Ministero dell'Interno

INDAGINE CONOSCITIVA SULLA DIGITALIZZAZIONE E INTEROPERABILITÀ DELLE BANCHE DATI FISCALI

Audizione del Dott. Giancarlo Verde

Direttore Centrale per le Risorse Finanziarie e Strumentali – Responsabile della Transizione Digitale

Ministero dell'Interno

Commissione Parlamentare di Vigilanza sull'Anagrafe Tributaria

17 novembre 2021

Ministero dell'Interno

PREMESSA

Signor Presidente, On.li Commissari,

sono Giancarlo Verde, Direttore Centrale per le Risorse Finanziarie e Strumentali, nonché Responsabile per la Transizione Digitale del Ministero dell'Interno, e in quest'ultima veste sono stato delegato a fornire un quadro esplicativo, quanto più ampio possibile, sulla tipologia delle infrastrutture tecnologiche e dei servizi digitali offerti, nonché sulla tutela dei dati critici e strategici detenuti, in relazione alla definizione del progetto di Cloud nazionale, la cui infrasttuttura è in fase di realizzazione nella forma del Polo Strategico Nazionale.

Stante la complessità della relazione che mi accingo ad illustrare, redatta con il fondamentale contributo dei Dipartimenti[1], per definire fin da subito lo spirito e la volontà che animano l'Amministrazione nel raggiungimento degli obiettivi su cui oggi siamo chiamati a rispondere e nel porgere a tutti i presenti il saluto ed il ringraziamento del Ministro dell'Interno per il lavoro che si sta svolgendo e per averci coinvolti in questa Indagine conoscitiva, ritengo utile richiamare, preliminarmente, alcuni passi del messaggio trasmesso dal Ministro dell'Interno Lamorgese lo scorso 25 ottobre ad un convegno organizzato dall'Università di Padova, con riferimento al cambiamento richiesto per la ripresa dalla crisi globale causata dalla pandemia Covid-19, nonchè alle notevoli risorse messe in campo dall'Unione Europea nell'ambito del Next Generation UE e del collegato Piano Nazionale di Ripresa e Resilienza (Pnrr) italiano.

«*Non abbasseremo mai la guardia, e cercheremo di garantire e sostenere il Paese nel cambiamento*».

[1] - Dipartimento per gli Affari Interni e Territoriali
- Dipartimento della Pubblica Sicurezza
- Dipartimento per le Libertà Civili e l'Immigrazione
- Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
- Dipartimento per l'Amministrazione Generale, per le Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie

Nell'occasione, il Ministro ha parlato di una «*sfida che tutti insieme siamo chiamati ad affrontare, attraverso una cultura di fare squadra*», per «*trasformare l'emergenza in un'occasione straordinaria*» di rilancio economico e sociale alla base del quale c'è la pubblica amministrazione.

In questo scenario, l'Amministrazione dell'Interno può giocare un ruolo cruciale, facendo leva sul modello di rete, con le Prefetture e gli altri Uffici territoriali, nella convinzione, ha concluso il Ministro, che «*tutti noi che abbiamo responsabilità pubbliche dobbiamo agire con maggior comunanza d'intenti e strategie per il rilancio del Paese*».

La riflessione del Ministro ha già dato un'idea della complessità delle attività e dei propositi che animano l'Amministrazione negli ambiti su cui oggi sono chiamato a relazionare, ed è proprio al concetto di una "cultura del fare squadra" a cui mi ricollego per una breve sintesi sulle attività che guidano l'Ufficio del Responsabile per la Transizione Digitale (RTD), prima di passare alla trattazione delle attività svolte dai singoli Dipartimenti, rilevanti per l'incontro odierno.

Punto di riferimento e cardine per la definizione, pianificazione e raggiungimento degli obiettivi dell'Ufficio è il Codice dell'Amministrazione Digitale (CAD – D.Lgs. 82/2005 e successive modifiche e integrazioni), certamente il Piano Triennale per l'Informatica nella PA, documento strategico ed economico, che mira allo sviluppo di un'amministrazione digitale e aperta; a servizi facilmente utilizzabili e di qualità; alla riduzione dei tempi e dei costi dell'azione amministrativa, che, tra l'altro, inserisce il RTD nella sezione della governance dell'informatica, con compiti di costruire un sistema di condivisione di obiettivi, di avviare iniziative di formazione e valorizzazione della conoscenza e della competenza, di stimolare il confronto, la condivisione e la promozione di conoscenze e progettualità.

La maggiore attività dell'Ufficio si concentra dunque nell'implementare il processo di collaborazione e confronto tra i Dipartimenti per il conseguimento di traguardi comuni come, ad esempio, la realizzazione dello Sportello Digitale Unico, la costruzione di un solido sistema di condivisione per il raggiungimento delle finalità individuate dalla Strategia

Nazionale Dati, la promozione delle competenze digitali del personale, soprattutto in collaborazione con l'Agenzia per l'Italia Digitale (AgID).

Fondamentale iniziativa è stata la formazione di un Gruppo Permanente di Lavoro, coordinato dal RTD ed al quale partecipano qualificati Referenti di tutte le componenti dell'Amministrazione, ai fini della predisposizione e condivisione di azioni comuni e della valutazione dei servizi offerti all'utenza in conformità alle direttive governative.

Tra queste attività, vi è stato sicuramente il coordinamento dei Dipartimenti per l'adesione alla ***PIATTAFORMA PagoPA*** al fine di consentire il pagamento in modalità digitale e standardizzata di tutti i servizi resi a pagamento.

L'Ufficio è inoltre coinvolto nel Piano d'azione del tavolo di coordinamento nazionale per l'attuazione del Regolamento UE 2018/1724, che istituisce lo **Sportello Digitale Unico**, allo scopo di facilitare l'accesso online alle informazioni, alle procedure amministrative e ai servizi di assistenza di cui cittadini e imprese hanno bisogno di fruire in un altro Stato Membro. In particolare, sono *on line* dallo scorso dicembre (sia in lingua italiana che in lingua inglese), le Informazioni relative a:

- **A1 – Documenti richiesti ai cittadini dell'Unione, ai loro familiari che non sono cittadini dell'Unione, ai minori non accompagnati, ai cittadini di paesi terzi quando viaggiano attraverso le frontiere all'interno dell'Unione** (carta d'identità, visto, passaporto);
- **D1 - Trasferimento temporaneo o permanente in un altro Stato membro**
- **D3 -Partecipazione alle elezioni comunali e alle elezioni del Parlamento europeo** (Diritto di voto e di eleggibilità dei cittadini dell'Unione europea residenti in Italia alle elezioni comunali e Diritto di voto e di eleggibilità dei cittadini dell'Unione europea residenti in Italia alle elezioni dei membri del Parlamento europeo spettanti all'Italia. Elezioni nel Paese di origine)
- **D4 - Prescrizioni in materia di carte di soggiorno**
- **D.5 -Condizioni per la naturalizzazione dei cittadini di un altro Stato membro** (Concessione della cittadinanza italiana per residenza sul territorio italiano e Acquisto della cittadinanza per matrimonio con cittadino italiano)

- **D6 - Norme applicabili in caso di decesso e in materia di rimpatrio della salma in un altro Stato membro**
- **F5 - Numero di emergenza Unico Europeo 112**

Il Regolamento, poi, impone agli Stati membri di garantire che gli utenti possano accedere e completare le procedure di cui all'allegato II, interamente *online*, purché tali procedure siano state istituite nello Stato membro interessato. Le procedure in capo al Ministero dell'Interno riguardano la **Richiesta di una prova della registrazione di nascita** e la **Richiesta di una prova di residenza**. Per entrambe, il progetto di ANPR "allargata" (rilevanti a tal fine sono i ***35 milioni di euro*** *previsti dal PNNR per il consolidamento dell'****Anagrafe Nazionale della Popolazione Residente*** di cui si fornirà più approfondita descrizione nel seguito) consentirà di raggiungere l'obiettivo.

Da ultimo, un progetto particolarmente rilevante che l'Ufficio ha sviluppato e coordinato riguarda la sostituzione della Tessera di riconoscimento cartacea, Mod. AT, precedentemente in uso e ormai obsoleta, con il modello elettronico **ATe,** a tutto il personale dell'Amministrazione, compresi Polizia di Stato, Vigili del Fuoco ed Uffici periferici, acquisito tramite "Accordo di collaborazione" stipulato dal RTD con lo Stato Maggiore della Difesa, uno dei numerosi e riusciti esempi di proficua collaborazione e integrazione tra Amministrazioni centrali pubbliche.

Il progetto nasce da un'approfondita valutazione in merito all'attuazione della trasformazione digitale e nell'ottica di avviare, anche nei processi interni, un cambiamento significativo, rendendo fruibile ai dipendenti uno strumento elettronico di identificazione, sia logica che fisica, rispondente ad elevati requisiti di sicurezza, in grado di gestire informazioni di carattere personale e di rendere possibile l'accesso ai servizi digitali, snellendo notevolmente le procedure burocratiche e implementando il processo di dematerializzazione. In particoalre, il modello ATe consente:

- Identificazione. Il modello ATe consente l'identificazione "a vista" del possessore della carta, senza l'ausilio di strumenti elettronici di verifica. Tale procedura è simile all'identificazione che avviene tramite i tradizionali documenti di tipo cartaceo. Nel caso del

modello ATe, il legame tra i dati personali ed il dato biometrico (immagine del titolare), che permette l'associazione visiva del titolare, è costituito dal supporto plastico realizzato ed inizializzato dall'Istituto Poligrafico Zecca di Stato (IPZS) mediante elementi di sicurezza contro la duplicazione e la contraffazione; il modello ATe è inoltre dotato di una zona leggibile in maniera automatica (MRZ - Machine Readable Zone). Oltre alle predette caratteristiche fisiche, il modello ATe consente l'identificazione dei titolari anche mediante strumenti elettronici, in virtù della capacità di memorizzare informazioni all'interno del proprio microchip. Questa tipologia di riconoscimento è indicata nei casi:

• di verifica di falso documentale, in quanto fornisce una prova inconfutabile che la carta è autentica e i dati non sono stati falsificati, senza richiedere all'esaminatore una particolare esperienza in questo tipo di controllo;

• di uso della carta per procedure automatiche (es. controllo accessi), con possibilità di sfruttamento dei dati biometrici conservati all'interno del supporto (es. impronte digitali);

• in tutti i casi in cui la semplice verifica elettronica dell'identità è sufficiente ad abilitare il personale ad operare.

- Autenticazione. Tale funzione permette l'uso del modello ATe come strumento di accesso ad una rete informatica, ad un portale web e ad una procedura informatica appositamente predisposta.

- Supporto alle funzionalità crittografiche. È previsto che il modello ATe possa essere utilizzato per la cifratura di eventuali comunicazioni/email o documenti a carattere confidenziale. Tale procedura è sviluppata attraverso l'utilizzo delle tecnologie crittografiche a chiave pubblica e richiede la presenza sulla carta della componente privata di una coppia di chiavi asimmetriche RSA.

- Firma Digitale. Il modello ATe consente la generazione di firme digitali con valore legale. Tale possibilità è garantita a tutto il personale.

- Gestione dei dati sanitari di emergenza (Emergency Card). Il modello ATe prevede la registrazione di informazioni di carattere sanitario utilizzabili con applicazioni appositamente realizzate.

- Strong Authentication. Utilizzando l'infrastruttura PKI della Difesa già esistente, è possibile inserire nel modello ATe un certificato X509 aggiuntivo che consente l'impiego di una strong authentication.

- Interoperabilità con CIE e CNS. Il modello ATe, per quanto riguarda le informazioni di identificazione, assicura l'interoperabilità con la Carta di Identità Elettronica (CIE) e con la Carta Nazionale dei Servizi (CNS).

Infine, è opportuno precisare che questa Amministrazione non ha aderito al progetto Polo Strategico Nazionale (PSN) in quanto ha in corso un proprio progetto Cloud privato, peraltro già finanziato, che consiste nella realizzazione di tre **Data Center** qualificati (di cui darò maggiori informazioni nel seguito della relazione), ovvero infrastrutture tecnologiche sicure, efficienti ed affidabili nelle quali migreranno i servizi digitali offerti dall'Amministrazione, pur mantenendo l'autonomia dipartimentale sul controllo e sulla gestione dei dati. Tuttavia, nell'ambito della strategia Cloud Italia - che indirizza l'adozione delle soluzioni Cloud della P.A. – dovranno essere definite le linee operative di interazione/integrazione atteso che numerosi servizi strategici e/o critici presuppongono lo scambio di informazioni e di dati con altre realtà della Pubblica Amministrazione.

A fronte delle numerose ed eterogenee competenze del Ministero dell'Interno, come noto costituito da cinque Dipartimenti, ognuno con specifici compiti istituzionali, per maggiore chiarezza espositiva, le attività ed i servizi digitali saranno declinati separatamente.

DIPARTIMENTO PER GLI AFFARI INTERNI E TERRITORIALI

Svolge funzioni di supporto alle attività di governo locale, di garanzia della regolare costituzione degli organi elettivi, del loro funzionamento e attività di collaborazione con gli Enti Locali, Albo dei segretari comunali e provinciali, Finanza locale, Servizi elettorali e Vigilanza sullo stato civile e sull'anagrafe.

Per quanto concerne il percorso di digitalizzazione avviato, si evidenziano i seguenti servizi, già attivi:

- ***SIEL (Sistema Informativo Elettorale Centrale):*** si tratta di un sistema informativo centralizzato che consente di gestire in diretta i risultati elettorali. Il sistema prevede, nella fase pre-elettorale, di acquisire i dati relativi al corpo elettorale, alle sezioni elettorali interessate, alle liste e ai candidati e, nella fase elettorale, le varie rilevazioni dell'affluenza alle urne ed i risultati delle operazioni di scrutinio. Le comunicazioni dei dati vengono effettuate dalle Prefetture e dai Comuni collegati al sistema centrale in modalità *web application* ovvero, attraverso *web services* che consentono una interazione più agevole tra il sistema informatico comunale e quello centrale. Il SIEL a chiusura degli scrutini effettua la ripartizione dei seggi elettorali ed indica ufficiosamente i candidati eletti. Gli aggiornamenti dei risultati elettorali vengono pubblicati sul sito "Eligendo" e sull'app "Eligendo Mobile". Il SIEL gestisce, inoltre, una procedura denominata "Servizi Elettorali per le Agenzie di Stampa (SEAS)", che consente alle Agenzie di stampa e ad altri utenti accreditati di acquisire in modalità *web services* tutte le informazioni riguardanti sia la fase pre–elettorale che quella elettorale. Al SIEL si collegano per la comunicazione dei dati elettorali, tutte le Prefetture, attraverso la rete privata del Ministero (VPN), nonché i Comuni, attraverso un apposito sistema di sicurezza.
- ***Archivio storico elettorale***: contiene una base unificata di informazioni relative alle consultazioni elettorali e referendarie dal 1946 ad oggi, dagli aggregati complessivi al dettaglio dei singoli Comuni, interrogabile online ed utilizzabile attraverso il servizio open data. Questa procedura, che si alimenta con i dati acquisiti dal SIEL, rappresenta un patrimonio informativo, di valore storico-culturale, unico in Italia.
- ***AMMEL (Amministratori Enti Locali)****:* cura la gestione e il costante aggiornamento dell'archivio anagrafico dei Sindaci e dei Consiglieri eletti e dei

Commissari ed Assessori nominati negli Enti locali e nelle Regioni. Anche questa procedura si alimenta con i dati elaborati dal SIEL che vengono poi aggiornati dalle Prefetture e dai Comuni attraverso una *web application*.

- ***SUT (Sistema Unico Territoriale)***: cura la raccolta e il costante aggiornamento dei dati inerenti il territorio geografico, comprensivo delle sezioni elettorali, e geopolitico nazionale ed internazionale. Il SUT gestisce un sistema completo di codifica degli enti utilizzato anche dalla Banca d'Italia utilizzando i servizi esposti via *web services*.
- ***Banca dati di Finanza locale***: gestisce la determinazione e l'attribuzione delle risorse finanziarie agli enti locali, compreso il riparto dei fondi assegnati per le numerose linee di finanziamento destinate ai progetti comunali.

  Il sistema acquisisce dagli enti locali - attraverso un dedicato canale telematico denominato "TBEL" – le informazioni e le certificazioni necessarie alla determinazione dell'entità delle risorse finanziarie da trasferire. Il sistema ha consentito di dematerializzare tutti gli adempimenti in materia di finanza locale ed anche le verifiche contabili e finanziarie vengono effettuate attraverso l'interazione con i sistemi del MEF (BDAP, Sicoge, Open CUP). Il sistema della finanza locale, gestisce, inoltre, i dati comunicati dai Comuni sui proventi derivanti dalle sanzioni per violazione al codice della strada che vengono resi disponibili al MIT. Infine, il sistema gestisce l'intero procedimento per la formazione dell'elenco dei revisori degli enti locali, dalla domanda di iscrizione on line fino alle operazioni di sorteggio dei revisori che vengono effettuate presso le Prefetture.
- ***Anagrafe Nazionale della Popolazione Residente (ANPR)***: prevista dall'art. 62 del D.Lgs. 7 marzo 2005, n.82 (come sostituito dal comma 1 dell'art. 2, D.L. n. 179/2012, convertito nella legge 17 dicembre 2012, n. 221/2012), che ha istituito presso il Ministero dell'Interno l'ANPR quale base dati di interesse nazionale, che subentra all'Indice Nazionale delle Anagrafi (INA), all'Anagrafe

della Popolazione Italiana Residente all'Estero (AIRE), nonché alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero, tenute dai Comuni.

L'ANPR è stata progettata e gestita da SOGEI S.p.A., ai sensi dell'art. 2, comma 5, della L. n. 221/2012, sotto la governance del Ministero dell'Interno; è regolata da provvedimenti normativi di attuazione che ne disciplinano le varie fasi (DPCM n. 109/2013 e n. 194/2014).

L'art. 10, comma 1, del D.L. n. 78/2015 (L. n. 125/2015) ha previsto che ANPR contenga, altresì, l'archivio informatizzato dei registri di stato civile tenuti dai Comuni (ANSC) e fornisca i dati ai fini della tenuta delle liste di leva, secondo modalità da definire con apposito decreto interministeriale.

L'art. 39 del D.L. n. 77/2021 (L. n. 108/2021), inoltre, ha recentemente previsto l'integrazione nell'ANPR delle liste elettorali e dei dati relativi all'iscrizione nelle liste di sezione di cui al decreto del Presidente della Repubblica 20 marzo 1967, n. 223, rinviando ad un apposito decreto interministeriale le relative modalità attuative.

I Comuni transitati sono poco più di 7800 e, unitamente al Ministero per l'Innovazione Tecnologica e la Dgitalizzazione e a Sogei Spa, si stanno pianificando le iniziative per completare il subentro di tutti i Comuni entro il prossimo 31/12/2021.

La predetta infrastruttura costituirà, una volta completata, la fonte unica di riferimento dei dati anagrafici dei cittadini, un sistema centrale e interoperabile con tutte le altre banche dati di settore.

Allo stato attuale, ANPR è interoperabile, oltre che con i Comuni subentrati, con le seguenti Amministrazioni: il Ministero degli Affari Esteri e della Cooperazione Internazionale, il Ministero dei Trasporti - Motorizzazione Civile, l'INPS, l'ISTAT e l'Agenzia delle Entrate.

Si evidenzia, al riguardo, che tutti i dati anagrafici inviati dai Comuni ai fini del subentro sono sottoposti alla validazione del codice fiscale previo confronto con l'Anagrafe Tributaria, ai sensi dell'art. 1, comma 2, lett. a) del DPCM n. 194/2014.

Per semplificare il procedimento di accesso ad ANPR da parte delle altre PA, è stata realizzata, in collaborazione con il Ministero per l'Innovazione Tecnologica e la Dgitalizzazione e con l'Agenzia per l'Italia Digitale (AGID), sentito il Garante per la protezione dei dati personali, una specifica piattaforma, denominata "**Accordi di Fruizione**", che consente alle pubbliche amministrazioni interessate di sottoscrivere, in modalità telematica, un apposito accordo con il Ministero dell'Interno, per la fruizione dei dati anagrafici necessari allo svolgimento delle proprie finalità istituzionali.

ANPR, inoltre, rende disponibili ai cittadini i servizi di "Rettifica di dati errati o incongruenti" e "di rilascio di certificati anagrafici *on line*", accessibili direttamente dal portale ANPR del Ministero dell'Interno. Dallo scorso 15 novembre, è possibile scaricare *online*, gratuitamente e in maniera autonoma, 14 tipologie di certificati (nascita, matrimonio, cittadinanza, esistenza in vita, residenza, residenza AIRE, stato civile, stato di famiglia, residenza in convivenza, stato di famiglia AIRE, stato di famiglia con rapporti di parentela, stato libero, anagrafico di unione civile, contratto di convivenza), per sé o per un componente della propria famiglia anagrafica, accedendo al portale con l'identità digitale (SPID, CIE o CNS), senza bisogno di recarsi allo sportello.

I certificati possono essere richiesti anche in forma contestuale e prima dell'emissione definitiva (che contiene il QRCODE ed il Sigillo elettronico qualificato del Ministero dell'Interno) occorre visualizzarne l'anteprima al fine di controllare i dati esposti; è possibile, infine, scegliere di scaricarli e/o di riceverli all'indirizzo di posta digitato nel Profilo Utente.

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

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 delle segnalazioni di eventi significativi per la sicurezza degli Operatori di servizi essenziali e dei soggetti componenti del Perimetro Nazionale di Sicurezza Cibernetica e punto di riferimento per le altre Autorità previste dal complessivo sistema di sicurezza nazionale.

L'attuale scenario, caratterizzato dall'esponenziale crescita del *cybercrime* e dalla centralità della sicurezza informatica, ha reso necessaria una riorganizzazione della struttura operativa di questo Dicastero impegnata nell'attività di prevenzione e repressione dei reati informatici, elevando il Servizio della Polizia Postale e delle Comunicazioni a "Direzione Centrale per la polizia scientifica e la sicurezza cibernetica" nella quale confluiranno le attribuzioni sinora svolte dal suddetto Servizio e dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), struttura dipartimentale incaricata in via esclusiva della prevenzione e della repressione dei 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 nel suo genere nel panorama internazionale, opera secondo consolidate procedure di info-sharing, attraverso:

- una Sala Operativa attiva 24 ore su 24 – 7 giorni su 7 deputata al monitoraggio della rete ed alla prima risposta in caso di attacchi cyber verso i sistemi informatizzati istituzionali e afferenti alle infrastrutture critiche.
- una Sezione investigativa composta da personale specializzato nel contrasto ai crimini informatici, a cui lo stesso articolo 7 bis L. 155/2005 assegna, con le prerogative di polizia giudiziaria, il compito di assicurare le indagini penali conseguenti agli attacchi informatici, con la possibilità di effettuare attività sotto copertura ed intercettazioni telematiche preventive.

In tale scenario operativo il costante e continuativo monitoraggio della rete (con riferimento a specifici contesti informativi in materia di sicurezza informatica, hacking ed in ambienti ideologicamente caratterizzati) così come la raccolta di dati e informazioni attinenti ai temi della sicurezza informatica e della minaccia criminale/terroristica, in qualsiasi modo e da qualsiasi fonte acquisibili (ad esempio reportistica di settore, segnalazioni delle I.C.I. – Infrastrutture Critiche Informatizzate – o di organismi investigativi e di intelligence) conferiscono al C.N.A.I.P.I.C. la possibilità di diffondere e condividere in tempo reale

preziose e strategiche informazioni, utili alla prevenzione di attacchi informatici diretti verso le infrastrutture critiche sia di matrice criminale comune che terroristica.

Valore aggiunto del CNAIPIC è l'operare secondo un modello partenariale-convenzionale con i soggetti erogatori dei servizi pubblici essenziali del Paese, che da meri enti passivi beneficiari di un servizio di tutela, diventano parti attive di un sistema di sicurezza, responsabilizzati da precisi obblighi di segnalazione di incidenti informatici rilevanti. La conclusione di apposite convenzioni dà vita ad un rapporto (non più di tipo verticale/unidirezionale, bensì) di tipo orizzontale/bidirezionale, che consente uno scambio quotidiano di informazioni tecniche e di Indicatori di compromissione (IoC), finalizzato da un lato alla garanzia, in chiave preventiva, della pubblica sicurezza cibernetica, e dall'altro, alla repressione dei crimini informatici di matrice comune, organizzata e terroristica.

La tempestiva condivisione dei c.d. "Indicatori di compromissione" dei sistemi informatici con i fornitori di servizi pubblici essenziali ha consentito di rafforzare gli strumenti volti alla protezione della sicurezza informatica, garantita anche dalla costante attività di monitoraggio in contesti di interesse.

Uno specifico protocollo di allerta (il "Protocollo Covid-Rosso") è stato attivato dal CNAIPIC per la ricognizione e l'allerta precoce delle minacce e degli attacchi più direttamente ricollegabili alle infrastrutture di carattere sanitario (ospedali, amministrazioni sanitarie, sistema farmaceutico, ecc.); con tale Protocollo il CNAIPIC, attraverso i corrispondenti nuclei operanti a livello locale nei Compartimenti polizia postale del territorio, ha previsto l'istaurazione di una ramificata rete di allerta con i referenti delle istituzioni sanitarie del Paese, rete che è immediatamente allertata in caso di attacco.

Di evidente incremento è l'attività di contrasto alla minaccia cyber svolta dal CNAIPIC, attestata dal rilevante aumento del numero di alert diramati alle infrastrutture critiche nazionali. Nel 2020 il CNAIPIC ha diramato 83.416 alert di sicurezza, mentre nel 2021 gli alert risultano ad oggi oltre 66.000, di questi oltre 24.000 sono gli alert riferibili a campagne di ramsomware per il 2020, per il 2021 ne risultano diramati già 14.000.

L'anno in corso conferma l'assoluto trend di crescita degli attacchi rilevati dal Centro, aumentati tra il 2019 ed il 2020 del 246%, con una gestione nel 2021 di complessivi 3.027 attacchi cyber significativi, di cui:

- ✓ 95 attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- ✓ 245 attacchi informatici diretti verso operatori di servizi essenziali (O.S.E.), pubbliche amministrazioni locali ed infrastrutture sensibili a livello locale;
- ✓ 2642 attacchi informatici diretti verso privati ed aziende;
- ✓ 45 richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

Tra le attività investigative condotte in tale ambito, si segnalano 50 indagini avviate nel 1° semestre 2021, che hanno condotto al deferimento all'AG di 98 persone, ossia un aumento delle persone deferite all'Autorità Giudiziaria pari al 78%.

I soli attacchi rilevati del tipo ramsomware diretti verso sistemi informatici nazionali hanno segnato nell'anno in corso un aumento notevole in riferimento al medesimo periodo (gen/ott 2020 165 attacchi, gen/ott 2021 230 attacchi).

Nell'attività finora descritta, il CNAIPIC non agisce come attore solitario, me è uno snodo essenziale e strategico per lo scambio informativo tra tutti i soggetti della *cybercommunity* partecipando ad un complesso sistema nazionale di sicurezza cibernetica, che poggia su un'architettura composita a carattere multilivello, derivante dalla stratiforme disciplina che le leggi ed i regolamenti, non soltanto nazionali, hanno soprattutto negli ultimi anni puntualmente delineato. Da ultimo, il mosaico dell'architettura nazionale preposta alla sicurezza cibernetica si è completato con l'istituzione dell'Agenzia per la Cyber sicurezza Nazionale (ACN) ad opera del Decreto-legge 14 giugno 2021, n. 82, che detta una disciplina organica nello specifico settore della cyber-resilience.

La nuova Direzione Centrale per la polizia scientifica e la sicurezza cibernetica, inoltre, ospiterà il *Computer Emergency Response Team* (CERT) e il Centro di Valutazione (Ce.Va.) del Ministero dell'Interno.

Il CERT sarà l'ufficio deputato a garantire la sicurezza delle reti e dei sistemi informativi del Ministero dell'Interno, attraverso la prevenzione e la gestione degli eventi critici diretti a comprometterne l'integrità.

A tal fine, il CERT assicurerà:

a) l'attività di prevenzione mediante raccolta di informazioni relative alle minacce cibernetiche attuali o potenziali, idonee a compromettere l'integrità e la sicurezza dei sistemi e delle reti ministeriali (cyber threat intelligence), nonché l'attività di monitoraggio, raccolta ed analisi precoce (early warning) delle vulnerabilità note;

b) l'attività di condivisione e scambio, ai sensi della normativa vigente, delle informazioni per la prevenzione e la gestione di attacchi cibernetici, con gli Enti e le Istituzioni rilevanti;

c) l'attività di identificazione e valutazione delle vulnerabilità dei sistemi e delle reti ministeriali (vulnerability assessment), anche attraverso la simulazione di attacchi (penetration test);

d) l'attività di gestione e di reazione agli eventi significativi di sicurezza informatica (incident handling/response), assicurando la preservazione dell'integrità e continuità dei servizi e coordinando le strutture preposte nell'ordinario alla gestione delle funzioni di sicurezza informatica presenti all'interno di ciascun Dipartimento;

e) l'elaborazione di proposte per l'adozione e l'aggiornamento di policy e direttive tecniche, a livello ministeriale, concernenti la complessiva gestione della sicurezza informatica.

f) La promozione di campagne ed iniziative di informazione e sensibilizzazione rivolte al personale del Ministero dell'Interno, allo scopo di implementare la cultura della sicurezza informatica (c.d. awareness).

Il Ce.Va. del Ministero dell'Interno assicurerà lo svolgimento delle attività di valutazione, controllo e certificazione – oltre ai relativi poteri ispettivi – inerenti alle forniture

di beni, sistemi e servizi ICT da impiegare sulle reti, i sistemi informativi ed i servizi informatici del Dicastero.

Inoltre, lo scorso mese di aprile è stato inaugurato, presso il Polo Anagnina, il *Cyber-Security operation center* (C-Soc), incardinato presso la Direzione Centrale della Polizia Criminale la cui mission è l'analisi e il monitoraggio delle policy di sicurezza per la prevenzione degli incidenti di cybersecurity attraverso l'analisi continua delle minacce, la scansione della rete e dei sistemi alla ricerca di vulnerabilità e l'implementazione delle adeguate contromisure.

La funzione del C-Soc sarà quella di vigilare che milioni di informazioni possedute dalle banche date delle forze di Polizia riguardanti cittadini, documenti, veicoli, indagini siano adeguatamente protetti.

Per tale sua natura il C-Soc rappresenta una struttura di primo piano nell'architettura di protezione cibernetica nazionale.

In questo contesto, l'operato della Polizia Postale si svolge soprattutto lungo la direttrice di natura informativa-preventiva che risiede elettivamente nell'assicurare interventi di tipo preventivo e di protezione, incentrati sulla capacità di analisi e di allerta precoce finalizzata alla diffusione, in tempo reale, di alert di sicurezza riferibili alle minacce in corso, a beneficio dell'intero panorama delle infrastrutture informatiche nazionali, a partire da quelle critiche convenzionate con il CNAIPIC (art. 7 bis DL 144 del 2005, convertito con modificazioni dalla L.155 del 2005).

Gli investimenti in misure tecniche ed organizzative per il rafforzamento delle difese cyber sono una priorità per l'Amministrazione perseguita anche grazie ai fondi del Next Generation EU (NGEU) (27+30 milioni di euro a valere sulla Missione "digitalizzazione" del PNRR per il potenziamento della propria capacità di risposta a eventuali attacchi informatici e a protezione dei propri sistemi) che puntano a garantire alti livelli di cybersicurezza quale componente essenziale del processo di transizione digitale.

Nell'ambito del potenziamento delle strutture digitali, sarà data priorità all'erogazione di servizi digitali al cittadino attraverso la realizzazione di una struttura cloud che consentirà di snellire le procedure, secondo il principio *once only* (per cui i cittadini e le imprese devono poter fornire "una sola volta" le loro informazioni ad Autorità e amministrazioni). Inoltre, grazie alla creazione del cloud sarà resa effettiva l'interoperabilità delle banche dati delle forze di polizia**,** al fine di permettere agli operatori di accedere, tramite un'unica interfaccia ed un unico meccanismo di autenticazione, ai dati di interesse.

La Polizia di Stato è primariamente impegnata sul fronte della sicurezza al cittadino, ma nel corso degli anni ha sempre più preso atto dell'esigenza del cittadino digitale, ampliando la platea dei servizi che sono disponibili attraverso le nuove tecnologie dell'informazione; a tal fine, attraverso il suo portale e altre piattaforme riconosciute, fornisce servizi al cittadino che semplificano e migliorano il suo rapporto con le Istituzioni.

Le categorie di servizi che la Polizia di Stato fornisce sono di tipo:

- **Informativo**
  - Portale web istituzionale
  - Feed RSS (categorizzati)
  - Canali social Facebook, Instagram, Twitter, YouTube, Telegram
- **Di supporto alle richieste del cittadino**
  - "Dove siamo"
  - Richiesta di documenti e/o stato delle pratiche (passaporto, permesso di soggiorno)
- **Di ricerca**
  - Informazioni relative ai veicoli rubati
  - Documenti smarriti
  - Banconote
  - Oggetti rubati e oggetti recuperati

A questi servizi, generalmente fruibili dal web o dalle app dei gestori delle piattaforme social si aggiunge lo sviluppo della piattaforma per gli smartphone YouPol.

Servizi di tipo Informativo

La comunicazione istituzionale dell'attività della Polizia di Stato ha come principale veicolo il portale web dal quale il cittadino, oltre a poter trovare tutte le informazioni necessarie sulle attività ordinarie e amministrative, può essere informato costantemente (attraverso i feed RSS) su azioni e attività in corso.

Tali contenuti informativi sono anche diffusi attraverso i profili social istituzionali: **Polizia di Stato e Agente Lisa**. L'uso di profili social è finalizzato alla comunicazione di informazioni utili per la prevenzione di reati, attività, novità ed eventi che riguardano l'organizzazione. Rappresentano uno spazio per raggiungere gli internauti che vogliono essere costantemente informati. Sfruttando le opportunità tipiche di questi servizi, la Polizia di Stato può condividere e rilanciare occasionalmente contenuti e messaggi di pubblico interesse e utilità realizzate da soggetti terzi (altri enti, soggetti o cittadini della comunità), verificandone la precisione e l'attendibilità. Inoltre gli uffici territoriali, in particolare le Questure, informano i cittadini sull'attività dei Commissariati, delle Divisioni e di tutte le specialità presenti nei territori, sulle ricorrenze istituzionali e sulle iniziative. I contenuti pubblicati riguardano comunicati stampa, ricorrenze, eventi, comunicazioni istituzionali e aggiornamenti in situazioni di emergenza.

Servizi per il cittadino

- ***"Dove siamo":*** il cittadino può individuare l'ufficio a lui più vicino ed in grado di soddisfare le sue ordinarie esigenze.
- ***Agenda Online:*** per consentire una rapida ed efficace emissione del **Passaporto** ed evitare al cittadino inutili attese e permanenze negli uffici delle Questure, è disponibile il servizio che consente di prenotare secondo gli orari più comodi al cittadino, l'appuntamento per la gestione del rilascio del Passaporto. E' accessibile tramite SPID o CIE. In collaborazione con le Poste Italiane si può richiedere per lo specifico del passaporto anche la consegna diretta al domicilio del cittadino.
- ***Il Tuo Permesso di Soggiorno:*** servizio multilingue attraverso cui il cittadino straniero, a seguito dell'inserimento del numero di pratica o dell'assicurata utilizzata

per la richiesta del permesso, può conoscere lo stato di avanzamento del rilascio. Oltre all'avviso visualizzabile tramite questo sistema informatico, viene inviato al cittadino straniero un SMS con l'indicazione delle modalità per il ritiro del permesso di soggiorno già pronto: giorno, ora e luogo.

Servizi di Ricerca

La Polizia di Stato, per lo specifico delle sue attività, detiene una serie di banche dati che contengono dati utili al cittadino sia per consentirgli di ricercare informazioni ma anche per consentirgli di aiutare la Polizia di Stato ad essere vicina alle sue esigenze.

Questi servizi permettono, tramite apposite pagine web, di poter ricercare **informazioni su autoveicoli rubati** o che si potrebbe ritenere di esserlo, inserendo la targa del veicolo; ricercare **informazioni su banconote false,** attraverso la verifica del numero di serie e **sulla validità di documenti di riconoscimento** (carte di identità, carte di identità elettroniche, passaporti, patenti di guida etc)

È inoltre presente un servizio che consente al cittadino di poter verificare dal portale gli oggetti che sono stati smarriti e/o oggetto di furto e quindi poterne rientrare in possesso.

Commissariato On-line

Uno sportello telematico che l'utente della rete può facilmente raggiungere compilando un form per formulare quesiti, chiedere consigli prima di eseguire qualsiasi tipo di operazione sul web evitando in tal modo di cadere vittima di illeciti.

Particolare rilevanza ha la sezione dedicata alle news, nella quale vengono evidenziati i fenomeni presenti sul web, i consigli utili per una navigazione sicura, dando spazio, altresì, a tutte le operazioni svolte dalla Polizia Postale in ambito nazionale ed internazionale.

Solo per dare qualche dato, anche nel corso del primo semestre dell'anno 2021, si è portata avanti un'attività di contrasto al fenomeno della disinformazione, agevolato dalla diffusione delle cosiddette *fake news* e sovente caratterizzato da un potenziale impatto negativo sulla salute pubblica e sulla corretta ed efficace comunicazione istituzionale, attraverso la predisposizione e diffusione di specifici alert, funzionali alla veicolazione delle corrette informazioni. Il progressivo innalzamento del livello di interazione con i cittadini è

confortato dai dati statistici. Nel primo semestre 2021 il Commissariato di P.S. Online ha ricevuto 54.634 segnalazioni, quasi il doppio (+ 92%) di quelle acquisite nell'analogo periodo dell'anno precedente (28.457).

La popolarità del sito è confermata anche dal numero degli accessi che sono stati nel periodo di riferimento oltre 32.500.000.

"Denuncia per Reati Telematici" *e* ***"Denuncia per furto o smarrimento":*** ogni denuncia compilata *on line* viene recapitata, in automatico e telematicamente, all'Ufficio della Polizia Postale e delle Comunicazioni prescelto dal cittadino, richiedendo a quest'ultimo di recarsi in seguito, e con comodo, presso l'ufficio scelto, per la sola formalizzazione.

YouPol

E' l'APP della Polizia di Stato. Permette all' utente di interagire con la Polizia di Stato inviando segnalazioni (video, audio, immagini e testo) relative a episodi di bullismo, spaccio di sostanze stupefacenti e violenza domestica. I contenuti sono trasmessi all'ufficio di Polizia in modalità geo-localizzata e consentono di conoscere in tempo reale il luogo e i dettagli degli eventi. E' possibile anche l'invio e la trasmissione in un momento successivo, con l'inserimento dell'indirizzo del luogo in cui si è verificato l'evento. L'applicazione, principalmente destinata ai ragazzi e al mondo della scuola, è stata realizzata per prevenire le fenomenologie del bullismo, per il contrasto allo spaccio di sostanze stupefacenti e per segnalare episodi di violenza domestica. L'app oltre a consentire un'esperienza d'uso immediata permette anche di comunicare in chat con la sala operativa della Polizia di Stato e ricevere direttamente messaggi e notifiche.

DIPARTIMENTO PER LE LIBERTÀ CIVILI E L'IMMIGRAZIONE

Il Dipartimento opera nell'ambito delle funzioni e compiti spettanti al Ministero dell'Interno, per la tutela dei diritti civili in materia di immigrazione, asilo, cittadinanza, confessioni religiose e non è specificamente coinvolto nella interoperabilità con le banche dati fiscali.

Per quanto attiene alle infrastrutture tecnologiche e ai servizi digitali, nel corso degli anni ha utilizzato diverse tecnologie per la realizzazione e l'esercizio di applicazioni e moduli software ad uso di utenti interni ed esterni. In tale ottica è in fase di completamento una piattaforma hardware/software (HW/SW) in grado di ospitare centralmente i servizi applicativi attuali e futuri.

La quasi totalità dei processi amministrativi di competenza è stata, poi, totalmente digitalizzata, mediante i seguenti applicativi:

- sistema di trattazione delle domande di riconoscimento della cittadinanza italiana **(CIVES)**
- sistema di gestione dei procedimenti di competenza degli Sportelli Unici per l'Immigrazione presso le Prefetture, ossia quelli inerenti alle domande di rilascio del nulla osta al lavoro subordinato, determinato o indeterminato, stagionale, per ricongiungimento familiare per i cittadini stranieri non comunitari residenti all'esterno **(SPI)**
- sistma di gestione dell'accoglienza in uso alle Prefetture, inteso a tracciare il percorso del migrante richiedente protezione internazionale dall'arrivo sul territorio nazionale, durante il periodo di accoglienza e fino all'uscita dai relativi centri **(SGA)**
- sistema di gestione delle attività di monitoraggio dei centri di accoglienza da parte delle Prefetture **(GCCA) –** in fase di collaudo
- sistema relativo all'esame delle domande di protezione internazionale in uso alle Commissioni Territoriali per la protezione internazionale ed alla Commissione Nazionale per il diritto di asilo **(VESTANET)**
- sistema integrato con il precedente, relativo alla verbalizzazione delle audizioni dei richiedenti protezione internazionale mediante un sistema di riconoscimento automatico del parlato **(SINDACA) –** in fase di avvio
- sistema relativo alla valutazione del Paese Europeo competente per la trattazione della richiesta di asilo **(DUBLINET)**

- sistema di gestione della procedura di ritorno volontario dei migranti nei propri Paesi di origine **(RVA)**
- sistemi deputati alla gestione dei Fondi europei e nazionali (**FAMI, FNASILO, LGNET, RELINT, UNRRA**).

Per i sistemi informatici per i quali è interessata un'utenza esterna (ad esempio SPI, CIVES) è altresì prevista la possibilità di monitorare l'andamento della pratica in modalità online.

Si sta implementando, inoltre, l'utilizzo dello SPID come modalità di accesso sicura per gli utenti esterni. Tale modalità è stata già resa operativa per il sistema di trattazione delle istanze di riconoscimento della cittadinanza italiana (CIVES) e per la nuova versione dell'applicativo di rilascio del nulla osta al lavoro (SPI.2) che entrerà in esercizio nei primi mesi del prossimo anno.

DIPARTIMENTO DEI VIGILI DEL FUOCO, DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE

I servizi online forniti dal Dipartimento, con gli strumenti e le piattaforme stabilite dal decreto legge semplificazione e innovazione digitale, sono numerosi e precisamente:

- ***Applicazione web Gestione concorsi pubblici***, raggiungibile all'indirizzo https://concorsionline.vigilfuoco.it per la compilazione e la presentazione online dell'istanza di partecipazione alle procedure concorsuali bandite dal Corpo Nazionale dei Vigili del Fuoco, presenta lo SPID come strumento unico di identificazione informatica.
- ***Portale della trasparenza delle procedure di acquisto del Dipartimento*** (https://www.vigilfuoco.it/Trasparenza/)
  Fornisce informazioni sulle singole procedure in formato tabellare, ai sensi dell'art.1, comma 32, L. 6 novembre 2012, n. 190, secondo le indicazioni fornite dall'Autorità Nazionale Anticorruzione con delibera n. 39 del 20 gennaio 2016, nonché ai sensi dell'art. 37, comma 1, lett. a) del D.Lgs 14 marzo 2013, n.33.

- ***Portale dei fornitori online*** (https://fornitorionline.vigilfuoco.it/FOL/)

  Il Dipartimento mette a disposizione dei propri committenti alcuni servizi online, accessibili solo tramite SPID, per la consultazione degli ordini e dei pagamenti emessi a loro favore dalle sedi del Dipartimento stesso e dei relativi documenti contabili riferiti all'ultimo biennio finanziario. Ulteriore servizio disponibile è la compilazione di una fattura elettronica in formato XML. Se si è già iscritti all'Albo Operatori Economici i servizi saranno attivati automaticamente in caso di contratti in essere.

App

- **App IO** - in corso di analisi la fruizione tramite l'**AppIO** per la consultazione dello stato dei procedimenti di Prevenzione Incendi avviati dal singolo cittadino/libero professionista e delle relative scadenze.
- **App VVF Cert** – Prodotti omologati e certificati dai VVF (Android), nata dall'esigenza della Direzione Centrale per la Prevenzione e la Sicurezza Tecnica del Dipartimento dei Vigili del Fuoco, di dare sempre risposte certe e sicure al cittadino e, in particolare, sulla verifica e sulla certificazione di prodotti testati dai Vigili del Fuoco o certificati dal Centro Studi ed Esperienze dei Vigili del Fuoco
- **App dei contatti delle sedi dei Vigili del Fuoco** (Android), fornisce indirizzo, recapiti telefonici, numeri di fax, indirizzi email e PEC delle sedi dei Vigili del Fuoco dislocate sul territorio nazionale. E' possibile filtrare le sedi per regione, provincia, tipologia (per esempio: Comandi Provinciali o Distaccamenti) ed è disponibile una ricerca con testo libero.
- **App VVF Prevenzione Incendi Mobile** (Android), fornisce servizi informativi di carattere generale riguardanti la prevenzione incendi, con particolare riferimento alle novità introdotte con il regolamento di semplificazione, DPR 151/2011. Consultazione delle nuove attività soggette a controlli dei Vigili del Fuoco

- **App INFOpratica** (Android), per gli utenti che hanno presentato domanda di prevenzione incendi e sono, quindi, in possesso di numero di pratica e codice PIN di sicurezza, l'applicazione rende possibile la consultazione dello stato di avanzamento del procedimento
- **App VVF Norme** (Android), consente la ricerca, il download e la consultazione dei principali testi normativi riguardanti la prevenzione incendi e la sicurezza sul lavoro. Tramite la ricerca Norme On line è possibile ricercare e scaricare le norme aggiornate dal database curato dalla Direzione Centrale per la Prevenzione e Sicurezza Tecnica
- **App NIA VVF – Investigazioni** (Android), fornisce un pratico riferimento, rispetto alle attività investigative da svolgere in caso d'incendio ed esplosione, così come descritte dall'NFPA 921 "Guide for File ed Explosion Investigations". L'uso dello smartphone, consente già dalle prime fasi d'intervento, la raccolta e la registrazione di dati per le successive fasi investigative
- **App VVF NotiFire** (IOS e Android), rilasciata dal Corpo Nazionale dei Vigili del Fuoco che segnala la presenza di interventi di soccorso nelle vicinanze. Lo scopo dell'app è di fornire l'intervento dei Vigili del Fuoco ai cittadini che si trovino in prossimità dell'area emergenziale. E' un servizio volto sia alla sicurezza dei cittadini sia a ridurre la congestione delle linee d'emergenza quando le squadre di soccorso sono già state allertate
- **App Kemler-ONU** (IOS e Android) – attualmente in corso di aggiornamento – tramite la quale è possibile reperire il significato dei codici riportati sulle targhe con sfondo arancione poste sui mezzi che trasportano le merci pericolose (il codice Kemler e il numero ONU). Non è noto a tutti, infatti, che il codice posto nella parte superiore della targa (codice Kemler) indica il tipo di pericolo relativo alla sostanza trasportata.

Il Dipartimento non detiene dati critici o strategici in relazione alla definizione del progetto di Cloud nazionale, in quanto tutti i dati inerenti l'anagrafe tributaria di persone fisiche e/o giuridiche sono sistematicamente trasmessi alle piattaforme gestite dal MEF.

DIPARTIMENTO PER L'AMMINISTRAZIONE GENERALE, PER LE POLITICHE DEL PERSONALE DELL'AMMINISTRAZIONE CIVILE E PER LE RISORSE STRUMENTALI E FINANZIARIE

Il Dipartimento – DPP - rappresenta il punto di riferimento in materai di programmazione, realizzazione, gestione e manutenzione delle risorse ICT per gli Uffici centrali dell'amministrazione civile dell'Interno e per le Prefetture-UTG.

Le attività estremamente variegate svolte in più campi specifici, attraverso l'impiego di applicativi informatici di gestione procedimentale automatizzata nonché le molteplici banche dati e i collegamenti telematici gestiti in via diretta, confermano la consolidata esperienza dei servizi informatici di questo dipartimento quale polo di riferimento per i progetti d'innovazione tecnologica delle prefetture e degli uffici centrali, per l'erogazione di servizi digitali verso cittadini ed imprese nell'ambito delle missioni di competenza e dei propri processi interni, soprattutto in materia di gestione delle risorse umane della carriera prefettizia, dei dirigenti del comparto delle funzioni centrali e del personale non dirigente dell'amministrazione civile dell'Interno.

Infatti, attraverso il Data Center sotto la diretta gestione[2] mette a disposizione la propria infrastruttura di comunicazione telematica anche per le consultazioni elettorali, per gli sportelli unici per l'immigrazione, per l'accesso alla rete SPC consentendo le cooperazioni applicative con la rete nazionale interbancaria e la centrale d'allarme interbancaria[3], la rete delle Camere di commercio, la rete dell'Agenzia delle entrate, il Casellario giudiziale del Ministero della Giustizia[4], la Motorizzazione Civile[5] e, in qualche caso, anche per la connettività verso la pubblica amministrazione locale[6].

[2] È in corso un progetto per la realizzazione di un nuovo data center di categoria A che farà parte del cloud privato del Ministero dell'interno nel contesto dei progetti d'innovazione tecnologica della Misura 1.6.1 "Digitalizzazione delle grandi amministrazioni centrali" del Next Generation EU.

[3] Nell'ambito delle sanzioni amministrative anche pecuniarie irrogate dai prefetti in tema di emissione di assegni senza titolo o provvista.

[4] Nell'ambio dei procedimenti di rilascio della documentazione antimafia da parte dei prefetti.

[5] Nell'ambito dei procedimenti di sospensione e revoca delle patenti di guida nonché della verifica dei requisiti dei candidati alla prova pratica di rilascio dei titoli abilitativi alla guida da parte dei prefetti.

[6] Nell'ambito dei procedimenti sanzionatori amministrativi relativi ai ricorsi al prefetto in materia di violazioni al codice della strada, alle disposizioni di contrasto alla diffusione dell'epidemia da SARS- Cov 2.

In particolare, il DPP, che ha portato a conclusione già nel 2008 un processo di consolidamento dei propri sistemi informatici e di telecomunicazione presso la propria server farm di Roma, ha da tempo completato la centralizzazione di tutti i servizi informatici erogati ai propri uffici centrali e alle prefetture, sia nell'ambito della gestione del personale dell'amministrazione civile, sia per quanto concerne i servizi di automazione dei più importanti procedimenti di competenza prefettizia in materia sanzionatoria amministrativa, di certificazione antimafia, di gestione delle risorse finanziarie, di valutazione della performance organizzativa, per l'accesso digitale ai benefici di legge per le vittime dell'estorsione e dell'usura, per il supporto informatico esterno alle attività di monitoraggio da parte dell'ufficio del Commissario straordinario del governo per le persone scomparse e alle attività di competenza del Programma nazionale per i servizi di cura all'infanzia e agli anziani non autosufficienti.

Gli interventi di profonda ristrutturazione tecnologica hanno consentito di razionalizzare l'architettura informatica precedente, fondata su sistemi server presso ciascuna prefettura, nell'unica server farm centralizzata con considerevoli risparmi di spesa per la manutenzione e per l'assistenza alla conduzione operativa dell'hardware e del software operativo.

La gestione diretta della rete di trasmissione dati (VPN/IP) delle prefetture ha consentito un aumento dell'efficacia operativa e un recupero di maggiore efficienza correlata al progressivo incremento dell'utilizzo della stessa per servizi sempre più crescenti, sia in termini di utilizzo di banda trasmissiva, che per maggior numero di utenti. Di questi ultimi, poi, si è registrato, soprattutto negli ultimi anni, un aumento considerevole, che comprende sostanzialmente l'intero personale dell'Amministrazione civile (circa 19.000 utenti) per i servizi legati all'accesso ad Internet e per quelli raggiungibili dalla Intranet dipartimentale; soprattutto, il bacino di utenza si è esteso agli enti esterni, sia della pubblica amministrazione centrale che locale, attraverso i servizi di automazione informatica basati sull'interconnessione e l'interoperabilità con banche dati interne ed esterne (tra le quali,

Banca dati Interforze SDI, Polizia Stradale, Arma dei Carabinieri, Motorizzazione civile, Agenzia delle entrate, Banca d'Italia, Casellario Giudiziale, InfoCamere, Polizie locali, ecc.).

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 ad informazioni senza la necessità di doversi recare agli sportelli delle prefetture (ad esempio, la Banca dati nazionale unica per la documentazione antimafia e i sistemi informativi **SANA** - in tema di ricorsi al prefetto per violazioni al codice della strada ed altre tipologie quali le disposizioni anticontagio da SARS-Cov 2 – e **SISA** – in tema di irrogazione di sanzioni da parte dei prefetti per l'emissione di assegni senza titolo o provvista.).

Gli interventi attuati per la razionalizzazione e l'ottimizzazione dei sistemi informatici hanno permesso di far fronte alla maggiore richiesta di servizi e all'aumento del numero di utenti con evidente evoluzione della struttura in termini di efficienza ed efficacia.

Il Dipartimento è impegnato nelle seguenti direttrici:

Progettazione e realizzazione di un nuovo Data Center

Il Dipartimento per l'Amministrazione Generale, per le Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie sta curando un ulteriore progetto che rientra nell'obiettivo complessivo del PNRR di costruire uno o più Poli Strategici Nazionali (PSN) verso cui «migrare» i data center di Cat. B delle amministrazioni pubbliche centrali, allo scopo di superare l'attuale frammentarietà degli asset infrastrutturali IT, mettere in sicurezza i CED ed i dati di interesse strategico e consentire a tutte le PA di evolvere verso l'erogazione di servizi digitali in sicurezza ed ad alta affidabilità.

Il progetto di realizzazione di un Data Center è la risposta all'esigenza di razionalizzazione dei sistemi informatici di questa Amministrazione, al fine di ridurne il numero e uniformarne le caratteristiche, in termini di efficienza e standardizzazione, eliminando nel contempo i costi causati da una eccessiva frammentazione.

Il Data Center unificato 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. Inoltre potrà essere aperta ad "ospitare" altre pubbliche amministrazioni, conseguendo così importanti economie di scala nel consolidamento delle infrastrutture digitali pubbliche, in coerenza con le indicazioni della "Crescita 2.0", coordinata dall'Agenzia per l'Italia Digitale.

L'iniziativa contribuisce a fornire anche un consistente e fondamentale apporto di questa Amministrazione alla definizione di una strategia di sicurezza cibernetica attraverso il miglioramento della visibilità delle minacce informatiche e l'incremento delle risposte preventive e proattive agli attacchi. Il progetto è finalizzato - ed in questo senso giustifica il considerevole investimento economico di poco meno di trenta milioni di euro - a rappresentare un polo tecnologico di rilevanza trasversale del Ministero dell'Interno e aperto anche alla collaborazione, auspicabilmente, di altre amministrazioni pubbliche.

La realizzazione del Data Center si inserisce, quindi, nel quadro degli investimenti per la Crescita Digitale del Paese, soprattutto in prospettiva di "cyber defence", riducendo il perimetro di esposizione a possibili attacchi informatici ad asset pubblici nevralgici e contribuendo all'efficace e completa realizzazione del progetto complessivo di digitalizzazione del Ministero dell'Interno nell'ambito degli interventi del Piano nazionale di ripresa e resilienza.

Automazione dei procedimenti sanzionatori pecuniari SANA

A partire dal 2007 è stato sviluppato, e progressivamente si è evoluto, un sistema informativo per l'automazione dei provvedimenti sanzionatori amministrativi di competenza delle Prefetture. In sintesi, la procedura informatica SANA provvede, in maniera centralizzata, alla digitalizzazione di tutti i documenti necessari alla trattazione delle pratiche, all'utilizzo di modalità telematiche per la trasmissione dei ricorsi al Prefetto avverso le violazioni amministrative e le controdeduzioni degli organi accertatori statali e locali, a funzioni massive di elaborazione di provvedimenti e di atti endoprocedimentali, comprese le

relative notifiche agli interessati e la formazione automatizzata nonché la trasmissione telematica delle iscrizioni a ruolo delle sanzioni pecuniarie.

A tale riguardo, i proventi in questione si riferiscono sia alla diretta attività sanzionatoria delle Prefetture, effettuata mediante ordinanze, ingiunzioni ed altri provvedimenti non pagati volontariamente, sia alle iscrizioni a ruolo che le Prefetture effettuano per accertamenti sanzionatori non pagati e non impugnati di organi dello Stato.

Il seguente prospetto indica i dati relativi alle sanzioni pecuniarie iscritte a ruolo dal 2013 al 31 dicembre 2021:

Anno	Somme iscritte a ruolo dalle Prefetture				
	con GR	con il portale di Equitalia o di Agenzia delle entrate-Riscossione	complessivamente	di cui effettivamente riscosso (fonte: Agenzia delle entrate-Riscossione)	numero di procedimenti trattati
2013	€ 200.257.529,15	€ 887.667.866,22	€ 1.087.925.395,37	€ 123.099.303,29	382.472
2014	€ 503.565.886,86	€ 562.146.510,91	€ 1.065.712.397,77	€ 126.275.395,21	940.401
2015	€ 502.259.195,48	€ 326.864.711,12	€ 829.123.906,60	€ 117.206.725,74	1.238.862
2016	€ 658.556.529,63	€ 260.431.927,55	€ 918.988.457,18	€ 114.780.028,96	1.595.553
2017	€ 1.168.275.701,11	€ 0,00	€ 1.168.275.701,11	€ 142.310.723,31	1.767.180
2018	€ 2.998.107.200,76	€ 0,00	€ 2.998.107.200,76	€ 120.967.484,00	2.983.261
2019	€ 1.851.548.318,00	€ 0,00	€ 1.851.548.318,00	€ 130.812.153,26	3.488.886
2020	€ 1.147.995.201,50	€ 0,00	€ 1.147.995.201,50	€ 73.312.212,89	1.847.250

Banca Dati Nazionale Unica per la Documentazione Antimafia

La Banca Dati Nazionale Unica per la documentazione Antimafia (BDNA), istituita presso il Dipartimento per l'Amministrazione Generale, per le Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie con il D.P.C.M. 30

ottobre 2014, n.193, è divenuta pienamente operativa a far data dal 7 gennaio 2016 ed è finalizzata ad accelerare le procedure di rilascio, da parte dei prefetti, della certificazione antimafia di cui all'art. 96 del D.Lgs. 6 settembre 2011, n.159.

La BDNA costituisce lo strumento esclusivo per il rilascio della documentazione antimafia (comunicazione e informazione) ed è sottoposta ad un continuo aggiornamento giuridico-operativo in relazione a sopravvenute norme ed a quesiti di operatori.

Anche nel corso del 2020, contraddistinto e profondamente influenzato dall'emergenza epidemiologica, sono state effettuate nuove implementazioni al sistema informativo della BDNA finalizzate a potenziarne la gestione automatizzata dei procedimenti amministrativi per le verifiche di competenza da parte delle Prefetture.

Al riguardo, sono state effettuate attività di particolare complessità tecnologica per l'adeguamento della BDNA al rilascio della cd. Liberatoria provvisoria, per effetto della disposizione introdotta dall'art. 3, comma 2, D.L. 16.7.2020, n.76, recante misure urgenti per la semplificazione e l'innovazione digitale, convertito con modificazioni nella L. 11 settembre 2020, n.120, da applicare fino al 31 dicembre 2021.

Inoltre, si è dato corso alle modifiche del sistema applicativo BDNA allo scopo di adeguarne il funzionamento alle esigenze correlate all'applicazione di idonee misure di prevenzione antimafia nei confronti dei beneficiari delle misure temporanee di sostegno alla liquidità di cui all'art. 1 del D.L. 8 aprile 2020, n.23, convertito con modificazioni nella L. 40/2020.

Particolare attenzione è dedicata a perseguire l'interoperabilità di banche dati istituite presso le diverse Amministrazioni statali attraverso apposite convenzioni, nell'ottica di migliorare l'efficacia dell'azione di tutte le Amministrazioni interessate.

In questa logica sono stati sottoscritti importanti protocolli d'intesa con il Ministero dell'Economia e delle Finanze e, rispettivamente, con la società SACE S.p.a. e l'Agenzia delle Entrate, nonché, da ultimo, con Cassa Depositi e Prestiti.

Di grande innovazione è poi la collaborazione attivata con l'Associazione Nazionale Costruttori Edili (ANCE), in base alla quale le articolazioni regionali della stessa ANCE potranno consultare direttamente la Banca dati nazionale unica (BDNA) per verificare il profilo antimafia dei propri partner commerciali della filiera edilizia, particolarmente sensibile al rischio infiltrativo.

Di seguito, alcuni dati relativi al funzionamento della BDNA alla data del 31 ottobre 2021:

Statistiche BDNA alla data del 31/10/2021							
		2016	2017	2018	2019	2020	2021
certificazioni rilasciate	comunicazione antimafia	267.969	289.874	321.029	372.437	337.704	312.334
	informazione antimafia	30.342	86.310	117.191	122.755	128.243	118.044
nulla osta non rilasciati per la presenza di provvedimento interdittivo	comunicazione antimafia	406	446	329	880	1169	928
	informazione antimafia	327	381	306	661	961	861

	nuove imprese censite
2016	195.377
2017	118.899
2018	123.594
2019	140.040
2020	112.797
2021	88.501
Totale	779.208

Utenti accreditati in BDNA	53.504

Applicazione di modalità di lavoro agile per i dipendenti dell'Amministrazione civile in servizio presso il DPP e nelle Prefetture

A seguito di un periodo di sperimentazione del lavoro agile nel 2018, che ha visto il coinvolgimento su base volontaria di 37 unità, di cui 27 presso gli uffici centrali del Dpp e 10 presso le prefetture-pilota di Foggia, Perugia e Ravenna, nel corso del 2019 sono state rese disponibili con successo le modalità di lavoro agile per 300 utenti ai quali questo Ufficio per l'innovazione tecnologica ha erogato anche un servizio di assistenza tecnica in caso di necessità.

Per l'anno 2020 era previsto l'avvio allo svolgimento della prestazione lavorativa in modalità agile per 500 unità negli uffici centrali di questo dipartimento e nelle prefetture.

A far data dall'avvio del periodo di emergenza epidemiologica questo Ufficio ha attivato finora per i medesimi uffici centrali e periferici - comprese le commissioni territoriali per il riconoscimento della protezione internazionale – il numero complessivo di circa 5800 collegamenti remoti, ottenendo il risultato di garantire la piena funzionalità delle Prefetture e del Ministero durante al crisi pandemica.

La sicurezza

Circa la *cybersecurity,* l'obiettivo del DPP è quello di incrementare sensibilmente la capacità di resilienza nazionale attraverso misure di investimento tecnologico in grado di migliorare la sicurezza cibernetica, la protezione dei dati e la continuità operativa dei servizi digitali delle prefetture e del DPP. Lo scopo è quello di garantire ad alti livelli la sicurezza cibernetica e la protezione del patrimonio informativo delle banche dati digitali attraverso il potenziamento degli apparati hardware e delle tecnologie software. In particolare le attività sono dirette ad integrare e introdurre tecnologie all'avanguardia che consentano la protezione della superficie di attacco nel cyberspazio che nel contempo cresce proporzionalmente alle dinamiche di trasformazione digitale, creando nuovi scenari di rischio sempre più preoccupanti in relazione all'aumento esponenziale della produzione di dati personali e sensibili. Questi ultimi costituiscono l'obiettivo principale di potenziali attacchi informatici finalizzati a compromettere il patrimonio informativo e a interrompere, sospendere o rendere problematica l'erogazione dei servizi digitali, con conseguenti danni d'immagine per l'Amministrazione.

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – PROGETTI DEL MINISTERO DELL'INTERNO

Il Ministero dell'Interno, con riferimento al cambiamento richiesto per la ripresa dalla crisi globale causata dalla pandemia Covid-19 ed alle notevoli risorse messe in campo dall'Unione Europea nell'ambito del Next Generation EU e del collegato Piano Nazionale di Ripresa e Resilienza italiano, ha programmato le seguenti linee d'azione:

1) ***DIGITALIZZAZIONE PA***

Investimento 1.4: Servizi digitali

Progetto per l'estensione dell'Anagrafe Nazionale della Popolazione Residente (ANPR) per un valore di 35 milioni

Investimento 1.5: Cybersecurity

Progetto del valore di 27 milioni per potenziare la capacità di risposta dei Nuclei Operativi Sicurezza Cibernetica (NOCS) agli attacchi informatici ai sistemi della Pubblica Amministrazione, compreso il sistema sanitario nazionale, ovvero alle realtà produttive presenti nei territori di competenza

Progetto del valore di 30 milioni per l'implementazione del Security Operation Center (SOC) per l'analisi e il monitoraggio delle policy di sicurezza per la prevenzione degli incidenti di cybersecurity attraverso l'analisi continua delle minacce, la scansione della rete e dei sistema alla ricerca di vulnerabilità e l'adozione delle adeguate contromisure.

Investimento 1.6: Digitalizzazione delle grandi amministrazioni centrali

Programma unitario, organico e strutturato, da realizzare entro l'anno 2026, comprensivo di 3 progetti di investimento per un valore di 107 milioni.

1. Potenziamento infrastrutture digitali del Ministero dell'Interno, che prevede la realizzazione di:

✓ Connettività a banda larga delle sedi del Ministero dell'Interno;

✓ Cabling degli uffici.

2. Interoperabilità banche dati del Ministero dell'Interno: si propone di potenziare i CED dell'Amministrazione attraverso la realizzazione di un cloud e meccanismi di interoperabilità tra le banche dati.

3. Sviluppo dei servizi applicativi e piattaforme abilitanti del Ministero dell'Interno: prevede interventi di digitalizzazione dei servizi interni, anche con strumenti di AI, finalizzati a fornire più efficaci servizi al cittadino grazie all'integrazione con le infrastrutture abilitanti, quali AppIO, Servizio Pubblico di Connettività, PagoPA ed altre app specifiche

2) TURISMO E CULTURA

Investimento 2.4: Sicurezza sismica nei luoghi di culto e restauro del patrimonio del FEC

Progetto di restauro dei luoghi di culto e del patrimonio di proprietà del Fondo Edifici di Culto, per un valore di 800 milioni di euro

3) RIVOLUZIONE VERDE E TRANSIZIONE ECOLOGICA

Investimento 2.2: Resilienza, valorizzazione del territorio ed efficienza energetica dei Comuni

Risorse pari a 6 miliardi destinate ad implementare i fondi del Dipartimento per gli Affari Interni e Territoriali (DAIT) che erogano contributi per la realizzazione di progetti in tema di efficientamento energetico dei territori comunali e di messa in sicurezza degli edifici e del territorio.

Investimento 4.4: Rinnovo flotte, bus e treni verdi

Rinnovo del parco veicoli dei Vigili del Fuoco attraverso l'ammodernamento del parco veicoli con l'introduzione di circa 3.600 veicoli elettrici e veicoli alimentati a gas per i servizi istituzionali e l'introduzione di 200 nuovi mezzi con alimentazione ibrida elettrico-endotermica negli aeroporti (424 milioni).

4) INCLUSIONE E COESIONE

Investimento 2.1: Rigenerazione urbana, volta a ridurre situazione di emarginazione e degrado sociale

Si tratta di risorse (circa 3,3 miliardi) destinate ad implementare il fondo del Dipartimento per gli Affari Interni e Territoriali che eroga contributi per la realizzazione di progetti in tema di rigenerazione urbana, allo scopo di ridurre le situazioni di marginalizzazione e di degrado sociale nei territori comunali.

Investimento 5: piani urbani integrati

Si tratta di risorse pari a 2,7 miliardi per progetti di rigenerazione urbana da realizzare nelle Città metropolitane.

TOTALE RISORSE DELLE PROGETTUALITÀ DEL MINISTERO DELL'INTERNO: 1,4 MILIARDI

- **ANPR** **35 milioni**
- **Cybersecurity** **57 milioni**
- **Digitalizzazione** **107 milioni**
- **Fondo Edifici di Culto (FEC)** **800 milioni**
- **Green Vigili del Fuoco** **424 milioni**

TOTALE RISORSE DESTINATE AGLI ENTI LOCALI: **12 MILIARDI**

- **Efficientamento energetico e messa in sicurezza** **6 miliardi**
- **Rigenerazione Urbana** **3,3 miliardi**
- **Piani urbani integrati** **2,7 miliardi**

TOTALE DEGLI INTERVENTI DEL MINISTERO DELL'INTERNO: **13,4 MILIARDI**

CONCLUSIONI

Come ha messo ben in evidenza questa relazione, l'Amministrazione dell'Interno è una struttura molto complessa ed eterogenea nella quale agiscono realtà imponenti, i Dipartimenti, che rispondono a normative diverse, nonché ad obiettivi peculiari alle "mission" assegnate, fattori questi che se da un lato possono rendere difficoltoso trovare un punto d'incontro comune, dall'altro costituiscono una formidabile opportunità di condivisione e di evoluzione, sicuramente anche in senso digitale, oltre che di consolidamento di una 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 perseguire la missione istituzionale del Ministero dell'Interno, con l'adozione delle tecnologie più moderne e più aderenti alle richieste dei cittadini e alle esigenze di sicurezza. L'ottimo clima di collaborazione che si è ormai instaurato tra le componenti dell'Amministrazione in materia ICT, è dimostrato anche dai progetti sviluppati dal Gruppo di Lavoro Permanente presieduto dal Responsabile per la Transizione Digitale.

L'opportunità offerta dalla 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 già sono offerti all'utenza, nonché le ulteriori progettualità evolutive e innovative di interesse strategico nazionale già avviate, tra le quali certamente spicca la 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 dal CNAIPIC, per la prevenzione e la repressione dei reati ai danni delle infrastrutture informatiche erogatrici di servizi pubblici essenziali.

Il contesto che ho 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, ed 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 ad offrire al cittadino servizi più efficienti. A ciò si aggiunga la disponibilità di 107 milioni di euro previsti dal PNRR che sicuramente consentiranno, entro tempi brevi (2026) un potenziamento delle infrastrutture digitali del Ministero dell'Interno: verranno rafforzati i sistemi di connettività a banda larga, completando così il processo di piena interoperabilità delle banche dati e sviluppando sistemi applicativi finalizzati a fornire servizi sempre più efficienti ai cittadini.

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.