Sezione centrale controllo gestione

5 – Sezione centrale controllo gestione; deliberazione 9 febbraio 2023; Pres. e Rel. Orefice; Agenzia della Cybersecurity nazionale.

Amministrazione dello Stato e pubblica in genere – "Rapporto Pnrr sull'Agenzia per la cybersicurezza nazionale II semestre 2022" – Corte dei conti – Rapporto al Parlamento.

L. 14 gennaio 1994, n. 20, disposizioni in materia di giurisdizione e controllo della Corte dei conti, art. 3, cc. 4 e 6; d.l. 31 maggio 2021, n. 77, convertito con modificazioni dalla l. 29 luglio 2021, n. 108, *governance* del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure, art. 7, c. 7; d.l. 14 giugno 2021, n. 82 convertito con modificazioni dalla l. 4 agosto 2021, n. 109, disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, art. 1.

La Sezione centrale di controllo sulla gestione delle amministrazioni dello Stato con la deliberazione in commento, avente ad oggetto il Rapporto Pnrr sull'"Agenzia per la cybersicurezza nazionale", ha aggiornato al secondo semestre 2022 lo stato di attuazione dell'investimento M1C1-1.5, fornendo ulteriori informazioni al riguardo e considerazioni rispetto a quelle formulate nella deliberazione del 14 luglio 2022, n. 31.

L'obiettivo dell'investimento analizzato consiste nel rafforzamento della difesa nazionale contro i rischi derivanti dalla criminalità informatica, in armonia con gli impegni assunti dall'Italia nell'ambito delle organizzazioni internazionali. Al predetto fine è stata istituita, in forza del d.l. n. 82/2021, l'Agenzia per la cybersicurezza nazionale che ha rilevato inizialmente i compiti assegnati al Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri (Dis) per poi vedersi assegnate, ai sensi del d.p.c.m. 15 giugno 2022 e del d.p.c.m. 1 settembre 2022, le funzioni di competenza del Mise e dell'Agid in materia di cybersicurezza.

Le risorse a tal fine destinate nell'ambito del Piano nazionale di ripresa e resilienza sono pari a 623 milioni di euro, a fronte delle quali gli impegni complessivamente assunti fino al secondo semestre del 2022 ammontano a circa 334 milioni di euro (53 per cento del totale), di cui circa 98 milioni riguardano impegni per attività a titolarità e le restanti risorse sono state impegnate per attività a beneficio di altri enti (a regia).

L'Agenzia è stata individuata quale soggetto attuatore dell'intervento, ai sensi dell'art. 9, c. 1, d.l. n. 77/2021.

Nelle conclusioni della deliberazione n. 31 la sezione aveva manifestato apprezzamento per l'impegno profuso dall'Agenzia, sia sul piano regolamentare che organizzativo, nel creare in tempi celeri le condizioni per consentire di fornire i servizi destinati alla sicurezza, nell'ambito del più ampio settore della sicurezza nazionale.

Alla luce dell'istruttoria condotta, la sezione ha preso atto che dai dati forniti dall'Agenzia e dalle evidenze finanziarie registrate in ReGis, le attività previste per il 2022 nel campo della sicurezza cibernetica e riferibili alle risorse del Pnrr risultano correttamente adempiute. Tuttavia, la sezione ha aggiunto che è necessario un'attenzione specifica nei confronti di alcuni settori particolarmente sensibili, fra cui quello degli operatori energetici, quello finanziario, quello delle telecomunicazioni e quello delle infrastrutture "critiche", in primis quelle sanitarie. In tale ottica, la sezione ha concluso considerando che le risorse del Pnrr dovranno portare "velocità", sia tra i cittadini che nelle pubbliche amministrazioni, per recuperare i ritardi che l'Italia nel tempo ha accumulato rispetto ad altri Paesi europei. (1)

6. *Conclusioni* – Dai dati forniti dalla Agenzia per la cybersicurezza e dalle evidenze finanziarie registrate in ReGis, le attività previste per il 2022 nel campo della sicurezza cibernetica e riferibili alle risorse del Pnrr risultano correttamente adempiute. Sulla disponibilità di 623 milioni di euro determinata in seno al Piano nazionale di ripresa e resilienza, gli impegni complessivamente assunti ammontano a circa 334 milioni di euro, cioè a poco più del 53 per cento del totale, di cui circa 98 milioni riguardano impegni per attività a titolarità (quasi completamente in corso), assunti per sostenere il costo di attività funzionali all'efficientamento organizzativo e strumentale del soggetto attuatore, mentre, per le attività a regia (attività che, per converso, sono espletate a e beneficio di

(1) I. - Il testo integrale del rapporto si legge in <www.corteconti.it>.

II. - Il rapporto in commento si iscrive nell'ambito dell'attività programmata e condotta dalla Sezione centrale di controllo sulla gestione delle amministrazioni dello Stato per l'anno 2022, ai sensi dell'art. 7, c. 7, d.l. n. 77/2021, convertito dalla l. n. 108/2021, che affida alla Corte dei conti l'esercizio di un controllo da esercitarsi ai sensi dell'art. 3, c. 4, l. n. 20/1994, svolgendo, in particolare, valutazioni di economicità, efficienza ed efficacia circa l'acquisizione e l'impiego delle risorse finanziarie provenienti dai fondi di cui al Piano nazionale di ripresa e resilienza. Tale controllo che deve ispirarsi a criteri di cooperazione e di coordinamento con la Corte dei conti europea, secondo quanto previsto dall'art. 287, del Trattato sul funzionamento dell'Ue, confluisce, in un referto, almeno annuale, al Parlamento sullo stato di attuazione del citato Piano.

L'attività della Sezione centrale del controllo sulla gestione delle amministrazioni dello Stato, ai sensi delle citate disposizioni ed in coerenza con le indicazioni fornite nella deliberazione delle Sezioni riunite n. 43/2022, concorre alla predisposizione del rapporto che le suddette Sezioni riunite sono tenute a trasmettere al Parlamento semestralmente, pur continuando a sostanziarsi nell'adozione di specifici rapporti sullo stato di avanzamento degli interventi del Pnrr, sottoposti a controllo sulla base dell'annuale programma di attività, adottato in coerenza con la programmazione del Collegio per il controllo concomitante.

In particolare, la deliberazione in commento approva il rapporto che riferisce in merito all'intervento M1C1-1.5 avente ad oggetto l'Agenzia per la cybersicurezza nazionale, fornendo gli aggiornamenti al II semestre 2022 rispetto allo stato dell'arte rappresentato dal rapporto già approvato con delib. n. 31/2022. La sezione ha *in primis* analizzato le attività poste in essere dall'amministrazione titolare dell'intervento al fine di superare le criticità osservate dalla sezione nella precedente deliberazione, analogamente a quanto riportato nelle altre deliberazioni adottate contestualmente dalla sezione con riferimento agli interventi oggetto di controllo e che si elencano di seguito: Corte conti, Sez. centr. contr. gestione, 8 febbraio 2023, n. 1, *Accordi per l'innovazione*; n. 2, *Servizio civile digitale*; n. 3, *Servizio civile universale*; n. 4, *Rete di servizi di facilitazione digitale*; 9 febbraio 2023, n. 5, *Agenzia della cybersecurity nazionale*; n. 6, *Rifinanziamento e ridefinizione del Fondo 394/81 gestito da Simest*; 15 febbraio 2023, n. 8, *Investimenti nella resilienza dell'agro-sistema irriguo per una migliore gestione delle risorse idriche*; n. 9, *Isole verdi*; n. 10, *Ricerca e sviluppo sull'idrogeno*; n. 11, *Sperimentazione dell'idrogeno per il trasporto ferroviario*; n. 12, *Utilizzo dell'idrogeno in settori* hard-to-abate; 16 febbraio 2023, n. 13, *Rafforzamento e potenziamento della ricerca biomedica del Ssn*; n. 14, *Misure per la gestione del rischio di alluvione e per la riduzione del rischio idrogeologico*; n. 15, *Servizi digitali e cittadinanza digitale - Piattaforme e applicativi (PagoPa e App IO)*; n. 16, *Dati e interoperabilità*; n. 17, *Intervento straordinario finalizzato alla riduzione dei divari territoriali nei cicli I e II della scuola secondaria di secondo grado*; n. 18, *Piattaforma notifiche digitali*; n. 19, *Ammodernamento del parco tecnologico e digitale ospedaliero*; n. 20, *Introduzione di dottorati innovativi che rispondono ai fabbisogni di innovazione delle imprese e promuovono l'assunzione dei ricercatori da parte delle imprese*; n. 21, *Infrastrutture digitali*; n. 22, *Sostegno alle persone vulnerabili e prevenzione dell'istituzionalizzazione - intervento 1) azioni volte a sostenere le capacità genitoriali e prevenire la vulnerabilità delle famiglie e dei bambini*; n. 23, *Interventi strutturati socio-educativi per combattere la povertà educativa nel Mezzogiorno a sostegno del terzo settore*; n. 24, *Investimenti in progetti di rigenerazione urbana, volti a ridurre situazioni di emarginazione e degrado sociale*; n. 25, *Sport e inclusione sociale*; n. 26, *Finanziamento di* start-up; n. 27, *Investimenti infrastrutturali per le zone economiche speciali*; n. 28, *Valorizzazione dei beni confiscati alle mafie*; n. 29, *Citizen* inclusion - *miglioramento dell'accessibilità dei servizi pubblici digitali*; n. 30, *Programma innovativo della qualità dell'abitare*; n. 31, *Sicuro, verde e sociale: riqualificazione edilizia residenziale pubblica*; n. 32, *Riduzione delle perdite nelle reti di distribuzione dell'acqua, compresa la digitalizzazione e il monitoraggio delle reti*; tutte in <www.corteconti.it>. [P. COSA]

altri enti e amministrazioni) si registrano impegni per circa 235 milioni (poco meno di 193 milioni in corso).

Bisognerà comunque mantenere l'attenzione alta, con la consapevolezza che gli investimenti dovranno raggiungere tutti i campi maggiormente sensibili ma non solo quelli.

I campi maggiormente a rischio sono gli operatori energetici, quelli finanziari e quelli delle telecomunicazioni. Bisognerà tutelare le infrastrutture critiche, tra cui quelle sanitarie *in primis*, che si trovano in una situazione non certamente uniforme: alcune sono bene organizzate, altre hanno problemi e sono in ritardo.

Va considerato che per affrontare al meglio le sfide del Paese, attraverso la Strategia nazionale di cybersicurezza, sono stati individuati tre obiettivi fondamentali: protezione degli asset strategici nazionali; risposta alle minacce, agli incidenti e alle crisi *cyber* nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale; sviluppo sicuro delle tecnologie digitali attraverso strumenti e iniziative volte a supportare i centri di eccellenza, le attività di ricerca e le imprese.

La ricerca di questi obiettivi può tuttavia risultare insufficiente se si considera la pari necessità di una stabilità di governance, un piano di investimenti razionale, un dirottamento in tempo reale di risorse ai centri di ricerca ed anche un sistema di valutazione rapido ed obiettivo delle competenze.

Come c'è da chiedersi se la spesa per le infrastrutture tecnologiche possa considerarsi adeguata o, come taluni ambienti affermano, ancora troppo bassa.

E poi c'è il fattore umano.

Le risorse umane previste per i prossimi anni raggiungeranno numeri considerevoli.

Ciò favorirà sicuramente una maggiore consapevolezza della trasformazione digitale e dei rischi che possono presentarsi e favorire un ritorno di cervelli fuggiti all'estero negli ultimi anni. Il cambiamento culturale favorito dalle risorse del Pnrr deve portare "velocità", sia tra i cittadini che nelle pubbliche amministrazioni, per recuperare i ritardi che l'Italia nel tempo ha accumulato nel campo della formazione. Non può essere infatti dimenticato ciò che gli stessi responsabili dell'Agenzia hanno dichiarato e cioè che "siamo 30 anni indietro rispetto alla Germania e 15 rispetto alla Francia […] abbiamo i giovani su cui contare, cerchiamo di recuperare con altissima velocità […] Per le persone che vengono dall'estero significa avere uno sgravio Irpef del 70 per cento, lavorare per il proprio Paese, prendere una parte della propria vita e dedicarla a chi verrà dopo di noi".

Una visione strategica quindi che dovrà puntare sulla velocità e sulla sinergia, incoraggiando in questo senso anche la collaborazione con l'Unione europea, già presente in alcuni recenti progetti varati in tema di sicurezza cibernetica. Una visione ed un'autonomia strategica che dovrà passare attraverso l'implementazione della nozione di "*work force*" nel nostro Paese. Laddove si dovesse pensare che la tecnologia ed il computer sostituiscano l'efficienza del lavoro umano si sarebbe perso di vista l'obiettivo.