Disegno di legge di conversione del decreto-legge 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"

Roma, 30 giugno 2021

1. Introduzione: l'importanza dell'Agenzia

Il Decreto-legge 14 giugno 2021, n. 82 recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"* costituisce un tassello fondamentale per la piena operatività della strategia di cyber-resilienza nazionale inaugurata con l'adozione della disciplina sul perimetro di sicurezza nazionale cibernetica.

Si tratta di un intervento straordinariamente rilevante che, partendo dalla constatazione della crescente centralità assunta dalla cybersecurity in un contesto socio-economico - complice anche la pandemia che ha operato come agente catalizzatore - sempre più digitalizzato e della crescente complessità del quadro normativo e regolamentare di riferimento, svolge un'opera di riordino, andando a concentrare presso un unico soggetto, la neoistituita Agenzia per la cybersicurezza nazionale (ACN), tutte le competenze in materia.

Dopo aver assistito per molti anni al proliferare di interventi normativi che si sono andati accumulando in maniera disordinata e disorganica - spesso in conseguenza della necessità di ottemperare ad obblighi discendenti dalla normativa europea o di far fronte a situazioni emergenziali - accrescendo il numero di soggetti con competenze in materia di cybersicurezza e rendendo a dir poco difficoltosa la ricostruzione del quadro normativo nazionale in materia, finalmente è stato adottato un intervento di semplificazione che, in una logica certamente ispirata al principio della certezza del diritto, cerca di fare ordine riassumendo in un unico soggetto, l'ACN, tutte le funzioni in materia di cybersecurity. Si tratta di

un'iniziativa straordinariamente importante non solo per l'effetto ordinatore che ad essa si accompagna, ma anche e forse soprattutto perché consentirà ai soggetti pubblici e privati di avere un interlocutore unico nazionale in materia di misure di sicurezza e attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi (direttiva NIS) e della sicurezza delle reti di comunicazione elettronica e di poter finalmente fare affidamento su un assetto di competenze chiaro e certo.

D'altronde negli anni è cresciuta la consapevolezza circa l'importanza di garantire un ecosistema sicuro ed un quadro normativo chiaro, in grado di creare quella fiducia indispensabile per incentivare gli investimenti delle imprese e della P.A. nel canale digitale ed incentivare la domanda di servizi digitali da parte dei cittadini e delle stesse P.A. In questa logica saranno certamente cruciali le funzioni di supporto allo sviluppo di competenze industriali, tecnologiche e scientifiche e le attività di comunicazione e promozione della consapevolezza attribuite all'ACN - alle quali peraltro potrebbero essere offerti, in sede di conversione, maggiori indirizzi - che dovranno necessariamente provare ad incidere su quell'immaturità digitale che caratterizza il nostro contesto nazionale e che incide a determinare, in grande misura, il tradizionale collocamento dell'Italia nelle ultime posizioni dell'indice DESI.

I dati lo dimostrano purtroppo in maniera impietosa. Nel quadro di un incremento complessivo degli attacchi a livello globale (+40% tra il 2017 e il 2020), secondo l'ultimo rapporto Clusit, l'Italia si posiziona al primo posto tra i principali Paesi in termini di computer compromessi con software malevoli (12,47%), davanti a Cina, Giappone, USA, Corea del Sud e Regno Unito. Per quanto riguarda i dispositivi mobili, invece, il dato sulle infezioni fatto registrare dall'Italia (5,01%) è secondo solo a quello degli USA (8,18%) ed è di due punti percentuali più elevato della media UE. Questi numeri fanno il paio con la spesa media delle organizzazioni italiane per la sicurezza IT, recentemente censita dall'agenzia europea ENISA (calcolata in relazione al budget complessivo in tecnologie dell'informazione), inferiore sia alla media USA che a quella dell'Europa a 27. Infatti, le organizzazioni USA investono in media il 6% del proprio budget IT in sicurezza, a fronte del 3,5% delle europee e del 3,1% delle italiane. Osservando gli ultimi dati ISTAT (2019) sulla sicurezza ICT nelle aziende con almeno 10 dipendenti, emerge come anche

pratiche semplici e che non richiedono competenze particolari – ad es. mantenere aggiornato il software (svolto dall'89,5% del campione), utilizzare una password complessa (82,2%) ed effettuare il backup dei dati (79,2%) – vengano attuate da una quota di imprese ancora lontana dalla totalità. Focalizzando l'attenzione sulle attività complesse – come l'utilizzo di sistemi di crittografia (20,4%) e l'esecuzione di test di sicurezza (33,5%) – la quota di imprese virtuose scende addirittura a meno di un terzo del totale.

2. Il confronto con gli altri grandi Paesi europei

La nuova Agenzia per la cybersicurezza nazionale rappresenta un unicum nel contesto istituzionale europeo legato alla sicurezza digitale, specialmente se si considera l'eterogeneità delle funzioni che vengono accentrate in essa (coordinamento, predisposizione della strategia nazionale, accertamento delle violazioni, irrogazione delle sanzioni amministrative, identificazione e gestione del perimetro nazionale di sicurezza cibernetica, etc.).

Ciò che rende l'esperienza dell'Agenzia italiana peculiare rispetto all'architettura istituzionale in tema di cybersecurity consiste proprio nella concentrazione di compiti e funzioni in seno ad un soggetto unico, che funga da inequivocabile punto di riferimento per l'intero settore digitale, laddove negli altri Paesi si rileva di solito la distribuzione di compiti tra agenzie di intelligence, ministeri e altri enti di coordinamento.

Rispetto ai casi di Francia, Gran Bretagna, Germania e Spagna, è l'assetto istituzionale francese quello strutturalmente più vicino al nascente sistema italiano. L'architettura del Paese transalpino fa perno su un soggetto polifunzionale, l'Agenzia Nazionale per la Sicurezza dei sistemi informativi (ANSSI), che, sebbene in seno al Segretariato Generale della Difesa e della Sicurezza Nazionale (SGDSN, i servizi di intelligence francesi) è sotto la responsabilità del Primo Ministro, così come previsto per l'agenzia italiana. Interessante notare, a tal proposito, come l'ANSII conti attualmente 600 dipendenti, peraltro in continuo aumento, rispetto ai 972 dipendenti complessivi dell'SGDSN, a riprova di come le attività relative alla cybersecurity siano in continua crescita rispetto a quelle tradizionali di intelligence.

Così come l'ACN italiana, l'ANSSI è tenuta alla stesura della strategia nazionale in materia digitale, è responsabile - anche a livello giuridico - della prevenzione e della reazione ad incidenti informatici ai danni delle istituzioni sensibili e si occupa della promozione di tecnologie, sistemi e know-how nel campo della sicurezza dei sistemi informatici sia a livello nazionale che europeo. L'ANSSI si occupa anche della LID, ovvero la Lotta Informatica Difensiva. Tuttavia, a differenza di quanto avverrebbe in Italia con l'istituzione dell'ACN, il raggio di azione dell'Agenzia francese in questo contesto è limitato dalla presenza di altri enti (il COMCYBER per le competenze delle Forze Armate e il DGSI, *Direction générale de la sécurité intérieure*, per il Ministero dell'Interno).

Analogie e differenze si rilevano anche tra il nuovo assetto italiano e il quadro tedesco. La strategia di cybersecurity presentata in Germania nel 2016 ha previsto ampie responsabilità in capo ai servizi di intelligence. Il monitoraggio dei network federali e dell'implementazione delle misure difensive è affidato all'ufficio federale per la sicurezza delle tecniche informatiche (Bundesamt für Sicherheit in der Informationstechnik, BSI), posto sotto il Ministero dell'Interno e dotato di oltre 1.100 addetti, mentre è il Servizio di Controspionaggio Militare (MAD) ad occuparsi della gestione e della risposta ad attacchi malevoli e crisi, con la possibilità di ricorrere anche a strumenti di natura offensiva. La nuova legge sulla cybersecurity approvata nel 2021 (la *IT Sicherheitsgesetz* o *IT SiG 2.0*), delinea una sorta di "perimetro" che estende la lista delle infrastrutture critiche alla gestione dei rifiuti e distingue tra *infrastrutture di particolare interesse pubblico* e *cyber-critical operators*, ovvero tutti quegli istituti il cui malfunzionamento causerebbe, seppur in maniera indiretta, problemi alle infrastrutture critiche. Inoltre, viene introdotto un meccanismo di assessment sulla sicurezza dei componenti delle infrastrutture critiche che non esclude *ex-ante* alcun vendor, ma richiede molteplici garanzie anti-sabotaggio, anti-spionaggio e anti-terrorismo, e richiede un periodo di valutazione di 2 mesi, consentendo anche la rimozione delle apparecchiature *ex-post* qualora rappresentino un pericolo per l'ordine pubblico o per la sicurezza della Repubblica Federale. Mentre quest'ultima istanza è in capo al Ministero dell'Interno (BMI), il BSI si occupa di stabilire i parametri minimi di sicurezza IT, di eseguire dei test di verifica e valutazione del rischio e di dare ordini dettagliati ai fornitori di telecomunicazioni, in caso di minacce specifiche.

Analogie e differenze si rilevano anche rispetto all'architettura cybersecurity spagnola, che da un lato fa perno sulla figura del Primo Ministro e dall'altro assegna a diversi Ministeri competenze differenti in materia digitale. In particolare, il Primo Ministro presiede le riunioni del *Consejo de Seguridad Nacional* (CSN), organo collegiale - composto da rappresentanti del Governo - che si occupa della direzione della politica di sicurezza nazionale. Il CSN è supportato da due enti: il *Consejo Nacional de Ciberseguridad* (CNC), con funzioni di coordinamento tra le diverse Pubbliche Amministrazioni in materia di cybersecurity e tra i settori pubblico e privato; ed il *Comité Especializado de Situación*, che si occupa della gestione delle situazioni di crisi.

Per quanto concerne il lato "ministeriale", 4 diversi enti operano alle dipendenze di altrettanti Ministeri: l'*Incibe-Cert*, sotto il Ministero degli Affari Economici e della Transizione Digitale, funge da centro di risposta per incidenti di sicurezza digitale rivolto a cittadini e imprese; il *Ccn-Cert*, sotto il Ministero della Presidenza si occupa degli attacchi diretti alle istituzioni governative; l'*Espdef- Cert*, operante nell'ambito del Ministero della Difesa, gestisce un team di risposta alle emergenze informatiche; ed infine l'*OCC*, in seno al Ministero dell'Interno, che svolge attività di coordinamento dei Cert nazionali.

Il Regio decreto legislativo 14/2019 ha introdotto misure a tutela della pubblica sicurezza in materia di amministrazione digitale, in particolare la rettifica dell'articolo 6, che ha rafforzato i poteri del Governo assegnandogli la facoltà di intervenire su qualsiasi infrastruttura, risorsa o elemento associato alle reti e ai servizi di comunicazione elettronica nel caso di circostanze che possono incidere sull'ordine pubblico e sulla sicurezza nazionale. Il disegno di legge sulla Cybersecurity 5G, attualmente in discussione in Parlamento, obbligherebbe gli operatori a condurre un'analisi di gestione del rischio ogni 2 anni e le autorità del mercato almeno ogni 6 anni. In questo contesto il Governo potrebbe subordinare l'utilizzo di un'apparecchiatura, programma o servizio 5G al previo conseguimento di una certificazione stabilita dal regolamento europeo sulla sicurezza informatica**.** Le valutazioni delle apparecchiature adotterebbero dunque un approccio neutrale nei confronti dei fornitori, basandosi sull'analisi di gestione del rischio e sul principio di diversificazione dei fornitori.

Piuttosto differente il modello scelto dal Regno Unito, in cui l'attuale discussione in Parlamento del *Telecommunication (Security) Bill* costituisce il punto di caduta di un dibattito in materia di cybersecurity iniziato nel 2018 e che ha visto la pubblicazione, tra gli altri, della *Supply Chain Review*, di due analisi del NCSC e della *5G Supply Chain Diversification Strategy*. Il Telecommunication Bill apporterà modifiche piuttosto sostanziali nel ridisegnare l'assetto istituzionale del Paese in tema di reti di telecomunicazioni puntando, a differenza del modello italiano, a rafforzare i poteri degli enti già esistenti, in particolare l'autorità indipendente di regolamentazione dei servizi di comunicazione (Ofcom). Nella cornice della nuova proposta di legge, che impone nuovi obblighi e requisiti in capo ai fornitori di apparecchiature di reti di telecomunicazione del Regno Unito, vengono spostati dal Parlamento all'Esecutivo alcuni nuovi poteri che consentono di stabilire specifici requisiti di sicurezza e codici di condotta, e vengono assegnati all'Ofcom strumenti e responsabilità per garantire il rispetto della normativa di settore, tra cui la possibilità di richiedere ai fornitori di eseguire test, emettere notifiche di violazione, indicare misure provvisorie per colmare lacune di sicurezza e, in caso di inadempienza, imporre sanzioni pecuniarie.

3. Alcuni suggerimenti

Se è senza dubbio positiva la valutazione delle finalità perseguite con l'istituzione dell'Agenzia ed il conseguente riassetto delle competenze in materia di cybersecurity, non possono non destare preoccupazione le tempistiche attuative. Ed infatti, se è fissato in 120 gg. il termine entro cui procedere all'adozione del regolamento che si occuperà di organizzare operativamente l'Agenzia, non può sottovalutarsi il già considerevole ritardo accumulato nell'implementazione del perimetro di sicurezza nazionale cibernetica che ancora risulta carente di due decreti (uno relativo alle categorie per le quali sarà necessario effettuare la notifica al CVCN ed uno relativo ai criteri per l'accreditamento dei laboratori competenti per le verifiche delle condizioni di sicurezza) e, dunque, le gravissime conseguenze che si produrrebbero in presenza di ulteriori ritardi dovuti ai tempi tecnici di costituzione dell'Agenzia. Sul punto è certamente da accogliere positivamente la disposizione che prevede l'utilizzo di risorse umane provenienti da amministrazioni già impegnate nell'attuazione del perimetro (così come si auspica che gli strumenti di coordinamento previsti con le amministrazioni settoriali siano resi operativi al più presto)

ma è fuor di dubbio che il progetto esecutivo debba essere messo a punto e monitorato con il massimo rigore per garantire che l'Agenzia si doti in tempi rapidi e certi del personale necessario.

Quanto poi alle risorse finanziarie da destinare all'Agenzia, premessa la necessità, se si vuole davvero garantirne la piena ed efficace operatività, di assicurare mezzi adeguati all'enorme mole e complessità delle funzioni ad essa assegnate, sebbene sia usuale la previsione di obblighi di contribuzione a favore delle autorità di regolazione e vigilanza a carico dei soggetti vigilati, va certamente prestata la massima attenzione e dunque disciplinata con rigore la previsione di entrate in parte provenienti da soggetti privati, al fine di scongiurare qualsiasi rischio di possibili conflitti di interesse. Dovrebbero dunque essere stabiliti criteri generali, che valgano per tutti i soggetti in possesso di determinate caratteristiche, conoscibili a priori e modificabili solo in base a procedimenti soggetti a consultazione pubblica.

A quest'ultimo proposito, proprio perché giustamente si vuole favorire l'interlocuzione dell'Agenzia con la società civile nella sua interezza, si dovrebbero prevedere e regolare i meccanismi di interlocuzione con gli stakeholder, per assicurarne da un lato la piena trasparenza e dall'altro poter consentire al più ampio numero di attori, pubblici e privati, di fornire elementi conoscitivi, utili a indirizzare la strategia e le policy nazionali. Naturalmente, in questo senso, sarà fondamentale garantire il rapporto costante con il Parlamento.

Seppur nel generale apprezzamento per la disciplina istitutiva dell'Agenzia, il riassetto delle competenze in materia di cybersecurity suggerisce anche una riflessione circa l'attuale modello che vede coesistere parallelamente la disciplina golden power, così come evolutasi nel tempo in senso estensivo, andando a ricomprendere anche le reti 5G nel caso di attori extra-UE e la normativa sul perimetro di sicurezza nazionale cibernetica. Ed infatti, sebbene sia ancora atteso il decreto che individuerà le categorie per le quali sarà necessario effettuare la notifica al CVCN, è concreta la possibilità che operazioni rilevanti per la normativa golden power lo siano anche per la disciplina sul perimetro, dando vita ad una serie di interazioni - e possibili duplicazioni di verifiche ed adempimenti per gli operatori soggetti ad entrambe le normative - che certamente potrebbero risultare inadatte alle rapide evoluzioni cui la tecnologia ci

sta abituando ed avere un impatto negativo sulle dinamiche di mercato e sulla competitività del sistema paese e che pertanto necessitano di essere chiarite e definite.