Il portale per la notifica di violazioni della sicurezza dei dati di cui all'articolo 24 nLPD (DataBreach) rappresenta un canale digitale sicuro attraverso il quale i titolari del trattamento possono notificare ogni violazione della sicurezza dei dati che comporta un rischio elevato per le persone interessate. Il modulo online agevola i titolari del trattamento nella registrazione strutturata e completa dei dati richiesti, garantisce un'elaborazione efficiente delle notifiche da parte dell'IFPDT e semplifica le analisi statistiche.

1.2 Giustizia, polizia, sicurezza

UDSC

Legge sulle dogane

Il progetto di revisione totale della legge sulle dogane è attualmente al vaglio delle Commissioni dell'economia e dei tributi del Parlamento. A tal riguardo, l'Incaricato è stato ascoltato dalla Commissione del Consiglio nazionale. In particolare, ha ribadito il carattere sensibile del progetto e l'accesso sproporzionato del Servizio delle attività informative della Confederazione al sistema informativo dell'Ufficio federale della dogana e della sicurezza dei confini (UDSC).

Il 24 agosto 2022 il Consiglio federale ha trasmesso al Parlamento il progetto di legge federale sulla parte generale della riscossione dei tributi e sul controllo del traffico transfrontaliero di merci e persone da parte dell'Ufficio federale della dogana e della sicurezza dei confini (Legge sui compiti d'esecuzione dell'UDSC). La Commissione dell'economia e dei tributi del Consiglio nazionale è incaricata di esaminare il progetto di legge e ha chiesto il parere dell'Incaricato il 24 ottobre 2022.

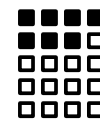
Il raggruppamento delle funzioni doganali e di polizia in seno all'UDSC ha costituito una sfida per la sorveglianza in materia di protezione dei

dati della Confederazione. La creazione del nuovo ufficio di polizia doganale ha comportato infatti un aumento del numero di persone incaricate del trattamento dei dati personali di pertinenza sia del diritto delle dogane sia di quello di polizia. L'uniformazione dell'amministrazione delle dogane ha permesso di designare una terza grande autorità di sicurezza a livello federale, in aggiunta all'Ufficio federale di polizia (fedpol) e al Servizio delle attività informative della Confederazione (SIC).

Come si legge nel capitolo 1.2 del nostro 28° rapporto d'attività 2020/21, dapprima il Dipartimento federale delle finanze ha posto in consultazione un progetto di legge inaccettabile dal punto di vista della sorveglianza in materia di protezione dei dati della Confederazione. Tale progetto di legge non specificava infatti le modalità del

trattamento dei dati personali da parte dell'ufficio di polizia doganale, lasciando alla discrezione della direzione dell'UDSC.

Nell'ambito di una lunga e intensa attività di consulenza abbiamo portato, d'intesa con l'Ufficio federale di giustizia,



l'UDSC a redigere una tabella comparativa tra il sistema attuale di trattamento dei dati personali da parte dell'AFD e quello

futuro da parte dell'UDSC. Questa tabella comparativa è stata inclusa nell'analisi dell'impatto in materia di protezione dei dati. Su questa base, l'UDSC ha modificato e chiarito nel dettaglio il capitolo dedicato al trattamento dei dati (cfr. 29° rapporto, n. 1.2). Nel frattempo, questi miglioramenti hanno permesso di eliminare le riserve di principio espresse dall'IFPDT durante la terza consultazione degli uffici e di rendere quindi accettabile il progetto trasmesso al Parlamento in termini di protezione dei dati.

Nonostante i miglioramenti apportati, il progetto LE-UDSC va tuttavia considerato scrupolosamente sotto il

STATUTO DI PROTEZIONE S

profilo del diritto in materia di protezione dei dati. Durante la terza e ultima procedura di consultazione degli uffici, è rimasta controversa la nuova possibilità prevista per il SIC di accedere al sistema informativo dell'UDSC. L'attuale legge sulle dogane non prevede tale possibilità di accesso, in quanto la collaborazione sporadica tra le dogane e il SIC può avvenire nell'ambito dell'assistenza amministrativa, in modo puntuale. L'insistenza su un accesso del genere denota la volontà delle tre principali autorità di sicurezza della Confederazione d'intensificare il trattamento dei dati personali concedendosi reciprocamente ampio accesso ai rispettivi sistemi informativi. Il Consiglio federale ha mantenuto l'accesso del SIC nella legge, pur consapevole del fatto che l'IFPDT lo reputi inutile e pertanto sproporzionato.

Applicazione «RegisterMe»

La Segreteria di Stato della migrazione (SEM) ha attivato un'applicazione con la quale i profughi possono presentare domanda per lo statuto di protezione S. L'Incaricato ha espresso alcune perplessità circa la sicurezza legata al salvataggio dei dati personali dei soggetti appartenenti a questa categoria vulnerabile e accoglie con favore la misura adottata in seguito dalla SEM.

Decine di migliaia di persone che prima della guerra in Ucraina sono dovute fuggire dal proprio Paese rifugiandosi in Svizzera hanno chiesto protezione temporanea (statuto S) alla Segreteria di Stato della migrazione (SEM). Per prenotare un appuntamento presso un centro federale d'asilo si utilizza l'applicazione «RegisterMe», attivata appositamente per gestire in tempi brevi l'elevato numero di domande e i relativi appuntamenti.

Già a pochi giorni di distanza dall'introduzione di RegisterMe, l'Incaricato ha identificato potenziali rischi per i dati personali dei soggetti interessati e ha espresso alla SEM le proprie perplessità in merito alla sicurezza. Avendo

inoltre riscontrato che nell'applicazione non era prevista la cancellazione dei dati di registrazione di queste persone vulnerabili, l'IFPDT ha suggerito alla SEM di elaborare una procedura di cancellazione e di cancellare immediatamente i dati una volta svoltosi l'appuntamento. In concreto, l'Incaricato ha consigliato la creazione e l'attuazione di una procedura di cancellazione.

La SEM ha protetto l'accesso ai dati personali mediante autenticazione a due fattori e predisposto il salvataggio dei dati in un centro di calcolo riservato ai dati degni di particolare protezione. Successivamente la SEM ha istituito una procedura di cancellazione, che ha attuato dal settembre 2022.

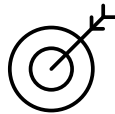
MITTO AG

Inchiesta preliminare su un possibile abuso dell'accesso al sistema di segnalazione

A dicembre 2021 l'IFPDT è venuto a conoscenza attraverso i media internazionali di un presunto trattamento illecito dei dati da parte di un dipendente della Mitto AG, una società con sede a Zugo. Dagli accertamenti condotti non sono emersi indizi di una violazione delle disposizioni sulla protezione dei dati. L'IFPDT chiude così la sua inchiesta preliminare con un rapporto finale senza formulare raccomandazioni.

Nel dicembre 2021 l'Incaricato federale della protezione dei dati e della trasparenza ha appreso dai media che in una pubblicazione del «Bureau of Investigative Journalism e Bloomberg News» un dipendente della Mitto AG, società con sede a Zugo, veniva accusato di trattamento illecito dei dati. Sempre

secondo tale pubblicazione il dipendente avrebbe abusato dell'accesso concesso dagli operatori di telefonia mobile alle loro reti per l'invio di SMS, allo scopo di ottenere informazioni per altri fini. Secondo il rapporto l'impiegato



avrebbe usato l'accesso al sistema di segnalazione (SS7) per consentire a terzi, dietro remunerazione, di effettuare una sorveglianza non autorizzata di individui (cfr. 29° rapporto d'attività, n. 1.3)

L'IFPDT ha quindi chiesto alla Mitto AG, in una procedura a tappe, una serie di informazioni circostanziate sulle misure di protezione tecniche e organizzative implementate dall'azienda. La Mitto AG ha dato seguito a tutte le richieste dell'IFPDT e ha commissionato le proprie inchieste esterne, mettendo poi i risultati a disposizione dell'IFPDT.

La Mitto AG ha documentato il quadro organizzativo del funzionamento del sistema e ha spiegato con quali misure è possibile prevenire o scoprire modifiche non autorizzate del software. Secondo la Mitto AG l'analisi dei dati di login non ha rivelato alcun indizio di abuso dei sistemi nel modo asserito dai media.

Secondo quanto affermato dalla Mitto AG – e confermato dagli operatori di telefonia mobile attivi in Svizzera invitati a esprimersi in merito – senza una modifica dei sistemi o del software i suoi dipendenti non possono accedere ai dati di localizzazione dei destinatari degli SMS.

L'IFPDT ha predisposto le verifiche necessarie e possibili con i mezzi a sua disposizione e non ravvisa indizi a conferma del sospetto di una violazione delle disposizioni sulla protezione dei dati.

Dato che le accuse relative al comportamento scorretto del dipendente della Mitto AG erano poco specifiche dal punto di vista tecnico, l'IFPDT ha chiuso l'inchiesta preliminare relativa alla Mitto AG con un rapporto finale senza formulare raccomandazioni.



1.3 Commercio ed economia

COMUNICAZIONE DI DATI AD AUTORITÀ FISCALI ESTERE

Il Tribunale federale si pronuncia negativamente in merito al diritto all'informazione di terzi nell'ambito dell'assistenza amministrativa internazionale in materia fiscale.

[Nel 2019 il Tribunale amministrativo federale ha accolto un ricorso dell'IFPDT concernente il diritto all'informazione di terzi nell'ambito dell'assistenza amministrativa internazionale in materia fiscale. Nella successiva procedura di ricorso dinanzi al Tribunale federale l'Incaricato ha nuovamente perorato la causa a favore del diritto all'informazione di terzi. A dicembre 2021 il Tribunale federale ha accolto il ricorso dell'AFC sulla base di un cambio di prassi intervenuto nel frattempo e ha annullato la sentenza del Tribunale amministrativo federale.](#)

Nell'ambito dell'assistenza amministrativa internazionale in materia fiscale il diritto di essere informati in merito a un procedimento di assistenza amministrativa in corso è collegato alla legittimazione a ricorrere di una persona (cfr. art. 14 della legge sull'assistenza amministrativa fiscale). Nel 2017 l'IFPDT aveva emanato una raccomandazione secondo cui, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, l'Amministrazione federale delle contribuzioni (AFC) deve informare preventivamente anche le persone non formalmente interessate dalla richiesta di assistenza amministrativa (ossia persone terze), i cui nomi non anneriti vanno resi noti

all'autorità estera richiedente (cfr. 25° rapporto, n. 1.9.2). L'IFPDT l'aveva motivata ritenendo che i terzi sono legittimati a difendersi da una trasmissione illegittima dei loro dati mediante ricorso. L'AFC ha respinto la raccomandazione e l'IFPDT ha adito le vie legali presentando ricorso al Tribunale amministrativo federale (cfr. 26° rapporto, n. 1.3). Nella sua sentenza del 3 settembre 2019 il Tribunale amministrativo federale è giunto alla conclusione che, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, in linea di principio devono essere informate preventivamente le persone non interessate



dalla domanda di assistenza amministrativa (persone terze), i cui dati non anneriti devono essere resi noti. Sono da prevedere disposizioni derogatorie nei casi in cui l'informazione richiesta può essere comunicata soltanto con un onere eccessivo e tale da non rendere possibile l'assistenza amministrativa o da ritardarne gravemente l'attuazione. L'IFPDT ha accolto con favore la sentenza in quanto essa tutela i diritti fondamentali dei dipendenti delle banche e di altre persone terze.

L'AFC ha interposto ricorso dinanzi al Tribunale federale. Quest'ultimo ha annullato la sospensione della procedura richiesta dall'AFC dopo che il

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

Tenuto conto di tale giurisprudenza, l'IFPDT ha riconosciuto dinanzi al Tribunale federale che, nell'ambito dell'assistenza amministrativa internazionale in materia fiscale, eventuali terze persone sono legittimate a ricorrere soltanto in via eccezionale. È rimasto tuttavia dell'opinione, confermata dal Tribunale amministrativo federale, che in linea di principio debbano essere informate preventivamente d'ufficio in merito alla trasmissione dei loro dati tutte le persone terze. Soltanto così tutte le persone terze, legittimate a ricorrere ai sensi della giurisprudenza del Tribunale federale, possono effettivamente fare uso del loro diritto di ricorso e difendersi contro un'imminente trasmissione di dati. L'IFPDT ha quindi prospettato nuovamente dinanzi al Tribunale federale come attuare

TECNOLOGIE DI TRACCIAMENTO

l'obbligo di massima in materia d'informazione cui soggiace l'AFC, senza che ne insorga un onere sproporzionato tale da ritardare eccessivamente l'assistenza amministrativa (cfr. 28° rapporto, n. 1.3).

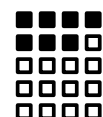
Con la sentenza del 21 dicembre 2021 (DTF 148 II 349), il Tribunale federale ha confermato la giurisprudenza formulata nella sentenza DTF 146 I 172, secondo cui l'AFC deve informare preventivamente d'ufficio in merito alla trasmissione dei dati solo le persone terze la cui legittimazione a ricorrere è evidente in base agli atti. Contrariamente all'interpretazione dell'IFPDT, esso ha ritenuto che ciò fosse disciplinato espressamente nell'articolo 14 capoverso 2 della legge sull'assistenza amministrativa fiscale. Il Tribunale federale ha negato un obbligo di informare generale ai sensi dell'articolo 18a capoverso 3 LPD precisando che la comunicazione di dati di persone terze è disciplinata espressamente dalla legge sull'assistenza amministrativa fiscale. Di conseguenza, ha accolto il ricorso dell'AFC e annullato la sentenza del Tribunale amministrativo federale del 3 settembre 2019.

Verifica di una possibile violazione della personalità nei confronti della popolazione svizzera da parte di Oracle

[L'IFPDT è venuto a conoscenza di una causa intentata negli Stati Uniti ad agosto 2022 contro la società americana «Oracle America Inc.», nei confronti della quale sono state mosse pesanti accuse di tracciamento illegale. Si intende ora verificare se le accuse avanzate riguardano anche la popolazione in Svizzera.](#)

Nella causa intentata negli Stati Uniti contro Oracle America Inc., la società americana è accusata di aver raccolto con tecnologie di tracciamento i dati di 5 miliardi di utenti di Internet e di averli accorpati in una banca dati. Oracle avrebbe analizzato e valutato le

informazioni acquisite per allestire una raccolta di dati riguardante tutte le persone coinvolte. Oltre ai nomi e agli indirizzi sono state raccolte informa-



zioni sul comportamento di ciascun utente di Internet, ad esempio le abitudini di acquisto, i dati GPS o informazioni sulla salute, e questo è stato fatto addirittura dai dispositivi degli utenti. Oracle America Inc. avrebbe utilizzato diverse tecnologie, in particolare i cosiddetti «cookie» o «pixel» nonché gli script Java integrati nei siti Internet e nelle applicazioni, al fine di tracciare gli utenti. La causa è ancora in corso; il Tribunale statunitense non ha ancora deliberato in merito alle accuse avanzate.

L'IFPDT ha preso atto delle accuse formulate nella causa e le sta analizzando assieme alle eventuali ripercussioni per le persone in Svizzera dal punto di vista della protezione dei dati. È inoltre in contatto con Oracle Software (Svizzera) Sagl. Dal punto di vista tecnico, i retroscena appaiono complessi, pertanto finora non è stata aperta alcuna indagine formale.

Rinuncia alla pubblicazione del conto

Con la richiesta dell'IFPDT a PostFinance di introdurre un'opzione di opt-out per la pubblicazione del conto, il completamento automatico dei dati del conto nell'e-banking dell'istituto risulterà in futuro limitato, allineandosi così alle pratiche in uso nel settore.

Nel precedente anno in rassegna abbiamo aperto un'inchiesta preliminare relativa al completamento automatico dei dati del conto (la cosiddetta pubblicazione del conto) nell'e-banking di PostFinance, dopo che alcuni cittadini ci avevano segnalato la possibilità di accedere ai dati di un numero indefinito di titolari di conti postali, in quanto il sistema completava il numero di conto digitato nell'apposito campo riservato ai pagamenti con il nome e l'indirizzo del titolare del conto (cfr. 29° rapporto d'attività 2021/2022, n. 1.3). Dopo che PostFinance aveva già adottato provvedimenti per impedire interrogazioni in blocco



vato ai pagamenti con il nome e l'indirizzo del titolare del conto (cfr. 29° rapporto d'attività 2021/2022, n. 1.3). Dopo che PostFinance aveva già adottato provvedimenti per impedire interrogazioni in blocco

per impedire interrogazioni in blocco

attraverso il proprio portale di e-banking, abbiamo chiesto di introdurre un'opzione di opt-out in modo tale che i clienti si potessero opporre al completamento automatico dei propri dati del conto.

PostFinance ha valutato in seguito le possibilità di implementare una simile procedura di opt-out e ha deciso di rinunciare in futuro alla pubblicazione del conto. Secondo un comunicato di PostFinance, saranno quindi completati automaticamente nell'e-banking dell'istituto solo i dati del conto che gli utenti hanno già utilizzato una volta per l'immissione di un ordine di pagamento. L'istituto si allinea così allo standard in uso nel settore ed effettuerà i dovuti adeguamenti nel corso del 2023. Provvederemo a verificare l'attuazione di tale misura.

Registrazioni nella banca dati sulla base della «famiglia di cattivi pagatori»

L'IFPDT ha concluso la procedura di accertamento dei fatti presso una società operante nel settore della riscossione e della verifica della solvibilità. È emerso che lo strumento della cosiddetta «famiglia di cattivi pagatori» non è ammissibile. Nel periodo 2019/2020, l'IFPDT ha avviato una procedura di accertamento dei fatti presso un grosso fornitore di servizi di riscossione e di verifica della solvibilità a causa di numerose presunte registrazioni errate nella banca dati che hanno portato a confondere persone con nomi e indirizzi uguali o simili. A causa di tale confusione sono stati inviati solleciti di pagamento a persone sbagliate o sono state memorizzate e rese note informazioni inesatte e negative sulla solvibilità. L'IFPDT ha inoltre indagato se fossero insorte difficoltà nella correzione delle registrazioni errate. Nel corso della procedura, il campo d'indagine è stato esteso all'ammissibilità della cosiddetta «famiglia di cattivi pagatori» (cfr. 27° rapporto, pag. 37; 28° rapporto, pag. 34; 29° rapporto, pag. 39).

Chi tratta dati personali deve accertarsi della loro esattezza (art. 5 cpv. 1

LPD). Situazioni di confusione dovute a registrazioni errate nella banca dati portano regolarmente a violazioni della



sfera personale, che nel singolo caso possono risultare gravi per le persone

interessate. Dopo un esame approfondito, l'IFPDT è giunto alla conclusione che la società oggetto d'indagine soddisfa i requisiti previsti dalla legislazione in materia di protezione dei dati per quanto riguarda le misure atte a garantire la correttezza, l'attualità e la completezza dei dati. Anche elaborando e adottando scrupolosamente le misure necessarie possono comunque verificarsi errori nelle registrazioni nella banca dati. È quindi importante che il trattamento dei dati sia riconoscibile da parte della persona interessata (trasparenza) e che sussista una procedura efficace di correzione e cancellazione, al fine di evitare conseguenze negative legate a registrazioni errate nella banca dati. Nel corso dell'indagine è emerso che la società in questione soddisfa anche questi requisiti.

Durante la procedura di accertamento dei fatti l'IFPDT ha valutato inoltre l'ammissibilità delle verifiche della solvibilità sulla base della «famiglia di cattivi pagatori» in virtù delle quali, nell'ambito di una verifica di solvibilità, vengono divulgate informazioni sulla cattiva solvibilità di altre

persone della stessa economia domestica. La comunicazione di questi dati – nella fattispecie a commercianti online – dovrebbe teoricamente impedire che persone con una cattiva solvibilità possano effettuare un acquisto contro fattura a nome di un membro della stessa economia domestica con una buona solvibilità (operazione di aggiornamento). A causa di tale prassi vengono associate le solvibilità di membri della stessa economia domestica, impedendo così ad altre persone della famiglia di effettuare acquisti contro fattura nonostante godano di una buona solvibilità. Nel corso



della sua indagine, l'IFPDT è giunto alla conclusione che questo metodo di trattamento dei dati viola il principio di trasparenza e proporzionalità sancito nella legge sulla protezione dei dati. Un siffatto trattamento dei dati non può essere giustificato. In particolare non è pertinente l'interesse preponderante che giustifica la valutazione del credito di una persona (art. 13 cpv. 2 lett. c LPD), poiché la cattiva solvibilità di un membro della famiglia non può essere determinante per la solvibilità della persona che stipula il contratto. Per questi motivi, l'IFPDT ha raccomandato alla società, nel suo rapporto finale, di sospendere le verifiche della solvibilità sulla base della «famiglia di cattivi pagatori».

La società ha accettato la raccomandazione.

CIBERATTACCO

Inchiesta preliminare presso Infopro SA e Fiducial Winbiz SA

L'IFPDT ha aperto un'inchiesta preliminare a seguito di un ciberattacco ai danni di un fornitore svizzero di servizi di cloud hosting. Ha valutato le misure adottate e ha reso attenti gli attori coinvolti sui loro doveri in materia di protezione dei dati.

A fine novembre 2022 è stato reso noto il ciberattacco ai danni dell'host Infopro AG, una società che tra l'altro tratta i dati personali per conto della società Fiducial Winbiz SA, la quale fornisce un software di gestione e di contabilità su cloud ampiamente utilizzato in Svizzera romanda. A causa del ciberattacco e delle misure adottate in seguito alcuni clienti commerciali hanno temporaneamente perso l'accesso all'applicazione e ai dati personali salvati nel cloud.

L'IFPDT ha ricevuto numerose domande dai clienti commerciali di Infopro SA in merito al ciberattacco e ha fornito loro consulenza. Trattandosi di dati personali, l'IFPDT ha fatto loro presente che erano tenuti a informare le persone coinvolte e a ridurre i

rischi in materia di protezione dei dati. Le aziende interessate si sono impegnate ad adempiere a tali obblighi in tempi brevi.

L'IFPDT ha contattato Infopro e Winbiz per accertare rapidamente i fatti, in particolare per verificare la fondatezza



dell'accusa riguardante la falla di sicurezza nel software di Winbiz che avrebbe permesso ad alcuni clienti di accedere ai dati di altri

clienti. L'IFPDT ha inviato un questionario a Winbiz, invitandola a prendere posizione sulla presunta violazione delle restrizioni di accesso, e un questionario a Infopro. In parallelo ha pure avuto colloqui con le autorità cantonali di protezione di dati (privatim) e con il Centro nazionale per la cibersicurezza (NCSC), il quale affianca le autorità di perseguimento penale competenti.

Le risposte pervenute hanno permesso all'IFPDT di constatare che le due società hanno adottato le misure necessarie a ristabilire il controllo sui dati personali e informato i clienti coinvolti. Poiché la presunta falla di sicurezza non è stata confermata, l'IFPDT non ha ritenuto necessario agire nell'immediato. Ha tuttavia chiesto a Infopro e a Winbiz di comunicargli eventuali incidenti particolari.

OPERATORE DI SERVIZI VOICE

La falla di sicurezza è stata eliminata tempestivamente

In seguito alla segnalazione di una falla di sicurezza, l'IFPDT ha condotto un'inchiesta preliminare presso un operatore di servizi Voice. La tempestiva adozione dei provvedimenti necessari da parte dell'operatore ha evitato all'IFPDT l'avvio di un procedimento formale.

Nell'anno in rassegna sono giunte all'IFPDT segnalazioni da parte di un cittadino e un giornalista, secondo cui attraverso il sito Internet di un operatore di servizi Voice si poteva accedere a dati personali in modo non protetto. Numerose conversazioni telefoniche registrate non erano protette da password e in alcuni casi i dati contenevano ulteriori informazioni che consentivano di risalire facilmente a una determinata persona.

In seguito a queste segnalazioni, l'IFPDT ha avviato un'inchiesta preliminare informale nei confronti dell'operatore di servizi Voice in questione, il quale ha provveduto a eliminare tempestivamente la falla, ad analizzare l'accaduto e ad adottare ulteriori provvedimenti necessari. L'IFPDT si è limitato a fornire qualche proposta di miglioramento, che l'operatore ha messo in pratica, e alla luce di ciò non ha ritenuto opportuno avviare una procedura formale di accertamento dei fatti, chiudendo così l'inchiesta preliminare.

APP DI INCONTRI

Analisi del trattamento di dati

Nell'anno in rassegna l'IFPDT ha sottoposto il suo rapporto finale al fornitore di un'app di incontri con sede in Svizzera ma operante a livello internazionale, il quale ha accettato le raccomandazioni che abbiamo formulato.

Nella primavera del 2021 l'IFPDT ha avviato un accertamento dei fatti riguardo al trattamento dei dati da parte di un'app di incontri, al fine di chiarire nello specifico se la gestione delle richieste di cancellazione e la trasmissione di dati personali a terzi fossero conformi alla legge in materia di protezione dei dati, nonché di verificare il rispetto dei requisiti in materia di trasparenza e sicurezza dei dati (cfr. 28° e 29° rapporto d'attività, n. 1.1).

L'IFPDT è giunto fra l'altro alla conclusione che le domande di cancellazione dei dati venivano sì trattate a breve termine, ma che il piano di cancellazione era insufficiente. Le informazioni sulle possibilità di cancellazione a disposizione degli utenti erano anch'esse

CORSE VIRTUALI

insufficienti e poco chiare. Sono inoltre state riscontrate lacune nelle informazioni sul trattamento dei dati eseguito nell'ambito dell'utilizzazione dell'applicazione. In particolare non era chiaro quali dati venissero utilizzati per quali scopi. L'IFPDT ha formulato diverse raccomandazioni al fine di colmare le lacune individuate e di garantire il rispetto dei principi di trasparenza, proporzionalità, buona fede e liceità nel trattamento dei dati.

Il fornitore si affida ad applicazioni di terzi per diverse funzionalità dell'app invece di svilupparle direttamente. In tal modo trasferisce il trattamento di dati personali a fornitori esterni. Secondo la nostra valutazione il fornitore, in quanto titolare del trattamento, non ha adottato i provvedimenti necessari, compresi gli accertamenti e accordi, al fine di garantire che i fornitori esterni si limitino a trattare i dati conformemente al mandato ricevuto e nel rispetto delle norme sulla protezione dei dati. Inoltre ha svolto soltanto test di sicurezza interni che, in presenza di dati sensibili, non sono sufficienti per rispondere alle esigenze in materia di sicurezza dei dati. L'IFPDT ha quindi emanato delle raccomandazioni al fine di rafforzare la sicurezza dei dati e la legalità del ricorso a servizi esternalizzati.

Il fornitore ha accettato tutte le nostre raccomandazioni. Non appena saranno attuate l'IFPDT potrà chiudere il procedimento

Miglioramento della protezione dei dati presso un fornitore di servizi nell'ambito delle corse virtuali

L'IFPDT ha ricevuto una segnalazione riguardo a problematiche inerenti alla protezione dei dati con un fornitore di eventi di corsa virtuali. Dopo che l'Incaricato ha effettuato le prime indagini e contattato il fornitore di servizi, quest'ultimo ha adottato immediatamente provvedimenti per aumentare il livello di protezione dei dati, cosicché l'IFPDT ha potuto rinunciare ad avviare un'indagine formale.

Grazie a un'app di un fornitore di servizi, gli appassionati di corsa possono effettuare «corse virtuali» e misurarsi tra loro. A seconda dell'offerta, le corse si possono svolgere anche non in tempo reale, ovvero entro un arco di tempo personalizzabile, in un luogo prestabilito oppure ovunque si desideri. I risultati vengono poi inseriti in una classifica. A

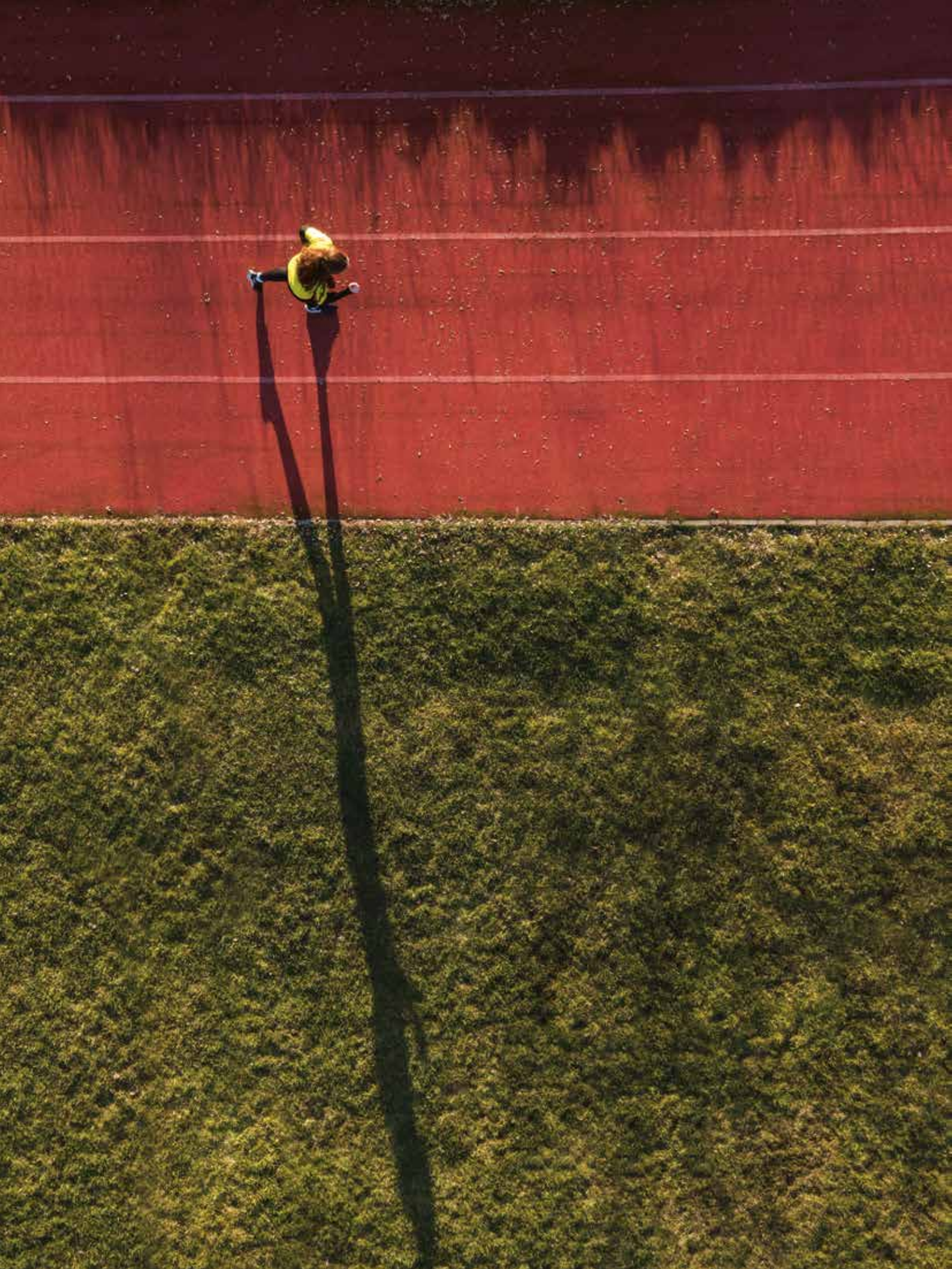
destare preoccupazione è stato il fatto che attraverso il tool di sviluppo via Internet si potessero raccogliere con pochi clic i dati delle classifiche di numerose persone, e ciò non era tra-



sparente per i soggetti interessati. In seguito al confronto con l'IFPDT, il fornitore di servizi ha precisato la propria dichiara-

zione sulla protezione dei dati integrandola nel processo di registrazione. Inoltre ha eliminato dalla classifica il parametro «domicilio», rendendo così difficile risalire a persone concrete. Abbiamo altresì constatato che nonostante fosse possibile iscriversi a una corsa virtuale con uno pseudonimo, numerose persone hanno indicato consapevolmente il proprio nome e cognome reali. Gli utenti hanno anche la possibilità di cancellarsi autonomamente dalla classifica.

In seguito allo scambio informale intercorso tra l'IFPDT e il fornitore di servizi è stato possibile incrementare immediatamente il livello di protezione dei dati, cosicché l'Incaricato ha potuto rinunciare all'apertura di un'indagine formale.



1.4 Salute

REGISTRO NAZIONALE DI DONAZIONE DI ORGANI

Scarsa sicurezza dell'autenticazione online

Si è conclusa l'inchiesta sul Registro nazionale di donazione di organi (RNDO) e il rapporto finale è stato pubblicato sul sito dell'IFPDT (in tedesco). Questo caso sottolinea l'importanza di disporre di mezzi d'autenticazione online affidabili. Le soluzioni di facile utilizzo esistono.

Nel corso del 2022 l'IFPDT ha svolto e concluso una procedura di accertamento dei fatti relativa al Registro nazionale di donazione di organi, gestito dalla fondazione Swisstransplant. Il registro permetteva di registrare su una piattaforma online la propria volontà riguardo alla donazione di organi in caso di morte. Questa informazione costituisce un dato sensibile ai sensi dell'articolo 3 lettera c numero 2 LPD poiché riguarda



la sfera intima. La procedura era stata avviata in seguito alla segnalazione fatta dai media dell'esistenza di una falla nella

procedura di registrazione; in pratica era possibile iscriversi nel registro altre persone a loro insaputa. La procedura si è svolta in più tappe:

- A metà giugno l'IFPDT ha trasmesso a Swisstransplant un primo rapporto nel quale formulava diverse raccomandazioni volte a migliorare l'affidabilità delle procedure d'autenticazione degli utenti al momento dell'iscrizione al registro ma anche per tutti i collegamenti e le modifiche dei dati successivi.
- Durante l'estate 2022 Swisstransplant ha preso posizione in merito a questo rapporto. In particolare la fondazione ha comunicato che rinunciava

a riaprire il registro in forma attiva: sarebbe ancora stato possibile consultarlo ma non effettuare nuove registrazioni né modifiche degli account esistenti (rimaneva possibile soltanto la cancellazione dell'account). Questa decisione ha reso prive di oggetto una parte delle raccomandazioni, ossia quelle riguardanti il miglioramento dei processi di autenticazione durante la registrazione online. Swisstransplant ha inoltre accettato la maggior parte delle altre raccomandazioni, tranne due riguardanti un rischio residuo legato alla cancellazione degli account.

- A metà ottobre l'IFPDT ha trasmesso il suo rapporto finale. Poco dopo Swisstransplant ha annunciato di aver deciso di abbandonare definitivamente la gestione del registro, il quale è stato effettivamente chiuso nel dicembre 2022 e dal quale tutti i dati sono stati cancellati.

A questo proposito occorre precisare che nella votazione popolare del 15 maggio 2022 il Popolo ha accettato il modello del consenso presunto per la donazione di organi e la creazione di un registro sotto la responsabilità della Confederazione. Il registro, che dovrebbe vedere la luce nel 2025, avrà una funzione simile a quella del registro gestito da Swisstransplant.

Mezzi d'autenticazione online

Il caso del registro di Swisstransplant è un tipico esempio delle insidie che si celano nella creazione di un registro online. Questo strumento è evidentemente molto pratico in quanto consente una consultazione a distanza e una gestione degli account da parte degli utenti stessi. Nell'intento di raggiungere un più ampio pubblico possibile si privilegiano le procedure semplici per la registrazione e la gestione degli account. Il rischio è tuttavia quello di scadere in qualcosa di troppo semplice, aprendo così la strada agli abusi da parte di malintenzionati (usurpazione dell'identità, hacking, azioni moleste ecc.). Il gestore di un registro deve essere veramente consapevole che è garante dell'esattezza e della sicurezza delle informazioni in esso

contenute, a maggior ragione se queste vengono utilizzate quali basi decisionali da parte di altri attori, come parenti e medici nel caso della donazione di organi. Al riguardo ricordiamo che esistono mezzi d'autenticazione online affidabili e di facile utilizzo, correntemente usati in particolare nel settore bancario. Possiamo anche citare le varie soluzioni d'identità elettronica già disponibili. Quando si prevede di aprire un registro di questo tipo con autenticazione online è importante informarsi prima in modo da scegliere soluzioni sicure. La digitalizzazione offre nuove possibilità al settore sanitario, ma cela anche nuovi rischi. È nell'interesse degli attori del settore mantenere alta la fiducia istituendo strumenti digitali validi e affidabili.

REGISTRI ONLINE

Rischi di protezione dei dati nel registro delle protesi mammarie

Si è conclusa la procedura di accertamento dei fatti nei confronti del registro delle protesi mammarie. Il caso illustra come la pubblicazione online di informazioni mediche implichi intrinsecamente l'assunzione di maggiori rischi. Si tratta dunque di pronunciarsi in merito alla necessità di tale assunzione di rischi. Se del caso, occorre disporre dei mezzi adeguati per garantire la sicurezza dei dati.

Nel 2022 l'IFPDT ha avviato una procedura di accertamento dei fatti nei confronti del registro delle protesi mammarie (cfr. 29° rapporto, n. 1.4), tenuto dalla Società Svizzera di Chirurgia Plastica, Ricostruttiva ed Estetica per registrare tutti gli interventi di mammoplastica con l'impiego di protesi e le eventuali difficoltà riscontrate durante le operazioni. Gli obiettivi sono molteplici: in primo luogo, si

tratta di migliorare la qualità del servizio facendo circolare le informazioni su eventuali incidenti. Il registro serve inoltre a garantire un certo monitoraggio delle protesi, per facilitare eventuali richiami dei prodotti qualora vengano riscontrati difetti in una serie di protesi. Infine, i dati raccolti servono anche per aggiornare le statistiche del settore.

L'IFPDT ha aperto un'indagine a seguito della segnalazione di una falla nell'architettura informatica del registro: chiunque, con poche manipolazioni, poteva accedere alle cartelle delle pazienti. Oltre ai dati identificativi (cognome, nome, data di nascita, ecc.), erano consultabili anche i dati medici relativi ai dettagli dell'operazione. La stesura del rapporto da parte dell'IFPDT è in corso e sarà completata nel corso dell'anno. Nel frattempo, il registro non è più accessibile online.

Assunzione dei rischi e necessità

Il caso sottolinea un altro aspetto delicato legato ai registri medici accessibili online. I dati che contengono sono per definizione sensibili, visto che riguardano la salute. Spesso si tratta anche di informazioni intime. Il fatto di renderle disponibili online comporta necessariamente maggiori rischi per i

dati dei pazienti e può inoltre nuocere al rapporto di fiducia con il proprio medico. In effetti i dati vengono regolarmente trasmessi direttamente dai medici, che sono tenuti al segreto professionale: per la trasmissione, a priori serve dunque il previo consenso dei pazienti. Pertanto, occorre sempre domandarsi se lo scopo del registro giustifichi l'assunzione del rischio e quali dati siano effettivamente essenziali per raggiungere tale scopo (secondo il principio di proporzionalità, sancito all'art. 4 cpv. 2 LPD). Se del caso, i gestori di tali registri devono quindi adottare misure adeguate e stanziare risorse sufficienti per prevenire questi rischi.



Procedura di accertamento dei fatti sulla banca dati dei centri di test COVID-19 privati

L'IFPDT ha condotto una procedura di accertamento dei fatti su una banca dati rivelatasi non sufficientemente sicura in cui vari centri di test COVID-19 privati registravano i propri risultati. Nel rapporto finale ha dichiarato che i dati erano esposti a notevoli rischi quanto alla loro sicurezza a causa di una nota vulnerabilità. Poiché, dopo essere venuti a conoscenza della falla, i responsabili hanno immediatamente avviato adeguate misure, il rischio per gli interessati ha potuto essere notevolmente ridotto e la procedura è stata conclusa senza raccomandazioni da parte dell'IFPDT.

Nel novembre 2022 un privato ha segnalato all'IFPDT e al NCSC una vulnerabilità nella sicurezza di una banca dati nella quale erano memorizzati i risultati provenienti da centri di test COVID-19 in diverse località in Svizzera. Approfittando di una falla del server Internet, il privato era riuscito a entrare nella banca dati tramite informazioni visibili in un file di configurazione liberamente accessibile e aveva scaricato una copia della banca dati. I responsabili hanno tolto dal server la banca dati il giorno stesso della segnalazione e l'hanno trasferita su un supporto fisico criptato.

Nell'ambito della procedura di accertamento dei fatti avviata in seguito alla segnalazione ricevuta e ai primi chiarimenti in merito, l'IFPDT ha constatato diverse vulnerabilità nella sicurezza



dei dati. Una manutenzione del sistema aveva reso il file di configurazione liberamente accessibile esponendo il sistema a una vulnerabilità critica poiché chiunque avrebbe potuto entrare nella banca dati. Inoltre il metodo di autenticazione tramite nome utente e password (entrambi contenuti nel file esposto) si è dimostrato insufficiente nella costellazione in questione: per garantire la sicurezza dei dati, avrebbe dovuto essere imposta per esempio un'autenticazione a due fattori.

Viste le implicazioni transfrontaliere del sistema, l'IFPDT ha intrattenuto diversi scambi con le autorità preposte alla protezione dei dati dell'Austria e del Principato del Liechtenstein nell'ambito di una procedura di assistenza amministrativa.

Il responsabile dei centri di test ha potuto confermare, sulla base dei registri di accesso, che non si sono verificati altri accessi non autorizzati ai dati. Grazie alle misure avviate immediatamente, non vi è stato più alcun rischio per gli interessati. Considerata questa specifica costellazione e visto che i centri di test COVID-19 non erano più operativi già molto prima che la vulnerabilità fosse resa nota, l'IFPDT ha concluso la procedura senza emanare raccomandazioni.

Aumento del numero di casi di hacker etici

Oltre al numero crescente di investigazioni giornalistiche sulle vulnerabilità in materia di protezione e sicurezza dei dati, l'IFPDT è sempre più confrontato a segnalazioni provenienti da hacker etici (detti anche «white hat hacker») e da attivisti informativi. Stando alla loro definizione ideale, questi hacker sono ben intenzionati poiché segnalano un caso all'IFPDT affinché intervenga presso l'operatore e apra eventualmente un'inchiesta. Le loro azioni, non inserite in un contesto ufficiale e prive del consenso dell'operatore dei sistemi, implicano spesso il trattamento di dati personali (ad es. dati dei clienti registrati nel sistema, dati degli impiegati, ecc.).

Va osservato che, parallelamente alle segnalazioni all'IFPDT, come nel caso dei centri di test COVID-19, a volte questi hacker informano direttamente il pubblico o i media sulle loro scoperte. A seconda delle informazioni trasmesse, questo tipo di comunicazione su larga scala è delicato perché può comportare rischi aggiuntivi per le persone a cui appartengono i dati interessati.



Progetto di salvataggio dei dati «lemievaccinazioni.ch»

Alla fine del 2021 è stato dichiarato il fallimento della fondazione che gestiva la piattaforma lemievaccinazioni.ch. Nel maggio 2022 l'IFPDT è venuto a conoscenza che il competente Ufficio fallimenti intendeva vendere a un'azienda privata i dati sulle vaccinazioni della piattaforma: questo lo ha spinto a emanare la raccomandazione di cancellare tali dati. Successivamente autorità e privati hanno chiesto che tali dati potessero essere salvati. Sulla base di un accordo di diritto pubblico voluto dall'IFPDT, il Cantone di Argovia li ha presi in consegna nel giugno 2022 allo scopo di esaminare, nell'ambito di un progetto preliminare ancora in corso, se fosse possibile restituirli agli interessati nel rispetto delle norme sulla protezione dei dati.

Nel 2021 sono state individuate gravi carenze sotto il profilo della protezione dei dati della piattaforma lemievaccinazioni.ch e compiuti vani tentativi per consentire agli interessati di accedere ai propri dati nel rispetto del diritto in materia di protezione dei dati. A fine 2021 il gestore della piattaforma ha dichiarato il fallimento (cfr. 29° rapporto, n. 1.4). Nel



maggio 2022 l'IFPDT è stato informato che i dati relativi alle vaccinazioni in questione sarebbero stati venduti mediante trattativa privata a un'azienda privata nell'ambito della procedura fallimentare. L'IFPDT, d'intesa con l'Incaricato per la protezione dei dati del Cantone di Berna, è quindi intervenuto emanando il 20 maggio 2022 una raccomandazione formale all'Ufficio fallimenti operante per conto della massa fallimentare, nella quale vieta la vendita e chiede la cancellazione di tutti i dati sulle vaccinazioni della piattaforma. L'Ufficio fallimenti ha accettato la raccomandazione.

In seguito alla raccomandazione dell'IFPDT diverse autorità, tra cui l'Ufficio federale della sanità pubblica (UFSP), e privati si sono pubblicamente espressi a favore del salvataggio dei dati e della loro restituzione agli interessati. Visto l'interesse pubblico a favore del salvataggio dei dati, in una lettera all'attenzione della direttrice dell'UFSP del giugno 2022 l'IFPDT si è dichiarato disposto a revocare il suo ordine di cancellarli. Questo a condizione che fossero trasmessi a un'autorità sanitaria della Confederazione o dei Cantoni sulla base di un accordo di diritto pubblico e allo scopo ivi esplicitato di tutelare i diritti degli interessati in materia di protezione dei dati.

Il 16 giugno 2022 la massa fallimentare rappresentata dall'Ufficio fallimenti di Bern-Mittelland ha concluso, con il sostegno dell'UFSP, un accordo di questo tipo con il Cantone di Argovia, permettendo all'IFPDT di revocare la raccomandazione del 20 maggio

2022. Conformemente all'accordo i dati sono stati quindi trasmessi al Cantone di Argovia e alla comunità di riferimento eHealth Aargau, operante su incarico del Cantone, affinché nel quadro di un progetto preliminare si esaminasse la possibilità di restituirli agli interessati nel rispetto del diritto in materia di protezione dei dati, tenendo conto della loro integrità e della fattibilità tecnica ed economica. Va inoltre esaminato il loro trasferimento in una cartella informatizzata del paziente, da subordinare a un consenso esplicito in ogni singolo caso. Se l'accertamento nell'ambito del progetto preliminare dovesse avere esito negativo, le dichiarazioni scambiate tra il Cantone di Argovia, la comunità di riferimento e l'UFSP prevedono l'interruzione del progetto e la cancellazione dei dati.

Al momento della stampa, l'esito del progetto preliminare del Cantone di Argovia, soggetto alla supervisione dell'Incaricato per la protezione dei dati dello stesso Cantone, era ancora aperto.

CARTELLA INFORMATIZZATA DEL PAZIENTE

Nuovi sviluppi

Nell'anno in rassegna il Dipartimento federale dell'interno (DFI) ha presentato al Consiglio federale un progetto da porre in consultazione per garantire il finanziamento transitorio della cartella informatizzata del paziente (CIP) sotto forma di sostegno finanziario fino alla revisione della legge. Nell'estate del 2023 dovrebbe essere tuttavia posta in consultazione una revisione totale della legge federale sulla cartella informatizzata del paziente (LCIP), volta a garantire il buon esito dell'introduzione e della diffusione della CIP.

In occasione della sua seduta del 27 aprile 2022 il Consiglio federale ha deciso di continuare lo sviluppo della CIP con l'ausilio di varie misure e ha incaricato il DFI di preparare un progetto per la consultazione sulla base di vari punti chiave definiti. La revisione totale della LCIP dovrebbe essere posta in consultazione nell'estate del 2023 (l'entrata in vigore non è prevista prima del 2027). Secondo la volontà espressa dal Consiglio federale, in futuro la CIP sarà ormai considerata uno strumento dell'assicurazione obbligatoria delle cure medico-sanitarie, il che conferirà alla Confederazione vaste facoltà normative. Gli assicuratori, tuttavia, non avranno accesso alla CIP.

I compiti, le competenze e, dunque, la garanzia del finanziamento della CIP da parte della Confederazione e dei Cantoni, sono chiaramente definiti. Per quanto riguarda il carattere facoltativo della partecipazione dei pazienti, saranno sottoposte a consultazione due varianti: il mantenimento del carat-



tere facoltativo e l'introduzione di un modello «opt-out», prediletto dal Consiglio federale. Tutti gli operatori sanitari che lavorano nel settore ambulatoriale sono tenuti a collegarsi alla CIP. Per i medici appena autorizzati, tale obbligo sussiste dal 1° gennaio 2022. Con il consenso dei pazienti, la comunità scientifica deve avere accesso ai dati della CIP. La memorizzazione centralizzata dei dati dinamici deve semplificarne il trattamento. L'utilizzo dell'infrastruttura tecnica della CIP diventerà possibile per servizi aggiuntivi, quali ad esempio il trasferimento dei pazienti ad altri operatori sanitari. Occorre chiarire la questione dell'utilizzo di un'Id-e per accedere alla CIP.

Per garantire il finanziamento della CIP fino alla revisione della LCIP, il Consiglio federale ha inoltre incaricato il DFI di porre in consultazione entro la primavera del 2023 un progetto di legge sul finanziamento transitorio della CIP, che sarà poi trasmesso al Parlamento e dovrà entrare in vigore il prima possibile. L'Ufficio federale della sanità pubblica (UFSP) ha iniziato i lavori inerenti queste due revisioni.

Inoltre, nell'ambito della revisione annuale del diritto di esecuzione della LCIP l'UFSP e eHealth Svizzera studiano le altre esigenze di sviluppo e l'aggiornamento della CIP, che dovranno concretizzarsi entro la primavera del 2023. Questi progetti di revisione sono volti a promuovere la diffusione e l'utilizzo della CIP, in particolare integrando un libretto di vaccinazione elettronico e un piano farmacologico elettronico nazionale. Sono inoltre al vaglio varie misure finalizzate a migliorare l'attrattiva della CIP.

L'IFPDT intrattiene scambi periodici con l'UFSP e puntualmente prende posizione in merito ai suoi progetti. Ha sempre ribadito di non essere contrario ad agevolare l'attuazione della CIP nell'interesse dei pazienti, anche se ciò non deve tradursi in un allentamento dei requisiti in materia di protezione dei dati. L'IFPDT continuerà a seguire da vicino lo sviluppo della CIP e a impegnarsi per garantire la protezione dei dati, in particolare se le misure previste si ripercuoteranno sui diritti inerenti la personalità delle persone interessate oppure nel caso in cui sia eliminato il carattere facoltativo della CIP per i pazienti.

Obbligo legale di trasmettere una copia della fattura medica

L'obbligo per i fornitori di prestazioni di trasmettere le copie delle proprie fatture mediche agli assicurati desta numerosi interrogativi, incertezze e commenti da parte degli assicurati, in particolare dal punto di vista della protezione e della sicurezza dei dati nel caso d'invio delle fatture per via elettronica.

A partire dal 1° gennaio 2022 tutti i fornitori di prestazioni di cui all'articolo 35 capoverso 2 della legge federale sull'assicurazione malattie LAMal (medici, farmacisti, chiropratici, ospedali, laboratori, ecc.) sono obbligati per legge a fornire agli assicurati una copia della loro fattura, in qualunque caso e senza che questi ultimi l'abbiano richiesto. Con il consenso esplicito degli assicurati la fattura può essere trasmessa per via elettronica. L'obbligo di comunicazione è stato adottato nell'ambito di varie misure volte a migliorare il controllo dei costi sanitari con la modifica dell'articolo 42 capoverso 3 LAMal, al fine di consentire agli assicurati di verificare le proprie fatture e di segnalare eventuali errori all'assicuratore. Di per sé l'obbligo non costituisce una novità, poiché esisteva già con il sistema del terzo pagante, ma in passato era disciplinato solo a livello di ordinanza.

In tale contesto l'IFPDT ha contattato l'Ufficio federale della sanità pubblica (UFSP), responsabile dell'attuazione di questa misura, per garantire che i fornitori di prestazioni siano

debitamente informati in merito ai propri obblighi, in particolare per quanto riguarda i requisiti di protezione e di sicurezza dei dati con l'invio di una copia della fattura per via elettronica. I dati relativi alla salute sono effettivamente degni di particolare protezione secondo la legge federale sulla protezione dei dati (LPD) e, per trattarli,



occorre adottare misure particolari. Pertanto, i fornitori di prestazioni che desiderano trasmettere le copie delle loro

fatture per via elettronica sono responsabili di garantire una comunicazione sicura adottando le misure tecniche e organizzative appropriate secondo l'articolo 7 LPD e l'articolo 8 e seguenti dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD). (L'obbligo di adottare misure di sicurezza adeguate è discusso anche nel capitolo dedicato al progetto per la futura trasmissione delle fatture elettroniche nell'assicurazione obbligatoria delle cure medico-sanitarie: cfr. articolo successivo).

Il mancato rispetto da parte dei fornitori di prestazioni dell'obbligo di garantire l'adozione di misure di protezione e sicurezza dei dati appropriate può comportare gravi ripercussioni di

natura civile e penale. La persona interessata potrà infatti intentare a titolo individuale una causa civile in caso di violazione illecita della propria personalità oppure un'azione per il risarcimento dei danni e del danno morale qualora sia danneggiata nel caso, ad esempio, di intercettazione dolosa di e-mail non criptate e della conseguente divulgazione a terzi dei propri dati sanitari. È inoltre possibile il perseguimento penale in caso di violazione del segreto medico, ad esempio se i dati medici sono comunicati a destinatari non autorizzati.

I fornitori di prestazioni che scelgono di trasmettere le copie delle proprie fatture per via elettronica devono anche aver informato preventivamente la persona assicurata dei rischi connessi a questa modalità di trasmissione. Devono inoltre assicurarsi che la persona assicurata abbia espressamente e deliberatamente fornito il proprio consenso alla trasmissione della copia della propria fattura per via elettronica. Se il paziente rifiuta di ricevere una copia della fattura per via elettronica, i fornitori di prestazioni devono rispettare tale scelta e inviare il documento cartaceo per posta tradizionale, senza costi aggiuntivi. Infine, occorre notare che la legge prevede altresì la possibilità per l'assicuratore e il fornitore di prestazioni di concordare che sia l'assicuratore a inviare la copia della fattura alla persona assicurata.

Progetto per la trasmissione delle fatture elettroniche nell'assicurazione obbligatoria delle cure medico-sanitarie

Una delle misure adottate dal Consiglio federale e volte a frenare i costi della sanità prevede che tutti i fornitori di prestazioni nei settori ospedaliero e ambulatoriale debbano trasmettere le fatture per via elettronica. L'IFPDT è intervenuto nella procedura di consultazione affinché si precisassero i requisiti in materia di protezione e di sicurezza dei dati.

Il 7 settembre 2022 il Consiglio federale ha adottato il messaggio concernente la modifica della legge sull'assicurazione malattie (Misure di contenimento dei costi – Pacchetto 2). Con il pacchetto è stata introdotta una modifica dell'articolo 42 capoverso 3ter LAMal secondo cui in futuro tutti i fornitori di prestazioni nei settori stazionario e ambulatoriale saranno obbligati a trasmettere le fatture per via elettronica, indipendentemente dal fatto che la remunerazione sia dovuta dall'assicuratore

malattie (terzo pagante) o dall'assicurato (terzo garante). Nel sistema del terzo pagante l'assicurato riceverà, elettronicamente o gratuitamente in forma cartacea se lo desidera, una copia della fattura inviata all'assicuratore, in modo tale da poterla controllare. Nel sistema del terzo garante la fattura sarà trasmessa all'assicurato per via elettronica o, se quest'ultimo lo desidera, gratuitamente in forma cartacea, per il controllo e il pagamento. L'assicurato la invierà all'assicuratore elettronicamente o la convaliderà sul portale online dell'assicuratore. In caso di fattura cartacea l'assicurato la invierà all'assicuratore, che chiederà poi al fornitore di prestazioni di trasmettergliela elettronicamente. I dettagli della procedura saranno disciplinati in un'ordinanza.

Le modalità di trasmissione elettronica delle fatture saranno definite dai partner tariffari. I fornitori di prestazioni e gli assicuratori o le loro federazioni dovranno concludere una convenzione su un unico standard nazionale. Il progetto prevede che la fatturazione avvenga su una piattaforma tramite un modulo standardizzato per garantire la sicurezza dei dati. Se, entro un periodo transitorio di due anni, le parti non concorderanno un sistema unico, sarà il Consiglio federale a deciderlo.

Nell'ambito della procedura di consultazione degli uffici l'IFPDT ha notato che la versione del progetto di messaggio posto in consultazione

doveva essere precisata quanto alle misure tecniche e organizzative da attuare. L'IFPDT ha inoltre ricordato che l'entrata in vigore al 1° gennaio 2022 del nuovo articolo 42 capoverso 3 LAMal sulla trasmissione elettronica di una copia della fattura agli assicurati aveva messo chiaramente in evidenza i pericoli insiti nell'utilizzo della trasmissione elettronica al posto della fattura cartacea e la necessità per i fornitori di prestazioni di adottare misure tecniche e organizzative adeguate, in particolare di crittografia e autenticazione a più fattori (l'obbligo di adottare misure di sicurezza adeguate è discusso anche nel capitolo sull'attuale obbligo di trasmettere una copia della fattura medica: cfr. articolo precedente).

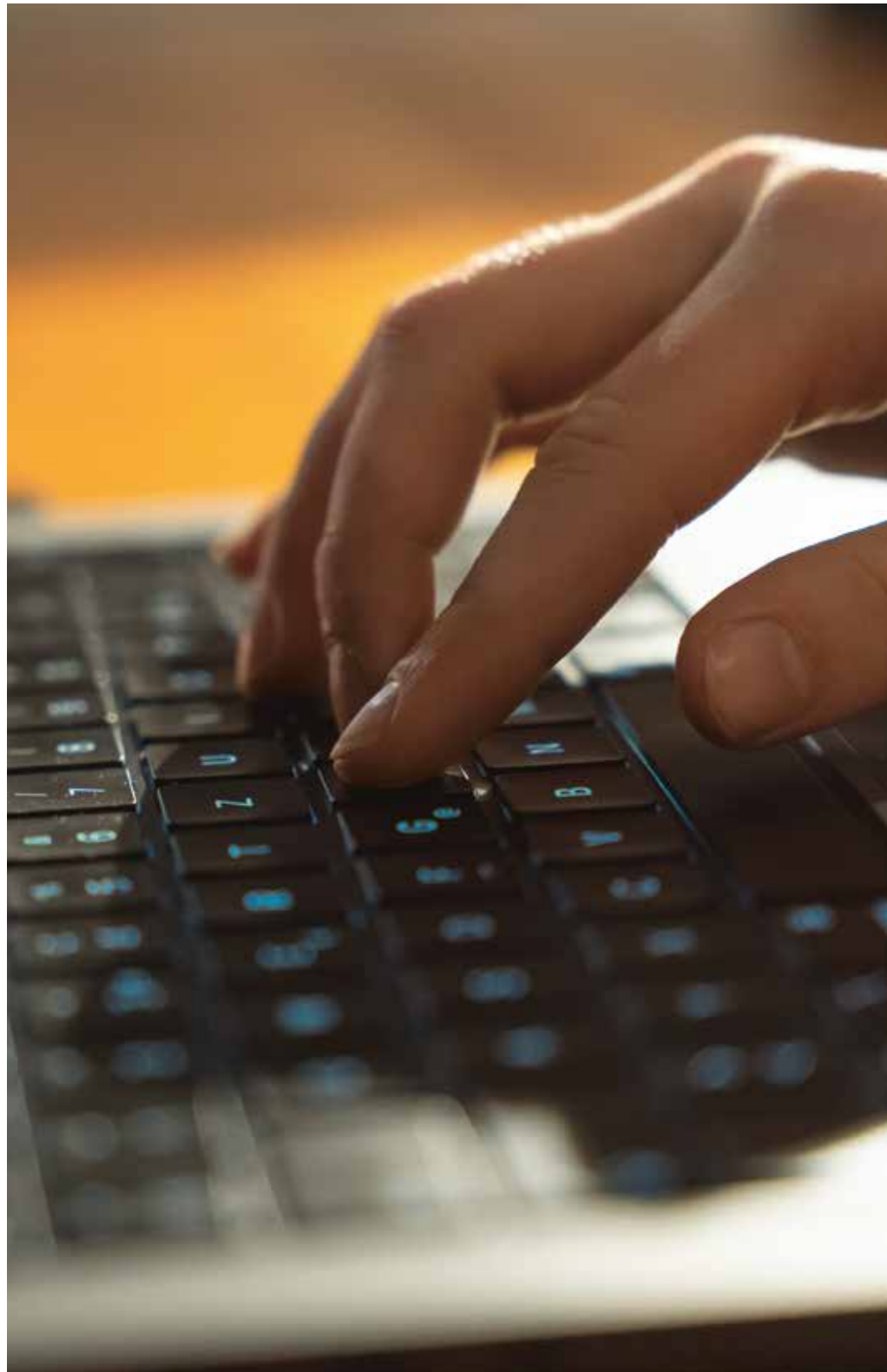
In considerazione delle nostre proposte il progetto di messaggio è stato modificato e il capitolo dedicato alla protezione dei dati è stato completato con un rinvio alle norme della LPD, in particolare all'obbligo di adottare

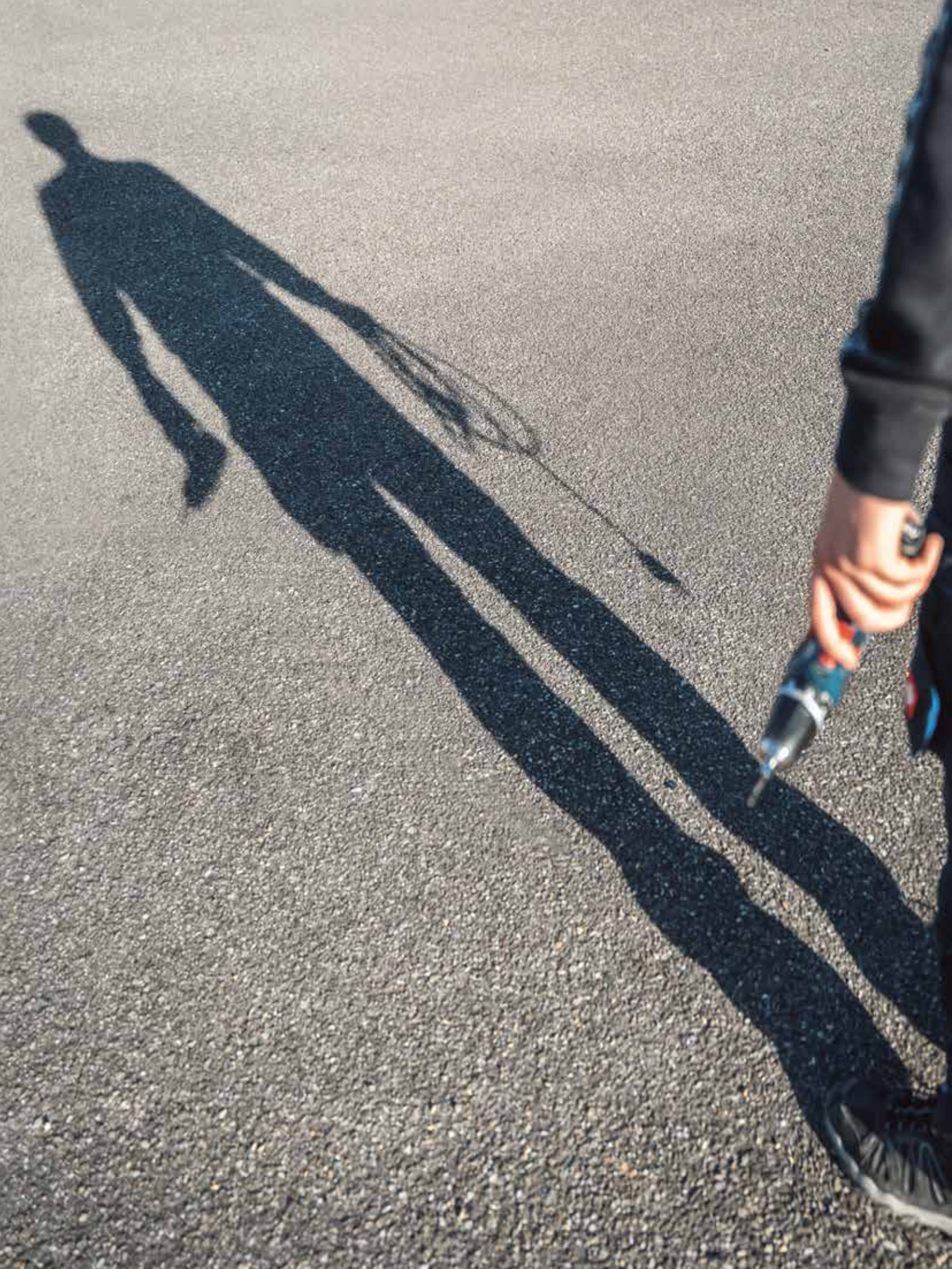
misure tecniche e organizzative appropriate contro qualsiasi trattamento non autorizzato. È stato inoltre sottolineato come le fatture contengano dati degni di particolare protezione secondo la LPD, dal momento che i fornitori di prestazioni devono includere nelle loro fatture tutte le indicazioni amministrative e mediche necessarie per verificare il calcolo della remunerazione, in particolare il dettaglio delle prestazioni fornite e le diagnosi. Il messaggio precisa che il trattamento di tali dati degni di particolare protezione implica l'adozione di misure particolari (trasmissione criptata, procedura di autenticazione a più fattori) di cui i partner tariffari dovranno tenere conto in sede di definizione di uno standard nazionale unico a garanzia della sicurezza dei dati. Infine, il messaggio è stato com-



pletato precisando che per l'elaborazione di questa norma uniforme, i partner tariffari dovranno tenere conto anche dei loro obbli-

ghi derivanti dalla revisione della LPD, in particolare del fatto che un progetto del genere dovrà essere oggetto di un'analisi d'impatto relativa alla protezione dei dati personali secondo l'articolo 22 della LPD rivista.





1.5 Lavoro

PERSONALE FEDERALE

Conservazione dei dossier presso l'UST

L'IFPDT ha aperto una procedura di accertamento dei fatti nei confronti dell'Ufficio federale di statistica (UST) in merito alla conservazione in forma cartacea dei dossier del personale della Confederazione oltre il limite legale di dieci anni. Dopo aver preso atto dell'adozione di misure correttive, ha chiuso la procedura senza emanare raccomandazioni.

Nel nostro precedente rapporto d'attività 2021/22 l'IFPDT ha riferito di aver chiarito con l'Ufficio federale di statistica (UST) la questione relativa alla gestione dei dossier cartacei degli ex collaboratori (cfr. 29° rapporto, n. 1.5). L'Incaricato era venuto a conoscenza del fatto che l'UST conservava molti dossier del personale oltre il limite legale di dieci anni. Su richiesta dell'Incaricato, l'UST ha riconosciuto la necessità d'intervenire e gli ha presentato un piano di attuazione e un calendario per ristabilire la legalità. I lavori necessari si sarebbero dovuti concludere entro l'estate del 2022. In considerazione del fatto che gli interventi necessari non

erano ancora stati attuati a tale data e del ritardo accumulato rispetto alla pianificazione, l'IFPDT è stato costretto ad aprire una procedura di vigilanza formale secondo l'articolo 27 LPD, in modo da assicurarsi che l'UST adottasse le misure necessarie per ripristinare la legalità in breve tempo e per informarlo delle misure adottate a tal fine.

Nel novembre del 2022 l'UST ha notificato all'IFPDT la conclusione del mandato per il ripristino della legalità: i vecchi dossier del personale erano stati trasmessi all'Archivio federale, che ne ha confermato la ricezione. I dossier privi di valore archivistico (compreso quello della persona responsabile della segnalazione all'IFPDT) erano stati cancellati e il protocollo di cancellazione trasmesso all'Archivio federale,

che ha già chiarito e concordato la procedura da seguire per i dossier personali relativi al periodo 2012–2017 (eDossier dal 2018).

L'IFPDT ha così ottenuto la conferma che i dossier cartacei con valore archivistico sono stati trasferiti all'Archivio federale e gli altri sono stati distrutti. Di conseguenza, l'IFPDT ha potuto constatare che l'UST non con-



serva più i dossier oltre il limite legale. Sono state inoltre adottate procedure di archiviazione chiare per soddisfare i requisiti legali

in materia di archiviazione e distruzione dei futuri dossier il cui periodo di conservazione è attualmente inferiore a dieci anni.

L'IFPDT ha potuto così chiudere la procedura nel marzo del 2023, senza emanare raccomandazioni, visto che l'UST aveva adottato misure correttive per ripristinare il rispetto del diritto in materia di personale della Confederazione e di protezione dei dati.

1.6 Trasporti

FFS

Sistema di misurazione della frequenza dei clienti nelle stazioni

A ottobre 2022 le FFS hanno informato l'IFPDT in merito a un progetto relativo alla misurazione della frequenza dei clienti nelle stazioni. Poiché il progetto è esposto a elevati rischi potenziali per i passeggeri in questione, prima della sua attuazione le FFS procederanno a una valutazione d'impatto sulla protezione dei dati e la sottoporranno all'IFPDT affinché si esprima al riguardo. A febbraio è apparsa sui media la notizia di un progetto delle FFS riguardante la raccolta di dati nelle stazioni allo scopo di ottimizzare i flussi di persone. Il testo della documentazione del relativo bando di concorso presentava

inizialmente una formulazione in parte fuorviante, per cui le FFS erano state accusate di voler sorvegliare la clientela con la tecnologia del riconoscimento facciale. Le FFS hanno smentito le accuse, assicurando pubblicamente che il sistema di misurazione della frequenza dei clienti utilizza dati anonimi che non verrebbero mai analizzati con riferimento alle persone.

Il responsabile della protezione dei dati delle FFS aveva informato l'IFPDT circa il progetto già a ottobre 2022.



Sebbene il nuovo sistema di misurazione della frequenza della clientela abbia unicamente lo scopo di ottimizzare i flussi di persone nelle stazioni senza identificare i passeggeri – i dati, quindi, non verrebbero utilizzati con riferimento alle persone – il progetto comporta un elevato rischio potenziale di (re)identificazione. Le FFS hanno

quindi assicurato all'IFPDT che prima di avviare il progetto provvederanno a effettuare una valutazione d'impatto sulla protezione dei dati per poi sottoporla allo stesso Incaricato.

Le FFS ritengono che il progetto sia attuabile nel pieno rispetto della legge sulla protezione dei dati. Alla fine del periodo in esame l'IFPDT non era in possesso di informazioni che potessero escluderlo. Si pronuncerà in merito al progetto una volta ricevuta la valutazione d'impatto sulla protezione dei dati.





1.7 Internazionale

EUROPA

Con l'attenuarsi della situazione pandemica, nello scorso anno di attività diverse conferenze internazionali hanno potuto svolgersi di nuovo in presenza. Anche l'IFPDT ha colto quindi l'occasione per partecipare dal vivo a svariati eventi internazionali, in particolare alle riunioni del Consiglio d'Europa, dell'Associazione francofona delle Autorità di protezione dei dati e alla Conferenza europea delle autorità di protezione dei dati personali.

La portata internazionale della protezione dei dati è emersa anche nel passato anno di attività. Nell'ambito della trasmissione transfrontaliera di dati personali, per alcune imprese operanti a livello internazionale sono sorte problematiche giuridiche delicate in relazione al salvataggio dei dati nei cloud e su server all'estero, per le quali in Svizzera non esiste ancora una giurisprudenza (cfr. n. 1.1). A fronte di tale situazione, l'IFPDT segue con particolare interesse gli attuali sforzi dell'UE di emanare una nuova decisione di adeguatezza riguardo agli Stati Uniti.

Consiglio d'Europa

Dopo l'espulsione della Russia dal Consiglio d'Europa, il Comitato consultivo ha dovuto decidere in merito alle condizioni di adesione del suddetto Paese. La trattazione della questione ha causato il rinvio della seduta plenaria di giugno a novembre. Il Comitato consultivo ha approvato inoltre le linee guida sull'identità digitale e ha nominato la rappresentante della Svizzera prima vicepresidente.

Le riunioni del Comitato consultivo della Convenzione 108 e del rispettivo ufficio sono tornate a svolgersi in presenza. La Convenzione 108 è definita «aperta», in quanto possono aderirvi anche parti contraenti che non sono Stati membri del Consiglio d'Europa. In seguito all'espulsione straordinaria della Russia dal Consiglio d'Europa, per tutte le convenzioni aperte si è posta quindi la questione di definire le future condizioni di adesione da parte del suddetto Stato. A fronte della necessità di attendere le disposizioni del Comitato dei Ministri e di accordarsi con altri comitati coinvolti, la seduta plenaria di giugno è stata rinviata a novembre. Pertanto, nel 2022 si è svolta solo un'unica seduta plenaria, anziché le consuete due, e ciò ha causato ritardi nella trattazione di diverse questioni.

Durante l'assemblea plenaria di novembre, il Comitato ha affrontato anzitutto la questione delle condizioni di adesione della Russia. In base alla situazione giuridica di partenza, uno Stato membro che viene espulso in via straordinaria dal Consiglio d'Europa continua a rimanere parte contraente della Convenzione 108, ma l'adesione può essere limitata o sospesa sulla base di regole procedurali. Alla luce di ciò, il Comitato ha adeguato l'ordinamento procedurale e limitato la partecipazione della Russia alle discussioni generali circa l'interpretazione della Convenzione 108. Si è inoltre definito che la Russia non potrà né presiedere il Comitato né essere membro del rispettivo ufficio.

Il Comitato ha inoltre discusso proposte relative allo scambio di dati tra Stati finalizzato alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo nonché a scopo fiscale; ha altresì esaminato clausole contrattuali tipo per la trasmissione transfrontaliera di dati personali. Riguardo a

EUROPA

quest'ultimo aspetto, la rappresentante dell'IFPDT svolge il ruolo di relatrice.

Il Comitato ha incaricato successivamente un gruppo di lavoro di preparare un documento interpretativo riguardo alle eccezioni e alle limitazioni del campo d'applicazione della Convenzione 108 modernizzata (la cosiddetta Convenzione 108+).

Durante l'assemblea plenaria il Comitato ha adottato le linee guida sull'identità digitale nazionale. Queste linee guida, che sono state pubblicate, indicano come vanno interpretati i principi di protezione dei dati della Convenzione 108+ in tale ambito e contengono numerose raccomandazioni per vari soggetti, tra cui organi con funzione legislativa, titolari del trattamento dei dati, produttori di dispositivi, fornitori di servizi e autorità di protezione dei dati.

Durante l'assemblea plenaria si sono svolte infine le elezioni per il rinnovo dell'ufficio del Comitato consultivo. La rappresentante dell'IFPDT, finora membro dell'ufficio, è stata eletta prima vicepresidente. La presidente del Comitato è ora la rappresentante tedesca; la seconda vicepresidente rimane la rappresentante senegalese.

Conferenza europea delle autorità di protezione dei dati a Dubrovnik

In occasione della Conferenza europea delle autorità di protezione dei dati personali si sono discussi gli ultimi sviluppi legati alla comunicazione transfrontaliera dei dati nonché la collaborazione tra le autorità di protezione dei dati in tale ambito. È stata inoltre adottata una risoluzione volta ad accelerare la ratifica della Convenzione 108+.

Dopo una pausa di due anni dovuta alla pandemia, su invito dell'autorità croata si è svolta a Dubrovnik dal 19 al 20 maggio 2022 la 30a Conferenza europea delle autorità di protezione dei dati personali. Oltre a discutere vari aspetti, tra cui gli ultimi sviluppi e i punti ancora in sospeso riguardo alla comunicazione transfrontaliera dei dati, si sono affrontati, sulla scorta di

esempi pratici, i temi relativi alla collaborazione tra le autorità di protezione dei dati e alla sensibilizzazione sulle questioni inerenti alla protezione dei dati.

La Conferenza ha esortato a promuovere la ratifica della «Convenzione 108+», la versione modernizzata della Convenzione 108, quale unico strumento giuridicamente vincolante esistente a livello internazionale nell'ambito della protezione dei dati. I Governi degli Stati membri del Consiglio d'Europa e degli Stati terzi contraenti, l'Unione europea e le organizzazioni internazionali sono stati invitati, mediante una risoluzione, ad accelerare il processo di sottoscrizione e ratifica della Convenzione. Con l'adozione di una seconda risoluzione si mira a garantire la continuità dello svolgimento della Conferenza riguardo a tutte le tematiche prioritarie condivise dalle autorità europee di protezione dei dati. L'IFPDT ha preso parte a un gruppo di lavoro che si concentra sul futuro della Conferenza e che ha proposto la suddetta risoluzione.

EUROPA

European Case Handling Workshop

Il workshop di quest'anno si è concentrato sulla gestione dei reclami ricevuti dalle autorità di protezione dei dati, aumentati sensibilmente dall'entrata in vigore del regolamento europeo sulla protezione dei dati (GDPR).

L'autorità di protezione dei dati georgiana (PDPS) ha organizzato e ospitato a Tbilisi, dal 17 al 19 novembre 2022, lo «European Case Handling Workshop» (workshop europeo sul trattamento dei reclami), un gruppo di lavoro che tratta e discute i vari casi legati alla protezione dei dati.

All'evento hanno preso parte oltre 50 rappresentanti di 26 autorità di protezione dei dati UE ed extra UE, come l'IFPDT. Erano rappresentati anche il Garante europeo della protezione dei dati e quello del Comitato Internazionale della Croce Rossa.

L'IFPDT ospiterà la prossima edizione del workshop, che si terrà a Berna nel novembre 2023.

INTERNAZIONALE

Assemblea mondiale per la protezione della vita privata

Riunitasi in occasione della sessione annuale dal 25 al 28 ottobre 2022, la 44a Assemblea mondiale per la protezione della vita privata (AMVP) ha adottato due risoluzioni. I partecipanti hanno deciso di rafforzare la cooperazione internazionale contro la cibersecurity e di fissare dei principi per regolamentare il riconoscimento facciale.

L'IFPDT ha partecipato virtualmente alla 44a conferenza dell'Assemblea mondiale della vita privata (AMVP) intitolata «Una questione di equilibrio: proteggere la vita privata in un'era di rapidi progressi tecnologici». La conferenza ha evidenziato l'importanza di trovare un equilibrio tra la vita privata e le tecnologie basate sul trattamento dei dati personali.

La parte di sessione aperta al pubblico è stata in gran parte dedicata alle discussioni in materia di protezione della sfera privata e di diritti umani, con gruppi di lavoro sulla sorveglianza in ambito commerciale e sulle sfide della protezione dei dati nelle crisi umanitarie, nonché alle discussioni sulla protezione dei dati e sulla concorrenza. Si è inoltre dato spazio a incontri più tradizionali in cui sono stati affrontati

temi di attualità come l'intelligenza artificiale, il rispetto della vita privata dei bambini e i trasferimenti transfrontalieri di dati.

Durante la sessione a porte chiuse, i partecipanti, tra cui l'IFPDT, hanno deciso di mobilitarsi per rafforzare le capacità di cooperazione internazionale nel campo della cibersecurity e di fissare dei principi per regolamentare il riconoscimento facciale. Parallelamente, l'IFPDT ha guidato in seno a questo gruppo i lavori sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione delle crisi. L'AMVP ha adottato due risoluzioni in questo ambito:

- una sulla cibersecurity, al fine di migliorare la regolamentazione in materia di sicurezza informatica e la comprensione dei danni causati dagli incidenti informatici. In particolare, vengono esaminate le possibilità di cooperazione internazionale, di condivisione delle conoscenze e delle

AMVP

informazioni, comprese la competenza tecnica e le buone prassi, tra i membri dell'AMVP al fine di facilitare le indagini e le attività normative in questo settore. Un apposito gruppo di lavoro proporrà un lavoro esplorativo su questo tema prima dell'autunno 2023;

- l'altra sul riconoscimento facciale. In questa risoluzione sono definiti sei principi e le maggiori aspettative nei confronti delle organizzazioni che intendono utilizzare questa tecnologia.

L'IFPDT ha contribuito attivamente ai lavori ed è stato coautore di entrambe le risoluzioni. Infine, il Commissario federale per la protezione dei dati e la libertà d'informazione di Jersey, Paul Vane, è stato eletto membro del Comitato esecutivo.

Gruppo di lavoro per l'azione umanitaria

La protezione dei dati personali è fondamentale nel contesto dell'azione umanitaria. Per questo motivo il gruppo di lavoro dedicato dell'AMVP (GT AID) ha organizzato varie attività finalizzate a rafforzare la protezione della vita privata in un contesto di emergenza.

In caso di crisi umanitaria, sia essa un conflitto armato o una catastrofe naturale, il rispetto delle norme di diritto non sempre trova piena applicazione. Per questo motivo, a due anni dalla sua istituzione, il Gruppo di lavoro sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario e nella gestione di crisi (GT AID) ha rafforzato le proprie attività.

Nel corso dell'anno in rassegna si è concentrato in particolare sulla modifica del proprio programma di lavoro 2021–2022, in linea con le priorità strategiche dell'AMVP, soprattutto con quelle relative all'evoluzione della protezione della vita privata a livello mondiale. A tal fine, ha distribuito un questionario, aggiornato la cartografia degli attori rilevanti e rafforzato i rapporti con altri organismi e reti internazionali che fanno progredire le questioni legate alla protezione dei dati e alla vita privata.

Conformemente agli obiettivi della risoluzione i membri del GT AID hanno perseguito i seguenti obiettivi generali:

- rispondere alla domanda di cooperazione degli attori interessati per sviluppare linee direttrici e promuovere lo scambio di buone pratiche in materia di protezione dei dati personali e della vita privata, tenuto conto delle specificità dell'aiuto internazionale allo sviluppo, dell'azione umanitaria internazionale e della necessità di agevolare queste attività;
- sviluppare una strategia di patrocinio e mobilitazione presso gli attori interessati.

Per raggiungere questi due obiettivi, il GT AID ha svolto principalmente le seguenti attività:

- stabilire un contatto permanente con gli attori interessati a livello sia bilaterale sia multilaterale e ampliare di conseguenza la portata della voce dell'AMVP rafforzando le relazioni con gli attori dell'aiuto internazionale allo sviluppo;

AFAPDP

- collaborare con gli altri gruppi di lavoro dell'AMVP, per valutare la possibilità di produrre documenti e strumenti di patrocinio per garantire meglio la protezione dei dati personali e della vita privata nelle attività pertinenti;
- promuovere e agevolare, per i Paesi beneficiari di queste attività che non sono dotati di un quadro di protezione dei dati personali e della vita privata, la loro integrazione nella comunità mondiale della protezione dei dati personali e della vita privata.

L'iniziativa prevede svariate attività, come per esempio l'aggiornamento periodico della cartografia dell'aiuto internazionale allo sviluppo e dell'aiuto umanitario internazionale nonché l'identificazione dei Paesi beneficiari di queste attività e non dotati di un quadro di protezione dei dati personali e della vita privata.

Il GT AID è stato istituito in occasione della 42a Assemblea mondiale per la protezione della vita privata (AMVP) nel 2020. Alla conferenza l'IFPDT aveva presentato una risoluzione sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione di crisi. Da allora, presiede il gruppo di lavoro dedicato a questo tema, che conta attualmente oltre 20 membri.

Associazione francofona delle Autorità di protezione dei dati

[Le autorità membri dell'Associazione francofona delle Autorità di protezione dei dati \(AFAPDP\), tra cui l'IFPDT, si sono riunite a Tunisi il 3 e 4 ottobre 2022 in occasione degli incontri francofoni sulla protezione dei dati personali.](#)

Due giornate che hanno riunito le autorità indipendenti di 23 Paesi accomunate da una lingua, una tradizione giuridica e valori comuni. Quest'anno gli incontri erano dedicati principalmente alla nozione d'identità in tutte le sue forme – di regalia o digitale – nonché alle questioni relative alla cooperazione e al ruolo della protezione dei dati personali nell'aiuto internazionale, moderato dall'IFPDT. La presidente del Comitato europeo per la

protezione dei dati (CEPD), Marie-Laure Denis, in veste di segretaria generale dell'AFAPDP, ha invitato in particolare le autorità indipendenti per la protezione dei dati a coordinarsi per far sentire la propria voce nell'attuazione della strategia della Francofonia digitale 2022–2026, in particolare a favore dello sviluppo della protezione dei dati e della regolamentazione dell'economia dei dati.

In contemporanea, l'AFAPDP ha tenuto la propria Assemblea generale annuale, occasione in cui membri hanno adottato la dichiarazione di Tunisi sulla protezione dei dati personali. Questa dichiarazione ribadisce l'importanza della protezione dei dati e sottolinea in particolare che essa costituisce un presupposto per l'esercizio degli altri diritti e delle altre libertà delle persone. In tal senso, la dichiarazione rappresenta un diritto fondamentale nelle nostre società democratiche. I membri hanno inoltre eletto il nuovo Ufficio, di cui fa parte l'IFPDT.



BILATERALE

Accolta di una delegazione tunisina

Nell'ambito del programma TRUST – Transizione responsabile per la società tunisina, la Svizzera intende mettere in luce la propria esperienza per migliorare il buon governo dei servizi pubblici tunisini rafforzandone la responsabilizzazione. Lo scopo è quello di aumentare la fiducia tra i cittadini e le istituzioni.

Nell'ambito di questo programma l'11 maggio 2022 l'Incaricato, Adrian Lobsiger, ha accolto a Berna i propri omologhi tunisini, il presidente dell'ente nazionale per la protezione dei dati personali (INPDP), Chawki Gaddès, e il presidente dell'ente nazionale per l'accesso alle informazioni (INAI), Adnène El Assoued.

Durante gli incontri si è discusso principalmente dei diversi quadri legislativi e delle sfide legate alla crescente digitalizzazione della società. La cooperazione internazionale assume un ruolo imprescindibile nelle attività dell'IFPDT e questo incontro è la prova dell'importanza che le viene attribuita. In particolare, è stata l'occasione per sottolineare il carattere universale e importante nelle nostre società democratiche di questo diritto fondamentale, condizione imprescindibile per esercitare altri diritti fondamentali diversi dalla protezione dei dati.

COOPERAZIONE INTERNAZIONALE

Privacy Symposium a Venezia

Oltre 170 partecipanti, tra cui l'IFPDT, si sono riuniti a Venezia dal 5 al 7 aprile 2022 per la prima conferenza «Privacy Symposium». L'evento mira a promuovere il dialogo internazionale, la cooperazione e la condivisione delle conoscenze sulle disposizioni in materia di protezione dei dati, sulla conformità e sulle tecnologie emergenti.

Dalla protezione dei dati sanitari fino all'intelligenza artificiale, passando per l'informatica quantistica e altri argomenti rilevanti per la vita privata attuale e futura: la conferenza ha dimostrato l'importanza di riunire gli esperti legali, gli operatori del settore e la comunità dei ricercatori. Ha evidenziato le potenzialità possibili quando si riuniscono le forze per sostenere e rafforzare la protezione dei dati oltre i confini e le tecnologie.

Una rappresentante dell'IFPDT è intervenuta per presentare la nuova legge federale sulla protezione dei dati, i più recenti sviluppi in materia di certificazione in Svizzera e il ruolo della protezione dei dati nell'azione umanitaria.

SCHENGEN

Boarder Travel and Law Enforcement Group

Il gruppo «Border Travel and Law Enforcement» (BTLE) del Comitato europeo per la protezione dei dati ha affrontato in presenza dell'IFPDT temi inerenti all'acquis di Schengen, come il riconoscimento facciale nell'ambito del perseguimento penale e la sentenza sull'uso dei dati del codice di prenotazione («Passenger Name Record») pronunciata nel 2022 dalla Corte di giustizia europea. L'IFPDT ha preso parte alle riunioni del Border Travel and Law Enforcement (BTLE), un sottogruppo di esperti del Comitato europeo per la protezione dei dati (EDPB) incaricato di trattare tematiche rilevanti in ambito Schengen.

Il gruppo ha affrontato il tema delle linee guida sull'uso della tecnologia di riconoscimento facciale da parte delle autorità preposte al perseguimento penale, approvate nel maggio 2022 (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement).

Il BTLE ha inoltre discusso la sentenza pronunciata il 21 giugno 2022 dalla Corte di giustizia europea (CGUE) circa l'applicazione della direttiva PNR («Passenger Name Record»), che disciplina l'utilizzo dei dati dei passeggeri aerei (dati PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e

SCHENGEN

della grande criminalità. La CGUE ha imposto agli Stati di limitare assolutamente allo stretto necessario le ingerenze derivanti dall'attuazione della direttiva PNR. In questo modo, le finalità menzionate nella direttiva sarebbero regolamentate in modo esaustivo. L'applicazione del sistema PNR è rivolta unicamente ai reati di terrorismo e alla grande criminalità, sono quindi esclusi gli atti di criminalità ordinari. Il periodo di conservazione generale di cinque anni non deve essere applicato indistintamente a tutti i dati personali dei passeggeri aerei.

In seguito ai lavori preliminari del BTLE, l'EDPB ha adottato la dichiarazione 5/2022 del 13 dicembre 2022 sugli effetti della sentenza della CGUE C-817/19 in merito all'applicazione della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) negli Stati membri. Sebbene la Svizzera non sia vincolata alle sentenze della CGUE, tale sentenza dovrebbe essere tenuta in considerazione nell'attuale processo legislativo riguardante una nuova legge sui dati dei passeggeri aerei (LDPA).

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

I temi affrontati dal gruppo di coordinamento di controllo del SIS sono stati in particolare il nuovo meccanismo di valutazione e di monitoraggio e il nuovo quadro giuridico relativo al SIS.

I gruppi di coordinamento di controllo dei sistemi SIS II, VIS ed Eurodac sono organi istituiti ai sensi del diritto UE incaricati di sorvegliare la protezione dei dati personali nei sistemi d'informazione corrispondenti. Essi sono composti da rappresentanti delle autorità nazionali di protezione dei dati e dal Garante europeo della protezione dei dati.

In virtù del nuovo meccanismo di valutazione e di monitoraggio, gli Stati Schengen, tra cui anche la Svizzera,

saranno sottoposti a valutazione ogni sette anni, e non più con cadenza quinquennale. Parallelamente è prevista la creazione di un pool di esperti. Per le valutazioni Schengen riguardanti la protezione dei dati l'IFPDT ha annunciato un esperto, che nel frattempo è stato nominato per una valutazione.

Il nuovo quadro giuridico del SIS prevede inoltre che il Garante europeo della protezione dei dati e le autorità nazionali di vigilanza, tra cui l'IFPDT, si incontrino almeno due volte l'anno nell'ambito del Comitato europeo per la protezione dei dati (EDPB). È stato inoltre approvato il rapporto d'attività biennale del SIS II SCG.

Com'è già consuetudine da anni in altri ambiti della valutazione Schengen, ora anche in quello della protezione dei dati i futuri esperti dovranno poter intraprendere una formazione. In futuro si dovrà inoltre evitare di far dipendere l'ammissione nel pool di esperti dal superamento del controllo di sicurezza relativo alle persone (CSP), la cosiddetta «security clearance».

SCHENGEN

Gruppo di coordinamento Schengen delle autorità svizzere di protezione dei dati

Durante una seduta del Gruppo di coordinamento Schengen, presieduto dall'IFPDT, si sono confrontate le autorità federali e cantonali di protezione dei dati e quelle del Principato del Liechtenstein.

L'IFPDT ha informato in merito ai risultati dei lavori svolti il 1°-2 giugno e il 22-23 novembre 2022 a Bruxelles dai gruppi di coordinamento di controllo europei riguardo ai sistemi d'informazione SIS II e VIS, mentre le autorità cantonali di protezione dei dati hanno riferito delle esperienze acquisite durante i controlli da loro effettuati.

Un sottogruppo di lavoro, composto da rappresentanti dell'IFPDT e dei Cantoni di Basilea Campagna e Zurigo, ha adeguato le linee guida relative al controllo dell'utilizzo del sistema d'informazione di Schengen sulla base del mutato quadro giuridico europeo. Le linee guida fungono principalmente da strumento di orientamento per le autorità di vigilanza cantonali in occasione dello svolgimento dei controlli. Infine, i rappresentanti hanno condiviso le proprie esperienze e constatazioni riguardo ai controlli effettuati dalle autorità, in particolare quelli dei file di registro. Le esperienze saranno raggruppate in maniera strutturata in un secondo momento.

SCHENGEN

Attività in ambito Schengen a livello nazionale

L'UE rinvia di due anni, al 2025, la valutazione della Svizzera.

La valutazione Schengen della Svizzera, prevista inizialmente dall'UE per i primi mesi del 2023, è stata rinviata di due anni. La decisione è stata presa in seguito all'emanazione del Regolamento (EU) 2022/922 sull'istituzione e sul funzionamento di un meccanismo di valutazione e di monitoraggio per verificare l'applicazione dell'acquis di Schengen, che in ambito UE è applicabile già da febbraio 2023. Ulteriore evoluzione dell'acquis di Schengen, questo regolamento potrà essere applicato in Svizzera solo in un secondo momento, in quanto deve essere prima approvato dall'Assemblea federale e successivamente dovrà essere recepito nel diritto nazionale. Data la successiva applicabilità del regolamento, la Commissione europea ha inoltre deciso di

sottoporre a valutazione la Svizzera nel 2025 e non più nel 2023 come previsto inizialmente.

La Commissione europea ha inoltre invitato gli Stati Schengen a nominare esperti in materia di protezione dei dati per la valutazione di altri Stati. A tale riguardo, l'Ufficio federale di giustizia e il DFAE hanno organizzato il 12 maggio 2022 un incontro tra esperti in materia di valutazione Schengen (SCHEVAL). Oltre a fornire consigli pratici, gli esperti dei vari ambiti specializzati, come cooperazione in materia di polizia, SIS/SIRENE e protezione dei dati, hanno informato i soggetti interessati e i futuri esperti in merito alla collaborazione con la Commissione europea, allo svolgimento di una valutazione e alle offerte formative.

Nell'anno in rassegna l'IFPDT ha inoltre avviato un controllo presso fedpol, quale punto di accesso centrale del C-VIS, in merito all'interrogazione dei dati VIS ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o di altri reati gravi. Per il momento l'Incaricato ha inviato un questionario e ottenuto le risposte alle domande rimaste in sospeso in occasione di una visita in loco. Una volta stilati i fatti, l'IFPDT procederà all'analisi giuridica.



Principio di trasparenza

2.1 In generale

La legge sulla trasparenza ha lo scopo di promuovere la trasparenza sulla missione, l'organizzazione e l'attività dell'amministrazione garantendo al pubblico l'accesso ai documenti ufficiali (cfr. art. 1 LTras). Il principio di trasparenza intende promuovere la fiducia nello Stato e nelle autorità facilitando la comprensione dell'operato dell'Amministrazione e aumentando così l'accettazione dell'operato dello Stato.

Il primo semestre dell'anno in rassegna 2022 è stato ancora influenzato dalle conseguenze degli ultimi strascichi della pandemia. Dalle cifre fornite dall'Amministrazione federale relative alle domande di accesso ai documenti ufficiali pervenute nel 2022 risulta che il bisogno manifestato dai media e dalla società di avere un'informazione specifica e trasparente è tuttora elevato. Seppur leggermente inferiore all'anno precedente, il numero di domande di accesso presentate alle autorità federali nell'anno in rassegna rimane elevato.

In molti casi il trattamento delle domande di accesso ha comportato un notevole impiego di risorse, non da ultimo perché spesso le domande erano estese o si è rivelato necessario un coordinamento fra gli uffici o i dipartimenti. Dalle cifre che seguono (cfr. cap. 2.2) si evince che la tendenza constatata negli ultimi anni relativa a una quota costantemente elevata di casi in cui l'accesso è stato completamente accordato può essere confermata anche per l'anno in rassegna.

Se i richiedenti o terzi interessati non concordano con l'intenzione delle autorità di accordare l'accesso, la legge sulla trasparenza offre loro la possibilità di presentare all'Incaricato una domanda di mediazione. Nell'anno in rassegna sono state presentate 129 domande di mediazione, il 13 per cento in meno rispetto all'anno precedente. L'obiettivo della procedura di mediazione è trovare rapidamente un accordo tra gli interessati. Le misure introdotte a questo scopo con il progetto pilota del 2017 e in particolare il primato delle mediazioni orali si sono dimostrate efficaci anche nel 2022. Dall'analisi delle domande di mediazione evase nell'anno in rassegna si evince che, quando è stato possibile effettuare una

seduta di mediazione, si è giunti a una soluzione consensuale nel 74 per cento dei casi.

A gennaio 2022, a fronte della situazione epidemiologica e dell'obbligo del telelavoro ancora in vigore, l'Incaricato si è visto costretto a rinunciare alle sedute di mediazione, poiché per motivi legati alla protezione delle informazioni non era possibile svolgerle in videoconferenza. In nessuna delle undici procedure di mediazione per le quali si è dovuto rinunciare a una seduta di mediazione a causa della pandemia è stato possibile giungere a un'intesa.

A causa della percentuale ridotta, correlata alla pandemia, di soluzioni consensuali e alla quota elevata di procedure svolte per iscritto, si sono altresì registrati tempi di elaborazione più lunghi per le procedure di mediazione nonché ritardi nella loro esecuzione.

Dalle cifre esaminate emerge quindi che condurre sedute di mediazione alla presenza degli interessati è imprescindibile al raggiungimento dell'obiettivo di svolgere rapidamente le procedure.

La pandemia, il numero costantemente elevato di domande di mediazione e l'accresciuta complessità dei quesiti di natura giuridica hanno fatto sì che l'Incaricato superasse il termine legale di 30 giorni in una percentuale di procedure sempre crescente. L'Incaricato prevede che anche grazie alle risorse aggiuntive stanziare dal Parlamento si riuscirà a ridurre nuovamente i tempi necessari per l'evasione delle domande (cfr. in proposito le informazioni specifiche nel cap. 2.3).

Anche nell'anno in rassegna si sono osservati nuovi tentativi di escludere ulteriori settori dell'attività amministrativa o determinate categorie di documenti dalla legge sulla trasparenza (ad es. piano di salvataggio per il settore dell'energia elettrica, cfr. cap. 2.4). Simili riserve del campo d'applicazione della legge sulla trasparenza provocano un

indebolimento del principio di trasparenza e della trasparenza dell'Amministrazione a cui esso è finalizzato. Nel presente rapporto d'attività l'Incaricato pubblica una panoramica delle riserve previste da leggi speciali ai sensi dell'articolo 4 LTras (cfr. cap. 2.5.)

L'Incaricato constata che il cambio di paradigma avvenuto con la legge sulla trasparenza è attuato e applicato anche attivamente dalla maggior parte dell'Amministrazione. Di fatto le autorità federali soggette alla legge sulla trasparenza non influiscono direttamente sul numero, sull'entità e sui tempi di evasione delle domande di accesso. Nell'anno in rassegna si constata una tendenza all'aumento delle domande di accesso a trascrizioni di comunicazioni in forma elettronica.

Nella sfera d'influenza dell'Amministrazione e dei consulenti sulla trasparenza delle unità amministrative rientra invece l'applicazione delle disposizioni della legge sulla trasparenza e della giurisprudenza in materia. Nella prassi l'Incaricato constata che alcune unità dell'Amministrazione federale sfruttano in maniera insufficiente le possibilità di tutelare i propri interessi al mantenimento del segreto offerte dalla legge e non fanno valere le limitazioni di accesso con il livello di dettaglio richiesto dalla legislazione. L'Incaricato rimanda in tale contesto alla prassi contenuta nelle sue raccomandazioni, pubblicate integralmente nel sito Internet (www.lincaricato.ch), e afferma che nell'anno in rassegna sporadicamente si sono verificati casi in cui l'Amministrazione ha rifiutato di applicare della legge sulla trasparenza: ha ad esempio negato all'Incaricato l'accesso, previsto obbligatoriamente dalla legge senza eccezioni, a documenti oggetto di una domanda di mediazione, impedendogli quindi di svolgere la sua attività di mediazione.

2.2 Domande di accesso. Lieve calo nel 2022

Secondo le cifre comunicate dalle autorità federali, nell'anno in rassegna sono pervenute 1153 domande di accesso (nel 2021 erano 1385), pari a una diminuzione del 15 per cento rispetto al 2021. Ad esse si aggiungono 27 domande di accesso evase nel 2022, ma presentate negli anni precedenti. Complessivamente, in 624 casi (il 53 %) le autorità hanno concesso l'accesso completo ai documenti (nel 2021: 694, pari al 50 %), mentre in 236 casi (20 %) un accesso parziale o differito (nel 2021: 324, pari al 23 %). In 99 casi (8 %) l'accesso è stato del tutto negato (nel 2021: 126, pari al 9 %). Secondo i dati forniti dalle autorità, 53 domande di accesso (5 %) sono state ritirate (nel 2021: 48, pari al 3 %), 69 erano ancora pendenti alla fine del 2022 e in 99 casi non esisteva nessun documento ufficiale.

Anche nei prossimi anni ci si dovrà attendere a un numero elevato di domande analogo a quello degli ultimi anni, sebbene nell'anno in rassegna il bisogno di trasparenza e di informazione, particolarmente spiccato durante la pandemia di coronavirus, si sia smorzato. Le autorità hanno effettuato una statistica delle domande di accesso ai «documenti COVID» e le hanno trasmesse all'Incaricato assieme ad altri

dati (cfr. la statistica evidenziata in giallo delle domande di accesso con riferimento ai documenti COVID). Secondo questi dati, 93 delle 1180 domande di accesso evase (8 %) avevano un rapporto con il coronavirus e risultano quindi in netto calo rispetto all'anno precedente (24 %). L'accesso completo è stato concesso in 29 casi (31 %), quindi con minore frequenza rispetto alla statistica globale. Sempre per quanto riguarda i documenti COVID le autorità hanno concesso un accesso limitato o differito in 35 casi (38 %), quindi più spesso, mentre nei quattro casi (4 %) in cui l'accesso è stato negato la quota risulta dimezzata rispetto alla statistica globale. Sette domande di accesso sono state ritirate, otto erano ancora pendenti alla fine del 2022 e in dieci casi non esisteva alcun documento ufficiale. Presumibilmente l'elaborazione da parte della società civile delle misure amministrative adottate dalle autorità contro la pandemia continuerà e anche nel 2023 potrebbero pervenire domande di accesso e di mediazione collegate al coronavirus.

In sintesi l'Incaricato constata che dal 2015 è stato concesso un accesso completo ai documenti richiesti in almeno il 50 per cento dei casi, mentre nel corso degli anni l'accesso è stato negato in quasi il dieci per cento dei casi.

Dipartimenti e uffici federali

Nel 2022 alcune unità amministrative si sono trovate particolarmente al centro dell'interesse dei media e della società. Dati i compiti che svolgono – e a causa della pandemia di coronavirus come già accaduto negli anni precedenti – soprattutto il DFI (198), il DDPS (294) e il DFAE (164) si sono visti confrontati con un gran numero di domande di accesso. Nel caso del DFI, il 38 per cento dei richiedenti domandava a livello interdipartimentale l'accesso a documenti ufficiali inerenti al coronavirus (nel 2021: 63 %). Secondo le autorità si trattava talvolta di domande molto voluminose e complesse. In numerosi casi è stato necessario organizzare un coordinamento interno tra gli uffici o i dipartimenti.

A livello di Uffici, dalle cifre comunicate si evince che, con 220 casi, l'UF-SPO ha ricevuto nel 2022 il maggior numero di domande di accesso. L'UFSP ne ha segnalate per l'anno in rassegna 91, di cui 57 riguardavano documenti relativi al coronavirus. Seguono l'UFAM con 61 domande e swissmedic e la

SECO con 37 domande ciascuno. 17 autorità hanno segnalato di non aver ricevuto nessuna domanda di accesso nell'anno in rassegna. All'Incaricato stesso sono state inoltrate 15 domande di accesso: in nove casi è stato concesso l'accesso completo, mentre in due casi è stato completamente negato. Una domanda è stata ritirata e tre erano ancora pendenti alla fine del 2022.

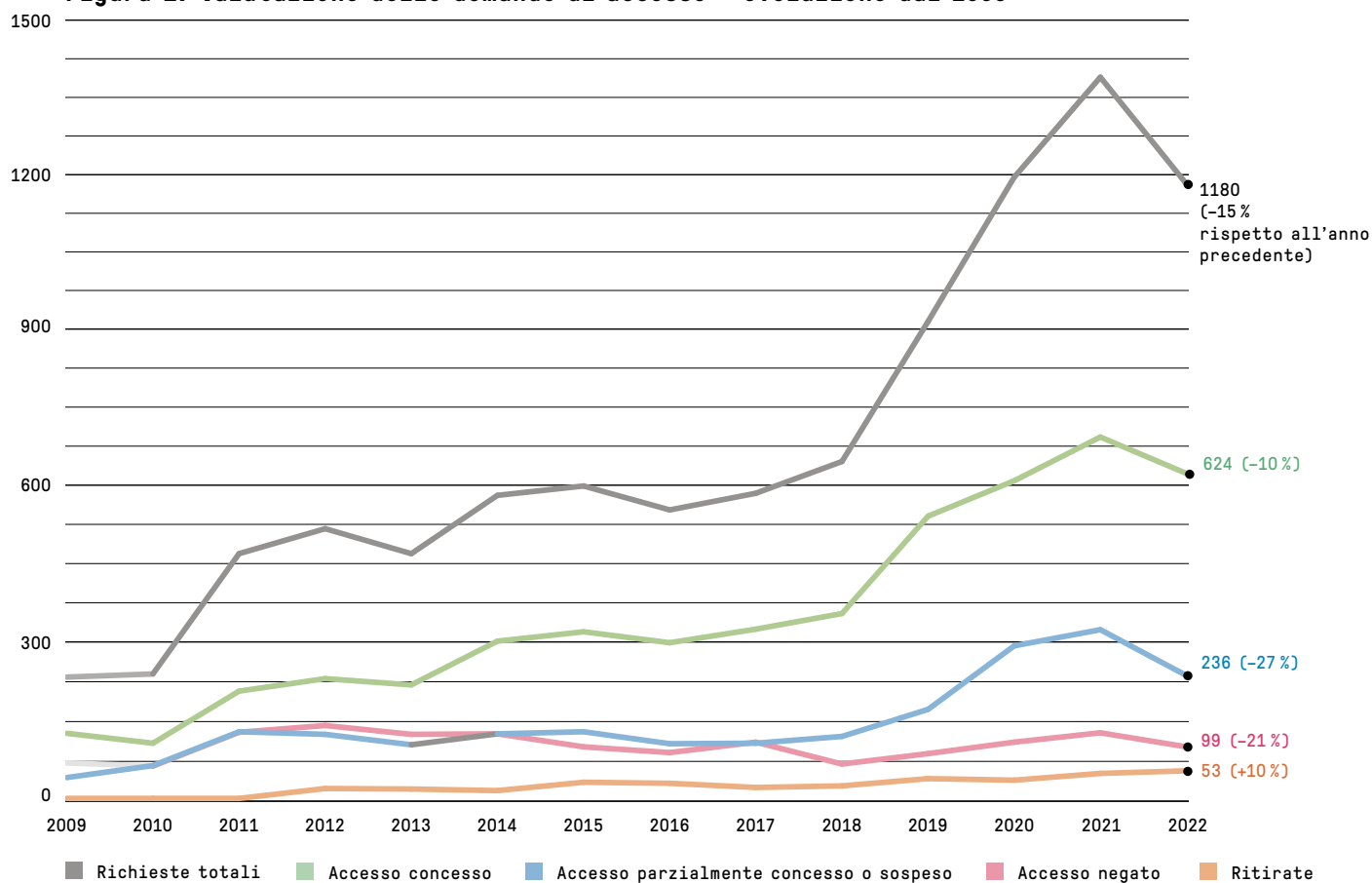
L'importo degli emolumenti riscossi nel 2022 per l'accesso ai documenti ufficiali ammonta a un totale di 24 582,05 franchi, il 65 per cento al di sopra

dell'importo dell'anno precedente (14 924,90 fr.). Mentre il DFAE, il DFF, il DDPS, i Servizi del Parlamento, il Ministero pubblico della Confederazione e la Cancelleria federale non hanno riscosso alcun emolumento, gli altri quattro dipartimenti hanno fatturato ai richiedenti una parte del tempo impiegato (DFI: 19 646,50 fr.; DEFR: 4185,55 fr.; DATEC: 500 fr.; DFGP: 250 fr.). Si noti al riguardo che soltanto per 29 delle 1180 domande di accesso trattate è stato riscosso un emolumento. Come negli anni precedenti, la

riscossione di emolumenti rappresenta un'eccezione: quasi il 98 per cento delle domande di accesso è stato evaso a titolo gratuito.

La prassi amministrativa osservata anche nell'anno in rassegna, secondo cui i documenti ufficiali possono essere consultati in linea di principio gratuitamente, sarà ancorata nella legge sulla trasparenza: il 30 settembre 2022 il Parlamento ha stabilito il principio dell'esenzione dagli emolumenti in relazione all'accesso ai documenti ufficiali. Anche dopo l'entrata in vigore della

Figura 1: Valutazione delle domande di accesso – evoluzione dal 2009





modifica legislativa, la cui data è ancora da definire dal Consiglio federale, potranno essere riscossi emolumenti in via eccezionale, qualora una domanda di accesso richieda un'elaborazione particolarmente onerosa. Nell'ambito della revisione dell'ordinanza sulla trasparenza si dovrà stabilire il numero di ore di lavoro a partire dal quale sarà possibile riscuotere un emolumento per l'evasione di una domanda.

Per quanto riguarda il tempo consacrato al trattamento delle domande di accesso, l'Incaricato rammenta che le autorità non sono tenute a registrarlo e che non esistono prescrizioni applicabili all'intera Amministrazione federale per una registrazione uniforme. I dati forniti all'Incaricato su base volontaria rispecchiano quindi solo in parte le ore di lavoro effettivamente prestate. Secondo tali dati, il tempo impiegato nell'anno in rassegna, ossia 5404 ore, è lievemente diminuito rispetto al 2021 (5562 ore).

Il fatto che l'onere per elaborare le domande di accesso comunicato dalle autorità corrisponde solo in parte al tempo effettivamente impiegato lo si evince, a titolo esemplificativo, dai dati forniti dall'UFSP, al quale sono pervenute molte domande di accesso correlate alla pandemia. Oltre al tempo

impiegato comunicato periodicamente dalle unità specializzate competenti dell'UFSP (443 ore) e al supporto giuridico offerto dalla relativa consulente sulla trasparenza, corrispondente a un tasso d'occupazione del 40 per cento, l'UFSP ha comunicato all'Incaricato per l'elaborazione delle domande di accesso in relazione alla COVID-19 (comprese le procedure di mediazione e di ricorso) un onere ancora elevato, pari ad almeno 3,5 posti a tempo pieno (Full Time Equivalent).

Si constata anche un aumento del tempo necessario comunicato per la preparazione delle procedure di mediazione: 1006 ore rispetto alle 865 dell'anno precedente (cfr. in proposito il 2020 con 569 ore, il 2019 con 473 ore, il 2018 con 672 ore e il 2017 con 914 ore).

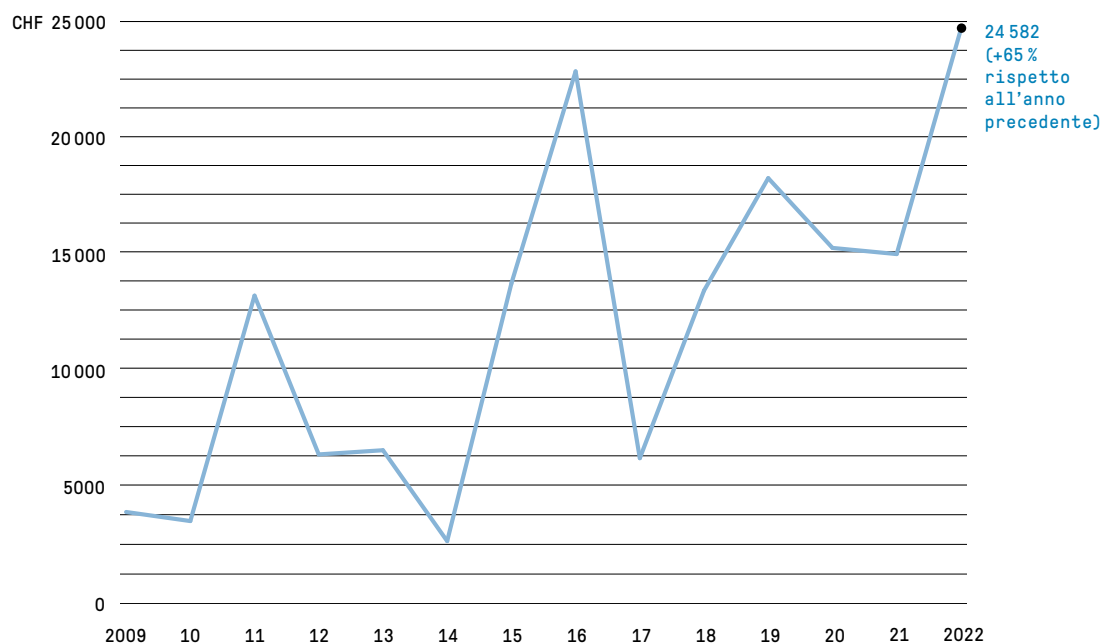
Servizi del Parlamento

In base ai dati comunicati, nell'anno in rassegna ai Servizi del Parlamento non sono pervenute domande di accesso.

Ministero pubblico della Confederazione

Il Ministero pubblico della Confederazione ha comunicato di aver ricevuto sei domande nel 2022. In cinque casi è stato concesso un accesso completo e in un caso è stato completamente negato.

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



2.3 Procedure di mediazione: leggero calo delle domande di mediazione

Nel 2022 sono state presentate all'Incaricato 129 domande di mediazione, il che corrisponde a un calo del 13 per cento rispetto alle 149 ricevute nel 2021. La maggior parte è stata presentata da giornalisti (47) e privati (37). Nei 434 casi in cui l'Amministrazione federale ha rifiutato completamente o in parte l'accesso oppure l'ha differito o ha dichiarato che non erano disponibili documenti ufficiali, 129 domande di mediazione sono state presentate, ossia nel 30 per cento dei casi. Di queste domande 13 (9 %) riguardavano documenti ufficiali correlati al coronavirus.

Nel 2022 l'Incaricato ha evaso 114 domande di mediazione, di cui 92 presentate nello stesso anno e 22 in quello precedente. In 49 casi è stato

possibile giungere a un accordo fra i partecipanti. L'Incaricato ha inoltre emanato 31 raccomandazioni, che hanno permesso di concludere 48 procedure per le quali non era stato possibile giungere a un accordo.

Tra i casi risolti vanno annoverate anche 13 domande che non sono state presentate entro il termine previsto, tre casi in cui non erano soddisfatti i requisiti per l'applicazione della legge sulla trasparenza nonché una domanda di mediazione che è stata ritirata.

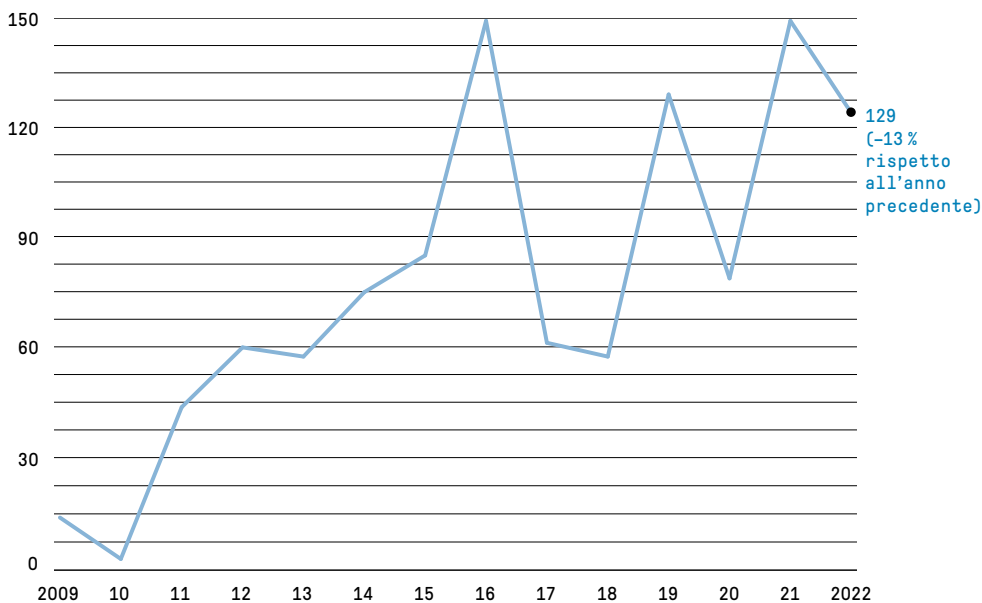
A fine anno 13 procedure di mediazione risultavano sospese, previo accordo tra le parti o su loro richiesta.

Percentuale di soluzioni consensuali

Le soluzioni consensuali (accordi fra le parti) presentano numerosi vantaggi: consentono di chiarire la situazione e di accelerare la procedura di accesso nonché di agevolare l'eventuale futura collaborazione tra coloro che hanno partecipato alla seduta di mediazione.

L'efficacia delle misure introdotte nel 2017 e dello svolgimento delle sedute di mediazione è dimostrata soprattutto dalla proporzione esistente tra le soluzioni consensuali e le raccomandazioni. Nell'anno in rassegna è stato possibile pervenire a 49 soluzioni consensuali e l'Incaricato ha emanato 31 raccomandazioni scritte per risolvere

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



48 casi, il che corrisponde al 51 per cento di soluzioni consensuali. A tal proposito occorre tuttavia chiarire che normalmente si può giungere a una soluzione consensuale solo quando si fa una seduta di mediazione. Nell'anno in rassegna, nelle 42 sedute di mediazione svolte si è potuti giungere a un'intesa in 31 casi (74 %). Come già menzionato nel capitolo 2.1, le misure poste in vigore per contenere il coronavirus hanno fatto sì che nel periodo compreso tra il 20 dicembre 2021¹ e il 3 febbraio 2022², e quindi in 11 casi, si è dovuto rinunciare a condurre sedute di mediazione in presenza degli interessati. In nessuna delle procedure svolte per iscritto si è potuti giungere a un'intesa, e ciò ha inciso negativamente sulle statistiche.

Da quanto esposto sopra si constata quindi che le sedute di mediazione sono indispensabili per raggiungere gli obiettivi legislativi nonché vantaggiose per tutte le parti interessate.

L'Incaricato continuerà a preferire e promuovere questo modo di procedere rispetto alla procedura scritta.

Tabella 1: Soluzioni consensuali

2022 (influsso coronavirus)	51%
2021 (influsso coronavirus)	44%
2020 (influsso coronavirus)	34%
2019	61%
2018	55%

Durata delle procedure di mediazione

La tabella sottostante è suddivisa in tre righe in base alla durata della procedura. Occorre precisare che la durata di elaborazione non tiene conto del periodo in cui una procedura di mediazione è sospesa su proposta o previo accordo dei partecipanti. Una sospensione si verifica in particolare quando, dopo la seduta, l'Amministrazione torna considerare la propria posizione o se deve consultare terzi interessati. Se la seduta viene differita su richiesta di una parte (ad es. a causa di assenza per vacanze, malattia ecc.), anche il periodo che intercorre tra il termine previsto inizialmente e il nuovo termine fissato o il conseguente prolungamento della procedura non è conteggiato nella durata di elaborazione.

¹ Art. 20 dell'ordinanza COVID-19 situazione particolare; DCF del 17 dicembre 2022.

² Art. 25 cpv. 5 dell'ordinanza COVID-19 situazione particolare; DCF del 2 febbraio 2022; Provvedimenti e ordinanze (admin.ch).

Dalla tabella si evince che – in parte ancora a causa della pandemia – solo il 26 per cento delle procedure di mediazione concluse nel 2022 è stato evaso entro il termine legale di 30 giorni. Nel 41 per cento dei casi la procedura di mediazione è durata da 31 a 99 giorni e nel 33 per cento dei casi persino più di 100 giorni.

Si noti che, delle 29 domande di mediazione evase entro il termine di 30 giorni, solo in 17 casi (59 %) la procedura si è conclusa con un'intesa o una raccomandazione e di conseguenza ha avuto luogo un esame materiale dell'oggetto della mediazione. Nei rimanenti 12 casi (41 %) non vi è stata alcuna valutazione nel merito; si è trattato in particolare di casi palesemente esclusi dal campo di applicazione della legge sulla trasparenza o che non adempivano ai requisiti formali per avviare una procedura di mediazione.

Come esposto in precedenza, anche nell'anno in rassegna la pandemia ha causato un allungamento della durata delle procedure e prolungato ulteriormente i ritardi nel disbrigo delle procedure. Oltre a ciò va considerato che il numero delle domande di mediazione pervenute è soggetto a oscillazioni. Se, ad esempio, a marzo e ad agosto è giunto all'Incaricato un numero molto elevato di domande (rispettivamente 21 e 27), a giugno ne sono state inoltrate solo tre e a novembre addirittura nessuna.

Negli anni precedenti il termine legale di 30 giorni per evadere le procedure di mediazione ha potuto essere di norma rispettato nei casi in cui le sedute venivano concluse con successo con un'intesa fra le parti. Nell'anno in rassegna ciò è stato possibile solo nel 29 per cento dei casi (rispetto al 60 per cento dell'anno precedente). Se l'Incaricato ha dovuto emanare una raccomandazione scritta in mancanza di una soluzione consensuale, ha potuto farla pervenire agli interessati entro 30 giorni dalla ricezione della domanda, quindi entro il termine legale, solo in tre casi (6 %).

Tra le cause più frequenti del superamento del termine si evidenziano delle domande di accesso estremamente voluminose, il numero elevato di terzi coinvolti nella procedura o la complessità delle questioni giuridiche, tecniche o politiche. Questi motivi valgono anche per i 38 casi il cui trattamento ha superato i 100 giorni. Il rispetto dei termini è stato reso ancora più difficoltoso dalla quantità di documenti o dal numero di persone coinvolte. Poiché in questi casi il trattamento risulta particolarmente dispendioso, secondo l'articolo 12a dell'ordinanza sulla trasparenza (OTras; RS 152.31) l'Incaricato è libero di prolungare ragionevolmente il termine legale.

Il legislatore ha concepito la mediazione come una procedura informale e non pregiudiziale intesa a comporre amichevolmente le controversie. L'esperienza mostra invece che quando i richiedenti o i terzi consultati coinvolgono

Tabella 2: Tempo di elaborazione delle procedure di mediazione

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

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

una rappresentanza legale sin dalla procedura di accesso e poi di mediazione, ciò non favorisce una soluzione semplice, pragmatica e rapida.

Numero di casi pendenti

I dati riportati di seguito evidenziano il numero di casi pendenti alla fine dei rispettivi anni in rassegna. A inizio gennaio 2023 erano pendenti 41 procedure di mediazione, di cui 13 sospese (una risalente al 2019 e una al 2020, tre al 2021 e otto all'anno in rassegna). 16 di questi casi hanno potuto essere conclusi entro la chiusura di redazione del presente rapporto.

Tabella 3: Procedure di mediazione pendenti

Fine 2022	41 (di cui 16 evase entro la chiusura di redazione e 13 sospese)
Fine 2021	27 (di cui 14 evase entro la chiusura di redazione e 8 sospese)
Fine 2020	17 (di cui 9 evase entro la chiusura di redazione e 8 sospese)
Fine 2019	43 (di cui 40 evase entro la chiusura di redazione e 3 sospese)
Fine 2018	15 (di cui 13 evase a febbraio 2019 e 2 sospese)



2.4 Procedura legislativa

CIBER SICUREZZA

Modifica della legge sulla sicurezza delle informazioni (LSIn)

La consultazione avviata dal DFF concerne l'avamprogetto relativo alla modifica della legge sulla sicurezza delle informazioni al fine di iscrivervi l'obbligo di notificare i ciberattacchi contro le infrastrutture critiche. Questa modifica comporta delle restrizioni al principio della trasparenza.

In risposta al moltiplicarsi dei ciberincidenti che colpiscono sia i privati e le imprese che le autorità, il Consiglio federale ha incaricato il DFF di elaborare un avamprogetto al fine di istituire le basi legali necessarie per introdurre l'obbligo di notificare i ciberattacchi contro le infrastrutture critiche.¹

Tale obbligo intende permettere al Centro nazionale per la cibersicurezza (NCSC) di avere una migliore visione d'insieme dei ciberattacchi in Svizzera,

di sostenere gli interessati nella gestione di questi attacchi e di avvertire tutti gli altri gestori di infrastrutture critiche. Oltre all'obbligo di notifica, nella LSIn dovrebbero essere definiti anche i compiti del Centro nazionale per la cibersicurezza (NCSC) e la sua funzione in qualità di servizio centrale di notifica.

L'avamprogetto elaborato dal DFF è stato sottoposto alla consultazione delle cerchie interessate. Una minoranza dei partecipanti (secondo il DFF, 6 su 102) ha chiesto di escludere le notifiche effettuate al NCSC dalla legge sulla trasparenza. Questa richiesta è stata presa in considerazione introducendo una disposizione speciale ai sensi dell'articolo 4 LTras nella LSIn: il nuovo articolo 4 capoverso 1bis prevede che le

informazioni relative a terzi di cui il NCSC viene a conoscenza tramite la ricezione e l'analisi di segnalazioni non possano essere rese accessibili secondo la LTras.

Benché capisca l'importanza che le notifiche e il loro trattamento rivestono ai fini della sicurezza della Svizzera, l'IFPDT si è opposto all'introduzione di questa nuova disposizione speciale ritendendola sproporzionata. In effetti essa viola il principio di trasparenza poiché impedisce ai cittadini di accedere a informazioni che hanno un legame diretto con lo svolgimento di un compito centrale del NCSC e di effettuare in tal modo il controllo statale voluto dal legislatore in un ambito al centro delle preoccupazioni della popolazione. L'IFPDT ha considerato in particolare che le numerose e svariate eccezioni (p. es. l'art. 7 cpv. 1 lett. c LTras che protegge la sicurezza interna o esterna della Svizzera, l'art. 7 cpv. 1 lett. g LTras che protegge i segreti d'affari o l'art. 7 cpv. 2 LTras che protegge la sfera privata) previste nella legge sulla trasparenza siano sufficienti per tutelare i diversi interessi. Per questi motivi l'IFPDT non ravvisa in che modo l'applicazione della legge sulla trasparenza

¹ Procedure di consultazione concluse – 2022 (admin.ch)

SETTORE DELL'ENERGIA ELETTRICA

possa ostacolare le funzioni del NCSC in quanto centrale di notifica e ha chiesto di stralciare la disposizione speciale.

Il DFF ha tenuto parzialmente conto del parere dell'IFPDT e ha limitato la portata dell'eccezione riformulando l'articolo 4 capoverso ibis nel modo seguente: «Le informazioni relative a terzi di cui il Centro nazionale per la cibersicurezza (NCSC) viene a conoscenza tramite la ricezione e l'analisi di segnalazioni secondo il capitolo 5 non possono essere rese accessibili secondo la LTras. Non sono considerati terzi le autorità, le organizzazioni e le persone menzionate all'articolo 2 capoverso 1 LTras.». Nonostante questa precisazione accolta favorevolmente dall'IFPDT, la divergenza è stata mantenuta per i motivi di cui sopra ed è riportata sia nel messaggio che nella proposta al Consiglio federale.

Avamprogetto della legge federale concernente un piano di salvataggio per il settore dell'energia elettrica

Le informazioni messe a disposizione dalle imprese di rilevanza sistemica del settore dell'energia elettrica in relazione alla fornitura di aiuti finanziari sono escluse dal diritto di accesso previsto dalla legge sulla trasparenza. Durante la procedura legislativa l'Incaricato si era pronunciato, senza successo, contro tale limitazione del principio di trasparenza.

Il cosiddetto piano di salvataggio per il settore dell'energia elettrica, ancorato nella legge federale sugli aiuti finanziari concessi a titolo sussidiario per salvare le imprese di rilevanza sistemica del settore dell'energia elettrica (LAISE), intende contribuire a garantire l'approvvigionamento energetico in Svizzera, disciplinando in particolare gli aiuti finanziari per le imprese di rilevanza sistemica del settore dell'energia elettrica. Secondo l'articolo 20 capoverso 4 LAISE l'accesso in virtù della legge sulla trasparenza alle informazioni e ai dati messi a disposizione dalle imprese di rilevanza sistemica è escluso. Nel messaggio è stabilito espressamente che si tratta di una disposizione speciale ai sensi dell'articolo 4 lettera a LTras.

Conformemente all'articolo 4 LTras, restano salve le disposizioni previste in altre leggi federali che dichiarano segrete determinate informazioni (lett. a) o prevedono condizioni divergenti da quelle previste dalla legge sulla trasparenza per l'accesso a determinate informazioni (lett. b). Pertanto le disposizioni della legge sulla trasparenza non sono applicabili per quanto riguarda l'accesso a tali informazioni. Ogni volta che viene introdotta una simile riserva si indebolisce sia il principio di trasparenza sia la trasparenza dell'Amministrazione a cui esso è finalizzato.

Poiché l'Amministrazione non ha coinvolto l'Incaricato nella consultazione degli uffici, quest'ultimo si è pronunciato contro l'introduzione di tale disposizione speciale soltanto nel quadro della procedura di corapporto e di consultazione, facendo presente che la legge sulla trasparenza persegue l'obiettivo di assicurare la tracciabilità dell'operato dell'Amministrazione e di

impedirne la cattiva gestione in relazione alla concessione di crediti e sovvenzioni statali ai danni dei contribuenti.

Il DATEC giustifica la limitazione del principio di trasparenza affermando che le informazioni e i dati messi a disposizione sono di carattere sensibile e spesso possono contenere segreti di fabbricazione o d'affari ai sensi della legge sulla trasparenza. Durante la procedura di consultazione l'Incaricato ha fatto notare, invano, che i legittimi interessi privati rimangono tutelati anche in caso di applicazione della legge sulla trasparenza. Infatti, essa garantisce esplicitamente la tutela dei segreti d'affari (art. 7 cpv. 1 lett. g LTras) e della sfera privata nonché dei dati personali di persone fisiche e giuridiche (art. 7 cpv. 2 e art. 9 cpv. 2 LTras nonché art. 19 LPD). L'Incaricato ha fatto notare infine che la legge sulla trasparenza verrebbe svuotata della sua sostanza, se alla popolazione venisse negata la possibilità di accedere ai documenti proprio nel contesto della delicata esecuzione di aiuti finanziari, com'è già accaduto nel caso della legge sulle fidejussioni solidali COVID-19 (cfr. 28° rapporto, n. 2.4).

Necessità di una revisione della legge federale sull'archiviazione

Il coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza e quindi la questione di quale diritto vada applicato in caso di consultazione dei documenti archiviati soggetti alla LTras durante il termine di protezione, deve essere chiarita con un adeguamento dell'ordinanza sull'archiviazione. A giudizio dell'Incaricato non è possibile chiarire questi aspetti in modo giuridicamente vincolante con una revisione parziale dell'ordinanza sull'archiviazione. La legge sull'archiviazione (LAr) e la legge sulla trasparenza disciplinano due diverse procedure di accesso a informazioni ufficiali, che per alcuni aspetti fondamentali sono strutturate in

maniera differenziata. La legge sull'archiviazione, entrata in vigore il 1° ottobre 1999, prevede ampi termini di protezione, che non da ultimo sono espressione del principio di segretezza applicato in quel periodo in seno all'Amministrazione federale. Solo a distanza di pochi anni il legislatore si è occupato del cambio di paradigma relativo al principio di trasparenza (con l'introduzione dell'informazione passiva, ovvero accesso su richiesta) senza però esprimersi in merito alla gestione dei documenti ufficiali soggetti alla legge sulla trasparenza dopo il periodo di archiviazione, pertanto non esistono disposizioni vincolanti sul coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza, né sul piano materiale né su quello formale. Valutare se e in che misura vada applicata la legge sulla trasparenza e/o la legge sull'archiviazione in caso di consultazione di documenti ufficiali archiviati ai sensi della LTras durante il termine di protezione genera una notevole incertezza giuridica che riguarda in egual modo le autorità incaricate dell'applicazione del diritto e i privati.

Una valutazione condotta su incarico dell'Archivio federale identifica nel corrispondente rapporto finale la necessità d'intervento definendo nove linee d'azione e formulando diverse raccomandazioni. Per quanto riguarda il coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza è stata formulata fra l'altro una raccomandazione affinché il legislatore stabilisca esplicitamente quale diritto si debba applicare alla consultazione secondo la LTras di documenti ufficiali archiviati durante il termine di protezione.

Secondo il parere dell'Archivio federale, le raccomandazioni formulate nel rapporto di valutazione della LAr – e quindi anche il coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza – possono essere attuate con una gestione adeguata della prassi

d'archiviazione e un adeguamento dell'ordinanza sull'archiviazione da parte del Consiglio federale. L'Archivio federale non ritiene quindi necessaria una revisione della legge sull'archiviazione.

Secondo l'Incaricato la problematica centrale risiede nella mancanza di un coordinamento a livello giuridico tra la legge sull'archiviazione e la legge sulla trasparenza e/o nelle procedure di accesso alle informazioni ufficiali, che talvolta presentano differenze significative. In futuro il numero di dossier archiviati contenenti documenti ufficiali soggetti alla legge sulla trasparenza aumenterà: si prevede quindi un sostanziale aumento delle domande da esaminare. Se non si chiariranno le questioni riguardanti il coordinamento a livello di legge formale, le autorità incaricate di applicare il diritto, e quindi anche l'Incaricato, rischiano di esporsi nel singolo caso all'accusa di by-passare la volontà del legislatore formulata nella LAr (con ampi termini di pro-

tezione) e nella LTras (trasparenza dell'Amministrazione), per il fatto di (non) aver applicato la legge sull'archiviazione o la legge sulla trasparenza. In sostanza, nell'ambito della consultazione degli uffici relativa al documento interlocutorio riguardo alla necessità di una revisione della legge sull'archiviazione, l'Incaricato ha affermato che il coordinamento tra la legge sull'archiviazione e la legge sulla trasparenza riveste una notevole importanza per via delle ampie conseguenze che ne conseguono e che quindi richiede una legittimazione da parte del legislatore. Di conseguenza reputa insufficiente il livello normativo dell'ordinanza del Consiglio federale previsto per regolamentare l'aspetto del coordinamento.

Entrata in vigore della legge sul riciclaggio di denaro e della relativa ordinanza

L'Ufficio centrale di controllo dei metalli preziosi viene escluso dal campo d'applicazione personale della legge sulla trasparenza nell'ambito della propria attività di vigilanza rilevata dalla FINMA. L'Incaricato si è opposto, invano, contro questa ulteriore limitazione del principio di trasparenza.

L'Ufficio centrale di controllo dei metalli preziosi, annesso all'Ufficio federale della dogana e della sicurezza dei confini, regola tutti gli affari risultanti dalla vigilanza del commercio in metalli preziosi e in lavori di metalli preziosi. Conformemente alla revisione della legge sul riciclaggio di denaro approvata nel 2021, l'Ufficio centrale assume la funzione di autorità di vigilanza in materia di riciclaggio di denaro rilevandola dall'Autorità federale di vigilanza sui mercati finanziari FINMA e dagli organismi di autodisciplina (OAD).

Nell'ambito della revisione dell'ordinanza sul riciclaggio di denaro si è deciso di escludere dal campo d'applicazione personale della legge sulla

trasparenza l'attività di vigilanza dell'Ufficio centrale legata ai saggiatori del commercio che trattano metalli preziosi bancari sulla base di quanto disposto all'articolo 2 capoverso 2 LTras o al relativo articolo 1a dell'ordinanza sulla trasparenza. La Segreteria di Stato per le questioni finanziarie internazionali (SFI), responsabile della modifica dell'ordinanza sul riciclaggio di denaro, ha motivato la decisione affermando che per i soggetti sottoposti a vigilanza, in precedenza della FINMA / degli OAD e ora dell'Ufficio centrale, devono valere prevalentemente le stesse regole applicate in passato.

Nell'articolo 2 capoverso 2 LTras il legislatore ha escluso la Banca nazionale svizzera e la FINMA dal campo d'applicazione personale della legge sulla trasparenza. Per contro, nell'ambito della revisione della legislazione in materia di riciclaggio di denaro e in

considerazione del principio di trasparenza, ha rinunciato a escludere l'Ufficio centrale di controllo dei metalli preziosi e le relative funzioni di vigilanza rilevate dalla FINMA. Il legislatore ha così assoggettato l'attività di vigilanza dell'Ufficio centrale al principio di trasparenza valido sostanzialmente per l'Amministrazione federale. Secondo l'Incaricato non vi è quindi alcuna volontà del legislatore di limitare il campo d'applicazione personale della LTras.

L'Incaricato ha inoltre fatto presente alla SFI che la formulazione dell'articolo 2 capoverso 2 LTras è chiara ed esclude in modo inequivocabile dal campo d'applicazione personale della legge sulla trasparenza (solo) la FINMA e la BNS e anche i materiali corrispondenti non contengono elementi che lasciano presupporre che questa disposizione possa essere integrata nell'ordinanza sulla trasparenza. L'Incaricato ritiene che l'articolo 2 capoverso 2 LTras non sia una base giuridica sufficiente o appropriata per escludere l'attività di vigilanza dell'Ufficio centrale dall'ambito d'applicazione personale della legge sulla trasparenza mediante la creazione di un'apposita disposizione d'ordinanza.

LEGGE SUI PRODOTTI DEL TABACCO

Revisione parziale della legge federale sui prodotti del tabacco e sulle sigarette elettroniche (LPTab)

Nel terzo trimestre del 2022 il Consiglio federale ha avviato una consultazione su una revisione parziale della LPTab, la quale prevede fra l'altro che gli importi delle spese pubblicitarie notificate dalle imprese all'UFSP non siano subordinate al principio della trasparenza.

L'Incaricato si oppone.

Il 1° ottobre 2021 il Parlamento aveva approvato la nuova legge sui prodotti del tabacco e sulle sigarette elettroniche (LPTab). In seguito all'adozione, il 13 febbraio 2022, dell'iniziativa popolare «Sì alla protezione dei fanciulli e degli adolescenti dalla pubblicità per il tabacco (Fanciulli e adolescenti senza pubblicità per il tabacco)», l'UFSP ha elaborato una serie di disposizioni volte a introdurre nella LPTab restrizioni supplementari alla pubblicità, alla promozione e alla sponsorizzazione relativi

ai prodotti del tabacco e alle sigarette elettroniche. L'avamprogetto prevede di escludere dal principio di trasparenza gli importi delle spese sostenute per la pubblicità, la promozione e la sponsorizzazione dichiarate all'UFSP da parte delle singole imprese. Questa esigenza è motivata da un interesse privato delle imprese interessate, ossia dalla tutela dei loro segreti d'affari.

Durante la consultazione degli Uffici, l'Incaricato si è detto contrario all'introduzione di tale eccezione considerandola superflua poiché la LTras prevede già oggi una norma derogatoria a tutela dei «segreti professionali, di fabbricazione o d'affari» (art. 7 cpv. 1 lett. g). L'Incaricato ritiene che la LTras tuteli e consideri in misura sufficiente l'interesse privato delle imprese in questione. Inoltre, nell'ambito della lotta al tabagismo l'interesse pubblico alla trasparenza è elevato e lo scopo principale della LPTab è proprio quello di ridurre il tabagismo.

L'avamprogetto posto in consultazione dal Consiglio federale ha tuttavia mantenuto questa divergenza. La trasmissione del messaggio al Parlamento è prevista per il primo trimestre del 2023.

ECONOMIA

Nuova legge federale sulla verifica degli investimenti esteri

Nel secondo trimestre del 2022 la Segreteria di Stato dell'economia (SECO) ha avviato una procedura di consultazione per l'introduzione della LVI. La limitazione del principio di trasparenza, prevista in un primo momento, è stata stralciata dal progetto in consultazione.

In adempimento della mozione 18.3021 Rieder, il 18 maggio 2022 il Consiglio federale ha avviato una consultazione relativa alla nuova Legge federale sulla verifica degli investimenti esteri (LVI). La verifica degli investimenti è volta a prevenire pericoli o minacce per l'ordine e la sicurezza pubblici, causati dall'acquisizione di imprese svizzere da parte di investitori esteri. La responsabilità per l'attuazione della verifica degli investimenti e per il coordinamento





con le unità amministrative cointeresate è affidata alla SECO. L'avamprogetto originario della SECO prevedeva che le informazioni comunicate e i documenti inoltrati nell'ambito della sua attività di verifica degli investimenti non fossero accessibili al pubblico. L'intenzione era di formulare una riserva totale in merito all'applicabilità della legge sulla trasparenza, giustificata dal trattamento di dati sensibili, come ad esempio i segreti d'affari o le informazioni messe a disposizione dal Servizio delle attività informative della Confederazione (SIC).

In una preconsultazione l'Incaricato si è pronunciato contro l'introduzione della riserva e ha fatto presente l'elevato interesse pubblico della verifica degli investimenti da parte della SECO. Per la tutela di possibili segreti d'affari degli investitori e di informa-

zioni messe a disposizione dal SIC, la legge sulla trasparenza prevede già deroghe di accesso esplicite (art. 7 cpv. 1 lett. g art. 4 LTras in combinato disposto con l'art. 67 LAIn). Inoltre risultano già protetti eventuali interessi pubblici riguardanti il singolo caso, come l'esecuzione appropriata di misure concrete di un'autorità (art. 7 cpv. 1 lett. b LTras), gli interessi della politica economica o monetaria della Svizzera (art. 7 cpv. 1 lett. f LTras) nonché la formazione dell'opinione di un'autorità in caso di imminenti decisioni (art. 8 cpv. 2 LTras). La riserva è stata stralciata dal progetto in consultazione.

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

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

all'articolo 4 LTras, restano salve le disposizioni previste in altre leggi federali che dichiarano segrete determinate informazioni (lett. a) o prevedono condizioni divergenti da quelle previste dalla legge sulla trasparenza

per l'accesso a determinate informazioni (lett. b). Pertanto le disposizioni della legge sulla trasparenza non sono applicabili per l'accesso a tali informazioni.

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

Atto normativo (forma breve) e abbreviazione	n. RS	Art. / cpv.	Data di entrata in vigore
Revisione parziale della LAMal (misure di contenimento dei costi - pacchetto 2)	832.10	Art. 52e AP-LAMal	Messaggio del 7 settembre 2022 (progetto non ancora trattato dal Parlamento)
Legge sulla sicurezza delle informazioni (LSIn)	128	Art. 4 cpv. 1 bis	(prevista per 1° gennaio 2024)
Ordinanza concernente mutui supplementari a sostegno della liquidità e la concessione da parte della Confederazione di garanzie in caso di dissesto per mutui a sostegno della liquidità erogati dalla Banca nazionale svizzera a banche di rilevanza sistemica	952.3	Art. 6 cpv. 3	16 marzo 2023
Legge federale sugli aiuti finanziari concessi a titolo sussidiario per salvare le imprese di rilevanza sistemica del settore dell'energia elettrica (LAiSE)	734.91	Art. 20 cpv. 4	1° ottobre 2022
Legge federale sugli appalti pubblici (LAPub)	172.056.1	Art. 48 cpv. 1 (accesso esplicito prescritto); Art. 11 lett. e (si applica solo come disposizione speciale durante la procedura di aggiudicazione)	1° gennaio 2021
Legge sulle fidejussioni solidali COVID-19 (LFiS-COVID-19)	951.26	Art. 12 cpv. 2	19 dicembre 2020
Legge federale sull'organizzazione dell'infrastruttura ferroviaria (OIF) (atto mantello)			
Legge federale sulle ferrovie (Lferr)	742.101	Art. 14 cpv. 2	1° luglio 2020
Legge sugli impianti a fune (LIFT)	743.01	Art. 24e	1° luglio 2020
Legge sul trasporto di viaggiatori (LTV)	745.1	Art. 52a	1° luglio 2020
Legge federale sulla navigazione interna (LNI)	747.201	Art. 15b	1° luglio 2020
Legge federale sulle attività informative (LAIIn)	121	Art. 67	1° settembre 2017
Legge sulle derrate alimentari (LDerr)	817.0	Art. 24 Disposizione speciale ai sensi del messaggio concernente la legge federale sulle derrate alimentari e gli oggetti d'uso del 25 maggio 2011	1° maggio 2017
Legge federale sulla promozione della ricerca e dell'innovazione (LPRI)	420.1	Art. 13 cpv. 4 (cfr. sentenza del TAF n. A-6160/2018 del 4 novembre 2019 consid. 4.)	1° gennaio 2014

Atto normativo (forma breve) e abbreviazione	n. RS	Art. / cpv.	Data di entrata in vigore
Legge sulle banche (LBCR)	952.0	Art. 47 cpv. 1	1° gennaio 2009 (lett. a e b) e 1° luglio 2015 (lett. c)
Legge sui brevetti (LBI) Ordinanza sui brevetti (OBI)	232.14 232.141	Art. 90 OBI, che si basa sull'art. 65 cpv. 2 LBI (cfr. sentenza del TF n. 4A_249/2021 del 10 giugno 2021)	1° luglio 2008
Entrata in vigore della legge sulla trasparenza			1° luglio 2006
Legge sul Parlamento (LParl)	171.10	Art. 47 cpv. 1 (cfr. sentenza del TAF n. A-6108/2016 del 28 marzo 2018 consid. 3.1.)	1° dicembre 2003
Legge sul controllo dei beni a duplice impiego (LBDI)	946.202	Art. 4 e 5 (cfr. sentenza del TAF n. A-5133/2019 del 24 novembre 2021 consid. 5.3.2.4.)	1° ottobre 1997
Legge federale sull'imposta federale diretta (LIFD)	642.11	Art. 110 cpv. 1	1° gennaio 1995
Legge federale sull'imposta preventiva (LIP)	642.21	Art. 37 cpv. 1	1° gennaio 1967
Legge federale sulle tasse di bollo (LTB)	641.10	Art. 33 cpv. 1	11° luglio 1974
Legge sull'IVA (LIVA)	641.20	Art. 74 cpv. 1	1° gennaio 2010
Legge federale sull'armonizzazione delle imposte dirette dei Cantoni e dei Comuni (LAID)	642.14	Art. 39 cpv. 1 Cfr. GAAC 2016.1 (pag. 1-14), edizione del 26 gennaio 2016: «Secret fiscal et accès à des documents officiels»	1° gennaio 1993
Legge sulla statistica federale (LStat)	431.01	Art. 14 (cfr. sentenza del TF n. 1C_50/2015 del 2 dicembre 2015 consid. 4.2. e segg.)	1° agosto 1993

(Elenco non esaustivo)

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

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

(Elenco non esaustivo)

L'IFPDT



3.1 Compiti e risorse

Prestazioni e risorse nell'ambito della protezione dei dati

Effettivi del personale

Nel suo messaggio concernente la revisione totale della LPD il Consiglio federale aveva prospettato all'IFPDT la creazione di risorse supplementari nella misura di 9-10 posti (FF 2017 6154). In un primo momento, con la nuova legge sulla protezione dei dati in ambito Schengen (LPDS, RS 235.3), il legislatore federale ha anticipato un aspetto parziale della revisione totale della LPD. Dopo aver posto in vigore la nuova legge al 1° marzo 2019, il Consiglio federale ha assegnato all'IFPDT tre ulteriori posti per l'attuazione dei nuovi compiti e delle nuove competenze, di modo che nel 2020 l'effettivo del personale è stato aumentato da 24 a 27 posti a tempo pieno. Considerato che l'entrata in vigore della LPD riveduta era prevista per il 2022, nella primavera del 2021 l'IFPDT ha proposto al Consiglio federale di autorizzare i rimanenti sei posti a tempo pieno, i quali sono stati approvati il 28 aprile 2021. L'effettivo di personale impiegato per la protezione dei dati è aumentato così di altre cinque unità (un posto è stato

trasferito alla Cancelleria federale per lo svolgimento di mansioni amministrative).

Nel 2006 è entrata in vigore la legge sulla trasparenza (LTras). Visto che i tre posti previsti a tal fine nel messaggio relativo alla legge non sono mai stati autorizzati dal Consiglio federale, per l'adempimento dei propri compiti conformemente alla LTras la nostra autorità ha dovuto far capo al personale incaricato della protezione dei dati già esistente presso l'IFPDT e, in parte, alle risorse della Cancelleria federale. Dopo che l'8 dicembre 2022 il Parlamento, cui ora compete l'approvazione del preventivo dell'IFPDT, aveva autorizzato i posti previsti nel messaggio di legge, l'IFPDT ha potuto restituire uno di questi tre posti all'ambito direzionale Protezione dei dati, il cui effettivo del personale è aumentato di un ulteriore posto, attestandosi quindi complessivamente a 33 posti. L'Incaricato ha assegnato i restanti due posti all'ambito direzionale Legge sulla trasparenza per via dell'aumento del volume di lavoro per le mediazioni (cfr. contributo successivo relativo alle prestazioni e risorse nell'ambito della legge sulla trasparenza).

A fronte dei considerevoli lavori preparatori necessari in vista dell'entrata in vigore della nuova LPD durante il periodo in rassegna (nuove direttive e testi per il sito Internet ecc.), l'impiego del nuovo personale reclutato ha inciso pesantemente dal punto di vista statistico, come si evince di seguito, sul gruppo di prestazioni «Informazioni».

Tabella 6: Posti attribuibili per trattare questioni riguardanti la LPD

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	27
2023	33

Prestazioni

Secondo il nuovo modello di gestione dell'Amministrazione federale (NMG), i compiti dell'IFPDT in quanto autorità di protezione dei dati competente per gli organi federali e l'economia privata sono attribuiti ai quattro gruppi di prestazioni «consulenza», «vigilanza», «informazione» e «legislazione». Nell'anno in rassegna, dal 1° aprile 2022 al 31 marzo 2023 le risorse di personale impiegate presso l'IFPDT che potevano essere destinate alla protezione dei dati sono state ripartite nei gruppi summenzionati nel modo seguente:

Tabella 7: Servizi protezione dei dati

Consulenza alla Confederazione	18,7%	
Consulenza a privati	21,1%	
Collaborazione con autorità estere	11,4%	
Collaborazione con i Cantoni	1,3%	
Totale Consulenza		52,5%
Vigilanza	14,7%	
Certificazione	0,0%	
Registro delle collezioni di dati	0,4%	
Totale Vigilanza		15,1%
Informazioni	20,2%	
Formazione / conferenze	2,0%	
Totale Informazione		22,2%
Legislazione	10,2%	
Totale Legislazione		10,2%
Totale Protezione dei dati		100,0%

Consulenza

Come illustrato nel capitolo iniziale «Sfide attuali», nel settore della consulenza l'IFPDT è confrontato a una continua crescita delle richieste derivante dalla necessità di accompagnare grandi progetti digitali. Nell'anno in rassegna, le risorse di personale impiegate nella consulenza ammontavano a circa il 52,5 per cento. Secondo il piano di controllo dell'IFPDT per il 2022, l'accompagnamento a titolo di consulenza è in corso per otto grandi progetti, quattro dei quali sono legati alla trasformazione digitale disposta dal Consiglio federale per l'Amministrazione federale.

I tre team dell'ambito direzionale Protezione dei dati hanno risposto mediamente ogni mese a 33 richieste e segnalazioni di cittadini, inviando agli

interessati una lettera standard che li informava sulle vie previste dalla procedura civile. A partire dall'entrata in vigore della nuova LPD, una parte di queste richieste andrà trattata sotto il profilo materiale.

Dato che i big data e l'intelligenza artificiale si stanno imponendo rapidamente come modelli aziendali e i rischi tecnologici legati alla protezione dei dati continuano ad estendere il campo di vigilanza dell'IFPDT, il numero di grandi progetti pubblici e privati che implicano un trattamento di dati continuerà verosimilmente a crescere.

Tabella 8: Consulenze svolte nel 2022 per grandi progetti

Diritti fondamentali	1
Legislazione nuova LPD	2
Commercio ed economia	1
Trasformazione digitale	4
Totale	8

Vigilanza

La dinamica delle applicazioni basate su cloud impone oggi un'esecuzione estremamente rapida dei controlli.

Questa accelerazione e la necessità, che si rivela sempre più importante, di disporre di una combinazione di conoscenze giuridiche e competenze tecniche escludono interruzioni prolungate nelle procedure di accertamento dei fatti, cosicché i controlli più estesi devono essere svolti da più collaboratori. Nel periodo in rassegna la quota di risorse impiegate per i controlli e le procedure di vigilanza era pari al 15,1 per cento, il che corrisponde al basso valore medio degli anni in rassegna

successivi al 2015. Secondo il piano di controllo per il 2023, queste risorse dovranno servire a svolgere 12 controlli su vasta scala. Dopo l'aumento del personale impiegabile per la protezione dei dati avvenuto negli ultimi due periodi in esame in vista della nuova LPD, l'Incaricato si adopererà affinché aumenti gradualmente la densità dei controlli sugli organi federali, sulle 12 000 grandi e medie imprese commerciali nonché sulle circa 10 000 fondazioni e associazioni attive in Svizzera.

Legislazione

Gli adeguamenti del trattamento dei dati personali conseguenti alla trasformazione digitale degli uffici federali devono avvenire nel quadro di basi legali. Tali adeguamenti comportano pertanto l'introduzione nel diritto federale di tutta una serie di prescrizioni nuove e rivedute sul trattamento dei dati, in merito alle quali l'IFPDT si esprime nell'ambito delle diverse procedure di consultazione. Nell'anno in rassegna ci sono pervenute 383 consultazioni degli uffici.

Revisione totale della legge sulla protezione dei dati

Con l'imminente entrata in vigore della nuova LPD e dell'ordinanza d'esecuzione, per l'IFPDT si prospettano onerosi lavori preparatori per quanto concerne i nuovi compiti e le nuove competenze come pure l'informazione tempestiva della popolazione e dell'economia. Anche grazie all'ulteriore personale reclutato, sarà possibile portare progressivamente a termine questi lavori dall'inizio dell'estate 2023, come previsto.

Prestazioni e risorse nell'ambito della legge sulla trasparenza

L'anno in rassegna è stato caratterizzato dalla fine della pandemia e dal numero costantemente elevato di richieste di mediazione (cfr. n. 2.3). Dopo che il Parlamento ha approvato l'8 dicembre 2022 i tre posti previsti nel messaggio relativo alla legge sulla trasparenza, ma mai assegnati all'IFPDT dal Consiglio federale, l'effettivo di personale dell'ambito direzionale Principio di trasparenza può essere aumentato da 4,4 a 6 posti a tempo pieno. L'Incaricato si adopererà affinché i ritardi nel disbrigo delle procedure legati alla pandemia e alla mancanza di personale vengano gradualmente eliminati nei prossimi periodi in rassegna. Se e con quali tempi ciò accadrà dipende anche dall'evoluzione futura delle richieste di mediazione.

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

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

- febbraio 2022: CSSS-S sulla problematica Swisstransplant;
- febbraio 2022: CIP-N sulle piattaforme digitali;
- aprile 2022: CIP-N sulla revisione dell'ordinanza relativa alla nuova LPD;
- giugno 2022: sottocommissione DFGP/CAF della CdG-N sul rapporto d'attività;
- ottobre 2022: CSSS-N e CIP-N sulla revisione della LAMal e sulle misure di contenimento dei costi;
- ottobre 2022: CET-N sulla revisione totale della legge sulle dogane;
- ottobre 2022: sottocommissioni CdF-S e CdF-N sul preventivo 2023;
- novembre 2022: CPS-N sulla revisione totale della legge sulle dogane;
- gennaio 2023: CAG-N sulla revisione totale della legge sulle dogane;
- febbraio 2023: sottocommissione DFGP/CAF della CdG-S sull'attuazione della LTras;
- marzo 2023: CAG-N sulla legge federale concernente le piattaforme per la comunicazione elettronica nella giustizia

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

Tabella 9: Obiettivi di efficacia 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. Dispone di un sito Internet moderno e di facile consultazione. Con l'entrata in vigore della legge riveduta sulla protezione dei dati saranno introdotti nuovi obblighi di notifica e saranno adeguati quelli esistenti. Le notifiche dovranno poter essere recapitate all'IFPDT in modo sicuro, semplice e in qualsiasi momento per il tramite di portali di notifica. In questo modo sarà possibile ridurre le discontinuità tra le fonti di informazione e implementare con maggiore efficacia il trattamento dei dati.
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

3.2 Comunicazione

Cifre

Nell'anno in rassegna l'IFPDT ha pubblicato 6 comunicati stampa, consultabili sul portale della Confederazione, e 12 brevi comunicati. Nel nostro monitoraggio dei media, basato su una selezione dei principali media svizzeri della carta stampata e online e di prodotti chiave della stampa internazionale, abbiamo registrato nel 2022 quasi 6000 contributi, confermando la tendenza del 2021, in cui si è riscontrato un notevole aumento rispetto all'anno precedente (cfr. 29° rapporto, n. 3.2). Il team Comunicazione dell'IFPDT ha risposto a circa 300 domande dei media. I giornalisti si sono concentrati su temi quali la trasmissione dei dati (ca. 100 domande), la cibersicurezza (45) e la vigilanza (30), e in parte anche su progetti di regolamentazione (15) come il controllo delle chat o la nuova legge sulle dogane. Abbiamo infine risposto a 12 domande dei media riguardo alla legge sulla trasparenza.

Il numero di richieste e segnalazioni da parte di cittadini in questo anno di riferimento è di 6200, quasi lo stesso dell'anno scorso (6600), quando abbiamo registrato un forte aumento di oltre il 50 per cento.

Temi prioritari

Osservando in generale le domande dei media pervenute nel periodo in esame e le misure di comunicazione da noi avviate possiamo trarre le seguenti conclusioni: dopo la pandemia di coronavirus, che ha sollevato numerosi quesiti dal punto di vista della protezione dei dati soprattutto per quanto riguarda il tracciamento dei contatti (contact tracing) e il rilascio del certificato COVID, il settore della salute rimane al centro dell'interesse generale. Alcuni giornalisti investigativi hanno individuato lacune in registri medici sul fronte della sicurezza dei dati e criminali informatici sono riusciti ad accedere abusivamente ai dati di pazienti salvati su server di studi medici e ospedali in modo non sufficientemente sicuro.

Sono stati compromessi dati sanitari degni di particolare protezione relativi a vari soggetti, come era già accaduto l'anno precedente con il registro elettronico delle vaccinazioni della Fondazione lemievaccinazioni (cfr. 29° rapporto, n. 1.4), con il Registro nazionale di donazione di organi e quello delle protesi mammarie. In entrambi i casi l'IFPDT ha aperto una procedura formale di accertamento dei fatti (cfr. n. 1.4). La fondazione Swisstransplant ha accolto la maggior parte delle raccomandazioni contenute nel rapporto di indagine dell'IFPDT e ha sospeso la gestione online del Registro nazionale

di donazione di organi. Il rapporto relativo al registro delle protesi mammarie è ancora in elaborazione; il registro è stato temporaneamente rimosso dalla rete.

Nel caso di Swisstransplant abbiamo diffuso comunicati stampa sia all'apertura del procedimento a gennaio sia in occasione della pubblicazione del rapporto finale a ottobre. Non appena sono stati resi noti gli attacchi da parte di hacker ai danni di studi medici nella Svizzera romanda, l'IFPDT ha contattato gli studi per far sì che i pazienti interessati venissero informati tempestivamente e in maniera esaustiva. Abbiamo pubblicato un breve comunicato al riguardo il 31 marzo 2022 sul nostro sito Internet. L'Incaricato si è espresso più volte nei media in merito alla problematica della carente sicurezza legata alla conservazione di dati sanitari.

Dopo la dichiarazione di fallimento della fondazione lemievaccinazioni alla fine del 2021 e la comunicazione della prevista vendita dei dati sulle

vaccinazioni da parte dell'Ufficio fallimenti competente a maggio 2022, l'IFPDT ha chiesto inizialmente la cancellazione dei dati e, in un secondo momento, ha reso possibile un tentativo di salvataggio dei dati da parte della direzione sanitaria del Cantone di Argovia. Abbiamo preso posizione in merito in un comunicato stampa (cfr. n. 1.4).

Nell'anno in rassegna è risultato evidente quanto i dati medici siano al centro dell'interesse generale anche dal punto di vista del principio di trasparenza, in particolare nel caso dei contratti per l'acquisto dei vaccini. Nella sua raccomandazione del 29 luglio 2022, l'IFPDT ha raccomandato all'UFSP di rendere pubblici i contratti. Tuttavia, quando si è trattato di pubblicare i documenti, l'UFSP ne ha annerito ampie porzioni, suscitando critiche tra l'opinione pubblica.

Trasmissione e commercio di dati

Accanto alla questione dei registri medici, quest'anno ci hanno tenuto impegnati in particolare anche la tematica dei cloud e la trasmissione di dati personali a terzi in ambito commerciale. Ci siamo pronunciati in maniera dettagliata in merito all'esternalizza-

zione di dati personali da parte di Suva in un cloud di Microsoft e il 13 giugno 2022 abbiamo pubblicato al riguardo un breve comunicato. Abbiamo espresso il nostro parere sui media anche riguardo alla strategia cloud della Confederazione (cfr. 29° rapporto d'attività, tema prioritario II).

L'IFPDT sta attualmente analizzando la causa intentata negli Stati Uniti contro la società «Oracle America Inc.» a causa del tracciamento illegale di utenti di Internet e il 27 settembre 2022 ha pubblicato al riguardo un breve comunicato (cfr. n. 1.3). La trasmissione di dati e il tracciamento di persone non rispondono solo a interessi commerciali ma sono funzionali anche per progetti di vigilanza dello Stato. Lo si è riscontrato durante i Mondiali di calcio 2022 con l'app chiesta dal Qatar, che ha spinto l'IFPDT a pubblicare un breve comunicato in cui raccomandava alle persone che desideravano recarsi in Qatar per assistere ai Mondiali di portare con sé un secondo smartphone. L'IFPDT non vede di buon occhio il progetto dell'UE riguardo al controllo

delle chat, tema anch'esso assunto agli onori della cronaca nel periodo in esame.

In occasione della Giornata internazionale della protezione dei dati 2023 abbiamo richiamato l'attenzione sulla versione aggiornata delle linee guida in materia di protezione dei dati in relazione alle elezioni e votazioni, rilevanti sia sul piano federale che su quello cantonale.

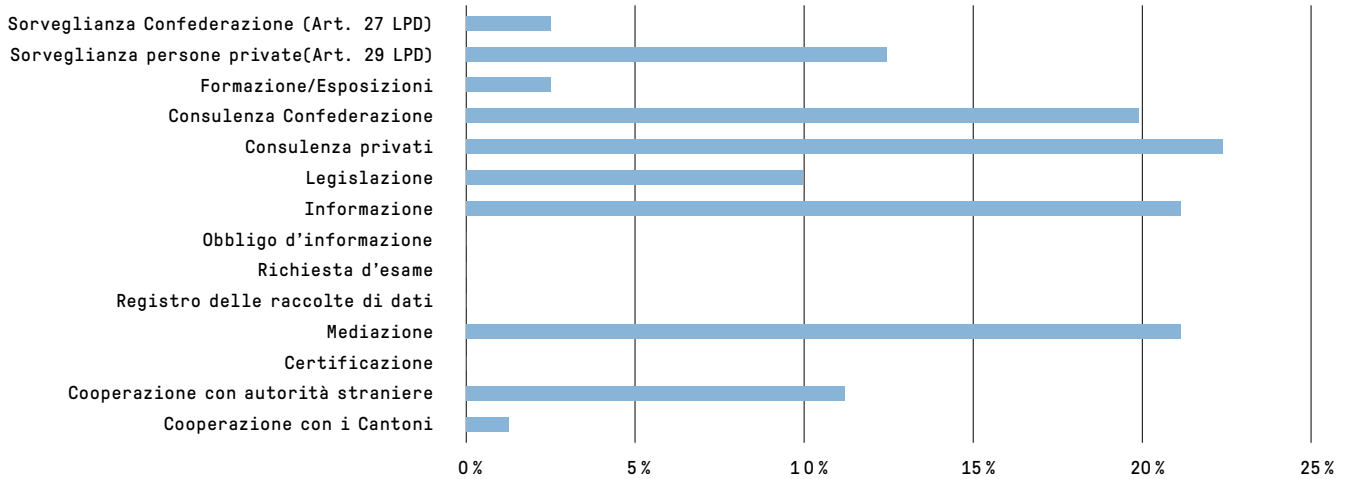
Nuovo sito Internet

Lo sviluppo del nuovo sito Internet, unito alla contestuale stesura del presente rapporto d'attività, ha rappresentato una sfida non indifferente per il team del servizio dei media. Con il rifacimento del sito non si intende solo aggiornare tutti i contenuti riguardanti la nuova legge sulla protezione dei dati che entrerà in vigore il 1° settembre 2023, ma si vuole anche snellire e ristrutturare l'intero sito per consentire agli utenti di trovare rapidamente le informazioni che cercano. Dal nuovo sito si potrà inoltre accedere velocemente ai tre nuovi portali di notifica: DataReg per la notifica dei registri delle attività di trattamento da parte degli organi federali, il portale per la notifica delle violazioni della sicurezza dei dati («DataBreach») e quello per la notifica dei consulenti per la protezione dei dati.

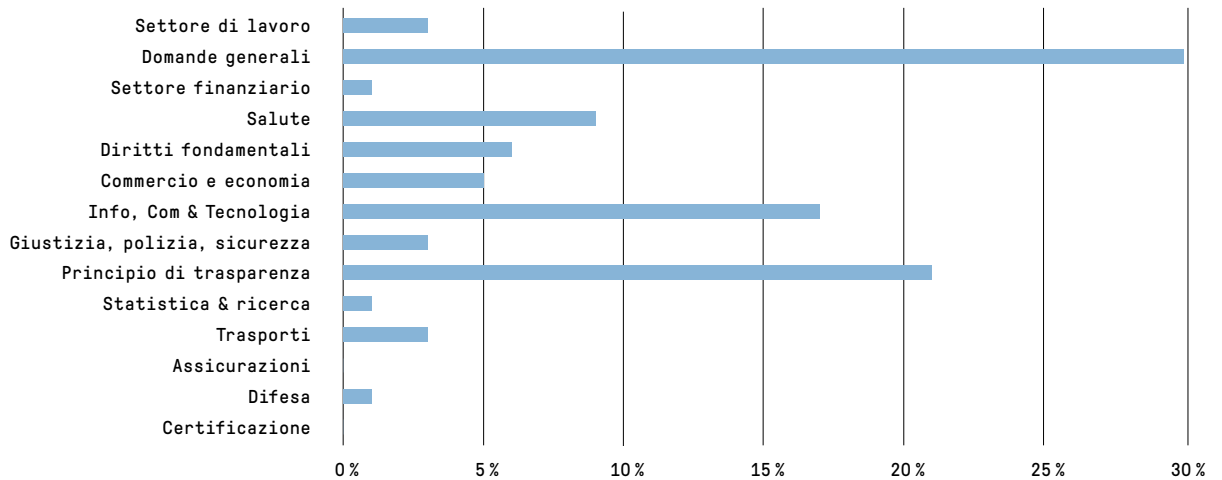
3.3 Statistiche

Statistiche sulle attività dell'IFPDT dal 1° aprile 2022 al 31 marzo 2023 (Protezione dei dati)

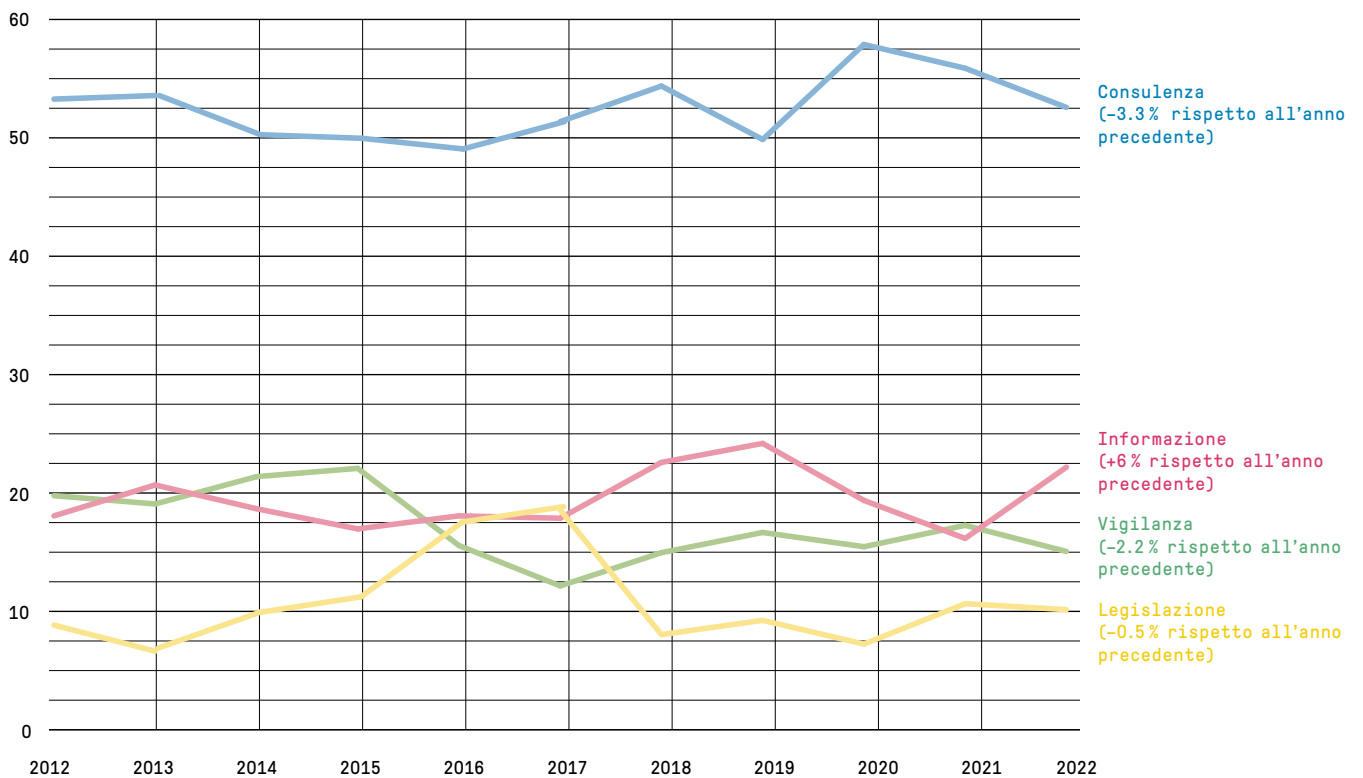
Carico di lavoro per compiti



Carico di lavoro per materie



Paragone pluriennale (in percentuale)



Panoramica delle domande d'accesso dal 1° gennaio al 31 dicembre 2022

Dipartimento	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
CaF	37	23	5	3	1	5	0
DFAE	164	83	18	29	8	10	16
DFI	207	73	15	73	14	14	18
DFGP	80	42	9	9	4	1	15
DDPS	295	237	17	18	3	5	15
DFE	110	37	15	23	10	15	10
DEFR	119	56	11	26	7	8	11
DATEC	162	68	8	55	6	11	14
MPC	6	5	1	0	0	0	0
SP	0	0	0	0	0	0	0
Totale 2022 (%)	1180 (100)	624 (53)	99 (8)	236 (20)	53 (5)	69 (6)	99 (8)
Totale 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (24)	48 (3)	78 (7)	115 (8)
Totale 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Totale 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Totale 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Totale 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	-
Totale 2016 (%)	554 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	-
Totale 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	-
Totale 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	-
Totale 2013 (%)	470 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	-
Totale 2012 (%)	518 (100)	230 (44)	140 (27)	123 (24)	19 (4)	6 (1)	-

**Statistica delle domande d'accesso secondo la legge sulla trasparenza
dal 1° gennaio al 31 dicembre 2022**

		Numero di domande	Inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	22	0	14	3	3	0	2	0
	IFPDT	15	0	9	2	0	1	3	0
	Totale	37	0	23	5	3	1	5	0
Dipartimento federale degli affari esteri DFAE	DFAE	164	0	83	18	29	8	10	16
	Totale	164	0	83	18	29	8	10	16
Dipartimento federale dell'interno DFI	SG DFI	10	0	2	2	1	0	2	3
	UFU	4	0	3	0	0	0	1	0
	UFC	8	0	5	1	1	1	0	0
	AFS	2	0	1	0	0	1	0	0
	METEO CH	1	0	1	0	0	0	0	0
	BN	0	0	0	0	0	0	0	0
	UFSP	91	0	22	3	44	8	8	6
	UST	4	0	1	2	1	0	0	0
	UFAS	11	0	11	0	0	0	0	0
	USAV	27	0	14	3	8	0	0	2
	MNS	0	0	0	0	0	0	0	0
	SWISS MEDIC	45	8	10	3	18	4	3	7
	SUVA	4	1	3	1	0	0	0	0
	compenswiss	0	0	0	0	0	0	0	0
	Totale	207	9	73	15	73	14	14	18
	Dipartimento federale di giustizia e polizia DFGP	SG DFGP	6	0	4	0	0	0	0
DFGP		22	0	9	2	1	0	0	10
FEDPOL		12	0	5	4	3	0	0	0
METAS		3	0	3	0	0	0	0	0
SEM		24	0	13	2	3	2	1	3
Servizio SCPT		0	0	0	0	0	0	0	0
ISDC		3	0	3	0	0	0	0	0
IPI		4	0	2	0	2	0	0	0
CFCG		3	0	1	0	0	2	0	0
CAF		0	0	0	0	0	0	0	0
ASR		1	0	1	0	0	0	0	0
CSI		1	0	1	0	0	0	0	0
CNPT		1	1	0	1	0	0	0	0
Totale		80	1	42	9	9	4	1	15

		Numero di domande	inottrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS	SG DDPS	33	1	6	7	11	1	1	7
	Difesa	3	0	2	0	0	0	0	1
	SIC	21	0	5	7	5	0	0	4
	AVI-AIn	0	0	0	0	0	0	0	0
	armasuisse	10	0	3	1	0	0	4	2
	UFSP0	220	0	218	2	0	0	0	0
	UFPP	4	0	1	0	2	0	0	1
	swisstopo	4	0	2	0	0	2	0	0
	UUC	0	0	0	0	0	0	0	0
	Totale	295	1	237	17	18	3	5	15
Dipartimento federale delle finanze DFF	SC DFF	36	2	8	3	17	2	0	6
	AFF	1	0	0	0	0	0	0	1
	UFPER	4	0	4	0	0	0	0	0
	AFC	11	0	5	3	2	0	0	1
	UDSC	30	6	8	6	2	3	11	0
	UFCL	7	0	4	0	0	0	3	0
	UFIT	4	0	2	1	1	0	0	0
	CDF	11	1	2	2	0	5	0	2
	SFI	3	0	1	0	1	0	1	0
	PUBLICA	1	0	1	0	0	0	0	0
	UCC	2	0	2	0	0	0	0	0
	Totale	110	9	37	15	23	10	15	10

		Numero di domande	inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	10	0	3	4	1	0	0	2
	SECO	37	0	11	4	9	3	4	6
	SEFRI	4	0	2	0	0	0	0	2
	UFAG	15	1	9	0	5	1	0	0
	Agroscope	0	0	0	0	0	0	0	0
	UFAE	9	0	3	0	4	0	2	0
	UFAB	1	0	0	0	1	0	0	0
	SPR	1	0	1	0	0	0	0	0
	COMCO	22	0	15	1	4	1	1	0
	CIVI	2	0	2	0	0	0	0	0
	UFDC	7	0	7	0	0	0	0	0
	FNS	0	0	0	0	0	0	0	0
	IUFFP	0	0	0	0	0	0	0	0
	ETH Rat	9	0	3	1	2	2	1	0
	Innosuisse	2	0	0	1	0	0	0	1
Totale	119	1	56	11	26	7	8	11	

Dipartimento federale dell'am- biente, dei trasporti, dell'en- ergia e delle comunicazioni DATEC	SG DATEC	9	1	3	1	2	0	0	3
	UFA	6	0	1	2	2	0	0	1
	UFAC	19	0	11	2	3	0	3	0
	UFE	25	0	5	1	18	0	0	1
	USTRA	11	0	4	0	1	1	2	3
	UFCOM	19	1	8	0	6	0	1	4
	UFAM	62	1	34	2	18	5	1	2
	ARE	0	0	0	0	0	0	0	0
	ComCom	0	0	0	0	0	0	0	0
	IFSN	8	3	2	0	4	0	2	0
	PostCom	0	0	0	0	0	0	0	0
	AIRR	2	0	0	0	0	0	2	0
	IFO	0	0	0	0	0	0	0	0
	SUST	0	0	0	0	0	0	0	0
	Totale	1	0	0	0	1	0	0	0
Totale	162	6	68	8	55	6	11	14	

		Numero di domande	inoltrate negli anni precedenti	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Ministero pubblico della Confederazione MPC	MPC	6	0	5	1	0	0	0	0
	Totale	6	0	5	1	0	0	0	0
Servizi del Parlamento SP	SP	0	0	0	0	0	0	0	0
	Totale	0	0	0	0	0	0	0	0
Somma totale		1180	27	624	99	236	53	69	99

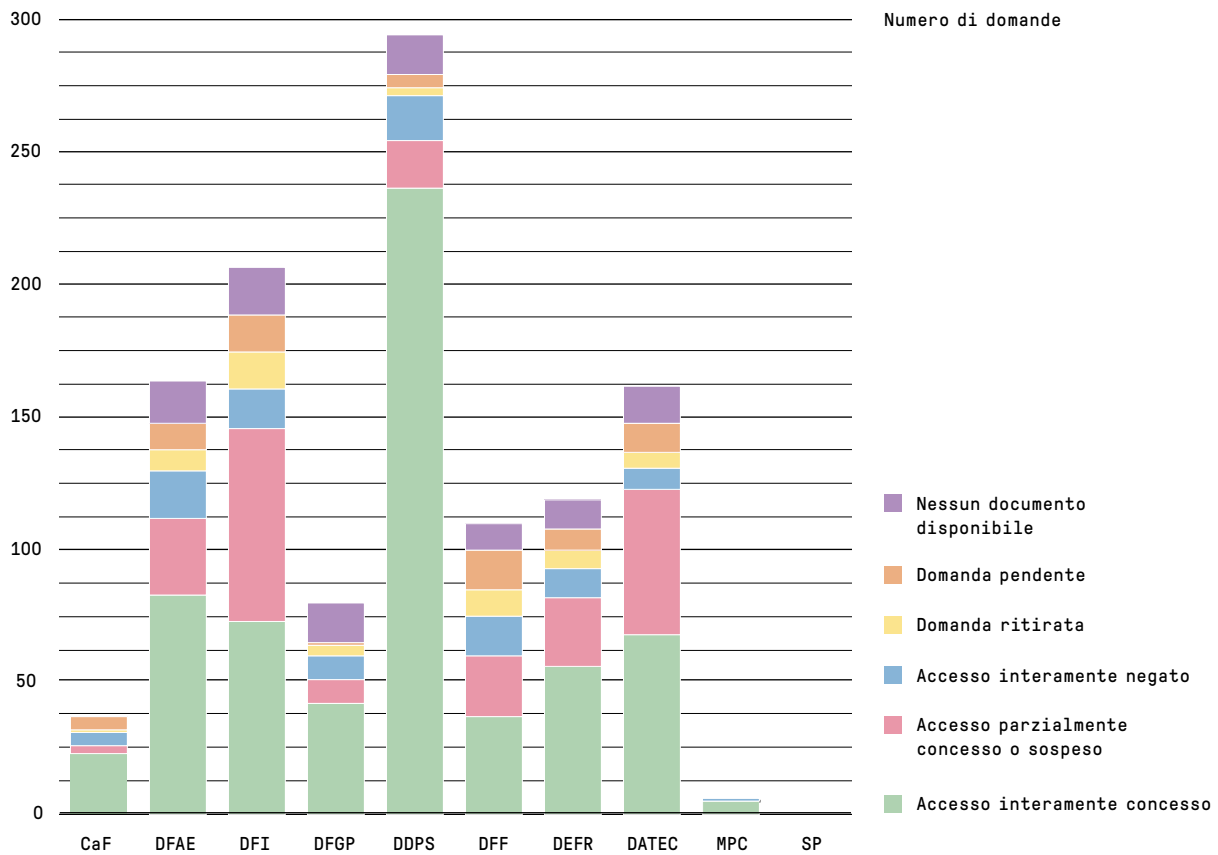
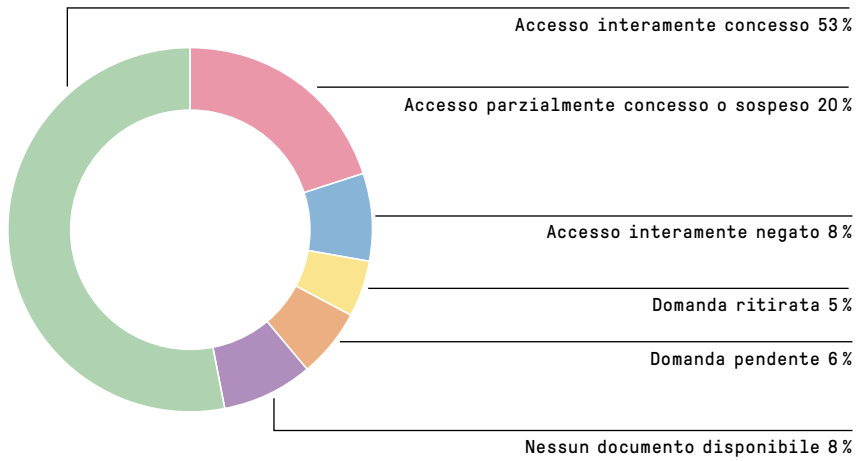
Domande di accesso 2022 con riferimento al coronavirus

		Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	Totale	0	0	0	0	0	0	0
Dipartimento federale degli affari esteri DFAE	Totale	0	0	0	0	0	0	0
Dipartimento federale dell'interno DFI	UFC	1	1	0	0	0	0	0
	UFSP	57	18	2	22	3	6	6
	swissmedic	18	4	0	6	4	2	2
	Totale	76	23	2	28	7	8	8
Dipartimento federale delle finanze DFF	SC DFF	6	0	0	5	0	0	1
	AFC	1	0	0	1	0	0	0
	UFIT	2	1	0	1	0	0	0
	CDF	1	0	1	0	0	0	0
	Totale	10	1	1	7	0	0	1
Dipartimento federale di giustizia e polizia DFGP	Totale	0	0	0	0	0	0	0
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	UFCOM	1	1	0	0	0	0	0
	Totale	1	1	0	0	0	0	0
Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS	UFPP	1	0	0	0	0	0	1
	Totale	1	0	0	0	0	0	1
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SECO	5	4	1	0	0	0	0
	Totale	5	4	1	0	0	0	0
Ministero pubblico della Confederazione MPC	Totale	0	0	0	0	0	0	0
Servizi del Parlamento SP	Totale	0	0	0	0	0	0	0
	Somma totale	93	29	4	35	7	8	10

Numero di domande di mediazione secondo la categoria di richiedenti

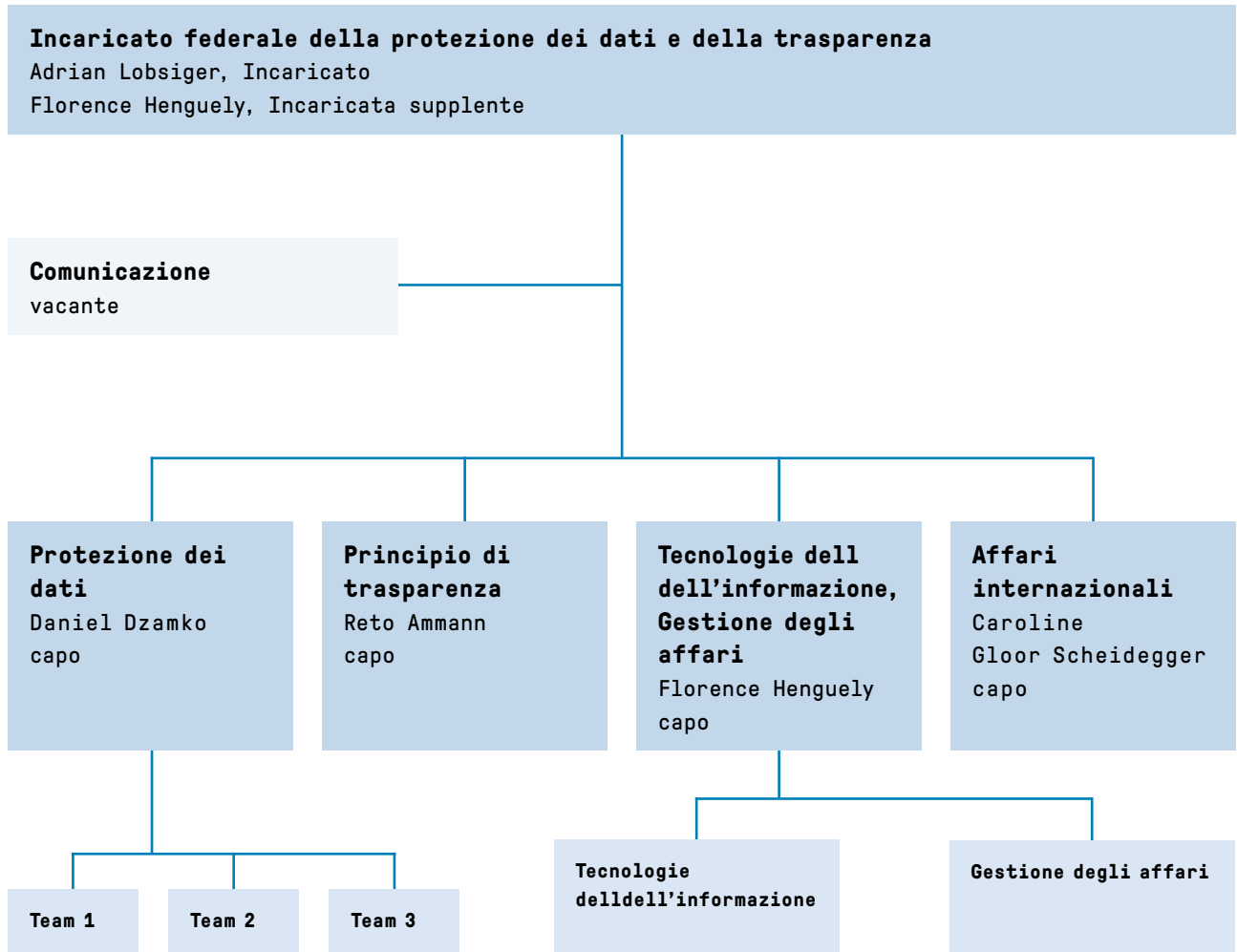
Categoria di richiedenti	2022	2021	2020	2019	2018	2017
Media	47	53	31	34	24	21
Privati (o nessuna assegnazione esatta possibile)	37	49	42	40	26	35
Parti interessate (associazioni, organizzazioni, società ecc.)	9	16	5	7	9	14
Avvocati	27	12	7	5	4	2
Aziende	9	19	7	47	13	7
Università	0	0	1	0	0	0
Totale	129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

Trattamento delle domande d'accesso dal 1° gennaio al 31 dicembre 2022



3.4 Organizzazione IFPDT (Stato 31 marzo 2023)

Organigramma



Personale dell'IFPDT

Numero di dipendenti	41		
FTE	34.1		
per sesso	Donne	20	49%
	Uomini	21	51%
per livello di occupazione	1-89%	31	76%
	90-100%	10	24%
per lingua	Tedesco	32	78%
	Francese	8	20%
	Italiano	1	2%
per età	20-49 anni	24	59%
	50-65 anni	17	41%
Posizioni dirigenziali	Donne	4	40%
	Uomini	6	60%

Abbreviazioni

AMVP Assemblea mondiale per la protezione della vita privata

CEPD Comitato europeo per la protezione dei dati

CIP Cartella informatizzata del paziente

DataReg Registro delle collezioni di dati

Fedpol Ufficio federale di polizia

GDPR Regolamento generale sulla protezione dei dati dell'UE

GEDP Garante europeo della protezione dei dati

IA Intelligenza artificiale

le Identità elettronica

LAr Legge federale sull'archiviazione

LCIP Legge federale sulla cartella informatizzata del paziente

LDP Legge federale sui diritti politici

LPD Legge federale sulla protezione dei dati

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

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

NaDB Programma di gestione nazionale dei dati

NCSC Centro nazionale per la cibersicurezza

nLPD Nuova legge federale sulla protezione dei dati

OCPD Ordinanza sulle certificazioni in materia di protezione dei dati

OPDa Ordinanza sulla protezione dei dati

PA Legge federale sulla procedura amministrativa

PNR Dati dei passeggeri aerei (Passenger Name Records)

Privatim Conferenza degli incaricati svizzeri per la protezione dei dati

RNDO Registro nazionale di donazione di organi

SAS Servizio di accreditamento svizzero

SIC Servizio delle attività informative della Confederazione

SIS II Sistema d'informazione Schengen di seconda generazione

TDT Settore Trasformazione digitale e governance delle TIC della Cancelleria federale

TIC Tecnologie dell'informazione e della comunicazione

UDSC Ufficio federale della dogana e della sicurezza dei confini (ex AFD)

VIPD Valutazione d'impatto sulla protezione dei dati

VIS Sistema centrale d'informazione visti

Elenco delle illustrazioni

Figure

Figura 1: Valutazione delle domande di accesso – Sviluppo dal 2009 p. 65

Figura 2: Tasse riscosse dall'entrata in vigore della LTras.....p. 67

Figura 3: Domande di mediazione dall'entrata in vigore della LTras p. 68

Tabelle

Tabella 1: Soluzioni consensuali p. 69

Tabella 2: Tempo di elaborazione delle procedure di mediazione..... p. 70

Tabella 3: Procedure di mediazione pendenti p. 71

Tabella 4: Disposizioni speciali ai sensi dell'articolo 4 LTra p. 80

Tabella 5: Nessuna disposizione speciale ai sensi dell'articolo 4 LTras p. 81

Tabella 6: Posti attribuibili per trattare questioni riguardanti la LPD..... p. 85

Tabella 7: Servizi protezione dei dati..... p. 86

Tabella 8: Consulenze svolte nel 2022 per grandi progetti p. 86

Tabella 9: Obiettivi di efficacia dell'IFPDT p. 87

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. 410.030.I

Layout: Ast & Fischer AG, Wabern

Fotografia: Joël Stäheli

Caratteri: Pressura, Documenta

Stampa: Ast & Fischer AG, Wabern

Carta: PlanoArt[®], senza legno, extra bianco



Cifre chiave

Carico protezione dei dati

53%

Consulenza

15%

Vigilanza

22%

Informazione

10%

Legislazione

Domande di accesso (LTras)

53%

interamente
concesso

20%

parzialmente
concesso o sospeso

8%

interamente
negato

5%

ritirata

6%

pendente

8%

nessun documento
disponibile

Preoccupazioni relative alla protezione dei dati



Informazione corretta

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



Possibilità di scelta

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



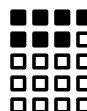
Analisi dei rischi

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



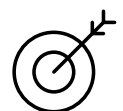
Esattezza dei dati

Il trattamento avviene con i dati corretti.



Proporzionalità

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



Finalità

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



Sicurezza dei dati

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



Documentazione

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




Responsabilità personale

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

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

E-mail: info@edoeb.admin.ch

Sito Internet: www.lincaricato.ch

 [@derBeauftragte](https://twitter.com/derBeauftragte)

Telefono: +41 (0)58 462 43 95 (lu-ve, 10-12)

Fax: +41 (0)58 465 99 96