COMMISSIONE PARLAMENTARE DI VIGILANZA SULL'ANAGRAFE TRIBUTARIA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

18.

SEDUTA DI MERCOLEDÌ 17 NOVEMBRE 2021

PRESIDENZA DEL PRESIDENTE **UGO PAROLO**

INDICE

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE UGO PAROLO

La seduta comincia alle 8.40.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata mediante l'attivazione dell'impianto audiovisivo a circuito chiuso e la trasmissione in diretta *streaming*, con modalità sperimentale, sulla *web-tv* della Camera dei deputati.

Audizione di dirigenti dell'Amministrazione del Ministero dell'interno e di ufficiali della Guardia di finanza.

PRESIDENTE. L'ordine del giorno reca l'audizione di dirigenti dell'Amministrazione del Ministero dell'interno e di ufficiali della Guardia di finanza.

Il Ministero dell'interno è rappresentato dal dottor Giancarlo Verde, Responsabile per la transizione digitale e direttore della Direzione centrale per le Risorse finanziarie e strumentali, articolazione amministrativa che assicura, *ex lege*, la funzionalità delle attività di innovazione tecnologica e di digitalizzazione, nonché dei sistemi informativi del Ministero dell'interno e delle Prefetture – Uffici Territoriali del Governo. Il dottor Verde è supportato dai dottori Angelica Saggese, Ivano Gabrielli, Carlo Foti e Roberto Andracchio.

Per la Guardia di finanza interviene il generale di brigata Giuseppe Arbore, capo del III Reparto – Operazioni, che è supportato dal direttore della Direzione telematica, colonnello Cesare Forte.

Tali audizioni sono volte ad acquisire una panoramica dei servizi digitali e delle basi di dati di rilevanza critica e strategica, in quanto relativi a sicurezza pubblica e polizia economico-finanziaria, nonché a conoscerne le prospettive di sviluppo anche alla luce del progetto di *Cloud* nazionale, la cui infrastruttura è in fase di sviluppo nella forma del Polo Strategico Nazionale.

Ringrazio quindi del contributo che i nostri ospiti ci vorranno rendere e cedo loro la parola iniziando, come da ordine di convocazione, dal dottor Verde.

Avverto che sono collegati con noi i senatori Gaudiano, De Bertoldi, Fenu e Marino, che stanno seguendo la Commissione, oltre ovviamente alla collega Cantone che è presente in seduta. Prego, dottor Verde.

GIANCARLO VERDE, *direttore della Direzione centrale per le Risorse finanziarie e strumentali del Ministero dell'interno*. Buongiorno ai presenti e ai collegati. Ringrazio per l'invito. Io sono il responsabile della transizione digitale del Ministero dell'interno. In tale veste il Ministro dell'interno mi ha pregato di rappresentarla qui per rispondere alle richieste della Commissione. In questa relazione ci interesseremo della tipologia delle infrastrutture tecnologiche e dei servizi digitali offerti dal Ministero dell'interno, che sono ampi e diversi. So che il tempo dato non è lunghissimo, quindi lascio agli atti una relazione molto completa, trattando qui stamattina alcuni punti.

Innanzitutto porto il saluto del Ministro Lamorgese, che ha partecipato a un convegno a fine ottobre, proprio a margine dei problemi della pandemia COVID e dei fondi del PNRR, in quell'occasione ha garantito che il Ministero non abbasserà mai la guardia e cercherà di garantire e sostenere il

Paese nel cambiamento. In particolare ha parlato di sfida che tutti insieme siamo chiamati ad affrontare, attraverso una cultura di fare squadra – questo è un punto molto evidente per la nostra azione – per trasformare l'emergenza in un'occasione straordinaria di rilancio economico e sociale per il quale la pubblica amministrazione è chiamata a fare la sua parte. Proprio il Ministero dell'interno può giocare un ruolo cruciale, facendo leva su un modello di rete con le prefetture e gli altri uffici territoriali, nella convinzione – ha testualmente affermato il Ministro – che tutti noi che abbiamo responsabilità pubbliche dobbiamo agire con maggiore comunanza di intenti e strategie per il rilancio del Paese.

Già da queste parole si ha un'idea della complessità dell'attività e di tutti i propositi che animano l'Amministrazione. In tutti gli ambiti in cui oggi siamo impegnati, siamo pervasi dalla cultura di fare squadra. Questa è una delle linee guida per me, in quanto responsabile della transizione digitale, per cui vorrei soffermarmi su quello che in tale contesto sto cercando di fare in questo periodo.

L'attività del responsabile della transizione digitale si sta concentrando sull'implementazione di tutti i processi di collaborazione e confronto tra i dipartimenti – il Ministero è articolato in cinque grandi dipartimenti – con notevoli ma anche diverse competenze – per conseguire i traguardi comuni, in particolare di recente la realizzazione dello sportello digitale unico e la costruzione di un solido sistema di condivisione per il raggiungimento delle finalità individuate dalla Strategia nazionale dati e la promozione delle competenze digitali. In più c'è una franca collaborazione con l'Agenzia per l'Italia Digitale – AGID.

Per fare questo abbiamo creato un gruppo permanente di lavoro, traversale, da me coordinato – e stamattina ne è un segno la presenza dei colleghi dirigenti, – al quale partecipano qualificati referenti di tutte le componenti dell'Amministrazione, in modo da condividere azioni comuni e valutare i servizi offerti all'utenza, affinché siano conformi alle direttive governative.

Recentemente abbiamo verificato che tutti gli uffici aderissero alla piattaforma pagoPA, che è una iniziativa molto importante per i cittadini che si confrontano con l'Amministrazione pubblica e, come dicevo prima, abbiamo intensamente lavorato sullo sportello digitale unico, per il quale c'è il progetto europeo per cui ogni cittadino di Stato membro, girando per l'Europa, deve poter sapere tutto quello che deve e può fare e trovarlo su un sito. Questo è complicatissimo. Lo stiamo preparando. Nonostante sia complicato, ci stiamo riuscendo, come è doveroso. Anche per evitare infrazioni europee, sarebbe disdicevole, ma anche in tema di diritti dei cittadini è una opportunità molto significativa.

In più, a livello organizzativo, stiamo provvedendo alla sostituzione della tessera di riconoscimento cartaceo, modello AT, che identifica tutti i dipendenti pubblici. Noi abbiamo circa 150 mila tra dipendenti della Polizia di Stato, Vigili del fuoco e impiegati civili. A questi soggetti stiamo sostituendo la tessera, che era un documento di riconoscimento tipo carta di identità, con un documento molto più moderno, che è la tessera elettronica ATe. Quindi sostituiamo quello che era un modulo identificativo con una carta di servizi. Identifica la persona, ma è anche uno strumento di firma digitale e di supporto alle funzionalità crittografiche e all'interoperabilità con CIE e CNS. In tal modo, anche nell'attività lavorativa questi soggetti avranno a disposizione uno strumento più moderno e adeguato ai tempi.

Devo chiarire che l'Amministrazione dell'interno non aderisce al Polo Strategico Nazionale in quanto ha in corso un proprio progetto di *cloud* privato che consiste, nei fatti, nella realizzazione di tre *datacenter* – uno presso la componente dell'Amministrazione civile, due presso la Polizia di Stato – che svolgono quelle funzioni e garantiscono comunque la sicurezza dei dati, e su cui magari dopo dirò qualche parola in più.

Dicevo prima che l'articolazione del Ministero è in cinque grandi dipartimenti. Il primo di cui tratto è il Dipartimento per gli

affari interni e territoriali ed è quello che si relaziona con il sistema delle autonomie locali. Si occupa del supporto alle attività di governo locale, a garantire la regolare costituzione degli organi elettivi, il loro funzionamento; la finanza locale, che è quel sistema che permette di fare arrivare tutti i fondi agli enti locali presto e bene; i servizi elettorali e la vigilanza sullo stato civile e sull'anagrafe, che in questi giorni è proprio all'attenzione positiva dei *media* con la novità dell'ANPR (Anagrafe nazionale della popolazione residente) in piena funzione.

Per quanto concerne il processo di digitalizzazione attivato, si evidenziano alcuni servizi importanti. Sono: il SIEL, che è il Sistema informativo elettorale centrale, che consente di gestire in diretta i risultati elettorali; l'archivio storico elettorale; gli amministratori degli enti locali; il sistema unico territoriale, e vi dico che l'informatica elettorale è avanzata da tantissimi anni perché in realtà pone le sue basi nella prima meccanizzazione degli anni Sessanta. Quello è stato sempre un settore, per la materia trattata, che doveva essere all'avanguardia delle tecnologie, e ancora oggi lo è naturalmente. Pensate che il primo sito Internet della pubblica amministrazione sbarcato sul web intorno al 1996 è quello DAIT (Direzione per gli Affari Interni e Territoriali). Si sono sempre colte tutte le tecnologie più avanzate e quasi sempre con risorse proprie, con piccoli aiuti esterni.

Abbiamo la banca dati di finanza locale, che gestisce l'attribuzione delle risorse finanziare agli enti locali, che si integra con il MEF (Ministero dell'economia e delle finanze) e con Banca d'Italia. So che l'integrazione e l'interoperabilità delle banche dati è un tema caldo per questa Commissione, per questo sottolineo che questa integrazione è evidente. Lo dimostra quello che si riesce a realizzare quando c'è l'interoperabilità.

Quando, in piena pandemia, il Governo ha inteso assegnare fondi ai comuni per le famiglie in stato di bisogno, il famoso assegno alimentare, 400 milioni stanziati di venerdì con decreto-legge, ebbene il martedì successivo, in cinque giorni, di cui due erano festivi, i fondi erano già nelle casse comunali, con un risultato fenomenale. Ne parlò anche il Presidente del Consiglio Conte nella conferenza stampa televisiva. Questo avvenne perché queste banche dati si parlano. Sono certamente uffici molto attenti per tradizione alla tempestività, ma ci sono stati strumenti adeguati che hanno permesso questo, con Banca d'Italia, con il collegamento dei comuni, con la tesoreria dello Stato, siamo riusciti a fare questo in cinque giorni. Operazioni veramente alla portata, se però usi bene la tecnologia.

In più l'Anagrafe Nazionale della Popolazione Residente (ANPR), istituita presso il Ministero dell'interno, che subentra all'Indice delle Anagrafi (INA), all'Anagrafe italiani residenti all'estero (AIRE) e a tutte le Anagrafi comunali. È stata progettata e gestita da Sogei (Società generale d'informatica), ma la *governance* ce l'ha da sempre il Ministero dell'interno, giustamente. I comuni transitati sono in questi giorni circa 7.800, e siamo vicini al 100 per cento perché si registra da tempo una contrazione dei comuni che ormai sono sotto gli 8 mila, mentre qualche anno fa arrivavano quasi a 8.200. Siamo, pertanto, vicini alla meta.

Unitamente al Ministero dell'innovazione e a Sogei si stanno pianificando le iniziative per completare il subentro di tutti i comuni entro il prossimo 31 dicembre 2021. Sono state create delle apposite *task force* Sogei, Ministero dell'interno, prefetture, per andare in ogni comune, perché i comuni che in questo momento non si sono collegati hanno problemi peggiori di altri. Molti comuni hanno problemi. Considerate che, su 8 mila comuni, 5.500 hanno meno di 5 mila abitanti e 2.000 ne hanno meno di 1.000. Organizzazioni, a volte, con soli quattro dipendenti. Se è andato in pensione chi si interessa di anagrafe, non fai più nulla in quel settore.

Comunque, con tutto il rispetto, e lo dico io, prossimo alla pensione, l'età media nei comuni è 58-59 anni, e anche questo incide sulla qualità della collaborazione. Si fanno i miracoli, si saltano ostacoli incredibili, ma su 8 mila c'è anche qualche piccola organizzazione dove veramente si è bloccato tutto e bisogna andare lì *manu*

militari ad aiutarli, perché non è possibile risolvere il problema diversamente. Ed è quello che è stato deciso, perché l'obiettivo è chiudere entro il 31 dicembre.

Tra l'altro si nota il gradimento della pubblica opinione e dei cittadini rispetto al fatto che farsi un certificato a casa e non perdere tempo con un certificato di residenza è veramente molto utile e comodo. Questa struttura informatica, una volta completata, sarà la fonte unica di riferimento dei dati anagrafici dei cittadini, e quindi è interoperabile con tutte le banche dati. Non serve solo il cittadino, ma serve qualunque altra amministrazione abbia bisogno dei dati anagrafici. Allo stato attuale già è interoperabile con il Ministero degli affari esteri, il Ministero dei trasporti, l'INPS, l'Istat, l'Agenzia delle entrate e la stessa Anagrafe tributaria, perché c'è la verifica per ogni soggetto del codice fiscale, in automatico. L'ANPR inoltre, come sappiamo, dà la possibilità di scaricare i certificati, che oggi sono 15, ai cittadini, e anche quello in termini di risultato è veramente notevole.

Passo al Dipartimento della pubblica sicurezza, che si pensa si interessi solo della sicurezza dei dati, ma in realtà dà una serie di servizi ai cittadini, che vanno forse più rivalutati e scoperti. È chiaro che l'architettura nazionale di sicurezza cibernetica affida un ruolo centrale al Ministero dell'interno quale generale autorità di contrasto alle minacce cibernetiche di matrice criminale, destinataria quindi di eventi significativi per la sicurezza degli operatori di servizi essenziali e dei soggetti componenti del perimetro nazionale di sicurezza cibernetica. Quindi il Ministero rappresenta un punto di riferimento per le altre autorità previste dal complesso sistema di sicurezza nazionale.

L'attuale scenario è caratterizzato dall'esponenziale crescita di *cybercrime* e dalla centralità della sicurezza informatica. Quindi ha reso necessaria una riorganizzazione della struttura operativa impegnata nell'attività di prevenzione. A tal fine il Servizio della polizia postale e delle comunicazioni è stato elevato a Direzione centrale per la polizia scientifica e la sicurezza cibernetica, nella quale a breve confluiranno anche le attribuzioni sinora svolte da un altro importantissimo ufficio, che è il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC). È una struttura dipartimentale incaricata in via esclusiva di prevenire e reprimere i crimini informatici di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica o di rilevanza nazionale.

Il centro, tra i primi del suo genere nel panorama internazionale, opera secondo consolidate procedure di *infosharing*, attraverso quindi una sala operativa che è attiva 24 ore su 24 e una sezione investigativa composta da personale specializzato nel contrasto ai crimini informatici, che hanno compiti di polizia giudiziaria. Il valore aggiunto del CNAIPIC è anche quello di gestirsi e operare con un modello partenariale convenzionale con i soggetti erogatori dei servizi pubblici essenziali, e partecipa a un sistema nazionale di sicurezza cibernetica che si è completato con l'istituzione recente dell'Agenzia per la cybersicurezza nazionale.

La nuova Direzione centrale per la polizia scientifica e la sicurezza cibernetica ospiterà anche il *Computer Emergency Response Team* (CERT) e il Centro di valutazione del Ministero dell'interno. Abbiamo questo assetto, validato ovviamente a livello governativo e dalle norme di legge. Il CERT sarà l'ufficio deputato a garantire la sicurezza delle reti e dei sistemi informativi.

Il Dipartimento, invece, ha attivato anche una serie di servizi diretti al cittadino, che sono di tipo informativo, fruibili via *web* con delle *app*. Abbiamo il famoso agente Lisa, che è un'entità astratta che sembra una persona, con cui si colloquia sul sito Internet. Oppure abbiamo la possibilità di supportare richieste dei cittadini con un « dove siamo » e fare capire dov'è il commissariato più vicino, o chiedere documenti o lo stato di alcune pratiche – nella relazione è spiegato come farlo – o anche, con spirito di servizio, cercare altre informazioni. Per esempio, se una macchina è rubata, se una banconota è falsa, se sono

stati ritrovati i miei documenti smarriti. Ci sono insomma tante *app*, che permettono di consultare molte pagine sui siti *web* gestiti dalla Polizia di Stato, dove si possono fare questo tipo di ricerche che per i cittadini sono molte comode. E poi in generale si sta sviluppando per lo *smartphone* la procedura YouPol.

Anche il Dipartimento per le libertà civili e l'immigrazione utilizza in modo avanzato l'informatica, ma è un Dipartimento che guarda più al cittadino. Si interessa della tutela dei diritti civili in materia di immigrazione, asilo, cittadinanza e confessioni religiose. Non ha tanto un problema di interoperabilità, ma di colloquio con gli utenti. Ci sono alcune procedure che permettono, per esempio, di verificare lo stato della domanda di riconoscimento di cittadinanza italiana, oppure si gestiscono i procedimenti degli sportelli unici per l'immigrazione presso le prefetture, che rilasciano un nullaosta. È anche consultabile lo stato delle pratiche e ci sono procedure che sostengono gli uffici in questo lavoro. Similmente, il Dipartimento dei Vigili del fuoco e del soccorso pubblico della difesa civile fornisce strumenti principalmente ai cittadini.

Sono molto interessanti alcune *app*, che non so quanto siano note. Una è l'*app* VVF Cert, che dà la possibilità di consultare quali siano i prodotti omologati e certificati dai Vigili del fuoco. Sono informazioni ai cittadini per vedere se questi materiali sono stati prodotti e testati dai Vigili del fuoco. Oppure il VVF Prevenzione Incendi Mobile, che dà invece servizi informativi di carattere generale sulla prevenzione incendi, sulle attività investigative da svolgere in caso di incendio o di esplosione, secondo una guida NFPA 921 (*National Fire Protection Association*).

Invece, per chi ama le gite in montagna o va spesso in giro per il territorio, consiglio di installarsi l'*app* NotiFire, che segnala la presenza di interventi di soccorso nelle vicinanze. Se stai camminando in alta montagna e vuoi sapere se vicino c'è un incendio e vuoi starne lontano, con un sistema di geo localizzazione sei avvisato se c'è qualcosa nelle vicinanze.

Vado infine al Dipartimento per l'amministrazione generale e per le politiche del personale, che rappresenta il punto di riferimento in ambito di programmazione, realizzazione, gestione e manutenzione delle risorse ICT (*Information and Comunication Technology*) per gli uffici centrali dell'amministrazione civile dell'interno e per le prefetture, e anche per l'erogazione di servizi digitali presso cittadini e imprese, ovviamente nell'ambito delle missioni di competenza.

Attraverso il *data center* sotto la sua gestione, viene messa a disposizione la infrastruttura di comunicazione telematica anche per altre attività del Ministero, consentendo per esempio l'accesso alla rete SPC (Sistema pubblico di connettività) per le cooperazioni applicative con la rete nazionale interbancaria, o la centrale di allarme interbancaria, la rete delle Camere di commercio, la rete dell'Agenzia delle entrate, il casellario giudiziale del Ministero della giustizia e la motorizzazione civile, in qualche caso anche con la pubblica amministrazione locale. In gran parte i contenuti riguardano le infrazioni al codice della strada, le multe che purtroppo paghiamo. Questo sistema è tutto gestito in modo veramente articolato e complesso.

La gestione diretta della rete di trasmissione di dati, la VPN delle prefetture, ha consentito un aumento dell'efficacia operativa e un recupero di efficienza correlato al progressivo incremento dell'utilizzo della stessa per servizi sempre crescenti. È un dato di fatto che, durante questo anno e mezzo, il sistema delle prefetture del Ministero non ha risentito di tutte le difficoltà operative sulle diverse modalità di lavoro dei dipendenti. Il Dipartimento è riuscito a gestire tutto senza creare nocumento alla cittadinanza e anche ad assumere tanti compiti nuovi che sono stati assegnati alle Prefetture durante la pandemia, grazie all'ottimale utilizzo di queste strumentazioni tecnologiche.

Si è registrato, infatti, da ultimo, anche un aumento considerevole degli utenti, che interessa non solo utenti privati ma anche utenti pubblici esterni, attraverso servizi di automazione informatica basati proprio sul-

l'interconnessione e l'interoperabilità con le banche dati interne ed esterne. Ricordo la Banca dati interforze, la Polizia stradale, l'Arma dei carabinieri, la motorizzazione civile, l'Agenzia delle entrate, Banca d'Italia, il casellario giudiziale, InfoCamere, Polizie locali. Colloquiamo con tutti.

In grandissima parte i progetti realizzati con le nuove tecnologie informatiche, anche attraverso l'impiego delle risorse professionali interne, hanno consentito di offrire servizi più moderni all'utenza privata tramite l'attivazione di canali di comunicazione Internet che hanno permesso l'accesso a informazioni senza la necessità di doversi recare agli sportelli delle prefetture, in particolare la Banca dati SANA e la Banca dati SISA, quella per gli assegni scoperti.

La Banca Dati SANA è quella che gestisce l'automazione dei processi sanzionatori pecuniari. In gran parte riguardano le sanzioni del codice della strada, ma ce ne sono tante altre. Da ultimo abbiamo acquisito la competenza per le sanzioni da COVID, che sono state affidate al sistema prefettizio. Questa procedura prevede la digitalizzazione di tutti i documenti necessari alla trattazione delle pratiche, all'utilizzo di modalità telematiche per la trasmissione dei ricorsi al prefetto e di tutto il procedimento, che riguarda un quantitativo enorme di pratiche, però che sono molto sensibili e che vengono istruite dal Ministero. Il personale è diminuito del 25 per cento solo negli ultimi cinque anni. Quella del Ministero dell'interno è l'età media più alta tra quelle delle Amministrazioni centrali. Infatti è intorno ai 56 anni. Gli strumenti informatici ci fanno fronteggiare questo problema, che è serissimo dappertutto.

Vorrei spendere anche qualche parola sulla Banca dati nazionale unica per la documentazione antimafia (BDNA), che è molto importante e che è pienamente operativa da cinque anni. Chiaramente non è mai uguale a sé stessa, ma è in evoluzione continua, a volte spasmodica.

Particolare attenzione è stata dedicata proprio per seguire l'interoperabilità di banche dati istituite presso le diverse amministrazioni, attraverso apposite convenzioni, per esempio con la SACE Spa, con Agea (Agenzia per le erogazioni in agricoltura), con l'Agenzia delle entrate, con Cassa depositi e prestiti, nell'ottica di migliorare l'efficacia dell'azione di tutte le amministrazioni interessate.

Proprio questo aspetto di interoperabilità, ci ha messi nelle condizioni di fare con rapidità grandi modifiche e passi avanti in questa gestione informatica durante il periodo dell'emergenza epidemiologica, perché il sistema si è dovuto fortemente implementare, in quanto ci sono stati dei nuovi princìpi normativi riguardanti la liberatoria provvisoria per effetto della disposizione di cui all'articolo 3 del decreto-legge n. 76 del 2020 e l'emissione temporanea di sostegno alla liquidità.

Tutti questi circuiti finanziari sono stati canali finanziari aperti tra Stato e soggetti privati. C'è sempre il problema dell'usura da una parte e del pericolo di infiltrazione eccetera. L'attenzione era massima e andava quindi richiesta la certificazione. Qui si è dovuti intervenire con colloqui massivi per poter dare informazioni in particolare alla SACE, che era il soggetto deputato dal Governo per questa attività. Li abbiamo sostenuti perché, se non fosse stata un'interrogazione massiva, i tempi sarebbero stati mostruosi. Per legge ci hanno imposto di provvedere in tal senso e abbiamo ottemperato nei tempi immaginati.

Come detto in precedenza, il Dipartimento è impegnato anche per la progettazione e la realizzazione di un nuovo *data center*, che risponde all'esigenza di mettere in sicurezza i CED (Centri Elaborazione Dati) e i dati di interesse strategico e consentire a tutte le pubbliche amministrazioni di evolvere verso l'erogazione di servizi digitali in sicurezza. Questo *data center*, unito ai due della Polizia di Stato, rappresenterà un'infrastruttura critica di rilevanza strategica per i servizi tecnologici delle diverse componenti del Ministero dell'interno, sia come sito primario che come sito secondario di *disaster recovery* o di *business continuity*. Potrà inoltre essere aperto a ospitare altre pubbliche amministrazioni, conseguendo così importanti eco-

nomie di scala nel consolidamento delle infrastrutture digitali pubbliche, in coerenza con le indicazioni di crescita 2.0 di AGID (Agenzia per l'Italia digitale).

Inoltre il Ministero è anche un attore del PNRR, perché abbiamo anche noi inteso approfittare della possibilità di avere i finanziamenti per iniziative ministeriali. Al Ministero sono indirizzati circa 13,4 miliardi di risorse, dei quali 1,4 miliardi sono per progetti ministeriali che vanno dalla *cybersecurity* alla digitalizzazione, ma anche a iniziative del Fondo Edifici di Culto, che è un altro ambito che gestiamo, o al *green* dei Vigili del fuoco. Ma la gran parte di questi fondi, pari a 12 miliardi, vanno agli enti locali per progetti di efficientamento energetico, rigenerazione urbana e piani urbani integrati. Ci riusciranno ad andare perché siamo informatizzati, perché quella banca dati di finanza locale che prima descrivevo sarà quella che dovrà gestire tutti i passaggi informatici di tali risorse, dalle domande che presenteranno gli enti ai controlli, all'erogazione dei fondi. Una massa di 12 miliardi in pochi anni. In qualche modo questa sfida la raccogliamo, forti del nostro stile di informatizzazione.

Per concludere, credo di aver rappresentato che l'Amministrazione dell'interno è una struttura molto complessa ed eterogenea, nella quale agiscono realtà imponenti, i Dipartimenti, che rispondono a normative diverse nonché a obiettivi peculiari alle *mission* assegnate; fattori questi che, se da un lato possono rendere difficoltoso trovare un punto di incontro comune, dall'altro costituiscono una formidabile opportunità di condivisione e di evoluzione, sicuramente anche in senso digitale, oltre che di consolidamento di un'antica attitudine alla collaborazione e integrazione interistituzionale.

Il contesto è quello tipico che vivono attualmente le pubbliche amministrazioni, a partire dalla carenza di risorse umane, ma sono tangibili i risultati estremamente positivi ottenuti nel proseguire la missione istituzionale con l'adozione delle tecnologie più moderne e più aderenti alle richieste dei cittadini e alle esigenze di sicurezza. L'opportunità offerta dall'ormai avviata politica nazionale ed europea in senso digitale è stata colta dopo qualche iniziale difficoltà e sostenuta da entusiasmo e spirito di condivisione di progetti, sistemi informatici e risorse, per il raggiungimento di obiettivi comuni nonché per l'efficace utilizzo delle risorse finanziarie finalizzate all'ICT.

I servizi digitali che sono già offerti all'utenza nonché le ulteriori progettualità evolutive e innovative di interesse strategico nazionale già avviate, tra le quali certamente spicca l'ANPR, danno atto del convinto ed efficace coinvolgimento del Ministero dell'interno nella modernizzazione del Paese: obiettivo ambizioso, complesso, ma certamente irrinunciabile. In tale direzione appaiono fondamentali anche le strutture messe in campo e le azioni attuate in ambito di sicurezza nazionale, in particolare con il CNAIPIC, per la prevenzione e la repressione dei reati ai danni delle infrastrutture informatiche.

Il contesto descritto mostra una situazione che, ritengo, si possa definire altamente confortante sulla risposta che il Ministero dell'interno ha saputo offrire sui delicati temi dell'efficientamento dei servizi, della semplificazione del rapporto tra utenti e pubblica amministrazione, della collaborazione tra amministrazioni pubbliche con la connessa interoperabilità informatica e infine, ma non in ordine di importanza, sul tema della sicurezza informatica.

La struttura organizzativa del dicastero è fortemente impegnata nello sviluppo di progettualità che, attivando nuove piattaforme informatiche, ovvero espandendo quelle esistenti, siano idonee a offrire al cittadino servizi più efficienti, sfruttando a pieno l'opportunità del PNRR. Siamo in presenza di un faticoso percorso a tappe, che è solo all'inizio e che vede una stagione di rinnovamento profondo anche per il Ministero dell'interno, chiamato a svolgere un ruolo di primo piano nel rilancio generale del Paese. Vi ringrazio per l'attenzione e sono disponibile per eventuali approfondimenti.

PRESIDENTE. Grazie, dottor Verde, anche per l'efficace sintesi dell'importante documento che ci avete prodotto. Lascio

ora la parola al generale di brigata Giuseppe Arbore, capo del III Reparto – Operazioni. Prego, generale.

GIUSEPPE ARBORE, *capo del III Reparto – Operazioni della Guardia di finanza*. Grazie, presidente. Buongiorno a tutti. Buongiorno agli onorevoli senatori e deputati in collegamento. Intanto consentitemi di porgere il saluto del nostro Comandante generale, il generale di corpo d'armata Giuseppe Zafarana, e il ringraziamento per questa opportunità, a cui unisco il mio personale ringraziamento.

Il tema della digitalizzazione e dell'interoperabilità delle banche dati è un tema fondamentale perché consente di traguardare obiettivi essenziali per lo sviluppo e per il sistema di competitività del nostro Paese. Mi riferisco alla semplificazione delle procedure, alla riduzione degli adempimenti per cittadini e imprese, e mi riferisco anche – per quanto il più diretto interesse è per la Guardia di finanza – all'azione di contrasto all'evasione e alle frodi fiscali.

La materia, inoltre, sarà importante anche perché costituisce un pilastro fondamentale del PNRR. È uno strumento per la realizzazione di ulteriori obiettivi ed è anche architrave delle riforme a carattere abilitante che accompagnano il Piano.

Del resto, per l'amministrazione finanziaria in generale e anche per la Guardia di finanza, capitale umano e digitalizzazione sono oggetto degli investimenti strategici più rilevanti. Leggo testualmente sul PNRR: « Un maggiore sfruttamento delle nuove tecnologie e strumenti di *data analysis* sempre più avanzati possono favorire l'acquisizione di informazioni rilevanti per effettuare controlli mirati sui contribuenti e possono stimolare un aumento dell'adempimento spontaneo e, conseguentemente, una riduzione del *tax gap* ».

Sicuramente l'innovazione tecnologica ha per la Guardia di finanza una valenza assolutamente strategica perché favorisce l'incremento generale dell'efficacia e dell'efficienza della nostra azione, non soltanto di contrasto all'evasione e alle frodi fiscali, ma in genere di contrasto a tutti gli illeciti di carattere economico-finanziario. Ma naturalmente la digitalizzazione comporta anche delle responsabilità. È necessario, infatti, gestire una grande mole di informazioni. Comporta la responsabilità di poterle gestire in sicurezza; quindi sicurezza del dato, continua disponibilità del dato, quindi evitare una fuoriuscita di dati ed evitare un sottoimpiego dei dati.

Il Corpo da tempo ha avviato un progetto di potenziamento della propria infrastruttura tecnologica, che naturalmente continuerà incessantemente nei prossimi anni. Sono progetti previsti, fra l'altro, nell'ambito del Libro Bianco, che è un grande progetto ideato e fortemente voluto dal nostro Comandante generale, su cui mi soffermerò fra poco, che in estrema sintesi ha l'obiettivo di ottenere il più elevato grado possibile di modernità ed efficienza del Corpo della Guardia di finanza attraverso una serie di progetti.

La consapevolezza dell'importanza di una gestione integrata dei dati è una consapevolezza che abbiamo da molto tempo. Considerate che già nel 1954 fu creato il cosiddetto « centro meccanografico » presso lo Stato maggiore, che aveva lo scopo di raccogliere e gestire una serie di informazioni e renderle fruibili agli operativi per l'attività istituzionale.

Avendo riguardo a quello che è il tema dell'audizione di oggi, mi soffermerò su questi argomenti. Intanto l'infrastruttura tecnologica di cui è dotata la Guardia di finanza, quindi i servizi digitali e l'interoperabilità (servizi digitali non soltanto a favore dell'utenza interna dei militari della Guardia di finanza, ma anche a favore di cittadini e imprese) e, quindi, il tema rilevante della sicurezza informatica. Infine mi soffermerò brevemente su alcuni progetti che intendiamo portare avanti e sulla possibilità che abbiamo anche noi di attingere ai fondi del PNRR.

Cominciamo dall'infrastruttura tecnologica. L'elemento strategico per la distribuzione dei nostri servizi digitali su tutto il territorio nazionale è rappresentato dal nostro Centro Elaborazione Dati, il CED, che è situato presso il comando generale. Il CED si propone di garantire l'erogazione di vari servizi, non soltanto ai militari del Corpo ma anche a privati cit-

tadini. Naturalmente per supportare questi servizi è necessario assicurare a questa infrastruttura adeguati livelli di sicurezza, di affidabilità e di efficienza. In questo senso il CED è stato oggetto di continui investimenti negli anni.

L'architettura è basata su un *private cloud*, quindi su un'infrastruttura di proprietà della Guardia di finanza, e impiega macchine convergenti e iperconvergenti che nel corso degli anni hanno permesso di incrementare di oltre il 60 per cento il numero dei CPU (*Central Processing Unit*) che sono impiegati, del 25 per cento la capacità di *storage* ordinario e di quasi il 600 per cento quella con funzioni di *backup*. A ciò si è accompagnata per finalità di sicurezza l'implementazione di specifiche funzionalità anti-*ransomware* e di cifratura dei dati.

Il secondo elemento strategico dell'infrastruttura digitale è rappresentato dalla nostra rete di telecomunicazioni. Attraverso questa rete noi garantiamo il flusso di dati fra le varie unità operative. Ciò è possibile attraverso un collegamento moderno in fibra ottica che consente l'interconnessione dello scambio dei dati fra il comando generale, la centrale operativa del comando generale, le sale operative situate presso ogni comando provinciale e, naturalmente, tutti gli altri reparti operativi.

La trasmissione delle informazioni avviene attraverso una rete detta « Interpolizie », perché condivisa con l'Arma dei carabinieri e la Polizia di Stato, e infrastrutture di trasporto, che è costituita da quattro dorsali, ognuna con una velocità di connessione pari a 2,5 gigabyte al secondo, che permette quindi di instradare, gestire le comunicazioni e il traffico dati fra i vari comandi.

Al momento sono collegati in fibra ottica 271 sedi, con l'interessamento di quasi 600 reparti, con una velocità di connessione fino a 10 gigabyte al secondo. Le altre 64 sedi sono collegate a mezzo di ponte radio ad alte prestazioni, con il coinvolgimento di altri 79 reparti. Le unità alla sede di Roma raggiungono una capacità di connessione ridondante di 40 gigabyte, mentre per assicurare il collegamento con la Sardegna ci siamo avvalsi di cavi sottomarini in fibra ottica.

Le quattro dorsali arrivano al comando generale con un collegamento pari a 10 gigabyte al secondo, che viene tutto instradato verso il Centro Stella costituito dal CED, attraverso il quale vengono fruiti tutti i servizi al Corpo. Attualmente è in atto anche un potenziamento per incrementare la velocità della tratta Roma-Milano, che abbisogna di un flusso dati molto consistente affinché raggiunga i 100 gigabyte.

Attraverso il CED è anche possibile accedere alla navigazione a Internet tramite un collegamento a 5 gigabyte fornito dal *provider*. Ci siamo dotati di un'infrastruttura di gestione dell'accesso alla rete Internet da parte delle macchine degli utenti di dominio, basata sul sistema proxy, che è configurato in alta affidabilità, che garantisce una profilazione sicura degli accessi.

La rete delle telecomunicazioni è completata da quello che è il sistema di videoconferenze: un sistema che ci ha consentito di continuare a gestire le comunicazioni in videoconferenza tra i vari reparti, e in questo periodo di pandemia è stato assolutamente fondamentale. In ogni comando provinciale è allestito un totem polifunzionale. Tutti questi totem si appoggiano alla rete proprietaria del Corpo, che è in grado di garantire elevati standard di sicurezza perché i flussi di videocomunicazione sono cifrati con una chiave a 256 bit, quindi ci consente di comunicare in assoluta sicurezza.

La potenzialità ha avuto un'importanza fondamentale nel periodo della pandemia. Consentitemi da ultimo una breve menzione sul tema della tutela ambientale. La Guardia di finanza da subito ha cercato di operare anche la transizione di carattere ecologico. Ancorché l'intera infrastruttura sia stata oggetto di interventi di potenziamento notevoli, quindi con un flusso dati molto in crescita, l'utilizzo di soluzioni iperconvergenti ci ha consentito di risparmiare il 33 per cento dei consumi.

Andiamo ai servizi digitali e all'interoperabilità delle banche dati, che è un po' il cuore dell'audizione di oggi. Natu-

ralmente noi offriamo, come dicevo in premessa, oltre ai servizi ai nostri militari, anche servizi ai cittadini. In primo luogo mi riferisco al sito Internet istituzionale. È un sito in cui sono reperibili numerose informazioni, anche informazioni utili per il cittadino per difendersi da una serie di truffe. Nel sito è anche possibile verificare la conformità di quel contrassegno che è generato elettronicamente, che è apposto sui fogli di servizio dei nostri militari e che viene notificato dal contribuente in occasione dei nostri controlli fiscali. Quindi il contribuente può da subito verificare la bontà e la genuinità del contrassegno; quindi sa di avere di fronte dei finanzieri autentici, consentimi l'espressione.

Inoltre il sito ha anche un portale concorsi che naturalmente, come dice il nome, gestisce tutte le fasi concorsuali, quindi i rapporti con i candidati, con i cittadini. Questo è attivo dal 2017. Veramente con poche risorse riusciamo a gestire tutta l'attività concorsuale attraverso questo sito. Dal 2017 abbiamo gestito 50 concorsi, con il coinvolgimento di circa 250 mila candidati.

Un altro sito importantissimo è il nostro SIAC (Sistema Informativo Anti-Contraffazione). È una pietra miliare nella lotta alla contraffazione, perché in questo sito interagiscono non soltanto le forze dell'ordine, alimentate dalla Direzione centrale di polizia criminale, ma anche i privati cittadini, le imprese. Si possono avere informazioni sui prodotti contraffatti, sui prodotti insicuri; ma gli stessi titolari dei marchi possono depositare, trasferire, caricare informazioni sui loro prodotti, in modo tale che le forze dell'ordine siano agevolate per l'individuazione dei falsi, ma anche i cittadini siano agevolati nel proteggersi dai falsi stessi.

Questi richiami a tali applicativi utili dal punto di vista operativo, ovviamente, mi consentono di introdurre il tema delicatissimo e importantissimo dell'interoperabilità delle banche dati. È chiaro, per una forza di polizia come la Guardia di finanza, che fa della sua interdisciplinarietà un po' la cifra identitaria del suo operare, avere a disposizione una perfetta interoperabilità delle banche dati è fondamentale, perché il nostro approccio operativo è sempre teso a individuare tutte le forme di illegalità comunque collegate alla specifica condotta.

L'interoperabilità è fondamentale, oltre a essere attuazione pratica del principio *once only*, che è stato introdotto dalla legge n. 241/1990, ribadito dallo Statuto dei diritti del contribuente e riaffermato, proprio in termini di divieto a carico dei contribuenti, dall'articolo 7 del decreto-legge n. 70 del 2011, dove si legge che i contribuenti non devono fornire informazioni che siano già in possesso del fisco e degli enti previdenziali, ovvero che da questi possono essere direttamente acquisiti da altre amministrazioni. Comprendete bene come diventa fondamentale per l'operatore poter acquisire in maniera massiva tutte le informazioni con riferimento allo specifico soggetto.

Questo è un principio che noi abbiamo già fatto nostro con il nostro manuale sull'attività di verifica, la circolare 1/2018, che è un po' l'insieme di tutte le disposizioni che regolano l'attività di controllo fiscale. Qui è chiarito che nessun tipo di ulteriore aggravio al contribuente deve essere portato laddove si abbia la possibilità di avere le informazioni autonomamente attraverso l'interoperabilità delle banche dati. Questa interoperabilità non è soltanto fondamentale nella fase di controllo, ma è anche e soprattutto fondamentale nella fase di preparazione del controllo, perché la piena interoperabilità delle banche dati ci consente di avere tutte quelle informazioni che ci dividono verso i target remunerativi, con ciò riducendo l'aggravio nei confronti degli imprenditori onesti. La piena interoperabilità consente non soltanto di trovare gli illeciti, ma anche di avere chiara contezza dell'onestà del contribuente, quindi del suo corretto adempimento fiscale. Questo ci consente di mirare sempre meglio ai nostri obiettivi.

Del resto la nostra azione è complementare, come sapete, a quella dell'agenzia fiscale, perché il nostro approccio è un approccio di polizia, quindi finalizzato a

individuare veramente le frodi più pericolose per il fisco. L'esperienza operativa ci dimostra, per esempio, come facendo interagire i dati della fatturazione elettronica con i dati dell'Anagrafe tributaria, con i dati di Polizia, possiamo individuare in maniera tempestiva le frodi. E, come sapete, la tempestività dell'intervento fa premio in questi casi, soprattutto nelle frodi fiscali, perché ovviamente inibisce l'ulteriore danno all'erario che la specifica frode può apportare.

In prospettiva, un ulteriore impulso in questa direzione potrà essere dato dall'attuazione, in armonia sempre con la normativa della *privacy*, dell'articolo 14 del decreto-legge 124, il decreto fiscale per il 2020, il quale prevede la memorizzazione integrale dei file XML delle fatture elettroniche fino al 31 dicembre dell'ottavo anno successivo, chiaramente finalizzato all'esecuzione dei controlli. Per tale via, infatti, gli organi di controllo non soltanto avranno informazioni sui dati fattura, cioè imponibile e soggetti sui quali interviene l'operazione, ma anche sulla natura dell'operazione. Avere contezza della natura dell'operazione è fondamentale per comprendere se vi è o meno una frode dietro un'apparente regolare transizione commerciale.

Recentemente si è registrata anche con favore un'ulteriore novità sul piano legislativo, tesa a valorizzare maggiormente le attività e i compiti di interesse pubblico svolti dalle pubbliche amministrazioni. Ci si riferisce all'articolo 9 del decreto-legge n. 139 del 2021, il cosiddetto « decreto capienze », che svincola la base giuridica, indispensabile per i trattamenti in ambito pubblico, da tassative previsioni legislative o regolamentari. Questo in un'ottica di semplificazione del quadro normativo e per allineare le pertinenti previsioni del codice della *privacy* al Regolamento Ue n. 679 del 2016, introducendo al contempo una forma di responsabilizzazione in capo alla pubblica amministrazione. In sostanza le pubbliche amministrazioni, nel momento in cui devono gestire e trattare dati per perseguire finalità pubbliche, lo possono fare anche se non vi è una base giuridica e regolamentare che le autorizzi. Tuttavia questo non vuol dire che vi sia assoluta discrezionalità. La pubblica amministrazione deve dimostrare, intanto, la finalità che intende perseguire, individuare il responsabile e dare piena pubblicità a questo trattamento dati.

Su tale delicata questione e sui contenuti della norma in esame sono tuttora in corso i ragionamenti e le valutazioni, che si stanno svolgendo nell'ambito del processo di conversione del decreto-legge. In ogni caso, tenuto conto dei significativi riflessi della suddetta novità legislativa rispetto all'attività di analisi operativa sistematicamente svolta dal Corpo, sarebbe opportuno chiarire che l'applicabilità o meno ai trattamenti eseguiti sia riconducibile anche ai trattamenti eseguiti per finalità di polizia. Naturalmente noi auspichiamo che ci sia questa estensione del portato della norma.

Del resto, l'analisi del rischio oggi è fondamentale e si coniuga con quella che è un'altra funzione tipica di una forza di polizia, che è il controllo economico del territorio. Come vi dicevo, la nostra attività deve essere sempre più mirata su target caratterizzati da elevati livelli di rischio. Il nostro intervento deve essere, passatemi il termine, « a colpo sicuro ». Per fare questo come ci siamo organizzati ? Noi abbiamo una componente speciale che ha il compito di svolgere analisi, e lo svolgimento dell'analisi passa necessariamente attraverso la piena interoperabilità delle banche dati. Sulla base delle linee strategiche dell'intervento, cioè su quali fenomeni vogliamo concentrare la nostra azione operativa – e questo lo facciamo sulla base delle indicazioni che ci pervengono dal nostro Ministro dell'economia e delle finanze – la componente speciale opera questa analisi e trasferisce i target alla componente territoriale per lo svolgimento delle attività operative. La quale componente territoriale entra nel processo di analisi attraverso il controllo economico del territorio, perché non tutte le informazioni sono ritraibili dalla mera consultazione delle banche dati. Talvolta, dal controllo fisico, dal controllo del territorio, è dato percepire quegli *alert* di rischio che invece sono sintomatici di un

fenomeno illecito e che vanno trasferiti comunque alla componente speciale perché deve integrare il suo processo di analisi al fine di ricomprendere ulteriori elementi di rischio che sul territorio vengono individuati.

Tutto questo dialogo di informazione deve passare attraverso una piena interoperabilità, che noi garantiamo attraverso quella che abbiamo definito « dorsale informatica », che è una moderna architettura tecnologica che unifica in un'unica piattaforma « federata » tutti gli applicativi in uso alla Guardia di finanza, ottimizzando così i processi di lavoro.

Grazie a questa infrastruttura, che è stata realizzata unitamente al nostro *partner* tecnologico, Sogei, e disegnata in piena aderenza alla normativa sulla *privacy*, possiamo esplorare nuove forme di analisi. È una piattaforma che agevola molto il lavoro del nostro operatore. Uno dei motivi è che consente addirittura di alimentare in automatico dei verbali veri e propri, perché abbiamo costruito dei moduli operativi standardizzati che, attraverso l'acquisizione di informazioni, vanno a precompilare addirittura i nostri verbali. Questo chiaramente agevola il lavoro dei nostri operatori. Non solo: chiaramente con un'unica interrogazione si va a interrogare tutte le banche dati, attraverso anche visualizzazioni delle relazioni fra le varie entità che emergono dall'interrogazione. Mentre su un soggetto, fino a qualche tempo fa, l'operatore doveva impiegare ore per interrogare tutte le 140 banche dati di cui disponiamo, creare relazioni e quindi dare un sunto di questa analisi, oggi lo si fa praticamente in via istantanea. Pensate che risparmio in termini di risorse, risorse che vanno riconvertite in attività operative.

Andiamo oltre in questa dorsale informatica. Stiamo lavorando e, a brevissimo, entro fine anno, dovremmo terminare l'implementazione a un'ulteriore funzionalità molto importante. Questa banca dati ci consente di mettere a sistema centinaia di informazioni di contesto esterno; mi riferisco a dati di carattere economico, di carattere sociale, di carattere criminale, criminogeno. Questo per georeferenziare i rischi sul territorio. Ogni nostro comando, ogni nostro reparto deve sapere benissimo sul suo territorio qual è l'evoluzione del contesto sociale, del contesto economico, quali possono essere le discrasie nella lettura combinata di questi dati, in un'ottica anche di prevenzione e non solo di repressione.

In tema di connettività un altro progetto importante, che noi abbiamo definito « Grifo », consente ai nostri operatori di interrogare anche da remoto le banche dati in mobilità attraverso specifici dispositivi criptati che sono in interconnessione con le nostre sale operative e che consentono anche la georeferenziazione, il che consente quindi alle sale operative di avere anche la mappatura di dove si trovano le pattuglie. Voi immaginate anche in caso di emergenza quanto questo sia fondamentale.

Passiamo al comparto aeronavale. Voi sapete, siamo da qualche anno la Polizia del mare. Questo ha fatto sì che destinassimo cospicui investimenti anche nella gestione informatica e telematica del comando e controllo della componente aeronavale. Abbiamo realizzato *in house* un sistema telematico proprietario che abbiamo chiamato con l'acronimo C4i. Le quattro C sarebbero comando, controllo, comunicazione compiuta e « i » sta per informazione. Questo sistema sostituisce intanto i 70 mila documenti cartacei che ogni anno governavano l'impiego del comparto aeronavale; introduce una rimodulazione della capacità operativa nello specifico settore verso un assetto di tipo cosiddetto « netcentrico », nel quale tutti gli elementi fisici, umani e organizzativi sono collegati fra loro e coordinati in modo nuovo; sfrutta tutte le intrinseche capacità della rete di raccogliere, trattare e distribuire in forma condivisa e protetta le informazioni di interesse operativo.

Vedete, le nostre unità navali o le società aeree, quando pattugliano, devono avere contezza piena dello scenario di riferimento. Tutte le informazioni comunque reperibili che attengono a quel teatro su cui stanno navigando o volando devono essere nella disponibilità dell'operatore, che deve poter interloquire direttamente con tutto il

centro di comando e controllo a livello locale e a livello centrale. Questa è la funzione del C4i.

Noi abbiamo due componenti aeronavali, cosiddette « costiera » e « alturiera ». La componente costiera è quella che dipende da ogni comando regionale. Noi abbiamo 15 comandi operativi aeronavali che dipendono quindi da 15 comandi regionali, che hanno una componente fatta di unità medio-piccole che hanno lo scopo di pattugliare il mare territoriale e, al più, spingersi verso la zona contigua, ulteriori 12 miglia. Ma voi sapete bene che i traffici illeciti partono da ben lontano, quindi abbiamo necessità di pattugliare anche l'alto mare. Lo si fa con la nostra componente alturiera, fatta da unità aeree e navali più performanti, con maggiore autonomia, che non possono dipendere da un comando territoriale, perché non c'è una riconducibilità diretta a un'operazione sul territorio, ma hanno lo scopo di pattugliare anche il mare e l'alto mare. Queste due componenti devono dialogare fra di loro, devono dialogare con il comando generale, devono dialogare con i vari comandi sul territorio; ed è questa la piattaforma comune di dialogo: il C4i.

Al fine di garantire poi una gestione centralizzata della messaggistica sia interna che esterna dei calendari, delle rubriche, che possono essere consultati dai nostri militari con l'ausilio di dispositivi quali *smartphone* e *tablet*, abbiamo anche investito in infrastrutture in locale della posta elettronica, che vede l'impiego di server dedicati in grado di ridurre al minimo i tempi legati a eventuali disservizi.

Ricordo infine che le attività formative e post formative, non solo in presenza ma anche a distanza, vengono effettuate attraverso la nostra rete telematica. Considerate che fra marzo 2020 e settembre 2021, quindi nel periodo di pandemia, non ci siamo fermati con la nostra attività formativa. Anzi, in modalità *e-learning* abbiamo erogato 75 corsi, facendo partecipare 44.800 frequentatori. Siamo 60 mila, quindi pensate bene come si è diffusa questa attività formativa. Ulteriori 21 costi di formazione del ruolo ufficiali ispettori, che hanno riguardato anche 8.142 allievi in formazione. Non solo: fra i beneficiari ci sono anche funzionari stranieri, perché la nostra scuola di polizia economico-finanziaria è considerata *Academy* per la *Tax Crime* dell'OCSE (Organizzazione per la Sicurezza e la Cooperazione in Europa). È punto di formazione della CEPOL (European Union Agency for Law Enforcement Training), è punto di formazione anche di Frontex (European Border and Coast Guard Agency). Non ci siamo fermati neanche nella formazione di funzionari stranieri. Abbiamo formato 4.887 funzionari stranieri, ovviamente in varie lingue, in vari Paesi.

Passo alla sicurezza informatica, tema naturalmente molto delicato. Come dicevo, lo sviluppo tecnologico si accompagna alla necessità di garantire un'adeguata cornice di sicurezza alla mole sempre più rilevante di informazioni presenti nei diversi applicativi. L'infrastruttura IT del Corpo beneficia degli interventi di evoluzione e di investimenti svolti, ovviamente, durante gli anni per contrastare la recrudescenza di attacchi cybernetici. Non solo interventi di natura tecnica, ma anche di tipo gestionale, perché si sono posti l'obiettivo di fare evolvere gradualmente i processi lavorativi in modo da introdurre gli strumenti IT necessari e le relative protezioni, considerando sia la natura del dato trattato, sia, più in generale, i rischi per l'organizzazione.

Da un punto di vista della tutela del dato, sia con riferimento al trattamento ordinario che di polizia, il principale esempio di rischio gestionale è l'attività continuativa di gestione del rischio. Consente di orientare gli investimenti tecnologici pluriennali e gli interventi di progettazione delle difese *cyber* in relazione alla criticità dello specifico servizio o dato da tutelare, alla probabilità di un evento avverso e al relativo impatto per il cittadino e per il Corpo.

I presidi sono di due tipi: c'è una sicurezza di carattere perimetrale e una interna. Le misure di sicurezza perimetrale sono quelle finalizzate a ridurre il rischio di accessi non autorizzati dalla rete Internet alla rete interna. La Guardia di finanza adotta i più moderni presìdi in questo

senso, costantemente aggiornati nel tempo, al fine di scongiurare eventuali tentativi di elusione delle difese, quindi consentendo di mantenere sempre in piena attività anche il nostro sito e anche i servizi nei confronti del cittadino.

Allo scopo di mitigare i rischi sono state poste in essere diverse iniziative, soprattutto di tipo preventivo, con attività costante di analisi delle potenziali vulnerabilità e alla conduzione proprio di *penetration test*, volti a rilevare debolezze di sistemi sfruttabili da male intenzionati.

A queste misure si affiancano iniziative di tipo deterrente, che non consentono mai il contatto diretto dell'utente con le macchine interne che offrono il servizio, grazie all'impiego di un bastione di difesa *ad hoc* che si interpone fra esse. Si affiancano anche iniziative di tipo reattivo, con l'analisi delle interazioni dell'utente e il blocco di quelle potenzialmente nocive.

Per ridurre i rischi di accessi di massa a un determinato servizio con il fine di renderlo indisponibile in virtù dell'elevato carico generato, anche il canale di comunicazione proveniente da Internet è opportunamente monitorato. Si devia all'occorrenza il traffico malevolo prima che possa causare disservizi.

Queste sono le misure di carattere perimetrale. Abbiamo anche adottato misure per la sicurezza interna. La sicurezza interna è promossa in primo luogo attraverso un'opportuna compartimentazione fisica e logica fra la rete interna e quella esterna, nonché fra le diverse reti interne che ospitano i servizi. Gli eventi relativi ai servizi e alle postazioni sono monitorati costantemente da una struttura specialistica dedicata, il *Security operation center*, che opera a livello nazionale per l'identificazione preventiva delle minacce all'interno della rete del Corpo e per l'eventuale pronta azione di risposta, in base a piani di interventi prestabiliti e preventivamente concordati, che ovviamente sono piani praticamente revisionati.

Il *Security operation center* ha lo scopo di gestire i principali apparati di sicurezza che proteggono i servizi telematici della Guardia di finanza e di monitorare gli eventi di sicurezza a livello nazionale sulla rete Gdfnet, rispondendo prontamente a eventuali incidenti di sicurezza e dando seguito alle segnalazioni proattive da parte del Ministero dell'economia e delle finanze e degli altri organi deputati alla *cybersecurity*. La Guardia di finanza rappresenta, infatti, una delle componenti del *Computer Emergency Response Team* del Ministero dell'economia e delle finanze.

In considerazione dell'elevata mole di eventi informatici che caratterizza la normale funzionalità di un complesso sistema informatico come il nostro, il *Security operation center* dispone di strumenti di analisi avanzata basati anche sull'intelligenza artificiale, che consentono di coadiuvare l'operatore specializzato nell'individuazione dei casi sospetti anche in via esclusivamente preventiva. Tali analisi sono supportate da un'attività di creazione di scenari standard di configurazione dei dispositivi dei relativi casi di uso, al fine di discriminare più semplicemente ciò che può essere effettivamente causato da attività malevoli.

Fra queste iniziative rientra quella di gestione dei diritti amministrativi degli utenti, orientata anche in funzione della tutela della *privacy* al principio del minimo privilegio, in base al quale a ciascun operatore vengono riconosciuti i livelli minimi di accesso dei quali ha bisogno per svolgere le proprie mansioni, in un'ottica di sussidiarietà.

Qualche parola sulle iniziative in tema di *cybersecurity* e *big data analysis*. Al fine di cogliere nuove opportunità che derivano dal vasto patrimonio informativo a disposizione del Corpo, a completamento del processo di digitalizzazione e interoperabilità delle banche dati, la Guardia di finanza ha avviato di recente importanti iniziative al fine di tutelare la sicurezza dei dati e garantire adeguate *performance* nella gestione dei flussi informativi, attraverso un continuo rinnovamento delle infrastrutture di collegamento fra le unità centrali e periferiche.

A questo fine, nell'ambito del PNRR, il Corpo ha proposto il progetto denominato « Missione digitale », per il quale è stato riconosciuto un finanziamento complessivo

di 32 milioni di euro, organizzato sulle due linee di sviluppo: *cybersecurity* e *data analysis*. In materia di *cybersecurity* le risorse saranno impiegate per rafforzare ulteriormente la sicurezza delle infrastrutture del Corpo, prevedendo strumenti evoluti di monitoraggio degli eventi sulla rete e automatizzando le azioni di contrasto agli attacchi, così da ridurre al minimo il periodo di reazione.

Gli interventi saranno finalizzati ad avviare un percorso di conformità ai requisiti stabiliti nel perimetro di sicurezza cybernetico nazionale previsto dal decreto-legge n. 105 del 2019, per meglio assicurare l'allineamento degli obiettivi di protezione della Guardia di finanza alle strategie di livello nazionale. Pertanto, si procederà innanzitutto a potenziare il *Security operation center* anche attraverso l'acquisizione di sistemi di analisi automatica dei *file* in ingresso dalla rete e di strumenti per la rilevazione di attacchi. Inoltre, interverremo sull'evoluzione delle infrastrutture di rete tramite un *refresh* tecnologico dei sistemi di sicurezza perimetrali, cosiddetti *firewall*, e un rafforzamento dei meccanismi di controllo degli accessi delle autorizzazioni di utenti e dispositivi, grazie all'implementazione di un sistema di autenticazione e autorizzazione a doppio fattore per le operazioni amministrative critiche. Infine potenzieremo la protezione informatica delle singole postazioni del Corpo, supportando il programma di consapevolezza *cyber* degli utenti attraverso l'acquisizione di strumenti per la formazione interattiva e per la gestione centralizzata della somministrazione dei corsi.

Come dicevo, la seconda linea di sviluppo, denominata *big data analysis*, mira invece alla creazione di un'infrastruttura per semplificare le operazioni di analisi avanzate di una grande mole di dati, al fine di contrastare più efficacemente i fenomeni illeciti in materia economico-finanziaria, anche con l'utilizzo di tecniche di intelligenza artificiale, che è quella che ci consente di svolgere una funzione di prevenzione, oltre che di repressione.

Il progetto si prefigge di applicare la *data science* in conformità alla normativa in materia di protezione dei dati, al fine di analizzare in tempi estremamente rapidi enormi quantità di informazioni contenute in diversi silos dal contenuto eterogeneo. Nel dettaglio provvederemo a strutturare una complessa iniziativa attraverso la progettazione dell'intera infrastruttura, l'acquisizione di *software* di analisi dedicate allo scopo, il reperimento di prestazioni professionali di *data scientist* e l'implementazione delle dotazioni *hardware*.

La combinazione sinergica di queste risorse consentirà di sviluppare percorsi di analisi sia di tipo predittivo, in grado di prevedere le possibili manifestazioni di illegalità, sia di tipo prescrittivo, volte a perfezionare la capacità di risposta agli eventi futuri. I *big data* e l'intelligenza artificiale supporteranno quindi le decisioni strategiche e tattiche, amplificando la capacità di conoscere e comprendere i fenomeni criminali. Per noi è fondamentale.

L'applicazione dell'intelligenza artificiale, in piena conformità alle prescrizioni del Garante della *privacy,* con cui abbiamo continue interlocuzioni sulle nostre progettualità, è fondamentale per intercettare, ancora di più prevenire, fenomeni illeciti proprio sulla base dell'interazione di quei dati di formazione comunque disponibili, ma messi in una logica di sistema diversa, attraverso percorsi di analisi, anche attraverso tecniche di *machine learning*.

Naturalmente, per fare questo abbiamo avviato collaborazioni scientifiche, cercando di attingere *know how* dalle migliori professionalità a livello globale. Abbiamo avviato collaborazioni con importanti istituzioni accademiche. Intanto abbiamo coinvolto ricercatori della Harvard University di Cambridge, dell'Einaudi Institute for Economics and Finance, per la creazione di modelli statistici anche in un'ottica previsionale, con il fine di prevenire e reprimere reati in materia di imposte sui redditi e sul valore aggiunto, ad esempio.

Abbiamo un progetto di analisi già strutturato. L'abbiamo sottoposto al Garante della *privacy*. Abbiamo in corso interlocuzioni con il Garante molto proficue per andare a esplorare qualsiasi rischio per la *privacy* del cittadino perché, come dicevo, il

nostro approccio è comunque assolutamente rispettoso della *privacy* dei cittadini.

Parallelamente, ci siamo dotati di un *software* per l'analisi automatizzata dei bilanci societari, così da individuare eventuali anomalie presenti, svelare possibili correlazioni e interferenze non riscontrabili attraverso il preventivo intervento umano. Quando parliamo di bilancio societario non parliamo naturalmente di dati sensibili sul piano della *privacy*, perché non attengono a persone fisiche. A questo fine, lo scorso mese di luglio abbiamo avviato una *partnership* con il Centro di ricerca interuniversitario sulle scienze della sicurezza e della criminalità di Trento, composto da docenti e ricercatori dell'università di Trento e di Verona.

Quanto ho finora esposto probabilmente ci consente di apprezzare gli sforzi che stiamo profondendo da tempo per rinnovare e potenziare la nostra « identità digitale ». Del resto, siamo ben consapevoli che la disponibilità di un efficiente e moderno sistema informatico assicura alle organizzazioni complesse come la nostra un'ampia gamma di benefici, che va ben oltre la mera efficienza interna, che deriva dalla sicurezza e dall'affidabilità dei dati e della loro continua fruibilità.

Per una forza di polizia economica finanziaria ciò è fondamentale, ma questo porta vantaggi anche per i cittadini. Proprio per questo la digitalizzazione – e vengo al Libro Bianco – è uno dei capisaldi del progetto Libro Bianco. Come dicevo, è un'iniziativa voluta dal Comandante generale. Nell'ambito di questa iniziativa sono delineati 57 progetti che impattano significativamente sulle diverse componenti dell'organizzazione in termini di processi lavorativi, strutture, culture organizzative, risorse umane e strumentali. È un progetto ovviamente di medio-lungo termine.

La gran parte di queste iniziative prende le mosse dalla rivoluzione tecnologica in atto, che ha guidato un po' come *leitmotive* tutti i 57 progetti che fanno parte del Libro Bianco. È una rivoluzione molto particolare quella che stiamo vivendo, che ha tre caratteristiche fondamentali: velocità, profondità e ampiezza di impatto di ciò che sta avvenendo. L'insieme di questi fattori, i cui effetti ben possono essere paragonati a una sorta di quarta rivoluzione industriale, ha posto il Corpo e tutte le amministrazioni pubbliche di fronte a sfide inedite.

Si dovrà quindi perseguire l'obiettivo, a qualsiasi livello, di un attento, diffuso, qualificato, consapevole utilizzo della tecnologia. Ci si dovrà avvalere di un maggior numero di ingegneri, di sistemisti, di analisti *software*, programmatori, specialisti in sicurezza informatica e altre figure di settore. Queste risorse saranno fondamentali per proseguire il processo di ammodernamento in atto e per seguire un programma di ulteriore potenziamento. Ecco perché la Guardia di finanza guarda con attenzione anche al Polo strategico nazionale previsto dalle nuove disposizioni, introdotte nel Codice dell'amministrazione digitale dal cosiddetto « decreto semplificazioni », in base al quale tutte le pubbliche amministrazioni sono tenute ad accreditarsi alla piattaforma digitale nazionale gestita dalla Presidenza del Consiglio dei ministri, con l'obiettivo di favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto per finalità istituzionali.

Riteniamo che tale piattaforma possa integrare sinergicamente l'infrastruttura tecnologica proprietaria del Corpo nella gestione di alcune tipologie di dati, in ragione della loro complessità e disponibilità.

Sottolineo ancora una volta che il processo di digitalizzazione è un volano di cui deve essere garantita l'efficienza, l'interconnessione e l'integrazione, al servizio dei cittadini e del bene comune, sulla base di regole giuridiche ed etiche condivise; un processo che nel suo inesorabile incedere deve essere governato e guidato da risorse umane professionalmente competenti e con lo sguardo sempre rivolto al futuro. È un connubio tra capitale umano e rafforzamento delle nuove tecnologie – su cui mi ero già soffermato in premessa – su cui continueremo a investire per dare il nostro contributo alle prospettive di rilancio e di sviluppo del nostro Paese. Vi ringrazio per l'attenzione e resto a disposizione per qualsiasi esigenza di approfondimento. Grazie.

PRESIDENTE. Grazie, generale Arbore, per averci illustrato la relazione che comunque ci avete fatto avere per tempo e averla sintetizzata anche in questo caso in maniera molto chiara. Si tratta naturalmente di azioni, come abbiamo potuto vedere, molto complesse, molto particolari, che ovviamente avrebbero bisogno di maggiore tempo per essere comprese nella loro completezza. Però credo che il quadro che ci avete fornito, sia per quanto riguarda la Guardia di finanza, sia per quanto riguarda il Ministero dell'interno, sia altamente soddisfacente per il lavoro che la Commissione intende svolgere. Chiedo se ci sono interventi. Prego.

CARLA CANTONE. Molto brevemente. Mi associo alle parole che il presidente ha già detto, anche per ringraziare sia il dottor Verde che il generale Arbore. Debbo dire che non sempre riesco a entrare in sintonia con le relazioni molto complicate di questa Commissione. Per voi è più semplice, ma per noi che ci occupiamo di tante cose ma non nello specifico bisogna fare molta attenzione. Io oggi sono veramente soddisfatta delle relazioni che ho ascoltato e me le riguarderò con calma, ma già penso che il lavoro che ci avete consegnato, come diceva il presidente, sia un lavoro eccezionale per la responsabilità e il ruolo che questa Commissione deve svolgere. Grazie davvero per le parole, la competenza e la serietà. Mi sentivo di dirvelo.

PRESIDENTE. Grazie, onorevole Cantone. Mi associo alle sue considerazioni. Chiede la parola il senatore Marino. Prego, senatore.

MAURO MARIA MARINO *(intervento da remoto)*. Grazie, presidente. Purtroppo da noi l'Aula è iniziata da 20 minuti, infatti ho visto che il senatore Fenu ha già dovuto abbandonare (questi sono i problemi delle bicamerali). Anch'io faccio i complimenti sia al dottor Verde sia al generale Arbore per due relazioni veramente esaustive. Faccio una domanda velocissima al generale Arbore rispetto all'interoperabilità. Qui parlo in qualità di presidente della Commissione d'inchiesta sul gioco illegale. Nella prima parte dell'audizione che noi abbiamo fatto al direttore dell'Agenzia delle dogane e dei monopoli, che verrà ripresa domani, c'era stata una *lamentatio* sull'interoperabilità e sulla possibilità di accesso ai dati da parte dell'Agenzia delle dogane e dei monopoli. Naturalmente era la prima parte della relazione, le domande le faremo domani. Volevo sapere se voi avevate ravvisato lo stesso tipo di problema e, qualora fosse così, se era un problema di protocolli di accesso o di sistemi che non si parlano fra di loro. Grazie.

GIUSEPPE ARBORE, *capo del III Reparto – Operazioni della Guardia di finanza*. Grazie, senatore Marino. Noi non abbiamo problemi di accesso alla banca dati gioco. È federata nella nostra dorsale informatica, quella struttura di cui parlavo prima. Tra l'altro è una banca dati per noi fondamentale, molto utile, perché individua attraverso il codice fiscale l'ammontare, anche il saldo, dei conti gioco dei cittadini. Ovviamente i gestori del gioco pubblico amministrato sono anche presidio antiriciclaggio, quindi svolgono un'adeguata verifica della clientela e dei cittadini. Chi vuole operare anche nel gioco *online* si deve identificare e viene aperta una sottopartita anche del conto del concessionario, per cui abbiamo contezza del saldo. Vi posso garantire che abbiamo anche delle sorprese, abbiamo dei bei saldi di conti gioco. Fra l'altro vi do un dato: in tutti quei casi in cui abbiamo inibito il reddito di cittadinanza in connessione con profili reddituali non veritieri, il 21 per cento era per un saldo del conto di gioco. È una banca dati che noi utilizziamo ed è interconnessa, anche quando effettuiamo sequestri per equivalente, quindi tesi ad aggredire qualsiasi disponibilità finanziaria. Consultiamo in maniera sistematica il conto gioco perché andiamo anche ad acquisire quel saldo, per cui non abbiamo problemi di connessione. Sinceramente non ho contezza dei problemi di connessione dell'Agenzia

delle dogane, ma noi non ne abbiamo. Grazie.

PRESIDENTE. Grazie, generale. Se non ci sono altre richieste da parte dei colleghi possiamo chiudere. Grazie ancora sia al generale che al dottor Giancarlo Verde per l'esaustivo intervento. Grazie ai colleghi.

Dichiaro conclusa l'audizione.

La seduta termina alle 9.55.

Licenziato per la stampa
il 19 gennaio 2022

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

18STC0165790