Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza IFPDT

L'Incaricato

CH-3003 Berna, IFPDT, EDÖB-A-3F3C3401/1

All'Ufficio federale della sanità pubblica

[redacted]

Suo riferimento:
Nostra sigla: EDÖB-A-3F3C3401/1
Responsabile: [redacted]
Berna, 11 maggio 2020

Parere secondo l'articolo 17*a* LPD sul test pilota con il sistema svizzero di tracciamento di prossimità (Swiss Proximity Tracing System, SPTS)

Gentili signore e signori,

l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) ha esaminato la documentazione presentata dall'UFSP ai fini del presente parere e si esprime secondo l'articolo 17*a* della legge federale sulla protezione dei dati (LPD; RS 235.1) come segue.

L'IFPDT ritiene che il test pilota del SPTS sia ammissibile dal punto di vista della protezione dei dati. Le misure di vigilanza e le raccomandazioni applicabili durante la fase pilota e dopo il passaggio alla fase operativa rimangono fatte salve. Nel dettaglio l'IFPDT presenta le seguenti osservazioni.

I. Sistema svizzero di tracciamento di prossimità (SPTS)

Sotto l'impulso determinante dei Politecnici federali di Losanna e Zurigo un gruppo internazionale di ricercatori provenienti da diversi Paesi ha sviluppato un sistema chiamato «Decentralized Privacy Preserving Proximity Tracing» (DP-3T) che la Confederazione intende mettere a disposizione della popolazione svizzera come strumento tecnico facente parte della sua strategia di lotta contro il virus SARS-CoV-2. Se impiegata sul proprio smartphone, l'applicazione mobile (di seguito app) registra in modo decentralizzato e anonimo tramite Bluetooth le distanze inferiori a due metri da altri smartphone che utilizzano la stessa app. L'app cerca in questi dati salvati nello smartphone i contatti con persone risultate positive al test e avverte l'utente se è rilevata un'esposizione sufficientemente lunga.

Nell'ambito del sistema svizzero di tracciamento di prossimità (Swiss Proximity Tracing System, SPTS) l'Ufficio federale della sanità pubblica (UFSP), in collaborazione con i Politecnici federali di Losanna e Zurigo, metterà a disposizione un'app e integrerà il back end con server nell'infrastruttura ge-

stita dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT). In qualità di organo federale responsabile per la gestione dell'app e di detentore di una banca dati secondo l'articolo 3 lettera i della LPD) l'UFSP deve assumersi le responsabilità corrispondenti.

Il Consiglio federale intende introdurre l'app SPTS dal 13 maggio 2020 sulla base di un'ordinanza di durata limitata (Ordinanza COVID-19 test pilota di tracciamento di prossimità, di seguito ordinanza SPTS) oggetto del presente parere, e testarla fino al 30 giugno 2020. Nella sessione estiva di giugno 2020 il Parlamento dovrebbe dibattere sul prospettato messaggio del Consiglio federale concernente una modifica urgente della legge sulle epidemie (LEp, RS 818.101).

II. Progetto e ruolo dell'IFPDT

Il progetto SPTS consiste nel trattamento complesso e automatico di grandi quantità di dati ottenuti da smartphone e da altri dispositivi intelligenti della popolazione che vengono completati con segnalazioni e codici generati da operatori sanitari tenuti al segreto. Siccome il progetto concerne queste fonti di dati relativi alle persone e sulla loro salute, la sensibilità del progetto nel suo insieme per i dati personali e le disposizioni in materia di protezione dei dati è evidente. Sebbene i partecipanti non possano essere identificati, il SPTS rimane legato soprattutto a rischi di re-identificazione che devono essere affrontati con accorgimenti tecnici volti a proteggere la sfera privata e l'autodeterminazione informativa degli interessati.

Nella sessione straordinaria di inizio maggio 2020 il Consiglio nazionale e il Consiglio degli Stati hanno deciso a stragrande maggioranza di sostituire l'ordinanza SPTS del Consiglio federale con una legge federale da dibattere nella sessione estiva 2020. Dalle deliberazioni tenute dalle Commissioni delle istituzioni politiche delle due Camere e dalla Commissione della sicurezza sociale e della sanità del Consiglio degli Stati, nelle quali è stato coinvolto l'IFPDT, è emerso che l'introduzione del SPTS programmata prima della legge federale preannunciata dal Consiglio federale non poggia sulle competenze esistenti o urgenti conferite dalla LEp bensì da quelle conferite dalla LPD. Eseguendo un test pilota secondo l'articolo 17*a* LPD, si dovranno testare per un breve periodo i preparativi progettuali e tecnici in attesa che il SPTS possa entrare in funzione a fine giugno come applicazione conforme ai diritti fondamentali e sostenibile nella pratica e che possa essere accettato in larga misura dalla popolazione, previa debita informazione.

Viste queste chiare direttive politiche, l'IFPDT dovrà tenere conto delle disposizioni legali dell'articolo 17*a* LPD in combinato disposto con l'articolo 27 dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD) in maniera da considerare le particolari circostanze della lotta contro la pandemia.

Dopo essere stato coinvolto in qualità di autorità esterna di vigilanza sulla protezione dei dati nella fase precoce del progetto DP-3T e aver informato la popolazione sul suo lavoro tramite diversi rapporti intermedi pubblicati sul suo sito Internet, l'IFPDT ha sottoposto al Consiglio federale il presente parere sul test pilota con il SPTS secondo l'articolo 17*a* LPD che sarà pubblicato come parte del decreto federale sull'ordinanza SPTS e quindi anche sul sito Internet dell'IFPDT.

In applicazione del principio della «privacy by design» sulla protezione dei dati, il 21 marzo 2020 il Politecnico federale di Losanna ha contattato l'IFPDT affinché dal giorno seguente potesse accompagnare il progetto DP-3T con la sua «Task Force Corona» in tutte le principali fasi secondo gli articoli 27–29 e 31 LPD contribuendovi con la sua vigilanza, la sua consulenza e i suoi pareri sulla conformità alla protezione dei dati. Questi ultimi si sono basati sulla documentazione disponibile su Github[1] e sui

[1] https://github.com/DP-3T/documents (consultato il 4 maggio 2020)

colloqui con i collaboratori del Politecnico federale di Losanna e dell'Amministrazione federale coinvolti nel progetto. Il 2 aprile 2020 abbiamo presentato una prima valutazione generale nella quale ci siamo pronunciati sulle principali questioni legate alla protezione dei dati come in particolare l'anonimizzazione dei dati personali e l'utilizzazione volontaria. Con lettera del 23 aprile 2020 è seguita una valutazione delle caratteristiche tecniche del back end sotto l'aspetto della protezione dei dati, mentre il 1°, il 4 e l'8 maggio 2020 abbiamo espresso il nostro parere nell'ambito della consultazione degli uffici sulle basi giuridiche del SPTS.

Il 22 e il 30 aprile nonché il 5 e il 7 maggio 2020 le Commissioni delle istituzioni politiche delle due Camere e la Commissione della sicurezza sociale e della sanità del Consiglio degli Stati hanno sentito l'IFPDT in merito al SPTS e ad altre applicazioni per la lotta contro la pandemia che segue sotto l'aspetto della vigilanza con la Task Force Corona.

III. Valutazione dell'applicazione

1. Criteri

Come l'IFPDT ha già constatato nel suo comunicato del 17 marzo 2020, gli organi federali che raccolgono sistematicamente e trattano automaticamente dati ottenuti da un numero elevato di fonti di dati personali come gli smartphone devono rispettare i principi di cui all'articolo 4 LPD.

Nel contesto attuale della lotta contro la pandemia sono di grande importanza i principi della proporzionalità e della finalità secondo cui il trattamento dei dati nell'ambito del SPTS deve limitarsi, quanto a tempo e portata, allo stretto necessario per apportare un contributo significativo alla lotta contro l'attuale crisi.

Considerati i rischi per la sfera privata e l'autodeterminazione informativa menzionati qui sopra, andrebbero dapprima esclusi tutti i trattamenti automatizzati nell'ambito del SPTS il cui funzionamento è inadeguato per raggiungere l'effetto minimo atteso e che quindi si rivelano essere sproporzionati. Andrebbero esclusi anche i trattamenti che vanno oltre lo scopo prefissato, come la prevenzione di nuovi contagi. Per prefissare nuovi scopi, occorrerebbe creare basi legali sufficientemente determinate e settoriali mediante la procedura legislativa ordinaria. Questo riferimento allo scopo non va perso di vista anche in considerazione del fatto che nel caso in cui il SPTS venisse effettivamente utilizzato nell'ambito dell'attuale lotta contro la pandemia non si può escludere che anche alle autorità non attive nel settore sanitario venga l'idea di impiegare il tracciamento di prossimità, ad esempio, per scopi di sicurezza o di polizia giudiziaria.

La valutazione qui appresso basata sui criteri della LPD tiene inoltre conto delle direttive del Comitato europeo per la protezione dei dati[2] e del Consiglio d'Europa[3] sulla lotta contro la pandemia.

2. Applicazione strutturata in modo trasparente e conforme alla protezione dei dati

Affinché il SPTS possa apportare un contributo efficace alla lotta immediata contro l'attuale crisi e all'abrogazione progressiva delle restrizioni sanitarie delle libertà fondamentali, l'app deve essere installata e attivata da una considerevole parte della popolazione che possiede uno smartphone dotato della tecnologia Bluetooth. Questo presuppone che l'app si basi su un trattamento dei dati affidabile secondo l'articolo 4 capoverso 2 LPD nel quale il gestore informa l'utente in modo approfondito e facil-

[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_de (consultato il 9 maggio 2020)
[3] https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 (consultato il 9 maggio 2020)

mente comprensibile sullo scopo e sul funzionamento del SPTS e struttura in modo intuitivo le possibilità di scelta ad esso legate. Presuppone inoltre che il gestore dimostri in modo comprensibile a chiunque che il SPTS è stato strutturato in modo conforme alla protezione dei dati (privacy by design).

2.1. Funzionamento

A grandi linee il funzionamento del SPTS basato sui principi del DP-3T può essere descritto come segue:

Gli utenti scaricano l'app SPTS dall'Apple Store o dal Google Play Store e la installano nel proprio smartphone. Durante l'installazione viene generato a caso un codice privato iniziale. In seguito è necessario attivare le funzioni «Notifiche» e «Bluetooth» che richiedono eventualmente una conferma.

L'app emette ora via Bluetooth identificatori casuali (Ephemeral ID, EphID) che cambiano continuamente a seconda del rispettivo codice privato, generato quotidianamente, e riceve quelli dell'app di altri smartphone che si trovano nelle immediate vicinanze. Il proprio codice privato, diverso ogni giorno, gli EphID ricevuti nonché la durata e l'ora approssimativa dell'incontro sono memorizzati per 21 giorni sul proprio dispositivo.

Se risultano positivi al test del Covid-19, gli utenti possono decidere volontariamente se inviare al server back end tramite una connessione criptata il giorno di inizio del periodo di infezione determinato da un operatore sanitario e il codice privato valido da questo momento. A tal scopo, necessitano del codice di autorizzazione fornito da un operatore sanitario. Questo codice è indispensabile affinché possano essere segnalate al SPTS solo le infezioni confermate dal punto di vista medico. Dopo la segnalazione al server back end, l'app emette un nuovo codice privato iniziale. Questo codice è rinnovato quotidianamente e non permette di risalire a un precedente codice privato.

L'app di ogni utente carica gli elenchi dei codici privati delle infezioni confermate memorizzati sul server back end e verifica, con i codici privati ricevuti sullo smartphone, se sono presenti EphID negli incontri memorizzati. Le informazioni inviate dalle persone infette (codice privato e data di inizio) non permettono di determinare l'identità di queste persone, né sul server back end né sullo smartphone.

L'approccio conforme alla protezione dei dati del SPTS si riflette in particolare sui seguenti aspetti progettuali:

- si tiene conto soltanto della vicinanza tra gli utenti, non vengono raccolti dati sulla localizzazione;
- nessun scambio di identificativi tra smartphone senza app;
- EphID continuamente diversi non permettono un tracciamento delle persone e dei dispositivi;
- fintanto che una persona risultata positiva non si segnala, non vengono caricati dati sul server;
- soltanto le situazioni di contatto a meno di due metri vengono registrate e generano una notifica in caso di durata complessiva di almeno 15 minuti al giorno;
- la durata di conservazione dei dati è limitata alla sua utilità nell'individuare eventuali infezioni;
- l'impiego del sistema è limitato alla durata della pandemia;
- il sistema si basa su un approccio decentralizzato (vedi sotto).

Un sistema di tracciamento di prossimità richiede un'infrastruttura di fondo. Attualmente, per trattare soltanto la quantità di dati assolutamente necessaria ai fini del tracciamento (minimizzazione dei dati), sono rilevanti in particolare due approcci: il modello centralizzato e il modello decentralizzato. I principi del DP-3T prevedono un sistema decentralizzato in cui il maggior numero possibile di dati deve rimanere sui dispositivi dell'utente. In nessun momento vengono raccolti su un server centrale i dati sugli incontri tenutisi. Un server esiste soltanto per permettere agli utenti di stabilire con il proprio dispositivo se si sono tenuti incontri rilevanti. Il server non registra alcuna informazione che possa essere assegnata alle persone e non trasmette identificatori. In questo modo è possibile escludere la possibilità di

una profilazione centrale. L'approccio decentralizzato riduce inoltre il rischio che possa essere cambiata la finalità nonché il rischio di attacchi al server, motivo per cui in una valutazione globale l'IFPDT lo ritiene preferibile rispetto all'approccio centralizzato.

Ai fini della trasparenza il DP-3T su cui si basa il SPTS è accessibile liberamente (open-source). La documentazione e il codice sorgente possono essere scaricati dalla pagina del progetto GitHub[4].

2.2. Soluzione di Apple e Google per la notifica di esposizione

Il 10 aprile 2020 Apple e Google hanno annunciato una soluzione per la notifica di esposizione basata sulla tecnologia Bluetooth per smartphone che dovrebbe sostenere gli sforzi profusi nel tracciamento dei contatti. L'interfaccia messa a disposizione (API) ha lo scopo di rendere più sicuro, preciso ed efficiente l'uso del Bluetooth per la misurazione costante della prossimità tra le applicazioni mobili autorizzate. L'uso dell'API dovrebbe in linea di massima essere limitato soltanto a un'app per Paese. Stando alle loro dichiarazioni, Apple e Google non riceveranno informazioni che permettono di identificare gli utenti, né dati di localizzazione e neppure informazioni su altri dispositivi nelle vicinanze dell'utente. Inoltre il progetto non verrà commercializzato. Le due aziende saranno tenute responsabili di queste loro dichiarazioni. Il SPTS e quindi l'app verranno aggiornati per associarli alle interfacce messe a disposizione da Apple e da Google per la comunicazione via Bluetooth una volta che queste saranno disponibili.

2.3. Dichiarazioni relative alla protezione dei dati e condizioni d'uso

Le dichiarazioni relative alla protezione dei dati e le condizioni d'uso presentate all'IFPDT si riferiscono al test pilota. Sono di natura provvisoria e, ad eccezione di alcuni punti minori ancora da migliorare, si dimostrano conformi alla protezione dei dati. Adeguamenti puntuali durante il test pilota rimangono fatti salvi.

2.4. In attesa della versione test dell'app

Siccome non è ancora disponibile un'app SPTS implementata e testabile, la valutazione dell'IFPDT si basa per il momento sul progetto DP-3T conforme alla protezione dei dati. Non appena saranno disponibili versioni testabili e visualizzate dell'app, l'IFPDT potrà valutare anche le condizioni di protezione dei dati e le condizioni d'uso così come la facilità d'uso della futura app operativa SPTS e, se necessario, chiedere gli adeguamenti del caso.

2.5. Risultato intermedio

Premesso quanto detto, l'IFPDT giunge alla conclusione che nello stato attuale di sviluppo il back end presenta un'architettura conforme alla protezione dei dati e soddisfa i principi di un trattamento dei dati affidabile e trasparente ai sensi dell'articolo 4 LPD.

3. Rischi e adeguatezza delle misure adottate per affrontarli

Conformemente alla prassi consolidata dell'IFPDT gli organi federali che sistematicamente rilevano e trattano dati ottenuti da fonti di dati personali devono dimostrare, nell'ambito di una valutazione d'impatto sulla protezione dei dati, i rischi che ne derivano per la sfera privata e le misure adottate per affrontarli. Questa valutazione deve analizzare in particolare i rischi di re-identificazione legati all'anonimizzazione dei dati personali nella presente app per lottare contro la pandemia.

Nell'ambito del progetto DP-3T sono stati presentati all'IFPDT documenti che corrispondono a una valutazione d'impatto del rischio in settori essenziali. Il 1° maggio 2020 è stato inoltre presentato

[4] https://github.com/DP-3T/ (consultato il 9 maggio 2020) e https://github.com/admin-ch

all'IFPDT un rapporto sulla valutazione d'impatto sulla protezione dei dati allestito dal Politecnico federale di Losanna e da una azienda di consulenza esterna[5], nel quale sono menzionati in particolare i seguenti rischi e mostrate le corrispondenti misure:

- accesso illecito ai dati
- identificazione di contatti positivi al test
- mancato invio di una notifica nonostante il contatto con persone infette
- false notifiche
- divulgazione dell'uso dell'app e tracciamento dei dispositivi degli utenti
- ottenimento di informazioni sull'utente dovuto all'accesso locale al dispositivo
- acquisizione di un significativo numero di EphID tramite Relay Attack
- uso dei dati per altri scopi / cambiamento di finalità / sorveglianza di massa
- sistema DP-3T non funziona come previsto
- limitazione della libertà quando l'app dell'utente non è usata

Sulla base di quanto precede, l'IFPDT giunge alla conclusione che l'applicazione dimostra sufficientemente i rischi per la sfera privata degli utenti e affronta tali rischi con misure adeguate. Ad esempio vengono criptate le trasmissioni e generati post fake (noise) per impedire a terzi di identificare le persone infette. Per maggiori dettagli si rinvia alla valutazione tecnica del 23 aprile 2020 e alla suddetta documentazione.

4. Idoneità

Il SPTS è parte di una strategia generale del Consiglio federale e dell'UFSP per superare l'attuale crisi pandemica ed eliminare gradualmente le restrizioni dei diritti fondamentali[6] dovute alle misure sanitarie. Affinché, in considerazione dei rischi per la sfera privata illustrati sopra, l'impiego del SPTS possa essere ritenuto proporzionato dal punto di vista delle disposizioni in materia di protezione dei dati, esso deve essere fondamentalmente idoneo ad apportare un contributo efficace a questa strategia generale o a ottenere un effetto parziale significativo.

Nei dibattiti pubblici sul SPTS la sua idoneità è stata messa in discussione a più riprese. È stato ad esempio messo in dubbio che ci sarebbe stato un considerevole numero di installazioni volontarie dell'app. Sono stati espressi anche timori sul fatto che il progetto possa fallire a causa della riluttanza a segnalare un'infezione tramite app o ancora è stato criticato che negli edifici verrebbero rilevate molte prossimità irrilevanti che potrebbero generare falsi allarmi oppure che il funzionamento continuo del Bluetooth consumi molta batteria. Un'altra critica è stata mossa al fatto che la grande maggioranza del gruppo dei più anziani con la più alta vulnerabilità non utilizza uno smartphone. Infine, in considerazione dei diversi approcci attualmente seguiti dal Consorzio paneuropeo PEPP-PT[7] e dell'uscita del gruppo DP-3T dal consorzio, è stata contestata la compatibilità internazionale del SPTS ai principi del DP-3T.

Stando a questa critica, non è possibile di fatto prevedere con certezza se il SPTS produrrà l'effetto desiderato. Tuttavia, il Consiglio federale, l'UFSP (in qualità di ufficio specializzato compente) e il Politecnico federale di Losanna ritengono molto probabile che il SPTS si dimostri valido e possa contri-

[5] https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (consultato il 9 maggio 2020)
[6] https://www.bag.admin.ch/dam/bag/de/dokumente/cc/kom/covid-19-faktenblatt-swiss-pt-app.pdf.download.pdf/bag_Faktenblatt_Coronavirus_Swiss-PT-App.pdf (consultato il 9 maggio 2020)
[7] https://www.pepp-pt.org/ (consultato il 9 maggio 2020)

buire così a un'ulteriore riduzione e a una migliore tracciabilità dei contagi potenzialmente letali. Inoltre, sondaggi rappresentativi, come quello dell'Alta scuola di scienze applicate di Zurigo[8], sembrano indicare che una maggioranza della popolazione non sia soltanto favorevole a installare l'applicazione ma anche a notificare un'infezione via app.

Alla luce delle previsioni favorevoli dell'UFSP, dell'ampia documentazione del Politecnico federale di Losanna e dei sondaggi scientifici, l'IFPDT, in qualità di autorità di vigilanza per la protezione dei dati, deve dare prova di una certa moderazione nell'esaminare l'idoneità del SPTS nella misura in cui non può porre il suo potere discrezionale al di sopra di quello dell'Ufficio competente e non vi sono indizi che l'UFSP non abbia operato correttamente. Oltre all'aspetto tecnico del SPTS, anche il comportamento dell'utente costituisce un'importante componente dell'idoneità. Sebbene questo comportamento possa essere influenzato dalla facilità d'uso dell'app, che deve ancora essere valutata dall'IFPDT, e dalla campagna prevista dall'UFSP sulla sua introduzione, esso permette di fare previsioni solo limitatamente. Sarà possibile ottenere dei primi risultati concreti sull'accettazione tramite la valutazione della fase pilota.

Considerato quanto detto, l'IFPDT ritiene che allo stato attuale delle conoscenze il SPTS sia uno strumento idoneo per contribuire parzialmente alla prevenzione di contagi potenzialmente letali. Si dimostra pertanto proporzionato. Tenendo conto dei dubbi sollevati e del fatto che per motivi di tempo si è dovuto rinunciare a un rapporto esplicativo sull'ordinanza SPTS, l'IFPDT si aspetta che l'UFSP ne giustifichi l'idoneità nel messaggio concernente la modifica della LEp e in particolare che risponda alle critiche espresse. Se nell'ambito della fase pilota o della fase operativa dovesse emergere che l'applicazione non può soddisfare le aspettative legali, l'IFPDT si riserva il diritto di raccomandare all'UFSP di rinunciare all'attivazione completa o di proseguire l'applicazione.

5. Base legale

Visti i rischi per la sfera privata e l'autodeterminazione informativa, gli organi federali che rilevano sistematicamente dati da una grande quantità di fonti di dati personali come dati di smartphone e li trattano automaticamente, devono disporre di una base legale ai sensi dell'articolo 17 capoverso 1 LPD. Questa esigenza vale anche se l'impiego dell'applicazione è volontario.

L'ordinanza SPTS emanata dal Consiglio federale, limitata nel tempo e oggetto del presente parere dell'IFPDT, si basa nell'ingresso sull'articolo 17*a* LPD e costituisce così una base legale sufficiente per lo svolgimento della fase pilota del SPTS. Nella sessione estiva del giugno 2020 il Parlamento potrà deliberare sul messaggio concernente la modifica urgente della legge sulle epidemie in relazione al coronavirus. Per quanto riguarda il contenuto, l'IFPDT ha espresso il suo parere sull'ordinanza SPTS. Le sue richieste sono state prese in considerazione nell'ambito della consultazione degli uffici.

L'UFSP dispone così di una base legale sufficiente per la durata della fase pilota del SPTS limitata fino al 30 giugno 2020. L'ordinanza SPTS e il relativo test pilota sono conformi alla protezione dei dati.

6. Ammissibilità della fase pilota del SPTS

In vista del nostro parere secondo l'articolo 17*a* capoverso 1 LPD in combinato disposto con l'articolo 27 capoverso 2 OLPD, l'UFSP ha presentato sia per e-mail del 7 maggio 2020 che nell'ambito della consultazione degli uffici sull'ordinanza SPTS i seguenti documenti:

[8] https://www.zhaw.ch/de/ueber-uns/aktuell/news/detailansicht-news/event-news/viele-schweizer-fuerchten-ueberwachung-durch-contact-tracing-app/ (consultato il 4 maggio 2020)

A. *una descrizione generale del test pilota:* vi si trovano indicazioni sullo scopo, sull'obiettivo e sulla pianificazione nella proposta del Consiglio federale. Queste asserzioni devono ancora essere adeguate nel metodo di gestione dei progetti Hermes;

B. *un rapporto attestante che l'adempimento dei compiti previsti dalla legge richiede il trattamento di dati degni di particolare protezione o profili della personalità e rende imperativa una fase sperimentale prima dell'entrata in vigore della legge in senso formale (art. 17a cpv. 1 lett. c LPD):* le spiegazioni presentate nell'ambito della consultazione degli uffici sull'ordinanza SPTS sollevano la necessità di un trattamento dei dati con il SPTS e di una fase prova.

C. *una descrizione dell'organizzazione interna e delle procedure di trattamento e di controllo dei dati (art. 21 OLPD):* manca il regolamento relativo al trattamento. Questo deve essere presentato al più tardi due settimane prima dell'inizio della fase operativa;

D. *una descrizione delle misure di sicurezza e di protezione dei dati:* l'IFPDT dispone della valutazione dei rischi e degli altri documenti riguardanti il piano DP-3T alla base del SPTS. Tuttavia, l'UFSP ha trasmesso all'IFPDT con e-mail del 7 maggio 2020 soltanto quattro documenti sull'analisi del rischio per il sistema generale[9]. Mancano ancora le seguenti informazioni e documenti che devono essere inviati in un secondo momento:

    - stato attuale della valutazione dei rischi NCSC e misure di attuazione
    - versione finale dei flussi di dati per la fase pilota
    - documentazione del sistema finale (incl. collegamento a sistemi esterni) per la fase pilota
    - analisi del bisogno di protezione (Schuban)
    - giustificativo della valutazione dell'analisi dei rischi
    - visualizzazione dell'app

E. *un progetto di ordinanza che disciplini le modalità di trattamento o le grandi linee di tale atto legislativo:* nell'ambito della consultazione degli uffici dell'8 maggio 2020 è stato presentato il progetto dell'ordinanza SPTS con la proposta motivata al Consiglio federale;

F. *le informazioni concernenti la pianificazione delle diverse fasi del test pilota:* manca una pianificazione della gestione del progetto, a cui però si può rinunciare vista la brevità del test pilota urgente.

Data l'urgenza causata dalla pandemia, è comprensibile che i documenti presentati all'IFPDT siano incompleti. L'introduzione del SPTS come misura aggiuntiva per combattere la pandemia non deve quindi essere ritardata. L'IFPDT si aspetta tuttavia che i documenti mancanti siano presentati in tempo utile prima dell'inizio della fase operativa.

Un test pilota secondo l'articolo 17*a* capoverso 1 lettera a LPD presuppone prima di tutto che i compiti che richiedono tale trattamento siano disciplinati in una legge in senso formale. Il Dipartimento federale dell'interno (DFI), nella proposta al Consiglio federale sull'ordinanza SPTS, afferma a tal proposito che questo presupposto rientra negli articoli 31 capoverso 2 e 33 LEp, i quali prevedono in particolare che le autorità federali competenti e quindi l'UFSP sostengano le autorità cantonali nella notifica delle persone sospettate di essere infette.

[9] Security Testplan Proximity Scanning, 14 aprile 2020, NCSC; Privacy Issue to be discussed v100, CSIRT-BIT/GovCERT-CH; valutazione del rischio legato al tracciamento di prossimità, 30 aprile 2020, CSIRT-BIT/GovCERT-CH; Checksums providing privacy in case a user mistypes its authentication code, 5 maggio 2020, NCSC.

Come secondo presupposto devono essere presi provvedimenti sufficienti per impedire lesioni della personalità secondo l'articolo 17*a* capoverso 2 lettera b LPD. Anche se non ha ancora potuto esaminare tutti gli aspetti rilevanti del SPTS, poiché non gli è ancora stata sottoposta una versione test dell'app, compresa la visualizzazione, l'IFPDT ritiene, alla luce delle conoscenze ottenute finora e della descrizione della fase pilota, che la messa in funzione del SPTS sia soddisfacente.

Tra i presupposti per un test pilota secondo l'articolo 17*a* capoverso 1 lettera c LPD figura infine che la messa in opera del trattamento dei dati esiga imperativamente una fase sperimentale prima dell'entrata in vigore di una legge in senso formale. Questo può essere il caso in particolare se si devono prima valutare gli effetti o l'efficacia delle novità tecniche necessarie e delle misure organizzative o tecniche (art. 17*a* cpv. 2 lett. a e b LPD). Nella proposta al Consiglio federale sull'ordinanza menzionata, il DFI afferma che i suddetti presupposti rientrano nelle nuove soluzioni che rendono una fase pilota indispensabile prima dell'introduzione definitiva. Visti i rischi e la complessità del SPTS, l'IFPDT condivide questo parere. Come osserva il DFI, la durata del test pilota previsto è breve, ma è comunque possibile raccogliere esperienze importanti per l'introduzione definitiva, in particolare per quanto concerne la messa in opera, compresa l'infrastruttura tecnica, l'efficacia delle misure tecniche per la sicurezza e l'uso dell'applicazione da parte dei partecipanti e degli specialisti con diritto di accesso. Inoltre lo svolgimento di un breve test pilota secondo l'articolo 17*a* LPD fino all'entrata in vigore del nuovo disciplinamento nella LEp corrisponde alla volontà espressa dalle commissioni parlamentari competenti (cfr n. II.). Lo svolgimento di un test pilota si dimostra quindi assolutamente necessario.

7. Conclusione

L'IFPDT ritiene che l'imminente fase pilota del SPTS da parte dell'UFSP sia ammessa dal punto di vista della protezione dei dati. I documenti mancanti devono essere presentati in tempo utile prima dell'avvio della fase operativa. Le misure di vigilanza e le raccomandazioni applicabili durante la fase pilota e dopo il passaggio alla fase operativa rimangono fatte salve.

Distinti saluti

Adrian Lobsiger