COMMISSIONE SPECIALE

per l'esame di atti del Governo

S O M M A R I O

ATTI DEL GOVERNO

Mercoledì 18 aprile 2018. — Presidenza del presidente Nicola MOLTENI. – Intervengono il sottosegretario di Stato per l'interno Domenico Manzione e il sottosegretario di Stato per l'economia e le finanze Pier Paolo Baretta.

La seduta comincia alle 9.15.

Schema di decreto legislativo di attuazione di una direttiva europea sull'uso dei dati del PNR a fini di pubblica sicurezza e penali.
Atto n. 8.

(Esame, ai sensi dell'articolo 143, comma 4, del regolamento, e rinvio).

La Commissione inizia l'esame dello schema di decreto ministeriale in oggetto.

Vittorio FERRARESI (M5S), *relatore*, segnala che lo schema di decreto legislativo in esame è adottato in attuazione della disposizione di delega recata dall'articolo 1 della legge 25 ottobre 2017, n. 163 (legge di delegazione europea 2016-2017), per il recepimento delle direttive elencate nell'allegato A, tra cui è ricompresa la direttiva 2016/681. Per quanto riguarda i termini, le procedure, i princìpi e i criteri direttivi della delega, è fatto rinvio alle disposizioni previste dagli articoli 31 e 32 della legge 24 dicembre 2012, n. 234. Rammenta che il termine per l'espressione del parere da parte delle Commissione parlamentari competenti era fissato al 2 aprile 2018, ma il parere del Garante per la protezione dei dati personali sullo schema di decreto legislativo è stato trasmesso alle Camere soltanto il 28 marzo scorso. Si dovrà pertanto concordare con il Governo un nuovo termine per l'espressione del parere che risulti coerente con

quello previsto per l'esercizio della delega legislativa, fissato al 21 maggio 2018.

L'articolo 12 della legge di delegazione europea reca specifici principi e criteri direttivi per l'attuazione della direttiva (UE) 2016/681, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Preliminarmente si ricorda che i « reati gravi » sono definiti in un elenco allegato (II) alla direttiva, che comprende tra l'altro fatti di associazione criminale, di narcotraffico, di violenza sessuale, di « corruzione », nonché vari altri reati gravi contro la vita e l'incolumità delle persone, oppure contro il patrimonio. La direttiva impone inoltre (articolo 3, n. 9) che i fatti in questione siano puniti con una pena detentiva pari almeno a tre anni. L'articolo 12 prevede due principi di delega ulteriori rispetto a quelli previsti in via generale dalla legge di delegazione europea. Il primo principio di delega prevede che il Governo dovrà, in sede di attuazione, collocare l'Unità d'informazione sui passeggeri (UIP), di cui all'articolo 4 della direttiva, presso il Ministero dell'Interno – Dipartimento della pubblica sicurezza. Il secondo criterio di delega prevede che il trasferimento a cura dei vettori aerei dei dati del PNR comprenda anche i voli *intra*-UE.

Avvertendo che lo schema di decreto in titolo si compone di 27 articoli, fa presente quanto segue.

L'articolo 1 individua l'oggetto del decreto che consiste nel recepimento dei contenuti della direttiva (UE) 2016/681 del 27 aprile 2016, del Parlamento europeo e del Consiglio, sull'uso del codice di prenotazione (PNR). Tale direttiva si propone di rafforzare il sistema di controllo avente ad oggetto le informazioni che ciascun passeggero fornisce ai vettori aerei in fase di prenotazione del volo, con finalità di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

In particolare, ai sensi del comma 1, il decreto disciplina: il trasferimento da parte dei vettori aerei dei dati PNR dei voli *extra*-UE e dei voli intra-UE e, a tale riguardo, si evidenzia che il Governo in sede di recepimento si è avvalso della facoltà riconosciuta dall'articolo 2 della direttiva comunitaria di estendere l'applicazione dell'obbligo di trasmissione dei dati PNR anche in relazione ai voli *intra*-UE; il trattamento di tali dati da parte delle autorità competenti, ivi incluse le operazioni di raccolta, uso, conservazione e scambio con gli Stati membri.

Il comma 2 estende l'oggetto del decreto anche alla disciplina del trattamento dei cosiddetti dati API, ossia dei dati relativi ai passeggeri che fanno ingresso nel territorio dello Stato italiano, che i vettori aerei hanno l'obbligo di trasmettere ai competenti uffici di polizia di frontiera. Si segnala in merito che tale disciplina è oggetto di un'altra direttiva europea – ossia la direttiva (CE) 2004/82 – che è stata già recepita nel nostro ordinamento con il decreto legislativo 2 agosto 2007, n. 144. La scelta di assorbire nello schema di decreto in esame anche la regolamentazione dei dati API è motivata – secondo quanto si legge nella relazione illustrativa – « dall'identità dell'oggetto, ossia l'obbligo di trasmissione di informazioni relative ai passeggeri, e l'identità del soggetto su cui tale onere grava, ovvero i vettori aerei ». A questo riguardo, il Garante per la protezione dei dati personali ha rilevato che « il regime di raccolta previsto in attuazione della Direttiva API dal citato decreto del 2007 che si intende abrogare prevede una selettività nell'individuazione dei voli in entrata, esclude i voli in uscita, prevede tempi brevi di conservazione dei dati (24 ore) e la loro cancellazione a meno che, in casi specifici, vadano a confluire nel CED (commissione di reati). Inserire quindi i dati API e la loro regolamentazione nello schema di decreto legislativo in questione, oltre ad apparire non strettamente necessario, potrebbe rivelarsi non proporzionale, attesa la mancanza di ogni valutazione d'impatto in merito e considerati i differenti ambiti regolati dalla rispettiva disciplina ». Alla luce di tali considerazioni, il Garante pertanto suggerisce « una rivisitazione delle disposizioni che riguar-

dano il trattamento dei dati API, facendo salve quelle sole disposizioni conformi alle puntuali previsioni della direttiva 681, espungendo le altre, qualora volte a modificare il d. lgs. 144/2007 ». Sul punto ritiene pertanto necessario acquisire un chiarimento da parte del Governo.

Il comma 3 definisce l'ambito di applicazione, precisando che l'attuazione della Direttiva non pregiudica l'applicazione degli accordi o delle intese bilaterali o multilaterali sullo scambio di informazioni tra autorità competenti entrati in vigore con Stati membri dell'Unione europea entro il 24 maggio 2016, data di entrata in vigore della direttiva, in quanto compatibili con la direttiva stessa, né l'applicazione degli obblighi derivanti da accordi bilaterali o multilaterali conclusi con Stati terzi, ossia non appartenenti all'Unione europea.

L'articolo 2 reca disposizioni di carattere definitorio. Oltre a recepire le definizioni contenute nella direttiva (UE) 2016/681, rientrano, in particolare, nella definizione di « autorità competenti nazionali »: le Forze di polizia di cui all'articolo 16, comma 1, della legge n. 121 del 1981; la Direzione Investigativa Antimafia; gli Organismi di informazione e sicurezza facenti parte del Sistema di Informazione per la Sicurezza della Repubblica, di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007; la Direzione Nazionale Antimafia e Antiterrorismo; le Autorità giudiziarie competenti a perseguire i reati di terrorismo e i reati gravi. Per Unità di informazione sui passeggeri (UIP) nazionale, ossia l'autorità competente in materia di prevenzione e repressione dei reati di terrorismo e dei reati gravi, che ai sensi della direttiva spetta a ciascuno Stato membro individuare, si intende l'Unità istituita presso il Dipartimento della pubblica sicurezza del Ministero dell'interno, nell'ambito della Direzione centrale della polizia criminale. Assumono rilievo, soprattutto ai fini dell'accorpamento delle discipline delle direttive 2016/681/UE e 2004/82/CE, anche le definizioni di: « dati PNR », con cui s'intendono le informazioni relative al viaggio di ciascun passeggero consistenti nei dati di cui all'allegato I della direttiva 2016/681/UE, necessari per il trattamento e il controllo delle prenotazioni da parte dei vettori aerei e contenuti nel codice di prenotazione; « dati API », con cui si intende parte dei dati PNR, comprendenti il tipo, il numero, Paese di rilascio e la data di scadenza del documento di viaggio utilizzato, la cittadinanza, il nome completo, il sesso, la data e il luogo di nascita, il valico di frontiera di ingresso nel territorio italiano, la compagnia aerea, il numero di volo, la data di partenza e di arrivo, l'ora di partenza, l'ora di arrivo e la durata del volo, l'aeroporto di partenza e di arrivo, il numero complessivo dei passeggeri trasportati con tale volo, il primo punto di imbarco.

L'articolo 3 disciplina le finalità del trattamento dei dati raccolti a norma dello schema di decreto. A tal fine, la disposizione considera la diversa tipologia dei dati a cui associa due distinte finalità. Da un lato, i dati PNR sono trattati, in ossequio alla direttiva 2016/681/UE, per fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi. Dall'altro, la finalità del trattamento dei dati API, raccolti e resi disponibili agli Uffici incaricati dei controlli di polizia di frontiera secondo le disposizioni del decreto, è di migliorare i controlli delle frontiere esterne e prevenire l'immigrazione illegale. La disposizione specifica che il trattamento dei dati API può essere esteso ai voli *intra-UE* in caso di ripristino temporaneo dei controlli di frontiera.

L'articolo 4 prevede al comma 1 l'istituzione del « Sistema Informativo » attraverso il quale verranno raccolti, trattati e trasferiti i dati del codice di prenotazione (PNR), di cui alla direttiva (UE) 2016/681, e le informazioni anticipate sui passeggeri (API), di cui alla direttiva 2004/82/CE. Il Sistema, ai sensi del comma 2, è istituito presso il Dipartimento della pubblica sicurezza del Ministero dell'interno, a cui sono attribuite anche le funzioni di titolare del trattamento ai sensi di quanto previsto dal Codice per la protezione dei dati personali. Le funzioni di responsabile del trattamento sono invece attribuite a due diverse articolazioni del Dipartimento,

ossia la Direzione centrale della polizia criminale per quanto concerne i dati PNR e la Direzione centrale dell'immigrazione e della polizia delle frontiere con riferimento ai dati API. I commi 3 e 4 dispongono che le interrogazioni del Sistema possono essere effettuate esclusivamente per le finalità indicate dall'articolo 3 dello schema e da parte del personale titolare di uno specifico profilo di autorizzazione. Ai sensi del comma 5 la disciplina tecnica del Sistema viene demandata ad uno o più decreti di natura non regolamentare adottati, entro tre mesi dalla data di entrata in vigore del decreto, dal Ministro dell'interno, sentito il Garante per la protezione dei dati personali. Il comma 6 rimanda ad uno specifico decreto per disciplinare le modalità di trasferimento delle informazioni dall'UIP agli organismi del comparto *intelligence*, secondo la procedura prevista per l'adozione di disposizioni regolamentari ai sensi della legge n. 124 del 2007 sul sistema di informazione per la sicurezza della Repubblica. Il comma 7 stabilisce i formati di dati e i protocolli informatici che il Sistema informativo deve utilizzare. Ai sensi del comma 8, i vettori aerei che non effettuano voli secondo un programma operativo pubblico specifico e che non possiedono l'infrastruttura necessaria a supportare i formati di dati e i protocolli di trasmissione di cui al comma 7 devono trasferire i dati PNR con un mezzo elettronico che offra adeguate garanzie rispetto alle misure di sicurezza tecniche, individuato dall'Unità d'informazione sui passeggeri nazionale con apposita prescrizione. A questo riguardo il Garante per la protezione dei dati personali ha rilevato l'opportunità di prevedere che tale individuazione avvenga sentito il Garante medesimo. Sul punto ritiene necessario acquisire l'avviso del Governo.

L'articolo 5, al comma 1, prevede l'obbligo per i vettori aerei di trasferire al Sistema informativo i dati PNR relativi ai voli in partenza, in arrivo o facenti scalo nel territorio nazionale raccolti nello svolgimento della loro attività. I vettori aerei, ai sensi del comma 2, devono utilizzare, per il trasferimento dei dati PNR, i formati di dati e i protocolli informatici comuni individuati con la decisione di esecuzione 2017/759/UE della Commissione, del 28 aprile 2017. Inoltre, al successivo comma 3, si prevede che nelle more dell'adeguamento dei propri sistemi informatici i vettori aerei effettuino il trasferimento dei dati PNR con un mezzo elettronico che offra sufficienti garanzie rispetto alle misure di sicurezza tecniche e alle misure organizzative relative ai trattamenti da effettuare. Secondo il Garante per la protezione dei dati personali, « sarebbe opportuno che le specifiche tecniche di tali mezzi elettronici di trasmissione siano oggetto di un preventivo parere da parte del Garante ». Sul punto reputa necessario acquisire l'avviso del Governo. I commi 4 e 5 individuano momenti distinti per il trasferimento dei dati PNR. Al comma 6 si dispone che, nell'ipotesi in cui vengano trasferiti dati diversi da quelli richiesti in base alla normativa europea (allegato I della direttiva PNR), l'Unità di informazione sui passeggeri nazionale provvede alla loro immediata cancellazione.

L'articolo 6 disciplina composizione e funzioni dell'Unità d'informazione sui passeggeri (UIP) nazionale. Ai sensi del comma 2, in particolare, l'UIP nazionale è l'organo deputato a ricevere dai vettori aerei i dati PNR e, soprattutto, l'organo competente ad analizzare, prima dell'arrivo o della partenza del volo, i dati ricevuti per individuare eventuali passeggeri che potrebbero essere implicati in reati di terrorismo o in altri reati gravi per i quali è necessario procedere ad ulteriori verifiche da parte delle autorità competenti. In attuazione del criterio direttivo previsto dalla legge di delegazione europea, il regolamento prevede che l'UIP nazionale sia incardinata presso il Dipartimento della pubblica sicurezza del Ministero dell'interno. Il comma 1 prevede che l'unità sia composta da personale delle Forze di polizia e rimette l'organizzazione e la pianta organica dell'Unità ad un decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, al pari di come avviene per l'organizzazione interna di tutte le articola-

zioni del Dipartimento della pubblica sicurezza. Per quanto concerne il contingente di personale, esso viene stabilito con decreto del Ministero dell'interno per il personale appartenente ai ruoli della Polizia di Stato, mentre per quanto riguarda il personale delle altre Forze di polizia con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze e con i Ministri interessati.

L'articolo 7 individua, in conformità alle previsioni oggi contenute nel decreto legislativo. n. 144 del 2007 di attuazione della direttiva API, gli uffici incaricati di effettuare i controlli delle persone alle frontiere esterne attraverso le quali i passeggeri entrano nel territorio dello Stato, come gli organi incaricati del trattamento dei dati API per agevolare tali controlli al fine di prevenire l'immigrazione irregolare.

L'articolo 8, comma 1, definisce le modalità operative del trattamento dei dati PNR, specificando in particolare come l'Unità nazionale procede all'analisi di tali dati per l'individuazione dei passeggeri sospettati. A tal fine, infatti l'UIP può mettere a confronto i dati PNR con le informazioni contenute nella Banca dati delle Forze di polizia, e le altre banche dati europee ed internazionali che possano contenere informazioni utili per prevenire i reati di terrorismo o i reati gravi. Il comma 2 dispone che l'UIP può altresì trattare i dati sulla base di criteri predeterminati dalla stessa Unità, dopo aver sentito le autorità competenti nazionali, nel rispetto dei principi di proporzionalità, specificità e non discriminazione, mentre il comma 3 prevede che anche le modalità di analisi devono essere non discriminatorie. Ai sensi del comma 4, in caso di riscontro positivo, ove cioè sia individuato un passeggero sospettato di essere implicato in un reato di terrorismo o in reati gravi, all'esito di un trattamento automatizzato dei dati PNR, si prevede l'obbligo di procedere altresì ad un esame non automatizzato sul singolo caso per verificare la necessità di adozione di provvedimenti da parte delle autorità nazionali competenti, sulla base delle norme vigenti. Al comma 5 si precisa che l'adozione di provvedimenti da parte delle autorità competenti non pregiudica il diritto di entrare nel territorio dello Stato delle persone che godono del diritto di libera circolazione all'interno dell'UE in conformità alle disposizioni contenute nel decreto legislativo n. 30 del 2007, di attuazione della direttiva 2004/38/CE relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri.

L'articolo 9 definisce le modalità operative del trattamento dei dati API. In proposito, si stabilisce che il Sistema informativo rende consultabili i dati API agli uffici incaricati dei controlli di polizia di frontiera immediatamente dopo la chiusura del volo, quando non è più possibile effettuare operazioni di imbarco e di sbarco dei passeggeri. I dati non necessari per le finalità di prevenzione dell'immigrazione irregolare sono resi invisibili agli Uffici incaricati dei controlli di polizia di frontiera entro ventiquattro ore dalla loro comunicazione ovvero dopo l'ingresso dei passeggeri nel territorio dello Stato. I dati rilevanti per la citata finalità restano nella disponibilità degli uffici di frontiera per sei mesi dal loro ricevimento.

L'articolo 10 stabilisce al comma 1 le condizioni per la conservazione dei dati PNR, fissando innanzitutto il principio in base al quale i dati PNR sono conservati all'interno del Sistema informativo per un periodo di cinque anni dalla loro trasmissione da parte dei vettori aerei. Ciononostante, decorsi sei mesi dal loro trasferimento, i dati vengono resi anonimi mediante un'operazione di mascheramento di una serie di elementi che potrebbero servire a identificare direttamente gli interessati a cui i dati PNR si riferiscono. Tali elementi vengono esplicitamente individuati mediante elencazione al comma 2. Tuttavia, al comma 3 si prefigura l'ipotesi che allo scadere del periodo di sei mesi sia ancora consentita la comunicazione dei dati PNR integrali. Ciò può avvenire solo

se necessario per corrispondere a una richiesta debitamente motivata, formulata ai sensi del precedente articolo 6, comma 2. In tali ipotesi, il comma 3 richiede altresì la preventiva autorizzazione dell'Autorità giudiziaria nel caso in cui la richiesta sia formulata nell'ambito di un procedimento penale o per l'applicazione di una misura di prevenzione personale o patrimoniale ai sensi del Codice delle leggi antimafia (decreto legislativo n. 159 del 2011) o del Vice Capo della Polizia, nel caso in cui la richiesta sia formulata per le finalità di prevenzione dei reati di terrorismo e dei reati gravi. Tale autorizzazione, ai sensi del comma 4, deve essere comunicata al responsabile della protezione dei dati personali, nominato ai sensi del successivo articolo 21 dello schema, per le verifiche di competenza. In proposito, come rilevato dal Garante per la protezione dei dati personali, non appare chiaro « se a seguito dell'operazione con cui i dati sono resi anonimi mediante mascheramento, sia ancora possibile reidentificare gli interessati ». In tal caso i dati non possono essere trattati come anonimi nell'accezione di cui all'articolo 4, comma 1, lettera n) del Codice (il dato anonimo è « il dato che in origine , o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile »). Sul punto ritiene necessario acquisire un chiarimento da parte del Governo.

Il comma 5 stabilisce che, decorso il termine di cinque anni, è prevista la cancellazione in via definitiva dal Sistema informativo dei dati PNR secondo le modalità previste nei relativi decreti ministeriali di regolamentazione del Sistema. Costituisce eccezione a tale regola l'ipotesi in cui le informazioni siano state trasferite a una delle autorità nazionali competenti e utilizzate in un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. Ove ciò accada, i dati seguono il regime di conservazione previsto nel codice di procedura penale, ovvero quello vigente per i trattamenti per finalità di polizia, ovvero ancora quello relativo ai trattamenti effettuati dagli organismi di *intelligence*. Al comma 6 la disposizione prevede inoltre che i risultati del trattamento dei dati PNR effettuato dall'UIP nazionale sono conservati per il tempo strettamente necessario a comunicare eventuali riscontri positivi alle competenti autorità nazionali ovvero alle Unità nazionali degli altri stati membri. Ai sensi del comma 7, ove riversati nel CED, i dati PNR e i dati API sono sottoposti alla specifica disciplina prevista per il medesimo CED.

L'articolo 11 prescrive l'obbligo dei vettori aerei di cancellare i dati API trasmessi al Sistema informativo entro ventiquattro ore dall'arrivo del volo, come già attualmente previsto dall'omologa previsione contenuta nell'articolo 4, comma 3, del decreto legislativo n. 144 del 2007, di attuazione della direttiva API.

L'articolo 12 disciplina la procedura di comunicazione delle informazioni a livello interno, vale a dire la trasmissione dei dati PNR o dei risultati del loro trattamento da parte della UIP nazionale alle competenti autorità nazionali. Il comma 1 specifica che i dati in questione, trasmessi dalla UIP nazionale alle competenti autorità nazionali, sono quelli ricevuti al fine di individuare i passeggeri sospettati di essere implicati in reati di terrorismo o in reati gravi, per i quali si rende necessario procedere a ulteriori verifiche. Il comma 2 ribadisce che le decisioni delle autorità competenti nazionali che producono conseguenze giuridiche negative sull'interessato non possono essere adottate esclusivamente sulla base del trattamento automatizzato dei dati PNR. Il medesimo comma 2 dispone, altresì, che le decisioni delle autorità competenti nazionali non possono essere fondate su ragioni discriminatorie così enumerate: origine razziale o etnica, opinioni politiche, religione o convinzioni filosofiche, appartenenza sindacale, stato di salute, vita sessuale od orientamento sessuale dell'interessato.

L'articolo 13 disciplina la trasmissione dei dati PNR o dei risultati del loro trattamento da parte della UIP nazionale alle UIP degli altri Stati membri. Il comma 1 prevede che, in caso di riscontro posi-

tivo, la UIP nazionale trasmetta i dati PNR pertinenti e necessari o i risultati del loro trattamento alle UIP di altri Stati membri. Il comma 2 disciplina la trasmissione dei dati PNR (o di una loro parte) ovvero dei risultati del loro trattamento da parte della UIP nazionale sulla base di una richiesta della UIP di altro Stato membro. La richiesta deve essere debitamente motivata in relazione a un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. Il comma 3 disciplina la specifica ipotesi di richiesta, da parte di UIP di altro Stato membro, di dati che siano stati resi anonimi mediante il mascheramento di specifici elementi idonei a identificare il soggetto cui si riferiscono. La « trasformazione in forma anonima » scatta decorsi 6 mesi dal trasferimento dei dati trasmessi dai vettori aerei nel Sistema informativo istituito presso il Dipartimento della pubblica sicurezza. Sono inoltre stabilite le condizioni per la trasmissione da parte della UIP nazionale.

L'articolo 14 definisce i presupposti in presenza dei quali la UIP nazionale è legittimata a trasmettere le informazioni direttamente alle autorità competenti di altri Stati membri.

L'articolo 15 disciplina le condizioni in presenza delle quali la UIP nazionale può presentare una richiesta di trasmissione di dati PNR (anche parziali) ovvero di risultati del loro trattamento alla UIP di altro Stato membro. Il comma 1 dispone che la richiesta di trasmissione di dati PNR da parte della UIP nazionale alla UIP di altro Stato membro sia debitamente motivata in relazione a uno specifico caso afferente la prevenzione e repressione di reati di terrorismo o reati gravi. Il comma 2 introduce una deroga ai tempi imposti ai vettori aerei per il trasferimento dei dati al Sistema informativo nell'ipotesi di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o altro reato grave.

L'articolo 16 sancisce il principio generale secondo il quale le autorità competenti nazionali dialogano con le UIP di altri Stati membri attraverso la UIP nazionale. Costituiscono, pertanto, eccezioni le ipotesi in cui le autorità competenti nazionali sono legittimate a rivolgersi direttamente ad una UIP di altro Stato membro. Il comma 1 dispone che le autorità competenti nazionali inoltrano le richieste di dati PNR alle UIP degli altri Stati membri tramite la UIP nazionale. Il comma 2 introduce una deroga al principio generale di cui al comma 1 per le situazioni di emergenza che non consentono di inoltrare la richiesta attraverso la UIP nazionale.

L'articolo 17 disciplina le modalità operative previste dai precedenti articoli per il trasferimento dei dati PNR o dei risultati del loro trattamento da UIP nazionale a UIP di altro Stato membro e, viceversa, da UIP nazionale all'autorità competente di altro Stato membro o da UIP di altro Stato membro alla competente autorità nazionale.

L'articolo 18 definisce i presupposti e le modalità per la trasmissione dei dati PNR o dei risultati del loro trattamento a *Europol*. Per quanto riguarda i presupposti della richiesta, il comma 1 prevede che *Europol* possa chiedere la trasmissione di dati PNR quando essi siano « strettamente necessari » per sostenere e rafforzare l'azione degli Stati membri tesa alla prevenzione e repressione di un reato di terrorismo o di altro reato grave, purché si tratti di un reato rientrante nella competenza di *Europol* ai sensi del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio dell'11 maggio 2016. Prevede inoltre che *Europol* eserciti la propria facoltà di richiesta entro i limiti delle proprie competenze e per l'adempimento dei propri compiti. Sono inoltre definite le modalità di richiesta dei dati.

L'articolo 19 stabilisce i presupposti per la trasmissione dei dati PNR o dei risultati del loro trattamento, in relazione a casi individuali, a Paesi terzi. Il comma 1 definisce, innanzitutto, il quadro normativo entro cui si inscrive la trasmissione di dati PNR, in relazione a casi individuali, alle autorità competenti di un Paese terzo: sono fatte salve le condizioni previste da eventuali accordi internazionali; la tra-

smissione deve conformarsi esclusivamente alle previsioni del provvedimento in esame; si applicano le disposizioni del Codice per la protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, riguardanti il trasferimento verso Paesi terzi di dati giudiziari ovvero di dati trattati per finalità di polizia. La trasmissione alle autorità competenti di un Paese terzo è ammissibile in presenza di determinate condizioni. Il comma 2 pone inoltre le condizioni alle quali i dati PNR possono essere ulteriormente trasferiti senza il previo consenso dello Stato da cui provengono.

L'articolo 20 individua l'Autorità nazionale di controllo, individuata nel Garante per la protezione dei dati personali. Le funzioni che il Garante è chiamato ad esercitare sono previste svolgersi secondo le modalità previste dal Codice in materia di protezione dei dati personali (decreto legislativo n. 196 del 2013). È altresì introdotta la previsione che il Garante esprima, su richiesta dell'interessato, pareri in merito all'esercizio dei diritti di protezione dei dati personali, in relazione alle disposizioni del decreto legislativo recato dallo schema in esame. Tale previsione è volta a recepire l'articolo 15, paragrafo 4, della direttiva, secondo cui ciascuna autorità nazionale di controllo, su richiesta, consiglia l'interessato in merito all'esercizio dei diritti derivanti dalle disposizioni adottate conformemente alla medesima direttiva.

L'articolo 21 introduce la figura del responsabile della protezione dei dati PNR, individuato entro la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza del Ministero dell'interno. La sua designazione è demandata ad un decreto del Capo della Polizia – Direttore generale della pubblica sicurezza. Il responsabile per la protezione dei dati è figura distinta dal titolare e dai responsabili del trattamento. A tale figura compete la vigilanza sulla correttezza e sulla liceità del trattamento delle informazioni. Inoltre garantisce l'attuazione di tutte le misure tecniche e di sicurezza, nel rispetto di quanto disposto dal Codice per la protezione dei dati personali, e funge da punto di contatto unico per gli interessati, per tutte le questioni connesse al trattamento dei dati che li riguardino. La collocazione del responsabile è ritenuta ottemperare ad uno svolgimento delle funzioni « indipendente », secondo il dettato della direttiva. Viene ritenuta dunque in una posizione di 'alterità' rispetto alla struttura organizzativa dell'Unità d'informazione sui passeggeri (UIP), la quale è l'autorità in materia di previsione e repressione dei reati di terrorismo e dei reati gravi di cui all'articolo 6 dello schema.

L'articolo 22 sancisce l'applicabilità ai trattamenti dei dati personali effettuati ai sensi del presente schema degli strumenti di tutela previsti dal Codice per la protezione dei dati personali. In particolare, il comma 7 prevede che l'UIP conserva per un periodo di cinque anni i registri delle attività di raccolta, consultazione, comunicazione e cancellazione dei dati. Detti registri riportano l'indicazione delle finalità, della data e dell'ora dell'operazione e gli elementi relativi all'identità della persona che ha consultato o comunicato i dati PNR, nonché dei destinatari di tali dati. I registri sono usati esclusivamente a fini di verifica, di autocontrollo, per garantire l'integrità e la sicurezza dei dati o di *audit*. Al riguardo, il Garante per la protezione dei dati personali ha evidenziato che « i registri degli accessi e delle attività, di cui al comma in questione, contengono anch'essi dati personali degli interessati e, pertanto, sarebbe opportuno modificare la disposizione prevedendo che andranno trattati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei registri stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità previste ». Sul punto considera opportuno acquisire l'avviso del Governo.

L'articolo 23 riconosce ai soggetti interessati dai trattamenti disciplinati dal presente schema i diritti previsti dall'articolo 10, commi 3, 4 e 5, della legge n. 121 del

1981. Si prevede che i diritti siano esercitati previa presentazione di istanza alla Direzione centrale della polizia criminale. Della presentazione dell'istanza devono essere informati il responsabile della protezione dei dati e l'UIP nazionale (nonché l'UIP dello Stato membro eventualmente interessato). La Direzione centrale della polizia criminale comunica all'interessato i provvedimenti adottati a seguito delle richieste formulate nell'istanza. Le disposizioni della legge n. 121 del 1981 sopra richiamate concernono i dati personali raccolti presso l'Amministrazione della pubblica sicurezza. In particolare, la persona alla quale si riferiscono i dati può chiedere alla Direzione centrale della polizia criminale la conferma dell'esistenza di dati personali che lo riguardino, la loro comunicazione in forma intellegibile e, se i dati risultino trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ne possa conseguire pregiudizio ad azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali. Chiunque venga a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale (del luogo ove risiede il titolare del trattamento) di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.

L'articolo 24 reca le sanzioni, oggetto dell'articolo 14 della direttiva in recepimento. Il comma 1 prevede, infatti, la sanzione amministrativa pecuniaria da 10.000 a 100.000 euro nei confronti dei vettori aerei che non trasmettono i dati o li trasmettono con modalità differenti da quelle previste dall'articolo 5 dello schema di decreto in esame o li trasmette in maniera incompleta o errata. La medesima sanzione è irrogata in caso di mancato rispetto dei termini fissati dall'Unità d'informazione nazionale sui passeggeri (UIP) nazionale – ai fini dello scambio dei PNR con le UIP istituite presso gli altri Stati membri e con *Europol* – disciplinata dall'articolo 6 dello schema di decreto. Il comma 2 individua nell'ENAC l'autorità competente ad irrogare le sanzioni. Trova applicazione il procedimento previsto dalla legge n. 689 del 1981 (recante « Modifiche al sistema penale »), il quale disciplina le fasi dell'accertamento, notificazione e contestazione delle sanzioni. Il comma prevede esplicitamente che l'ENAC sia destinataria del rapporto contenente la prova delle eseguite contestazioni o notificazioni, come previsto dall'articolo 17 della citata legge n. 689. In caso di reiterazione delle violazioni, ai sensi del comma 3, l'ENAC può disporre la sospensione (da uno a dodici mesi) oppure la revoca della licenza, autorizzazione o concessione, relative all'attività svolta o al mezzo di trasporto utilizzato, rilasciate dalle autorità italiane. Il comma 4 stabilisce la sanzione amministrativa pecuniaria da 5.000 a 50.000 euro per la mancata cancellazione dei dati API prevista dall'articolo 11 dello schema di decreto. In tali casi l'autorità competente ad irrogare la sanzione è il Garante per la protezione dei dati personali. Ai sensi del comma 5, resta fermo quanto previsto dall'articolo 12, comma 6, del Testo unico immigrazione, di cui al decreto legislativo n. 286 del 1998: esso pone in capo al vettore (aereo, marittimo o terrestre) l'obbligo di accertare che lo straniero trasportato sia in possesso dei documenti richiesti per l'ingresso nel territorio dello Stato e a riferire all'organo di polizia di frontiera i casi di irregolarità dei passeggeri stranieri a bordo. In caso di inosservanza anche di uno solo degli obblighi di cui al presente comma, si applica la sanzione amministrativa da 3.500 a 5.500 euro per ciascuno degli stranieri trasportati; nei casi più gravi si può disporre la sospensione (da uno a dodici mesi) ovvero la revoca della

licenza, autorizzazione o concessione. Anche in questi casi trova applicazione la disciplina dettata dalla legge n. 689 del 1991.

Riguardo al tema delle sanzioni il Garante ha chiesto di valutare l'opportunità di applicare il medesimo trattamento sanzionatorio di cui all'articolo 24, comma 1 (sanzione da 10.000 a 100.000 euro) anche agli illeciti previsti dal comma 4 del medesimo articolo (mancata cancellazione dei dati API, per i quali si prevede una sanzione da 5.000 a 50.000 euro), in quanto caratterizzati da un disvalore non minore rispetto a quello che connota i primi. Sul punto appare opportuno acquisire l'avviso del Governo.

L'articolo 25 pone in capo al Ministero dell'interno alcuni obblighi di comunicazione di dati concernenti i PNR trasmessi alla UIP nazionale.

L'articolo 26 reca disposizioni transitorie e finali.

L'articolo 27, coerentemente con quanto già disposto dalla norma di delega di cui all'articolo 12, comma 2, della legge n. 163 del 2017, reca una apposita clausola di neutralità finanziaria, in considerazione del fatto che il provvedimento non stanzia ulteriori risorse. A tale proposito si ricorda infatti che, prima della data di entrata in vigore della citata legge n. 163 del 2017, l'articolo 1, comma 608, della legge di bilancio 2017 (legge n. 232 del 2016) aveva stanziato risorse per l'attuazione della direttiva PNR pari a 5,5 milioni di euro per l'anno 2017, 16 milioni per l'anno 2018 e 4,5 milioni a decorrere dal 2019. Tali risorse sono allocate sui seguenti capitoli dello stato di previsione del Ministero dell'interno: 7505 (»Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR) » – parte capitale); 2563 (»Spese per la gestione e manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR) » – parte corrente). Nel bilancio di previsione per il 2018 e per il triennio 2018-2020 (legge n. 205 del 2017), il cap. 7505 reca uno stanziamento di 16 milioni di euro per il 2018; il cap. 2563 reca uno stanziamento pari a 4,5 milioni di euro annui a decorrere dal 2019. Inoltre, la relazione tecnica posta a corredo del presente schema segnala che la Commissione europea ha reso disponibili ulteriori 5,98 milioni sul Fondo Sicurezza Interno-Programma Nazionale d'Italia, per il 50 per cento di quota europea, ai fini dell'attuazione della direttiva PNR.

In conclusione, desidera richiamare l'attenzione del Governo in particolare sui rilievi contenuti, in relazione a talune disposizioni del presente schema di decreto, nel parere espresso dal Garante per la protezione dei dati personali, di cui a suo giudizio si dovrà debitamente tenere conto, anche sotto forma di osservazioni o condizioni, in sede di predisposizione della proposta di parere. A tale ultimo riguardo, nell'ottica di uno spirito collaborativo, ritiene utile che i gruppi parlamentari possano far pervenire eventuali osservazioni e contributi sul provvedimento in esame auspicabilmente già entro la fine della settimana in corso, al fine di poterne tenere debitamente conto in sede di elaborazione della proposta di parere in vista della seduta programmata per la prossima settimana. Ribadisce che le maggiori criticità, come peraltro emerso nel corso della sua relazione, attengono all'esigenza di un adeguato livello di sicurezza, anche sotto il profilo della tutela dei principi di riservatezza, nel trattamento dei dati PNR e API, preoccupazione quest'ultima che assicura sarà attentamente valutata in sede di stesura della proposta di parere.

Per elementi di maggior dettaglio in merito ai profili finanziari del provvedimento, rinvia infine alla documentazione predisposta dagli uffici.

Nicola MOLTENI, *presidente,* osserva come il parere espresso dal Garante per la protezione dei dati personali sollevi questioni indubbiamente meritevoli di approfondimento.

Il sottosegretario Domenico MANZIONE fa presente che, pur comprendendo le preoccupazioni manifestate dal Garante per la protezione dei dati perso-

nali in riferimento al tenore di talune disposizioni dello schema di decreto in esame, i dati API costituiscono comunque un sottoinsieme dei dati PNR e pertanto, in questa ottica, affidarne la relativa disciplina a differenti fonti normative potrebbe risultare disfunzionale rispetto alla finalità della direttiva oggetto di recepimento, che è essenzialmente quella di rafforzare gli strumenti di prevenzione ed indagine nei confronti, in particolare, dei reati di terrorismo. Ritiene altresì che il fatto di avere unificato le discipline concernenti i dati PNR e API non è suscettibile di recare, di per sé, alcun pregiudizio alla salvaguardia di un adeguato livello di tutela della riservatezza nel trattamento dei dati personali.

Francesco BOCCIA (PD) apprezza l'invito rivolto dal relatore ai gruppi parlamentari a presentare, qualora lo ritengano utile, proprie osservazioni sul provvedimento in titolo ai fini della predisposizione della proposta di parere, auspicando peraltro che il relatore possa inoltrare ai gruppi medesimi, anche per le vie brevi, una bozza di parere con un congruo anticipo di tempo.

Vittorio FERRARESI (M5S), *relatore*, nel rassicurare il deputato Boccia su tale ultimo aspetto, confida di inoltrare ai gruppi una bozza di parere già entro la giornata di lunedì prossimo. In riferimento all'intervento del sottosegretario Manzione, pur condividendo le finalità in chiave antiterroristica sottese allo schema di decreto, segnala tuttavia che la questione relativa all'accesso delle banche dei dati PNR e API, e più in generale quella concernente la tutela dei diritti di riservatezza, richiede una riflessione particolarmente approfondita, anche nell'ottica di pervenire all'espressione di un parere quanto più possibile condiviso.

Il sottosegretario Domenico MANZIONE manifesta la piena disponibilità del Governo ad interloquire in merito ai singoli aspetti evidenziati dal Garante per la protezione dei dati personali, nonché ad individuare un nuovo termine per l'espressione del parere da parte della Commissione. A tale proposito, nel rilevare che il nuovo termine dovrà comunque risultare coerente con quello già previsto per l'esercizio della delega, suggerisce – analogamente a quanto già stabilito nella seduta di ieri in relazione agli atti del Governo nn. 2 e 3 – di fissare il predetto termine alla data del prossimo 3 maggio.

Nicola MOLTENI, *presidente*, nel prendere atto, concorde la Commissione, del nuovo termine del 3 maggio prossimo per l'espressione del parere, nessun altro chiedendo di intervenire, rinvia quindi il seguito dell'esame ad altra seduta.

Schema di decreto legislativo di attuazione di una direttiva europea sulla sicurezza delle reti e dei sistemi informativi.
Atto n. 10.

(Esame, ai sensi dell'articolo 143, comma 4, del regolamento, e rinvio).

La Commissione inizia l'esame dello schema di decreto ministeriale in oggetto.

Stefano BUFFAGNI (M5S), *relatore*, avverte che lo schema di decreto legislativo di attuazione della direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, è stato trasmesso nel corso della scorsa legislatura (in data 21 febbraio 2018) e quindi assegnato alla Commissioni riunite I (Affari costituzionali) e IX (Trasporti) nonché, per le conseguenze di carattere finanziario, alla V Commissione (Bilancio). In data 12 aprile 2018 la Presidenza ha nuovamente proceduto alla assegnazione della medesima richiesta di parere parlamentare alla presente Commissione speciale. Fa presente quindi quanto segue.

Lo schema di decreto legislativo costituisce esercizio della delega che, come di consueto, viene attribuita dalla legge di delegazione europea 2016-2017 con riguardo alle direttive elencate in allegato,

tra cui la direttiva (UE) 2016/1148 (inserita nell'Allegato A), il cui termine di recepimento nell'ordinamento interno è fissato al 9 maggio 2018. La delega in oggetto – per effetto del meccanismo di scorrimento del termine, funzionale a consentire tempi adeguati per l'espressione del parere parlamentare e la valutazione delle indicazioni in esso recate – scade il 21 maggio 2018.

La citata disposizione di delega prevede quaranta giorni dalla data di trasmissione per l'espressione del parere parlamentare. Segnala, peraltro, che non è stato ancora reso il parere della Conferenza Unificata e, pertanto, ad oggi la Commissione, ancorché il termine per l'espressione del parere sia scaduto il 2 aprile 2018, non è nelle condizioni per concludere l'esame dell'atto. Si dovrà quindi concordare con il Governo un nuovo termine per l'espressione del parere che risulti coerente con quello previsto per l'esercizio della delega.

Oltre che sui profili di merito, la Commissione speciale è chiamata ad esprimersi anche sui profili finanziari. Al riguardo, ove il Governo non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81 della Costituzione, è tenuto a ritrasmettere alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, da rendere entro venti giorni.

La direttiva oggetto di recepimento con il presente schema di decreto legislativo – c.d. « direttiva NIS – *Network and Information Security* », del 6 luglio 2016 – muove dalla finalità di conseguire un livello elevato di sicurezza delle reti e dei sistemi informativi in ambito nazionale, nonché incrementare il livello comune di sicurezza nell'Unione europea.

È noto che gli incidenti informatici sono causa quotidiana di gravi danni economici e che i rischi della criminalità cibernetica aumentano in maniera esponenziale per effetto di minacce sempre più sofisticate e imprevedibili. In questo quadro, poiché la sicurezza complessiva dipende dall'anello più debole della catena, occorre innalzare i diversi livelli di capacità tecnica degli Stati membri per giungere ad un livello comune elevato di sicurezza delle reti e dei sistemi informativi, pubblici e, soprattutto, privati.

Nelle relazione AIR allegata al testo si citano alcuni dati esemplificativi tra cui: l'impatto economico della cibercriminalità sarebbe aumentato di cinque volte tra il 2013 e il 2017 (»e potrebbe quadruplicarsi entro il 2019 »); l'attacco *ransomware WannaCry* nel maggio 2017 ha colpito più di 400.000 computer in oltre di 150 Paesi.

Per dare attuazione agli obblighi previsti dalla direttiva, lo schema di decreto legislativo in esame detta quindi la cornice legislativa delle misure da adottare ed individua i soggetti competenti, completando e innovando la normativa vigente.

In questa sede, si può sinteticamente ricordare che l'architettura strategica nazionale per la protezione cibernetica e la sicurezza informatica è stata delineata per la prima volta con il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013. In sua attuazione sono stati adottati il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica che contengono gli obiettivi strategici e operativi della cyber security italiana.

Da ultimo, nelle *Gazzette Ufficiali* del 17 febbraio e del 1° giugno 2017 sono stati, rispettivamente, pubblicati il decreto del Presidente del Consiglio dei ministri in materia di protezione cibernetica ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica relativo al 2017.

Nell'insieme questi documenti individuano, in maniera organica, i compiti affidati a ciascuna componente istituzionale, nonché meccanismi e procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.

Nel rinviare alla documentazione predisposta dagli uffici per una disamina

analitica dell'articolato e dei relativi profili finanziari, fa presente che provvederà a riassumere in questa sede i principali contenuti dell'atto, che si compone di 22 articoli distinti in sette capi.

La finalità di conseguire un livello elevato di sicurezza della rete e dei sistemi informativi nei termini già descritti viene perseguita attraverso tre azioni principali.

In primo luogo (articoli 1 e 6), si prevede l'adozione – con atto del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR) – della « strategia nazionale di sicurezza cibernetica », nonché delle relative linee di indirizzo attuative, in cui includere previsioni in materia di sicurezza delle reti e dei sistemi informativi. Tale atto è trasmesso alla Commissione europea entro tre mesi dalla sua adozione. Come atto strategico, esso reca obiettivi, priorità, *governance* del sistema, misure da adottare, programmi di formazione, piani di ricerca e sviluppo; la valutazione dei rischi e l'elenco dei vari attori coinvolti nell'attuazione.

Tale strumento costituisce quindi una nuova declinazione dell'attuale Piano nazionale per la protezione cibernetica e la sicurezza informatica adottato nel marzo 2017.

La seconda linea di intervento riguarda la costruzione di una adeguata architettura istituzionale. Gli articoli 1, 7, 8, 9, 10 e 11 individuano i soggetti istituzionali competenti e li inseriscono nelle corrispondenti strutture comunitarie per la cooperazione e il reciproco scambio di informazioni.

Sono quindi designate come « autorità NIS » i singoli ministeri in base agli ambiti di competenza (Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, Ministero della salute, Ministero dell'ambiente e della tutela del territorio e del mare) e, per taluni profili, le regioni e province autonome: esse sono responsabili dell'attuazione del provvedimento – esercitando altresì le relative potestà ispettive e sanzionatorie – e individuano gli operatori essenziali soggetti agli obblighi del presente provvedimento.

Il Dipartimento delle informazioni per la sicurezza (DIS) è designato come punto di contatto unico, quale organo incaricato a livello nazionale di compiti di coordinamento e cooperazione a livello di Unione europea.

Come « Gruppo di intervento per la sicurezza informatica in caso di incidente in ambito nazionale » (CSIRT – *Computer Security Incident Response Team*) viene istituito – presso la Presidenza del Consiglio dei ministri – un nuovo organismo, il CSIRT italiano, con un contingente di 30 persone e lo stanziamento di specifiche risorse finanziarie al quale sono attribuite le funzioni attualmente svolte dal CERT (*Computer Emergency Response Team*) e dal CERT-PA, a decorrere dall'entrata in vigore del relativo decreto di organizzazione e funzionamento.

L'« autorità di contrasto » è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, cui è già attualmente attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale.

La terza linea di intervento riguarda la definizione di obblighi – e relativi controlli e sanzioni – a carico degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante.

Occorre premettere che l'articolo 1 esclude dall'ambito di applicazione del provvedimento (in quando soggette ad una diversa disciplina) le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, nonché i fornitori di servizi fiduciari qualificati e non qualificati. Inoltre, viene espressamente salvaguardata la disciplina vigente riguardante l'individuazione e la designazione delle infrastrutture critiche europee e la relativa protezione, nonché le misure adottate per la salvaguardia delle funzioni essenziali dello Stato e, in particolare, di tutela della sicurezza nazionale.

In questa cornice, la nuova disciplina trova applicazione nei confronti degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Gli operatori di servizi essenziali (articoli 4 e 5) sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori e sotto-settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali).

Le rispettive autorità NIS entro il 9 novembre 2018 (termine fissato già dalla direttiva europea) identificano gli operatori con sede nel territorio nazionale, che forniscono un servizio essenziale per il mantenimento di attività sociali e/o o economiche fondamentali, la cui erogazione dipende dalla rete e dai sistemi informativi e che, in caso di incidente, causerebbe effetti negativi rilevanti per il numero di utenti, la dipendenza di altri settori essenziali, l'impatto sulle attività economiche e sociali o sulla pubblica sicurezza, la quota di mercato, la diffusione geografica o il mantenimento di un livello sufficiente del servizio.

L'elenco nazionale – presso il Ministero dello sviluppo economico – è aggiornato almeno con cadenza biennale e il punto di contatto unico trasmette alla Commissione europea le informazioni necessarie riferite alla formazione dell'elenco

Gli obblighi in capo agli operatori dei servizi essenziali (articolo 12) riguardano le misure tecniche e organizzative relative alla gestione dei rischi, le misure per prevenire e minimizzare gli impatti degli incidenti nonché le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti.

Tali misure devono essere assunte tenendo conto delle linee guida predisposte dall'apposito gruppo di cooperazione dell'Unione europea e delle specifiche misure definite dalle autorità NIS sentiti gli operatori interessati.

Il mancato adempimento di questo duplice obbligo, legato rispettivamente alla gestione dei rischi e prevenzione e minimizzazione degli incidenti, salvo che il fatto costituisca reato, è sanzionato con l'irrogazione di una sanzione amministrativa di medesimo importo compresa tra 12 e 120 mila euro (articolo 21, commi 1 e 2).

Ritiene che andrebbe valutata l'opportunità di riformulare la fattispecie di cui al comma 2 dell'articolo 21 facendo riferimento, come indicato nel testo dell'articolo 12, comma 2, « alle misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali ».

Sussiste inoltre un obbligo di notifica al CSIRT italiano nonché alla competente autorità NIS, da adempiere « senza ingiustificato ritardo » degli incidenti che abbiano un impatto rilevante sui servizi forniti, anch'esso assistito, qualora il fatto non costituisca reato, da una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro (articolo 21, comma 3).

Per valutare la rilevanza dell'incidente si tiene conto del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all'area interessata dall'incidente.

La notifica consente gli opportuni scambi di informazione tra gli organismi interni ed internazionali.

Per quanto riguarda la diffusione di informazioni al pubblico concernenti l'incidente essa può essere prevista « qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso », previa valutazione dell'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento, a cura della competente autorità NIS, d'intesa col CSIRT e previa consultazione dell'operatore di servizi essenziali (articolo 12, comma 13).

L'articolo 13 individua i poteri di controllo delle autorità NIS nei confronti degli operatori di servizi essenziali in merito al rispetto degli obblighi previsti dall'articolo 12, anche sotto il profilo degli effetti sulla sicurezza della rete e dei sistemi informativi.

L'autorità, indicando lo scopo delle richieste e specificando il tipo di informazioni da fornire, può richiedere sia le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza, sia la prova dell'effettiva attuazione delle politiche di sicurezza, anche attraverso le risultanze di un apposito audit curato dal medesimo NIS o da un revisore abilitato.

Gli operatori di servizi essenziali sono tenuti a fornire le informazioni richieste e, qualora non lo facciano, sono soggetti, salvo che il fatto non costituisca reato, a una sanzione amministrativa pecuniaria compresa tra 12 mila e 120 mila euro (articolo 21, comma 4).

Qualora dalla valutazione degli elementi forniti emergano delle carenze l'autorità NIS può emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porvi rimedio. Qualora l'operatore non osservi le istruzioni fornite, salvo che il fatto non costituisca reato, è assoggettato ad una sanzione amministrativa pecuniaria compresa tra 15 mila e 150 mila euro (articolo 21, comma 5).

Se l'incidente comporta violazione dei dati personali l'autorità competente opera in stretta cooperazione con il Garante per la protezione dei dati personali.

I fornitori di servizi digitali (articoli 14, 15 e 16) sono presi in considerazione con riferimento all'erogazione dei servizi indicati dall'allegato III: mercato online, motori di ricerca *online*, servizi di *cloud computing*. In questo ambito, sono però escluse dall'applicazione della normativa le microimprese e le piccole imprese come definite dalla raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.

I fornitori di servizi digitali sono tenuti ad adottare misure tecniche e organizzative dirette ad assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al servizio e alla gestione dei rischi, nonché alla prevenzione degli incidenti e minimizzazione del loro impatto.

Qualora essi non provvedano, salvo che il fatto non costituisca reato, l'articolo 22 prevede l'irrogazione di una sanzione amministrativa compresa tra 8 mila e 80 mila euro (articolo 22, comma 1, ultimo periodo e comma 2, ultimo periodo).

Sono inoltre tenuti a notificare « senza ingiustificato ritardo » gli incidenti che abbiano un impatto rilevante al CSIRT italiano nonché alla competente autorità NIS. L'omessa notifica invece comporta, ai sensi dell'articolo 21, comma 6, qualora il fatto non costituisca reato, una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

Per la rilevanza dell'incidente si prendono in considerazione parametri legati al numero di utenti interessati, la durata, la diffusione geografica, la portata del disservizio e l'impatto sulle attività economiche e sociali.

Tuttavia l'obbligo di notificare un incidente si applica ai fornitori di servizi digitali solo nel caso in cui essi abbiano accesso alle informazioni necessarie per valutare l'impatto di un incidente con riferimento ai parametri individuati al fine di valutare la rilevanza dell'incidente e si precisa che, fatto salvo questo obbligo, non sono imposti ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali.

Inoltre la disposizione prevede anche il caso in cui un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per l'erogazione di un servizio indispensabile per attività economiche e sociali fondamentali: in tal caso l'obbligo di notifica ricade direttamente sull'operatore e il mancato adempimento, salvo che il fatto non costituisca reato, comporta l'irrogazione della sanzione amministrativa pecuniaria tra 12 mila e 120 mila euro (articolo 21, comma 7).

Non sono invece assistiti da sanzioni indicate in questo testo gli obblighi legati all'applicazione delle disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente le misure tecnico-organizzative dirette ad assicurare un livello di sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III.

Qualora l'incidente riguardi due o più Stati membri, sono previste forme di comunicazione agli altri Stati membri coinvolti, a cura del CSIRT italiano, sia pure con modalità che tutelino la sicurezza e gli interessi commerciali del fornitore di servizi digitali, nonché la riservatezza delle informazioni.

Per quanto riguarda la diffusione di informazioni al pubblico concernenti l'incidente, viene rimessa al CSIRT, svolte le opportune consultazioni, la facoltà di informare il pubblico o di chiedere al fornitore di servizi digitali di provvedervi « qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso o qualora sussista comunque un interesse pubblico alla divulgazione dell'incidente » (articolo 14, comma 11).

L'articolo 15 individua i poteri di controllo delle autorità NIS nei confronti dei fornitori dei servizi digitali, consentendo di adottare misure di vigilanza ex post adeguate alla natura dei servizi e delle operazioni in caso di mancato rispetto degli obblighi previsti dall'articolo 14.

La disposizione prevede quindi gli obblighi in capo ai fornitori di servizi digitali, che sono tenuti a fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza, nonché a porre rimedio ad ogni mancato adempimento degli obblighi di cui all'articolo 14.

Tali precetti sono assistiti, salvo che il fatto non costituisca reato, dalla sanzione amministrativa pecuniaria fissata tra 12 mila e 120 mila euro (articolo 22, comma 8).

L'articolo 16 individua i criteri per definire a quale giurisdizione sia assoggettato il fornitore di servizi digitali, facendo riferimento alla sede dello stabilimento principale.

Con riferimento ai fornitori di servizi digitali che non sono stabiliti nell'Unione europea, si prevede l'obbligo di designare un rappresentante nell'Unione europea, in cui si radica anche la giurisdizione. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.

Come già evidenziato, l'articolo 19 attribuisce alle autorità competenti NIS i poteri ispettivi e di verifica necessari, anche in funzione dell'irrogazione, ai sensi degli articoli 20 e 21, delle sanzioni amministrative.

Infine, l'articolo 22 reca le relative disposizioni finanziarie, prevedendo, al comma 1, che agli oneri derivanti dagli articoli 7 (Autorità nazionali competenti e punto di contatto unico) e 8 (Gruppi di intervento per la sicurezza informatica in caso incidente – CSIRT) si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234. Con riferimento alle altre disposizioni del decreto è invece prevista, dal comma 2, la clausola di invarianza finanziaria.

Il sottosegretario Pier Paolo BARETTA si riserva di intervenire nel prosieguo della discussione.

Stefano FASSINA (LeU) rinnova la richiesta – già avanzata nell'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, della Commissione dello scorso 12 aprile – di procedere, nell'ambito dell'esame del presente schema di decreto, allo svolgimento di un ciclo di audizioni e segnatamente a quella dei rappresentanti della Cassa depositi e prestiti spa, in considerazione del recente ingresso della medesima società nel capitale azionario di TIM, vicenda quest'ultima che presenta evidenti riflessi anche sul versante della sicurezza delle reti.

Nicola MOLTENI, *presidente*, in relazione alla richiesta di svolgimento di audizioni testé formulata dal deputato Fassina, rinvia la questione all'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, della Commissione, che si svolgerà al termine della seduta in corso. Nessun altro chiedendo di intervenire, rinvia

quindi il seguito dell'esame ad altra seduta.

Schema di decreto del Presidente della Repubblica concernente modifiche al decreto del Presidente della Repubblica 7 settembre 2001, n. 398, recante regolamento di organizzazione degli uffici centrali di livello dirigenziale generale del Ministero dell'interno.
Atto n. 18.

(Esame, ai sensi dell'articolo 143, comma 4, del regolamento, e rinvio).

La Commissione inizia l'esame dello schema di decreto ministeriale in oggetto.

Guido CROSETTO (FdI), *relatore*, fa presente quanto segue.

Lo schema di regolamento in esame, che si compone di due articoli, dispone alcune modifiche al regolamento di organizzazione degli uffici centrali di livello dirigenziale generale del Ministero dell'interno di cui al decreto del Presidente della Repubblica n. 398 del 2001, volte ad aggiornare la compagine organizzativa e funzionale degli uffici che compongono la struttura del Dipartimento della pubblica sicurezza del medesimo dicastero. In particolare, è disposta la soppressione di una struttura di livello dirigenziale generale, con conseguente ridistribuzione delle relative funzioni.

L'iniziativa presenta, dunque, un oggetto circoscritto in attesa, come si legge nella relazione governativa, di una complessiva ridefinizione delle strutture del Ministero, prevista dall'articolo 12, comma 1-*bis*, del decreto-legge n. 13 del 2017. Tale disposizione ha, infatti, assegnato al Ministero dell'interno il compito di predisporre, entro il termine del 31 dicembre 2018, il nuovo regolamento di organizzazione ai sensi dell'articolo 2, comma 7, del decreto-legge 31 agosto 2013, n. 101, con la finalità, in particolare, di potenziare le strutture finalizzate al contrasto dell'immigrazione illegale e alla predisposizione degli interventi per l'accoglienza legati ai flussi migratori e all'incremento delle richieste di protezione internazionale.

Il provvedimento è stato adottato in attuazione delle disposizioni di cui agli articoli 4, 5, 14 e 15 del decreto legislativo 30 luglio 1999, n. 300, e successive modificazioni, recante riforma dell'organizzazione del Governo, a sua volta attuativo della delega di cui all'articolo 11, comma 1, lettera *a)*, della legge 15 marzo 1997, n. 59, che ha previsto l'emanazione di decreti legislativi diretti a razionalizzare l'ordinamento della Presidenza del Consiglio dei ministri e dei Ministeri.

Il regolamento in esame è emanato ai sensi dell'articolo 17, comma 4-*bis*, della legge n. 400 del 1988, introdotto dall'articolo 13 della citata legge n. 59 del 1997. Tale norma prevede che l'organizzazione e la disciplina degli uffici dei Ministri siano determinate con regolamento emanato ai sensi del comma 2 del medesimo articolo 17, cioè con regolamento di delegificazione in materia non coperta da riserva assoluta di legge. Il regolamento è adottato su proposta del Ministro competente, d'intesa con il Presidente del Consiglio dei ministri e con il Ministro dell'economia e delle finanze.

Il termine per l'espressione del parere è fissato a 30 giorni dall'assegnazione (12 maggio 2018).

L'articolo 1 prevede, al comma 1, la soppressione della Direzione centrale per gli affari generali della Polizia di Stato all'interno del Dipartimento della pubblica sicurezza, che costituisce una delle cinque articolazioni centrali del Ministero.

Il comma 2 individua gli uffici ai quali sono da riassegnare le competenze e le funzioni svolte dalla Direzione di cui è prevista la soppressione, in quanto già titolari di competenze contigue.

Si tratta, nel dettaglio, dei seguenti: la Segreteria del Dipartimento; la Direzione centrale dei servizi tecnico-logistici e della gestione patrimoniale; la Direzione centrale per le risorse umane, che il medesimo decreto provvede a ridenominare in Direzione centrale per gli affari generali e le politiche del personale della Polizia di Stato.

Gli obiettivi dell'intervento di aggiornamento della struttura del Dipartimento

della pubblica sicurezza, come esplicitato nell'analisi tecnico-normativa (ATN), consistono, oltre che in una semplificazione della struttura dipartimentale, nella volontà di implementare un modello di organizzazione che consenta una più efficace programmazione dei processi di spesa curati dal Dipartimento, nonché, attraverso accorpamenti di strutture e funzioni, la centralizzazione delle procedure di acquisto per le Forze di polizia.

L'articolo 2 dispone, al comma 1, che la Direzione centrale per gli affari generali della Polizia di Stato continua ad operare, in via transitoria, anche dopo l'entrata in vigore del regolamento correttivo, fino all'adozione dei provvedimenti organizzativi conseguenti alla sua soppressione. Si ricorda, infatti, che l'articolo 5, comma 7, della legge n. 121 del 1981 stabilisce che le competenze degli uffici, dei servizi e delle divisioni in cui si articola il Dipartimento della pubblica sicurezza, nonché la determinazione delle piante organiche e dei mezzi a disposizione sono effettuate con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia. Il comma 2 contiene la clausola di neutralità finanziaria, che esclude nuovi o maggiori oneri a carico del bilancio dello Stato per l'attuazione del provvedimento in esame.

Sul provvedimento in esame il Consiglio di Stato, nell'adunanza dell'8 marzo 2018, ha espresso parere favorevole, senza osservazioni.

Per quanto riguarda i profili di carattere finanziario del provvedimento rinvia, per elementi di maggior dettaglio, alla documentazione predisposta dagli uffici. A tal proposito precisa che, a suo avviso, il provvedimento non implica maggiori spese, trattandosi solo di una ripartizione di funzioni all'interno di una struttura già in essere.

Infine chiede al Governo di precisare la logica sottesa alla scelta di un intervento circoscritto come quello in esame.

Il sottosegretario Domenico MANZIONE fa presente che il provvedimento in esame è stato adottato per la necessità di intervenire in modo limitato e mirato sul Dipartimento di pubblica sicurezza, in attesa del ben più complesso e significativo provvedimento di riorganizzazione della struttura del Ministero.

Nunzio ANGIOLA (M5S) esprime una posizione nel complesso favorevole sul provvedimento in esame. Condivide quanto affermato dal relatore sull'invarianza di spesa.

Ricorda nel contempo che la questione della riorganizzazione del Dipartimento della pubblica sicurezza è datata, tanto che se ne parla da circa venticinque anni. Osserva che lo schema di decreto sopprime una direzione del Dipartimento anche al fine di arrivare a un'unica centrale di committenza. Fa però presente che tale obiettivo non viene colto dal provvedimento se non in modo limitato, dato che le centrali di committenza del Ministero sono attualmente ben sette, senza contare gli istituti di formazione. Si sarebbe quindi aspettato un intervento più ampio e non adottato in maniera estemporanea. Ritiene in conclusione necessario adottare provvedimenti con maggiore organicità, anche per rispondere alle esigenze poste dalla cittadinanza.

Il sottosegretario Pier Paolo BARETTA, ricordando che il comma 2 dell'articolo 2 dello schema prevede la clausola di invarianza finanziaria, conferma che dal provvedimento non derivano nuovi o maggiori oneri per il bilancio dello Stato.

Nicola MOLTENI, *presidente*, nessun altro chiedendo di intervenire, rinvia quindi il seguito dell'esame ad altra seduta.

La seduta termina alle 9.35.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

L'ufficio di presidenza si è riunito dalle 9.40 alle 10.25.