COMMISSIONE PARLAMENTARE DI INCHIESTA SUL LIVELLO DI DIGITALIZZAZIONE E INNOVAZIONE DELLE PUBBLICHE AMMINISTRAZIONI E SUGLI INVESTIMENTI COMPLESSIVI RIGUARDANTI IL SETTORE DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

RESOCONTO STENOGRAFICO

AUDIZIONE

21.

SEDUTA DI MARTEDÌ 28 MARZO 2017

PRESIDENZA DEL PRESIDENTE **PAOLO COPPOLA**

INDICE

PRESIDENZA DEL PRESIDENTE PAOLO COPPOLA

La seduta comincia alle 10.40.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso impianti audiovisivi a circuito chiuso.

(Così rimane stabilito).

Audizione del Prefetto Domenico Vulpiani, responsabile della transizione alla modalità operativa digitale del Ministero dell'interno e del viceprefetto Antonina Coduti, difensore civico digitale.

PRESIDENTE. L'ordine del giorno reca l'audizione del Prefetto Domenico Vulpiani, ispettore generale di amministrazione e responsabile unico del centro elaborazione dati del Ministero dell'interno, del viceprefetto Antonina Coduti, capo ufficio coordinamento e affari generali dell'ispettorato generale di amministrazione, accompagnati dal sovrintendente capo Stefano Gaudini, che ringrazio per la loro presenza.

Ricordo ai colleghi commissari che in una nota inviata al presidente della Commissione in data 16 marzo 2017 il capo dipartimento per le politiche del personale dell'amministrazione civile per le risorse finanziarie e strumentali, Luigi Varratta, ha comunicato che il Prefetto Vulpiani è stato nominato responsabile della transizione alla modalità operativa digitale, ai sensi dell'articolo 17, commi 1 e 1-*ter*, del codice dell'amministrazione digitale e che il viceprefetto Coduti è stata nominata difensore civico digitale ai sensi dell'articolo 17, comma 1-*quater*, del codice dell'amministrazione digitale.

Avverto i nostri ospiti che della presente audizione sarà redatto un resoconto stenografico e che, facendone espressa e motivata richiesta, in particolare in presenza di fatti illeciti sui quali siano in corso indagini tuttora coperte da segreto, consentendo la Commissione, i lavori proseguiranno in seduta segreta, invitando comunque a rinviare eventuali interventi di natura riservata alla parte finale della seduta.

Si tratta di un'audizione di natura prettamente conoscitiva, per la quale chiedo al dottor Vulpiani e alla dottoressa Coduti di fornire un quadro esplicativo quanto più ampio possibile dei loro compiti e dell'esperienza maturata durante il loro mandato, che non mi sembra lunghissimo per ora. Comunque magari ci potete raccontare cosa avete intenzione di fare per fare in modo che la vostra funzione sia efficace.

Cedo dunque la parola a Domenico Vulpiani e Antonina Coduti per lo svolgimento della relazione introduttiva, al termine della quale seguiranno eventuali domande o richieste di chiarimento da parte dei commissari.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Grazie, presidente. Buongiorno a tutti. Sono onorato di essere qui a rappresentare che cosa si sta facendo al Ministero dell'interno a proposito della razionalizzazione dei sistemi informatici. Volevo, se è ritenuto utile, fare un breve *excursus* sulla mia vita professionale, che, anche se al tramonto, è stata abbastanza ricca.

Provengo dai ruoli dalla Polizia di Stato. Ho iniziato a 19 anni. Volevo mettere in

evidenza alcuni aspetti che ho trattato durante questa mia esperienza perché potrebbero essere utili per quanto si va dicendo. Sono laureato a Roma. Ho fatto tutta la carriera nella Polizia di Stato. Nel 2011 sono stato nominato prefetto e mi hanno conferito due incarichi che hanno attinenza con quello che stiamo dicendo.

Nel corso della mia carriera mi sono occupato di antiterrorismo, di sicurezza informatica e di contrasto al *cyber crime*, perché sono stato il capo della Polizia postale per nove anni e, quindi, ho lavorato nella parte dell'informatica cosiddetta « investigativa », di *intelligence*, sia *cyber security* che *cyber terrorism*.

Prima della nomina a Prefetto, con la qualifica di dirigente generale ho avuto un incarico di « coordinatore di sicurezza informatica della protezione delle infrastrutture critiche del Paese » per circa due anni. Dopodiché, nel 2013 ho avuto l'attuale incarico di « coordinatore del gruppo di lavoro per la reingegnerizzazione e razionalizzazione dei sistemi informatici e delle infrastrutture di telecomunicazione del Ministero dell'interno ». In sostanza, stiamo attuando un consolidamento dei *data center* del Ministero dell'interno, un progetto che abbiamo portato avanti e che vi illustrerò più nel dettaglio. Mi sembra utile, perché è un tentativo che parte da lontano per avere un'organizzazione infrastrutturale informatica del Ministero più importante del nostro Paese in una maniera più moderna e più vicina anche alle esigenze dei cittadini.

Parallelamente a questi incarichi, ho avuto anche un incarico che ha poco a che vedere con l'informatizzazione. Sono commissario straordinario per la gestione del Municipio di Ostia, che è stato sciolto per mafia circa un anno e mezzo fa.

Desidero rivolgere una piccola nota di merito a un organismo che è diventato famoso nel nostro Paese. Ho assunto la direzione della Polizia postale nel 2001 e l'ho organizzata proprio per contrastare i crimini informatici, che vanno dalla pedopornografia alle frodi *on line*, al *cyber terrorism*, alla protezione delle infrastrutture critiche, che è un argomento ormai molto noto sulle cronache quotidiane.

Durante la mia direzione sono state create tre strutture. La prima è molto importante e riguarda il contrasto alla pedofilia. Si tratta di un fenomeno che ha tutta una sua logica e che si sviluppa dentro la rete in maniere molto differenziate. Avevamo bisogno di cambiare i processi investigativi rispetto al modello tradizionale che ricerca il reato. Per intenderci, le investigazioni condotte dal Commissario Montalbano sono investigazioni tradizionali. Combattere un crimine informatico significa che si ha davanti un computer, come l'ho io adesso, e che il criminale potrebbe essere dall'altra parte del mondo. Non si sa chi c'è dietro, chi è colui che sta operando. C'è stato un film straniero che si rifà alla trilogia di Larsson, che penso molti di voi abbiano visto. In effetti, la procedura è quella adottata dalla protagonista. Anzi, è posta in essere un'azione anche più sofisticata da parte di questi soggetti. In sostanza, si tratta di digitalizzare i processi investigativi. Già nel 2006 la Polizia postale aveva degli operatori che agivano attraverso un computer e che magari non incontravano mai i criminali dall'altra parte, perché poi chi li arrestava era qualcun altro e non quelli che operavano sul computer. È una logica che, secondo me, va applicata anche ai servizi al cittadino. Fare digitalizzazione non significa prendere un computer e utilizzarlo come macchina da scrivere. Bisogna digitalizzare proprio i processi e, quindi, anche i processi di organizzazione delle informazioni che vengono fornite a qualunque scopo.

Io ho fatto questa esperienza sulle informazioni investigative che mi servivano per prendere i criminali. È diverso il caso quando occorre dare un servizio al cittadino. Si debbono rivedere tutti i processi che stanno a monte, cioè far entrare la digitalizzazione nel processo stesso. È quello che dovrà essere fatto in futuro anche nel Ministero dell'interno e che in parte è stato fatto. Non è che siano stati fermi.

Un altro organo importante era il CNAIPIC, in sostanza, una sala operativa dedicata esclusivamente alle grandi aziende pub-

bliche o private che gestiscono i servizi essenziali per il Paese. Questo centro consente di avere un rapporto diretto con la Polizia postale, anche con la presenza di soggetti appartenenti a queste imprese, all'interno del nucleo investigativo della Polizia postale. La loro attività, molto spesso, è riservata, per ragioni di varia natura, per esempio quella di non compromettere in borsa le attività economiche di queste società. Molto spesso non è opportuno divulgare se queste aziende sono state « bucate », per ragioni di immagine anche del Paese. Bisogna più tacere che dire, ma anche in quel caso è stato realizzato un processo di investigazione integrato tra pubblico e privato. Le potenziali vittime hanno fornito, molto spesso, le notizie che potevano servire all'investigazione già in fase preventiva.

Da ultimo, è stato creato il « commissariato virtuale » per consentire direttamente la denuncia in rete dei crimini informatici. Una frode *online* non va considerata come singola denuncia. A volte fa parte di una serie di denunce, perché molto spesso la diffusione dei *virus* è « a pioggia ». Quando ne trovi due o tre dello stesso livello, allora cominci fare le indagini, perché devi focalizzare la frode partendo da tante vittime e arrivando all'autore.

Ovviamente, questa mia esperienza sia nel campo dell'antiterrorismo, sia nel campo informatico ha fatto sì che queste due esperienze unite assieme abbiano anche esagerato la mia competenza in alcune attività. Quindi, spesso sono stato chiamato a raccontare quello che facevo.

Col presidente avevamo già parlato, in tempi non sospetti, di questo. Eravamo all'inizio, mi pare tre anni fa. Quando ho avuto questo incarico del gruppo di lavoro, andai a trovare il presidente Coppola, proprio perché sapevo che era una persona...

PRESIDENTE. Non ero presidente allora.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*....che aveva una *vision* molto vicina a quella che noi volevamo proporre. Devo dire che ottenni anche un grande incoraggiamento, perché eravamo proprio all'inizio.

Forse i miei colleghi che sono venuti qui prima di me hanno già esposto alcune delle funzioni del Ministero dell'interno. I dipartimenti del Ministero dell'interno sono cinque, con funzioni con *core business*, per usare un termine aziendale anche nel Ministero, completamente diversi uno dall'altro. Hanno lavorato sempre in queste condizioni e, quindi, hanno sviluppato un loro sistema informatico con un loro CED, o anche con più di un CED. Il più complesso di questi dipartimenti è il dipartimento della pubblica sicurezza, all'interno del quale c'è un Corpo di Polizia, la Polizia di Stato, ma non solo, c'è anche il coordinamento delle varie Forze di polizia e di altri enti che vi fanno capo. Il Capo della Polizia è anche direttore generale della pubblica sicurezza. Scusate se abuso di un termine, ma è come se fosse il « Ministro dell'interno tecnico », è il braccio destro del Ministro dell'interno nell'ambito della sicurezza. Nell'ambito del Ministero dell'interno si sono una serie di funzioni che vanno da funzioni interne di organizzazione (che sono state informatizzate), a funzioni e servizi erogati per il cittadino.

La prima cosa che abbiamo tentato di capire, anche attraverso il frutto dell'esperienza, è che c'erano dei servizi erogati ai cittadini perbene e dei servizi dati ai cittadini « per male ». Ovviamente, anche per questi ultimi sono state create numerose banche dati, che sono legate al sistema investigativo, il che poteva essere, ed è sicuramente, diverso dal fornire una carta d'identità elettronica. Sono cose completamente diverse. Tenendo conto di questo, siamo partiti intanto dall'unificare ciò che si poteva unificare, praticamente le scatole. Ogni dipartimento aveva la sua scatola, anzi più di una scatola, dove metteva i suoi giocattoli. È come avere tanti giradischi per casa per quanta musica uno vuole sentire. Almeno unifichiamo i giradischi. Bisogna anche vincere determinate mentalità. Questi dipartimenti sono gestiti anche da personaggi di grande spessore e hanno una loro identità. I Vigili del fuoco hanno una

loro identità e la sentono anche come Corpo. Bisogna anche vincere le tradizioni, nel senso positivo del termine. Pertanto, abbiamo messo in ordine queste cose e abbiamo fatto una ricognizione generale soprattutto sotto il profilo dell'*hardware* che esisteva. Essendoci più *data center* per lo stesso dipartimento, lo scopo era cercare di eliminarli e farne, al massimo due, uno di continuità di servizio e uno più forte, in cui potessero tutti convogliare.

Tenete presente che la Polizia di Stato il suo consolidamento dei *data center* l'aveva già fatto e lo sta facendo. Il 90 per cento è stato consolidato a Napoli, in un unico *data center* che riguarda la Polizia di Stato, mentre un consolidamento delle funzioni tra le varie Polizie, Carabinieri, Finanze e tutto ciò che è interforze è stato concentrato in un polo ad Anagnina, dove c'è la banca dati interforze, che è la banca dati cui tutti accedono per vedere i precedenti. Quando ci controllano i documenti per strada, la pattuglia entra in questa banca dati e vede se siamo ricercati e se la nostra patente è rubata, tutto in automatico. Tutto questo segue, come dicevo, una procedimentalizzazione che è stata già innescata negli anni, perché serviva a far funzionare meglio i servizi di Polizia, anche perché nell'emergenza la sicurezza detta sempre regole più veloci rispetto all'ordinario.

Sull'ordinario, invece, volevamo intervenire organizzando i servizi dei cittadini, come dicevo prima, mettendo intanto a posto l'infrastruttura sottostante. Un altro dato che ci serviva era vedere quante persone fossero addette a questi CED. Parliamo dei primi quattro dipartimenti. Abbiamo verificato la presenza di un totale di 290 persone addette ai CED, delle quali alcune anche in *outsourcing*, cioè personale che lavora all'interno del Ministero dell'interno, ovviamente con tutte le dovute procedure, ma in numero eccessivo. Un *data center* normale si gestisce con dieci persone. Se poi queste sono dieci tecnici, sono più che sufficienti. Noi ne abbiamo addirittura 290.

Consolidare i *data center* significa anche risparmiare sul personale, e dedicare il personale specializzato allo sviluppo delle applicazioni in maniera più mirata. Se deve dedicarsi sempre a far funzionare i *data center*, lo stesso ingegnere non può lavorare su due fronti. Se togliamo tutta la parte gestionale, che è uguale per tutti, non c'è bisogno che chi gestisce l'informazione in un *data center* sappia che cosa sta gestendo. Deve gestire in sicurezza, mettere in sicurezza e farlo funzionare, controllando che i processi di *business continuity* funzionino. È un controllo da affidare a degli addetti in grado di farlo. Si tratta di sviluppare, invece, il *cloud* sul piano applicativo. Quindi, avremo anche un risparmio significativo. Si tratta di arrivare a un'organizzazione di questo tipo. Una volta unificati i *data center*, si realizza un livello infrastrutturale che parte dall'infrastruttura fisica fino all'infrastruttura operativa che sia comune per tutti. Anche la *cyber security*, una volta che si unifica il perimetro difensivo, la riduci di moltissimo. L'esposizione all'esterno è molto più ridotta se si ha tutto concentrato, così anche se si spezzetta l'informazione. Il segreto della sicurezza è quello di avere un *data center*, che però deve essere collegato ad altri *data center* con lo stesso livello di sicurezza, e distribuire le informazioni in maniera differenziata. È questo che fanno colossi come Google ed Apple. Per questo sono sicuri.

Tutto questo va benissimo. Intanto si realizzano delle infrastrutture informatiche. Una parte delle nostre informazioni che riguardano la sicurezza dello Stato non può essere gestita tutta in *cloud* o affidata a operatori esterni che non siano al servizio dello Stato. Se privati, devono essere ben controllati, altrimenti rischiamo di cedere il nostro controllo a entità che potrebbero cambiare sulla base di cambiamenti politici. Una certa parte, come si dice nel gergo *on premise*, la dobbiamo tenere nel nostro Paese. Dobbiamo sapere dove sta. Per molti servizi, però, non è necessario utilizzare queste tecniche, che sono più sicure, ma sono anche meno performanti rispetto a un sistema in *cloud*.

Adesso vorremmo passare un attimo in seduta segreta, perché si sa dove si farà, ma si tratta di una località ben precisa.

PRESIDENTE. Oppure rimandiamo.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Va bene. Possiamo dirlo. Non dico la località, ma sarà quella. Abbiamo individuato una località vicino Roma, dove abbiamo una struttura del Ministero dell'interno, della Polizia di Stato in realtà, già sorvegliata. Questo è abbastanza noto, perché abbiamo fatto sopralluoghi. Non è riservato. Poi, alla fine, esporrò la parte riservata. Ci sono 12 capannoni industriali, per ora non utilizzati, perché erano i magazzini di quando avevamo il servizio di leva. I poliziotti che facevano la leva avevano tante divise. Adesso, proprio grazie all'informatizzazione, non abbiamo più le rimanenze di magazzino da gestire. Come si fa dappertutto, anche noi, se assumiamo uno, gli facciamo la divisa su misura, perché basta mandare le misure al fornitore e il fornitore fa tutte le divise per quel soggetto. È inutile avere le riserve. Una volta si dovevano avere tante taglie. Era un magazzino. Ora questi capannoni industriali sono perfetti per essere utilizzati come *data center*, ovviamente con i dovuti accorgimenti. Abbiamo individuato questo sito dove poter installare il *data center*. Uno o due al massimo di quei capannoni industriali – di estensione di circa 1.200 metri quadri l'uno – sono più che sufficienti per le esigenze del Ministero dell'interno, ma anche per quelle di eventuali altri ospiti che potremmo tenere dentro. È già sorvegliato. C'è vicino un ufficio di Polizia operativo. Si risparmia anche su quello.

Qual è il vantaggio di un *data center* unificato ? Intanto, ha il vantaggio di avere una continuità operativa che può essere realizzata lasciando dentro il Viminale un *data center* minore. Ci sarebbero, quindi, due *data center*, uno più grande in questa struttura a 30 chilometri dalla città, che può garantire la continuità operativa con zero tempi di interruzione. Ovviamente, in continuità operativa, a questi livelli, metteremo tutte le funzioni più importanti, per quanto riguarda i servizi del cittadino. Al contrario, per quanto riguarda l'archivio del personale, se c'è una risposta da un *disaster recovery* collocato in un'altra città, non è un grosso problema. Al dipendente della Polizia che deve andare in licenza, se si forniscono tempi di risposta di un'ora, non succede niente, mentre garantire una continuità operativa a zero tempo è indispensabile per tutta una serie di servizi critici. Una volta che si ha la struttura, lo si fa con un clic di *mouse*.

Il problema del Ministero dell'interno è che ha una struttura, per esempio, per il servizio elettorale che funziona due o tre volte l'anno. Funziona benissimo, ma per il resto del tempo non è impiegata per altre funzioni. Anche lo stesso personale continua a gestire il suo giocattolino e prepara le elezioni successive, ma è come tener ferme delle macchine e non farle camminare, non utilizzarle. L'unificazione consentirebbe di decidere, in questo periodo, di spostare tutte le applicazioni che riguardano i servizi elettorali, metterle a 30 chilometri e lavorare su queste in continuità operativa, perché in questo momento ci sono le elezioni ed è necessario garantire un servizio efficiente.

Il dipartimento del personale ha già tolto tutti i *server* nelle prefetture e ha già unificato in un unico *data center*. Quindi, le prefetture non hanno già più i *server* sotto il tavolo, dentro la cantina della prefettura, come era in passato. Sono tutti dentro il Ministero dell'interno. Non se ne sono accorti, ma abbiamo tolto tutti i *server* con un'operazione di organizzazione dell'*hardware*. Loro continuano a lavorare sul computer, ma non hanno più il problema che si blocchi il sistema, perché lo gestiamo in maniera centralizzata. Questa è la filosofia che deve guidare la riorganizzazione.

Quali sono i vantaggi ? Intanto eliminiamo 10-15 *data center*, più tutto quello che è parcellizzato, consentendo un riordino. Dovendo fare un *data center* nuovo, tutto quello che possiamo dare via lo sostituiamo con macchine più efficienti, che consumano di meno e hanno una continuità operativa. Adesso nei *data center* TIER IV è fondamentale il sito in cui viene collocato. Il luogo che abbiamo scelto ha un grande vantaggio, ossia che climaticamente ha due o tre gradi in meno. Le macchine nuove possono lavorare a temperatura mag-

giore. La temperatura esterna è più bassa e il gradiente che dobbiamo raffreddare si riduce molto di più. Se si riducono all'interno del *data center* anche gli spazi, alla fine l'energia costa molto meno. Inoltre, con una doppia linea di connettività, come prevedono i nuovi *data center*, si porta tutto a livello di sicurezza enorme anche come efficienza del servizio, con risparmio energetico, riduzione degli apparati e impiego di energie ambientalmente ecosostenibili. I *data center*, essendo dei capannoni, si possono riallestire come si vuole. Si smontano. Sono tutti pannelli di cemento armato che vanno smontati. Abbiamo già fatto il progetto. Questo è un progetto che è già stato rilasciato sotto il profilo edilizio. L'hanno rilasciato già un anno e mezzo fa. Andava solo finanziato. Ne derivano riduzione delle spese e forniture razionalizzate.

Tutto questo consentirà un passaggio successivo alla razionalizzazione dei sistemi operativi molto più facile anche per gli aspetti che riguardano la *cyber security*, perché si ha un sistema uniforme, omogeneo e all'avanguardia. Molte delle macchine che si acquisteranno e che si sostituiranno hanno già, di per se stesse, un sistema di *default*. C'è una serie di vantaggi economici notevolissimi.

Tutto questo può poi portare a securizzare in maniera più forte le banche dati. In questa *slide* ho citato le banche dati del Ministero dell'interno più importanti, ma ce ne sono tantissime altre. Già funziona la Banca dati antimafia, l'ANPR speriamo che decolli quanto prima, il servizio elettorale è un gioiellino, perché funziona, come ho detto prima.

PRESIDENTE. L'ANPR, però, è nel *data center* di Sogei.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Una volta che si ha il *data center*, i dati li riportiamo anche in casa. Almeno possiamo fare la continuità operativa con loro.

PRESIDENTE. Quindi, l'idea finale è di riportare...

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Questa era la mia idea, che ho suggerito nel progetto di riorganizzazione.

SEBASTIANO BARBANTI. Si tratta, quindi, di spostare da Sogei a...

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Oppure, poiché la Sogei è sempre ente pubblico, la continuità operativa la può tenere anche Sogei.

Dobbiamo immaginare come la continuità operativa dovrebbe essere in futuro. Non deve essere più un punto-punto per ogni dato. Per securizzare il settore, dobbiamo ragionare come ragionano quelli più bravi di noi. Con *Facebook* la mia immagine è situata in Irlanda, il mio nome in America e il cognome da un'altra parte. C'è uno spezzettamento del dato. Quella è la soluzione. In più, duplicano sempre più le informazioni. Quindi, per l'organizzazione sicura delle informazioni si deve fare bene la criptazione, perché ci sono sistemi che vanno reingegnerizzati sotto il profilo del *software*. Intanto, però, si devono avere delle strutture che, se ne cede una, automaticamente funzioni l'altra. Questo riguarda non solo il Ministero dell'interno, ma anche il Ministero dell'economia e delle finanze. Abbiamo fior fiori di aziende, compresa qualcuna italiana. Cito, per esempio, Aruba e la Telecom, che ha la Nuvola. L'80 per cento di questi servizi potrebbero essere mandati in *cloud*. Non è necessario reingegnerizzare. Si può averlo come servizio.

Quindi, l'infrastruttura va rivista in un'ottica diversa. Sto citando le fonti scritte sul Codice dell'Agenzia per l'Italia Digitale. Noi abbiamo seguito quelle linee guida. Abbiamo fatto una collaborazione con l'AgID e abbiamo seguito tutte le indicazioni che l'AgID ci ha fornito. AgID ha un disciplinare dedicato al consolidamento dei *data center*, che è una delle nostre aspirazioni maggiori.

Riepilogando, il progetto che abbiamo fatto – poi vi farò vedere un'ultima *slide* di

cronistoria per mostrarvi a che punto siamo – costa circa 30 milioni. Abbiamo seguito le indicazioni dell'AgID, e l'abbiamo fatto certificare da una società di certificazione.

VINCENZA BRUNO BOSSIO. Qual è ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. La Gartner. Il ritorno dell'investimento è di due anni. Se si fosse agito come un privato, avremmo potuto avere questo finanziamento e avremmo potuto già restituirlo. Ci saremmo trovati subito 30 milioni, perché con i risparmi, dopo due anni, saremmo riusciti a ripagare il debito. È un'operazione che nello Stato non si può fare, ma con il *project financing* si poteva anche tentare. Noi abbiamo cercato la strada ordinaria, quella tradizionale. Il ritardo nello sviluppo di questo progetto è dovuto al fatto che abbiamo dovuto cercare le fonti di finanziamento. Il progetto l'abbiamo realizzato utilizzando quelle risorse che abbiamo visto prima, ossia ingegneri della Polizia o del nostro Ministero. Si è formato un gruppo di lavoro che si è dedicato a fare questo. Non è soltanto un'idea, è un progetto che ha una sua storia. È stata creata la scatola e come deve essere l'interno. Ovviamente, più tempo passa, più la parte interna, il cuore, può essere performante. Nel momento in cui si acquistano quelle macchine e quei *software*, sicuramente se ne troveranno di natura migliore rispetto a quelli che avevamo visto due anni fa, perché le cose cambiano completamente nell'informatica.

Abbiamo fatto anche approvare e classificare il progetto dal nucleo di valutazione del Ministero dell'interno, che l'ha messo come priorità numero 1. L'Agenzia per l'Italia Digitale ci ha fornito varie indicazioni, di cui abbiamo tenuto conto nel progetto. Come dicevo prima, ho avuto dei contatti informali con altri ministeri che erano disponibili a valutare, in futuro, una loro collaborazione a un *masterplan* di sviluppo condiviso delle applicazioni, ma anche dell'infrastruttura, almeno per quanto riguarda la *business continuity*.

Noi abbiamo iniziato nel 2014 con quest'incarico. Abbiamo fatto una ricognizione di tutti i CED e del personale impiegato, che ho sintetizzato prima. Nel febbraio-dicembre 2014 ho visitato i migliori *data center* italiani per avere un'idea di come dovesse essere il nostro, trovando delle cose anche molto interessanti e sorprendenti. Se qualcuno fa meglio di te una cosa, tanto vale copiare.

VINCENZA BRUNO BOSSIO. Qual è uno, per esempio, che ha trovato interessante ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Ho trovato interessante Aruba, almeno sotto il profilo dell'organizzazione, molto interessante. Sotto il profilo della sicurezza forse andava migliorata la difesa fisica. A loro serviva curare l'immagine e quindi si sono regolati di conseguenza, però sono molto bravi questi di Aruba.

Poi, ovviamente, TIM. Tutte le società telefoniche hanno dei propri *data center*, altrimenti non riuscirebbero a funzionare. Hanno dei *data center* efficienti, altrimenti non parleremmo con i telefoni. Per loro è un *core business* così forte che tentano sempre di migliorare.

La TIM ha creato un *data center* importante adesso. L'ha finito e dovrebbe essere ad Acilia. L'ho letto da qualche parte nei giorni scorsi. L'andrò a visitare, perché l'hanno classificato TIER IV, quindi è interessantissimo. TIER IV significa il massimo del livello dello standard TIA 942. La classificazione della efficienza e sicurezza dei *data center* va da TIER I a TIER IV. Già con II si è a un buon livello. In Italia, nella pubblica amministrazione, ci si attesta tra I e II. Il III ce l'hanno pochissimi e il IV è quasi inesistente, anche perché il IV costa tanto, dovendo prevedere una ridondanza di sistemi enorme. Quindi, ci si può accontentare di stare tra il III e il IV, cioè di prevedere il livello IV per alcune procedure che si ritengono strategiche per il Paese e il livello III per tutto il resto. Se poi si uniscono le forze e si fa un *cloud* ibrido, un po'

privato, un po' pubblico, si riesce a mettere in sicurezza tutto il Paese. È un discorso che va affrontato insieme.

Il piano di fattibilità l'abbiamo rilasciato nel 2014. Nel novembre 2014 ci siamo visti proprio con il presidente Coppola. Gli ho portato la prima bozza. Appena rilasciata, l'ho fatta vedere al presidente, per avere qualche indicazione. L'abbiamo poi presentata al ministero. Nel dicembre 2014 abbiamo avuto i primi incontri informali con altri enti per condividere l'iniziativa, una volta finita la nostra. Nel 2015, a febbraio abbiamo consegnato il progetto con integrazioni e a maggio 2015 l'abbiamo integrato con le osservazioni di Gartner.

Poi abbiamo collaborato con AgID per avere la stesura definitiva e l'abbiamo consegnato al nostro Ministro, al Ministro Alfano, nella versione definitiva, illustrandolo in termini ovviamente molto più veloci di quelli che sto ripercorrendo ora. Mi scuso per essere così prolisso. Da quel momento in poi il progetto è diventato oggetto di attenzione anche di altri rappresentanti istituzionali e proprio nel gennaio di quest'anno è stato fatto rientrare in 15 progetti nel Documento pluriennale di programmazione del Ministero dell'interno. È messo tra i primi come importanza strategica per il Ministero dell'interno.

Quello che volevo sottolineare è che sarebbe importante un appoggio anche verso il Governo perché venga approvato.

VINCENZA BRUNO BOSSIO. Il finanziamento viene inserito nel PON sicurezza ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. No, l'abbiamo messo prima. Il PON sicurezza ci impone, molto spesso, di utilizzare il Sud. C'erano già altri enti che avevano individuato questa soluzione. Non potevamo mettere tutto insieme. Poi la capitale è la capitale e alcune cose devono stare nella capitale, anche per ragioni di opportunità. Nulla vieta, però, che alcuni fondi europei possano essere utilizzati. Almeno una parte deve essere presa dai fondi ordinari. Una seconda parte potrebbe essere presa dai fondi FAS e dai fondi strutturali. All'inizio avevamo cercato uno stanziamento del CIPE, ma probabilmente non siamo riusciti. Adesso l'unica cosa certa è che nel 2017 il progetto è stato inserito nella richiesta di finanziamento. Abbiamo la lettera. Se vuole, presidente, gliela lascio.

PRESIDENTE. Certamente, grazie. Mandatecela in formato elettronico, perché noi usiamo solo la modalità elettronica.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. A me l'hanno girata ieri sera. L'abbiamo già in formato elettronico. Comunque è importante questo documento.

Il futuro digitale come lo immaginiamo noi, al Ministero dell'interno ? Abbiamo 3-4 famiglie che gestiscono l'infrastruttura centrale del Ministero dell'interno, con *core business* orientato al cittadino sotto il profilo economico, al cittadino sotto il profilo della sicurezza, e alla difesa dei cittadini. I vari ministeri sono dediti a questo. Occorre immaginare una nuvola in cui condividere un *cloud* privato razionalizzando quei *data center*. Alcuni non hanno bisogno di essere modificati. Il *data center* di Sogei non ha bisogno di molte modifiche, e neppure quello dell'INPS. Hanno fior fiori di *data center*. Va fatto un processo di integrazione delle informazioni che possono essere condivise.

Il Ministero dell'interno è più affine al Ministero degli affari esteri, al Ministero della difesa e al Ministero della giustizia, ma bisogna anche tener presente che al Ministero della giustizia alcune informazioni sono come quelle delle Forze dell'ordine. Le vogliono settorializzate. I magistrati hanno un grande interesse a mantenere riservate le istruttorie. Mi sembra logico. C'è una parcellizzazione delle informazioni che va rispettata, perché le leggi la impongono, anche se magari si potrebbero gestire, almeno in alcune parti, segretandole in maniera più efficiente.

Con questo avrei finito la mia esposizione. Nei prossimi mesi cercherò di dare contezza anche di quello che ho qui illustrato.

PRESIDENTE. Do la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

VINCENZA BRUNO BOSSIO. Mi pare una bellissima iniziativa. La ringrazio se riuscirete già a risolvere i problemi dei diversi CED all'interno del Ministero. Naturalmente, quello è un sogno, ma speriamo che prima o poi si realizzi. È un obiettivo importante.

Voglio capire come questa cosa si lega con i CERT. Voi avete un CERT anche al Ministero dell'interno, o meglio ce l'ha la Difesa, non voi. O anche voi avete un CERT ? Poiché ci sono anche gli altri CERT, sicuramente alla Funzione pubblica, al MiSE e non so se anche alla Presidenza del Consiglio – su questo c'è molta confusione; quindi, è una domanda anche conoscitiva da questo punto di vista – vorrei sapere se questo ragionamento punta anche all'unificazione del CERT. Il tema della *cyber security* è anche questo: fondamentalmente non abbiamo un unico CERT con cui interfacciarci con il resto d'Europa e il resto del mondo. La *cyber security* senza questa connessione non può essere fatta, né in un solo Paese, né, tantomeno, in un solo ministero.

In secondo luogo, in merito a questa idea che riguarderebbe anche i CERT e come si possano utilizzare non solo sui CED, ma anche sulla novità del *cloud*, una novità ormai già abbastanza « vecchia » da questo punto di vista, chiedo se si possa immaginare anche questo collegamento del pubblico e del privato. Penso che ci siano alcuni CERT di imprese private o pubbliche, come Poste, per esempio, che hanno già fatto dei passi avanti molto importanti. Come si collegano a questa strategia della sicurezza ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Per quanto riguarda i CERT, in realtà esiste già un CERT nazionale presso il Ministero dello sviluppo economico. Quel CERT fa da...

VINCENZA BRUNO BOSSIO. Scusi se la interrompo, ma Calenda diceva, l'altra volta, che è disposto a chiudere il CERT perché non è il posto giusto, come diceva lo stesso Ministro. Dirlo da parte del Ministro che lo possiede è una bella cosa.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. La *cyber security*, come, del resto, tutto il mondo digitale, ha un'evoluzione continua, che dipende dagli attaccanti e dalle strutture che si devono difendere. Sono due mondi che si contrappongono e che hanno un'evoluzione continua.

Il Ministro Calenda ha posto l'accento, secondo me, su un fatto giusto, nel senso che il CERT era stato inventato quindici anni fa a tavolino dagli americani, come *Computer Emergency Response Team*. Il problema è che la maggior parte delle vittime non segnala, quando viene colpita da un *virus*. Venne creato proprio per fronteggiare i *virus*. Le informazioni sui *virus* è più facile trovarle in rete direttamente che attraverso un CERT. Quindi, va rivista l'organizzazione. Calenda ha ragione, perché l'orientamento attuale del nostro Governo, che è conforme a quello degli altri Paesi, è quello di centralizzare la regia della *cyber security* sotto un unico organismo che sia la Presidenza del Consiglio. Mi sembrerebbe logico che la Presidenza del Consiglio gestisca il CERT nazionale. Si tratta solo di spostare le competenze, non le macchine. Dove stanno, stanno. La strategia viene gestita da un altro organismo.

Il Ministero dell'interno, anzi la Polizia di Stato, sta realizzando un CERT che riguarda tutto il Ministero dell'interno, in cui tutti i vari *data center* dovrebbero far confluire informazioni rispetto agli attacchi informatici. Già di per se stesso funziona. Una volta che avremo un *data center* unificato, questo CERT verrà inglobato lì. Di fatto, è stato già finanziato quello per il Ministero dell'interno. Lo sta portando avanti un collega, che è stato mio successore alla Polizia postale e che ora sta seguendo questo progetto, che è finanziato. Segue la logica dei CERT. Il vertice del CERT, Calenda ha detto bene, non lo devo guardare io. Io mi occupo di economia e di sviluppo. Sono un soggetto che potrebbe

essere attaccato, non che debba difendere. La difesa in questo campo spetta al DIS, a mio avviso, essendo la sicurezza nazionale gestita dal DIS. Così è stato anche nelle ultime norme di riforma. Credo che debba essere inglobata. A mia opinione, questa difesa dovrebbe essere inglobata sotto la vigilanza del DIS.

Per quanto riguarda l'altro aspetto che diceva l'onorevole Bruno Bossio, le nostre infrastrutture informatiche che sono gestite da aziende private, o anche da aziende private con una connotazione pubblica, come Poste Italiane e come la stessa Telecom, secondo me, con una semplice riorganizzazione, potrebbero partecipare a questa nuvola. La parte di *cloud* privato la possiamo dare a loro, ma di fatto già c'è, perché alcune gare sul *cloud* le hanno vinte alcune aziende. Adesso non mi ricordo...

VINCENZA BRUNO BOSSIO. Via Consip, sì.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Sì, via Consip. Tutti gli enti della pubblica amministrazione che vogliono acquistare prodotti di *cloud*, sia per *software*, sia per piattaforme o per infrastrutture, si devono rivolgere a Consip. Ci sono già gli acquirenti.

Quello che mi sembra utile suggerire è utilizzare i *data center* pubblici che già esistono per altre funzioni. Sono grandissimi. Quello dell'INPS è enorme. L'INPS, per esempio, ha una chiave d'accesso per 18 milioni di italiani, mentre lo SPID ne ha attualmente solo un milione. Il passaggio del rilascio dello SPID potrebbe essere rivisto. Aspettare che il cittadino si vada a prendere lo SPID da solo senza una ragione rischia di non funzionare, perché il cittadino non lo fa. Se, invece, deve andare a vedere la pensione, come ho fatto io recentemente, perché mi hanno comunicato di prendere lo SPID se volevo sapere quando sarei andato in pensione, il discorso cambia.

VINCENZA BRUNO BOSSIO. Sì, ce l'hanno raccontato.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Allora io me lo sono andato a prendere. Una delle cose che volevo introdurre è l'accesso dei cittadini attraverso lo SPID anche ai siti del Ministero dell'interno. Tuttavia, solo alcune procedure hanno bisogno di una certificazione così forte per l'ingresso. Faccio un esempio pratico, che ho visto qualche giorno fa a un convegno. La regione Lazio ha immesso lo SPID tra le chiavi di accesso ai suoi siti per la parte sanitaria, ovviamente mantenendo anche le sue chiavi d'accesso precedenti. Se il cittadino deve accedere lì, adesso come faranno lo *switch-off* ? Quando lo fa la regione ?

VINCENZA BRUNO BOSSIO. Quando lo fa anche l'INPS ? Lo abbiamo chiesto.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Bisogna trovare un modo perché il cittadino che va ad accreditarsi attraverso il sito della regione acquisisca anche lo SPID. La regione gli potrebbe dire che, se vuole, lo SPID glielo fa rilasciare lei. Cliccando lì, con la stessa autenticazione, si prende anche lo SPID, visto che è gratis. Si dovrebbero fare, quindi, gli accordi tra amministrazione ed enti rilasciatori. Il cittadino può scegliere tra cinque, tra cui Telecom e altri. Non si può tornare indietro dopo aver impostato questa cosa in questo modo, perché tornare indietro, in informatica è sempre peggio. Si può, però, migliorare come rilasciarlo, vedere come farlo funzionare, o dire alla stessa INPS, a mano a mano che gli utenti si collegano, di fornire loro anche lo SPID, oppure di utilizzare il proprio codice INPS che vale come SPID.

È un modo di organizzazione che va considerato per non essere vittime delle proprie opinioni in questo settore. In questo settore bisogna sempre avere l'umiltà di ammettere se c'è qualcuno che ha fatto qualcosa meglio e di copiare l'idea. Così funziona Internet. Si copia dappertutto. Copiano pure al rovescio e poi indicano il professore come plagiatore. In realtà, è lui

che è stato copiato. Bisognerebbe solo mettere la cronologia dell'invenzione.

Questa è una delle cose che si potrebbero fare. Questo mondo è affascinante. Abbiamo tante risorse in Italia, ma noi italiani abbiamo una pecca. L'ho notato quando ho organizzato il CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche). Si tratta di una centrale operativa a cui sono collegati tutti. Dovendo risolvere il problema degli attacchi alle infrastrutture critiche del Paese, dovevo garantire loro che, se parlavano con me, parlavano con un padre confessore, tutelandoli con il segreto istruttorio. Allora ci hanno detto quando erano in difficoltà. Abbiamo dovuto fare indagini interne e abbiamo dovuto garantire una sicurezza informatica a tutto tondo di tipo operativo, sia quando stavano per essere colpiti che quando erano stati colpiti. Tutto questo ha innescato un meccanismo positivo, ma nessuno ammetterebbe mai di aver avuto una fuga di dati se può evitare di dirlo alla stampa.

I CERT hanno difficoltà a funzionare perché presuppongono, soprattutto nel campo delle infrastrutture private di tutti i tipi, di ammettere di essere stati « bucati », che a volte significa aver fallito. E se è una banca a essere « bucata » ? Non è bello.

Con riguardo alle carte di credito, per esempio, le centrali che rilasciano le carte di credito l'hanno messo nel conto. Se uno vuole denunciare che gli hanno clonato la carta di credito, non c'è problema. Non fanno alcuna indagine, anche se non è vero. Rimborsano i soldi. Perché ? Perché hanno messo nel conto l'uno per cento di perdite. Se dicono che hanno scoperto qualcuno che ha frodato e che è un finto frodato, perdono il cliente. Tendono ad aumentare il volume degli acquisti fatti con le carte di credito, non a diminuirlo. A volte siamo stati noi ad avvisarle che avevano clonato le loro carte di credito – noi Polizia intendo – piuttosto che loro a raccontarlo a noi. Non so se mi sono spiegato.

Bisogna entrare in queste logiche integrandosi con i percorsi che segue chi gestisce un servizio informatico. Adesso la gran parte delle nostre aziende strategiche, soprattutto le *utility*, si sta rivolgendo verso il mondo del *cloud*, comprese quelle che lavorano all'estero, perché è l'unico modo per unificare i servizi. C'è un'azienda, nostra, importantissima che sta in quattro continenti e produce energia di tutti i tipi, ma le bollette sono sempre le stesse. Il rapporto con gli utenti è sempre lo stesso, a prescindere dal Paese d'appartenenza. Le conviene avere il *cloud*, piuttosto che un *data center* suo da gestire, con tutte le ramificazioni. Costerebbe di più. Probabilmente si rivolge a Google o magari a Microsoft. Pensate che Google si è creato una rete in fibra ottica in 3 o 4 continenti. Gli investimenti che fa sono sulla fibra. Ha fatto un « gomitolo » di fibra ottica che riguarda tutto il mondo per sviluppare questi servizi. Farà concorrenza alle banche, perché i *social network* si stanno mettendo a lavorare sul piano del credito. Se le banche non cambiano atteggiamento e non modificano i loro processi – alcune l'hanno fatto – non solo subiranno delle crisi finanziarie, ma finiranno anche per non essere più competitive. Il denaro i risparmiatori lo mettono dove hanno più vantaggi e meno scocciature.

PRESIDENTE. Adesso, però, stiamo un po' divagando dallo scopo della Commissione. Ci sono altre domande ? Io ne avrei alcune.

Rispetto al progetto dell'unificazione dei CED, intanto quant'è il tempo necessario che avete stimato per l'unificazione e quali sono le difficoltà più grandi che immaginate di incontrare ? A me sembra, per esempio, con riferimento ai 290 sistemisti attuali che, come Lei ha detto, devono essere ridotti non so se a 10, ma comunque a un numero assai inferiore a 290, che ci sia la necessità di riconvertire le persone, o comunque di capire che cosa far fare a quelle in eccesso. Immagino che non sia il licenziamento, ma un uso efficace del personale.

Vorrei sapere i tempi e le difficoltà che pensate di trovare. Inoltre, perché non avete scelto, per esempio, di appoggiarvi direttamente a un *data center* già realizzato da qualcun altro ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Rispondo a partire dall'ultima domanda. Di tutti i nostri *data center* che avevamo già, nessuno era espandibile e nessuna delle condizioni di sicurezza che prevedevano...

PRESIDENTE. Per esempio, Sogei si offre di fare da gestore di *data center* di vari altri enti.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Sarebbe innanzitutto una concentrazione eccessiva in un soggetto. Se vogliamo crescere bene in futuro, dobbiamo avere dei *data center* ridotti di numero, ma potenti per capacità digitale e comunque diversificati, altrimenti, se concentriamo tutto in un unico *data center*, è anche più rischioso sotto il profilo della sicurezza. Occorre, quindi, fare una rete di *business continuity* che interessi più *data center*. Questa è una delle ragioni.

C'è anche una ragione psicologica. La struttura del Ministero dell'interno – se parliamo del Ministero dell'interno – vuole avere il controllo di dove vanno i suoi dati. È un fatto che, come dicevo prima, magari i nostri figli non comprenderanno. Diranno che siamo antiquati, ma adesso abbiamo questa realtà.

Per quanto riguarda la riconversione del personale, avevamo pensato intanto a una riqualificazione del personale verso lo sviluppo di applicazioni per il miglioramento dei servizi ai cittadini fatte con personale interno.

PRESIDENTE. Quindi, nel progetto è prevista una parte di risorse finanziarie per la formazione del personale, oppure questo finanziamento deve essere trovato nelle risorse finanziarie generali ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Una parte si può ritrovare. Nel momento in cui si cambia sistema, nei contratti che si fanno, chi fornisce il sistema deve fornire anche la formazione e la parte di sicurezza generale. Non si può non tener conto di questo aspetto.

L'altro aspetto è che fare la formazione di quelli che avanzano – mettiamola così – significa rivolgere le stesse persone, nella verticalizzazione dei sistemi, a sviluppare applicazioni, perché sono sempre sistemisti. Prendo un esempio proprio dal dipartimento dove ho i miei uffici. Il personale che deve preparare un concorso *on line* è sempre lo stesso. Se contemporaneamente Vigili del fuoco e Polizia fanno un concorso, questa risorsa non ce la fa a farli insieme. Anche in quel caso ci sono risorse che mancano e ci si deve rivolgere al privato. Se queste risorse vengono riqualificate, possono gestire tutto quello che normalmente avviene nella vita di un ministero. Pensiamo al Ministero del lavoro, che ha cambiato l'Agenzia e ha cambiato gli ispettorati del lavoro. Potrebbe succedere anche da noi.

Per esempio, io ho diretto l'Ispettorato generale della Polizia di Stato per un anno-un anno e mezzo. Mi sono reso conto che lavoravano col metodo tradizionale. La prima cosa che ho fatto – credo che il capo della Polizia attuale stia seguendo il mio metodo – è stata cambiare il modo di fare le ispezioni. Non si trattava più di andare col « quadernino », ma di poterlo fare in maniera informatica digitalizzata. Occorreva, però, formare anche le persone e avere dei sistemisti che creassero i programmi da fornire poi agli ispettori, abbastanza *friendly* per poter operare e per fare quei *test* di *auditing* come quelli che fanno nelle aziende. Si tratta, quindi, di riconvertire quelle persone per profilo e di farle intervenire non solo come tecnici richiamati alla bisogna – se si è rotto il computer – ma negli stessi uffici. Devono stare accanto a chi gestisce, perché, se quello ha un problema da risolvere, il sistemista gli serve per fare il suo programma, che poi può rilasciare per altre funzioni. Bisogna seguire il modello delle aziende, che è quello di far intervenire nei processi la risorsa digitale. Per ora sono considerate delle *uti-*

lity separate. Vincere questo aspetto sarebbe già un grosso vantaggio.

PRESIDENTE. Quindi, Lei ha intenzione di proporre una riorganizzazione interna di questo tipo ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Noi avevamo anche accennato a una proposta di riorganizzazione già nel 2015. Quando si risparmiano queste persone e si gestisce l'ordinario soltanto con la base infrastrutturale, tutto il resto del personale che già è assunto può essere destinato negli uffici che devono gestire problemi nei servizi ai cittadini o anche nei servizi interni. Magari ne avessero dati a me di sistemisti da poter utilizzare alla Polizia postale. A volte ci sono indagini specifiche che richiedono la costruzione di un programma investigativo. Io affidavo questo compito a degli ingegneri. Se non li avevo, dovevo ricorrere a risorse esterne.

PRESIDENTE. Visto che parla di risorse, c'è una domanda che mi è venuta. La sua nomina a responsabile della transizione al digitale è molto recente, ma noi sappiamo che la normativa, sin dal 2011, prevedeva che un unico ufficio fosse responsabile di una serie piuttosto corposa di azioni. L'ufficio che Lei dirige ha risorse sufficienti, secondo Lei, per portare avanti tutte le funzioni che la legge Le affida, che – lo ricordo ai commissari – comprendono il coordinamento strategico dello sviluppo dei sistemi informativi e di telecomunicazione, in modo da assicurare la coerenza con gli standard tecnici e organizzativi; l'indirizzo e il coordinamento dello sviluppo dei servizi, sia interni che esterni; l'indirizzo, la pianificazione, il coordinamento e il monitoraggio della sicurezza informatica; l'analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione; l'indirizzo, il coordinamento e il monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e così via ?

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. In questo momento sono stato solo nominato. Nello stesso decreto di nomina, però, a onor del vero, hanno provveduto a sanare un *vulnus* che era evidente e che è stato evidenziato. Con separato provvedimento del capo del dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie verranno individuate le risorse degli uffici in questione, sia il mio, sia quello, nascente, del difensore civico.

PRESIDENTE. Quindi, al momento non ha ancora risorse ? Non ne ha una.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Nel gruppo di lavoro avevo preso risorse dai vari dipartimenti, ma, finita l'attività, non sono stati più impegnati. Posso comunque iniziare, tenendo presente che ho individuato in alcuni dipartimenti delle risorse che sono in grado di impiegare. Si tratta di coinvolgerle in questa riorganizzazione. Va fatta prima l'organizzazione.

PRESIDENTE. Se mi permette un piccolo suggerimento, vedendo il decreto di nomina, magari si potrebbe iniziare dal fatto che la pubblica amministrazione deve formare gli originali con le tecnologie dell'informazione, e il timbro che vedo lì di sicuro non rientra tra le tecnologie dell'informazione. Questa è una piccolissima cosa, un piccolissimo suggerimento che si può dare agli uffici.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Sotto c'è, con il codice a barre.

PRESIDENTE. Sotto c'è, ma gli originali devono essere formati con le tecnologie dell'informazione. Sicuramente è una pic-

colissima cosa. Ci rendiamo conto che in questo momento è ancora presto per potervi chiedere quali sono le azioni che avete fatto. Dal 2011, però, queste azioni devono essere previste, soprattutto per quanto riguarda l'organizzazione, perché, come Lei giustamente ha sottolineato più volte, la coerenza dell'organizzazione con gli strumenti digitali è assai importante.

DOMENICO VULPIANI, *responsabile della transizione alla modalità operativa digitale del Ministero dell'interno*. Bisogna fare un *auditing* informatico.

PRESIDENTE. Lo dovrà fare Lei, visto che Lei è responsabile. Poi riferirà direttamente al Ministro, perché la legge dice che Lei, per quanto riguarda queste funzioni, ha un riferimento diretto al Ministro e non tramite altri uffici.

Non so se la dottoressa Coduti può intervenire. Per esempio, Le chiedo un'informazione, visto che Le è stato notificato venerdì scorso che Lei è il difensore civico digitale del Ministero. I cittadini che volessero rivolgersi a Lei che strumento devono utilizzare ?

ANTONINA CODUTI, *difensore civico digitale*. La PEC o qualsiasi altro strumento in forma digitale.

PRESIDENTE. Lei ha una PEC specifica ?

ANTONINA CODUTI, *difensore civico digitale*. Non ce l'ho. Ce l'ha il mio ufficio in cui attualmente lavoro. Il mio percorso di studi e anche lavorativo è stato sempre giuridico. Infatti, mi sono occupata sempre di contenzioso. Forse la scelta è stata operata sulla mia persona proprio per questa esperienza nel ramo del contenzioso, anche se poi ho potuto notare che il compito del difensore civico non è come quello del contenzioso normale, quello che si presenta alle autorità giurisdizionali. È soltanto quello di raccogliere questi reclami dei cittadini e poi di invitare l'ufficio competente a provvedere.

Infatti, leggendo gli articoli di legge, ho avuto anche qualche perplessità in merito alla costituzione delle commissioni, perché il decreto non specifica quali siano queste commissioni a cui bisogna riferire nel caso in cui l'amministrazione non ottemperi a queste segnalazioni.

PRESIDENTE. Mi sfugge il discorso delle commissioni.

ANTONINA CODUTI, *difensore civico digitale*. A un dato punto, il decreto dice che il difensore civico dovrà riferire alle commissioni di disciplina competenti. Non so siano delle commissioni disciplinari...

PRESIDENTE. L'ufficio competente per il procedimento disciplinare, certo.

ANTONINA CODUTI, *difensore civico digitale*. Queste commissioni per il procedimento disciplinare non ho capito se siano le commissioni che attualmente sono nell'ambito dei nostri cinque dipartimenti, oppure se siano delle commissioni che bisogna istituire *ad hoc* proprio per questo servizio. Bisogna organizzarsi anche in questo senso.

PRESIDENTE. No, vengono utilizzati gli uffici competenti attuali.

ANTONINA CODUTI, *difensore civico digitale*. Per quanto riguarda la parte informatica, ci sarà una struttura, perché io sono preparata dal punto di vista giuridico e non informatico. Quindi, ci sarà una struttura che mi farà da supporto e che provvederà a realizzare questa parte tecnica. Dovrà individuare, nei vari dipartimenti, le varie risorse che dovranno interagire con me, senza oneri. Speriamo che ci sia chi si offre. Comunque, vengono individuate anche delle persone abbastanza competenti che possono supportarmi in questo mio incarico.

PRESIDENTE. Quindi, al momento, se i cittadini vogliono comunicare con Lei, devono utilizzare l'indirizzo di posta elettronica certificata del suo ufficio, che è...

ANTONINA CODUTI, *difensore civico digitale*. L'ispettorato generale di amministrazione presso il dipartimento delle politiche del personale. Dobbiamo avere ancora il tempo di poterci organizzare, anche perché poi bisognerebbe pubblicare sul sito il mio nominativo e altro.

PRESIDENTE. Certamente. Se non ci sono altre domande, possiamo passare alla parte segreta, perché mi sembrava che ci fossero alcune informazioni riservate.

Apprezzate le circostanze, propongo che il seguito dell'audizione si svolga in seduta segreta.

(La Commissione concorda – I lavori proseguono in seduta segreta, indi riprendono in seduta pubblica)

PRESIDENTE. Non essendoci altre domande, dichiaro conclusa l'audizione.

La seduta termina alle 12.

Comunicazioni del Presidente.

La seduta comincia alle 12.05.

PRESIDENTE. Comunico che da oggi sono in distribuzione le *password* per accedere al servizio di *file transfer* che sarà utilizzato dalla Commissione per il trasferimento dei *file* cifrati relativi ai documenti riservati richiesti in consultazione dai singoli commissari. Una volta scaricati i *file*, sarà necessario decrittarli con il proprio certificato personale, secondo le modalità presentate nella seduta del 17 gennaio scorso.

Ricordo ai commissari che questo servizio è stato avviato sperimentalmente con la collaborazione del Servizio informatica della Camera, per evitare di utilizzare la posta elettronica per questo tipo di trasferimenti. In ogni caso, il trattamento dei file relativi ai documenti riservati della Commissione deve avvenire sempre con la massima cura e attenzione.

Comunico, inoltre, che nella seduta odierna l'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, ha ritenuto di integrare il programma delle audizioni con l'audizione del Poligrafico e Zecca dello Stato in merito alla carta d'identità elettronica.

Comunico, altresì, che sempre nella seduta odierna, l'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, ha ritenuto di conferire a Synapta un incarico di ricerca relativo all'analisi dei dati dei contratti pubblici nel settore ICT.

Infine, comunico che, durante le scorse sedute, la Commissione ha ricevuto documentazione da ANCI, Ministero dell'interno, Agenzia delle dogane e INPS che, d'accordo con gli autori, ritiene di includere nella categoria degli atti liberi e di pubblicare quindi, come di consueto, sul sito *web* della Commissione. Lo stesso avverrà per la documentazione ricevuta in data odierna dal prefetto Vulpiani, a parte le *slide*, che rimarranno riservate.

Non essendoci interventi, dichiaro conclusa la seduta di comunicazioni.

La seduta termina alle 12.10.

Licenziato per la stampa
il 1° giugno 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

17STC0023230