2021

Audizione del dott. Eugenio Santagata, CEO di Telsy Spa.

NELL'AMBITO DELL'ESAME DEL DISEGNO DI LEGGE C. 3161, 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*".

INTRODUZIONE

(Presentazione, considerazioni generali e struttura del documento)

Presentazione di Telsy

Telsy quest'anno compie 50 anni di attività industriale. L'azienda, nata dall'intuizione dell'ingegner Martelli nel 1971, si è sempre occupata di sistemi di sicurezza delle comunicazioni, lavorando al fianco dell'intelligence, delle Forze Armate e delle Forze dell'Ordine. Principalmente in ambito nazionale.

Negli anni 90 Telsy entra nel Gruppo TIM, che oggi le assegna il ruolo di "fabbrica della sicurezza" a 360 gradi. Siamo quindi impegnati a mantenere ed allargare la nostra attività "core", di sicurezza delle comunicazioni, che vogliamo sempre di più internazionalizzare. Ma da alcuni anni ormai siamo lanciati nel mercato della Cybersecurity che forniamo ai clienti del Gruppo TIM, sia attraverso prestigiose partnership internazionali, ma anche e sempre di più grazie allo sviluppo di soluzioni tecnologiche proprietarie.

Considerazioni generali sul DL

La riforma ha una portata molto impegnativa. Mette insieme le competenze e le capacità disperse in vari organismi e gangli dello Stato (DIS, AGID, MISE…) e questo non può fare che piacere alle imprese, che avranno un unico punto di interlocuzione.

Altro fattore molto importante è che viene coniugato il ruolo operativo con quello politico e programmatico in ambito Cyber. La medesima autorità quindi potrà grazie all'operatività quotidiana, fare esperienza delle problematiche di tipo legislativo, regolatorio, politico, industriale, formativo ed assumere iniziative di proposta o anche di risoluzione diretta delle criticità. Anche questo è un punto positivo, perché il mondo Cyber è fortemente dinamico e duttile e non ci si può permettere che le analisi sulla situazione del paese impieghino anni per trasformarsi in scelte politiche sostanziali.

Il nostro contributo

Il contributo che vogliamo fornire alla discussione Parlamentare sull'istituzione dell'Agenzia per la Cybersicurezza nazionale, si concentra su quattro punti di miglioramento possibili: il ruolo dell'Agenzia nell'attuazione del PNRR, le modalità concrete di attuazione dei partenariati pubblico / privato cui l'Agenzia potrà dare vita; gli strumenti attraverso i quali conseguire, nel concreto, l'obiettivo ambizioso e cruciale dell'autonomia tecnologica nell'ambito di prodotti e servizi; la necessità di menzionale esplicitamente il settore della crittografia come ambito di competenza e di intervento dell'Agenzia; la definizione delle regole di ingaggio e l'individuazione dei centri di responsabilità nelle attività di risposta e reazione (Cyber deterrence).

A ciascuno di questi punti è dedicato un paragrafo del documento, che si conclude con una proposta di miglioramento della norma oggetto della discussione parlamentare, che potrebbe essere recepita nella fase emendativa.

AMBITI DI MIGLIORAMENTO DEL DECRETO LEGGE

(Analisi e relative proposte su PNRR, partenariati Pubblico / Privato, Autonomia Tecnologica Nazionale, Crittografia e Cyber Deterrence)

PNRR

Nelle premesse del Decreto si rintraccia nel PNRR una delle ragioni per cui si dà corso alla nascita dell'agenzia e, implicitamente, sul perché tale azione di riforma sia condotta attraverso la Decretazione d'urgenza.

Il Piano Nazionale di Ripresa e Resilienza contiene al suo interno una specifica misura sulla cybersicurezza e prevede la nascita dell'Agenzia. Quindi l'impostazione è corretta. Tuttavia è necessario guardare oltre. Nel suo complesso il PNRR ha per un terzo, un impatto digitale. Uno dei criteri di valutazione del Piano, da parte della Commissione UE, è stato proprio quello dell'impatto degli investimenti sulla realizzazione delle politiche per il decennio digitale che l'esecutivo guidato da Ursula Von del Leyen ha messo al centro della sua azione di guida delle istituzioni europee.

Allora è necessario che vi sia una vigilanza attiva e proattiva su tutta la parte digitale del Piano e che questa attività sia affidata all'agenzia. Pensare che il rapporto tra Agenzia e PNRR si esaurisca con l'attuazione dell'investimento che di "Cybersicurezza" porta il nome nel titolo sarebbe quantomeno riduttivo. Né possiamo pensare che la rispondenza degli investimenti digitali del PNRR, dalla scuola all'ambiente, dai trasporti al settore idrico, possa esaurirsi nel semplice ottenimento della certificazione dei beni ICT che dovrà svolgere il CVCN che, correttamente, con il Decreto, passa dal MISE all'Agenzia.

E' necessaria un'azione sistemica che garantisca che ogni euro speso per l'attuazione degli investimenti previsti dal PNRR che necessitino di implementazione digitale, contribuisca fattivamente ad innalzare il livello di resilienza cibernetica del Paese. Questo principio andrebbe declinato in una apposita norma, che sancisca il ruolo dell'Agenzia come *watchdog* del miglioramento della cybersicurezza all'interno di ciascun investimento che contempli un' "anima" digitale.

Partenariato Pubblico / Privato

Nel Decreto sono molti gli obiettivi che l'agenzia perseguirà in partnership con l'industria. E'un importante riconoscimento per il settore privato, che contribuisce in maniera fondamentale alla costruzione dello "scudo" Cyber del Paese. Nell'Articolo 7 il partenariato pubblico privato è richiamato come strumento per cogliere opportunità nell'ambito della progettualità internazionale, della formazione e dello sviluppo delle tecnologie. Tale partnership si sostanzierà attraverso la possibilità riconosciuta all'agenzia, di costituire, con i privati, appositi strumenti di cooperazione, come fondazioni o società.

A tal proposito, pur apprezzando che la formulazione della norma rimanda "alle finalità" dell'Articolo 7 e quindi sembra escludere una attività dell'Agenzia "in concorrenza" sul mercato con le aziende private che già operano nel settore (rafforzato dal fatto che l'Agenzia possa "partecipare" e non "costituire" questi tipi di veicoli giuridici), riteniamo necessario richiamare esplicitamente il principio della trasparenza nella selezione dei partner privati, che deve premiare il merito industriale e non

avvenire in ambito completamente discrezionale, pur nella consapevolezza che la delicatezza del settore può giustificare -in casi limitati- la valorizzazione di privative industriali già esistenti.

Per rendere più trasparente e dialogico il rapporto tra l'Agenzia e i privati, si propone di istituzionalizzare il dialogo tra la struttura ed il comparto industriale, attraverso strumenti ben identificati. Ad esempio costituire un "albo" di fornitori di prodotti e servizi certificati dal CVCN ovvero dai Centri di Valutazione di Interno e Difesa, che siano "in automatico" coinvolgibili in attività di dialogo istituzionale, sul modello ad esempio dei Gruppi di Lavoro istituiti presso il NIAG della NATO. In quelle sedi gli operatori in possesso di certificazioni, si confrontano tra di loro e con gli utilizzatori, per la preparazione di documenti, soluzioni, bandi e gare che siano conformi alle esigenze ed al passo con la ricerca scientifica e tecnologica.

Autonomia tecnologica nazionale

All'articolo 7, comma 1 lettera a), si affida all'Agenzia -tra gli altri compiti- quello di coordinamento delle azioni per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore.

Si tratta di un punto sostanziale e cruciale di politica industriale del Paese, dell'Unione Europea e dell'Alleanza Atlantica. E' già molto che venga enunciato. Ma dobbiamo assicurare all'Agenzia gli strumenti necessari perché esso sia effettivamente perseguito, nella concretezza.

Nel decreto possiamo rintracciare alcuni elementi che vanno in questa direzione, come l'indicazione dell'Agenzia come nodo italiano della rete europea dei Competence Center che andranno a gestire i 4,5 Miliardi a disposizione della Strategia europea sulla Cybersicurezza. Questa previsione non è sufficiente ad assicurare che l'obiettivo dell'autonomia tecnologica sia centrato.

E' quindi necessario mettere in campo una serie di azioni che aiutino gli investimenti privati e che contribuiscano alla sostenibilità dell'impresa.

L'Unione Europea consente la creazioni di Zone Economiche Speciali, l'Italia le sta attuando, con una qualche fatica. Ad oggi, soprattutto nella loro connessione con logistica e portualità, esse sembrano più declinate a favorire le economie tradizionali. Potrebbe essere utile dedicare una Zona Economica Speciale alle aziende della Cybersicurezza, spingendo attraverso sistemi di vantaggi fiscali autorizzati dall'Unione Europea, le realtà produttive ad insediarsi in un luogo che possa avere, come prospettiva operativa il campus di Ber'Sheva in Israele.

Anche una scelta di questo tipo però, non risolverebbe il 100% del problema. La sostenibilità dell'impresa infatti si realizza da un lato attraverso investimenti e riduzione di costi fiscali, ma dall'altro attraverso ricavi certi e programmabili che possano supportare e giustificare i budget necessari per la ricerca. E' necessario quindi che in questo ipotetico "cluster" della Cybersicurezza "Made in Italy", si introduca un vantaggio, una priorità negli acquisti di prodotti, soluzioni e servizi che lo Stato farà per aumentare le capabilities di Cyber Resilience ed anche di Cyber Defense e Cyber Deterrence. In quest'ottica è fondamentale il raccordo con il sistema della Difesa e delle Forze Armate: se infatti l'agenzia si caratterizza per un ruolo essenzialmente "civile" non possiamo negare che proprio le Forze Armate, sia in ottica di rafforzamento nazionale, che di partecipazione alla "bussola strategica" UE e quindi di compartecipazione al "set of forces" messo a disposizione della NATO, hanno budget necessari (si pensi al fondo per gli investimenti della Difesa, di recente istituzione nel nostro bilancio,

ma anche allo European Defence Fund) per sostenere attraverso la domanda, lo sviluppo di soluzioni, prodotti e servizi nativi nazionali frutto della ricerca di aziende messe in grado di programmare e quindi di sapere che, investendo X in ricerca e sviluppo e centrando gli obiettivi qualitativi, possono attendersi un rientro in termini di ricavi derivanti da quella ricerca e da quello sviluppo, in un tempo definito.

Encryption

Nel Decreto non è mai citata la crittografia (o encryption), come strumento di cybersicurezza o, comunque come attività su cui vi sia una specifica responsabilità dell'agenzia. Questo nonostante che l'Agenzia vada ad acquisire tutte le competenze, oggi presso il MISE, che attengono la sicurezza delle comunicazioni (e che hanno per oggetto le TELCO).

Proprio per questa ragione, la mancata menzione della crittografia deve essere intesa come una dimenticanza, da sanare nella fase di esame parlamentare.

Infatti l'utilizzo di tale strumento come cardine della sicurezza è ormai metabolizzato in ambito UE, che -non senza un acceso dibattito- si accinge a risolvere la dicotomia tra "Sicurezza dei servizi, delle reti e dei sistemi informativi" (NIS) e "Sicurezza delle comunicazioni" (Codice Comunicazioni Elettroniche), riportando, con la proposta di Direttiva di Revisione della stessa direttiva NIS (NIS2) queste ultime -e quindi anche la crittografia- all'interno del perimetro della sicurezza cibernetica "a 360°".

Proponiamo pertanto di inserire una modifica al testo in discussione, che richiami, esplicitamente, tra le funzioni dell'Agenzia, quella di sviluppare azioni tese a rinforzare l'utilizzazione di soluzioni crittografiche a protezione delle comunicazioni e dei dati, nonché lo sviluppo di tecnologie in grado di assicurare la sicurezza dell'ambito crypto anche negli scenari dello sviluppo del computer quantistico, nonché a tutela del sempre maggior ricorso al cloud (crittografia omomorfica), sostenendo attraverso specifiche politiche il miglioramento ed il rafforzamento dell'industria nazionale e la valorizzazione di algoritmi proprietari e certificati, non solo nell'ambito delle informazioni riservate o classificate.

Cyber Deterrence

All'articolo 7, comma 1, lettera n), compare per la prima volta nell'ordinamento italiano il concetto di "risposta" agli attacchi cyber. Il tema è ripreso nell'ambito dell'articolo 9, comma 1, lettera b) ed è richiamato anche nella modifica al Decreto Legislativo NIS, contenuta all'articolo 15, comma 1, lettera q) punto 1), che ridefinisce le funzioni del CSIRT Italia.

All'articolo 10 comma 4, poi, si menzionano – ancor più chiaramente- le attività di "reazione", che -leggendo il testo- si capisce siano da considerarsi cose diverse da quelle di "stabilizzazione", da adottarsi di fronte ad un evento avverso di natura cibernetica.

Sebbene la lingua italiana possa essere soggetta alle interpretazioni, appare chiaro che il nostro Paese, con questo provvedimento, apre alla possibilità di portare a compimento operazioni di contro-offensiva cyber, vale a dire azioni che hanno come obiettivo quello di colpire le properties e le capabilities del soggetto ostile che ha portato un attacco cibernetico al nostro Paese o che stia per compierlo.

Tale assunto andrebbe meglio chiarito, sebbene già le formulazioni citate rappresentino un grande passo in avanti: è infatti necessaria maggiore chiarezza per evitare che vi siano difficoltà interpretative o dubbi di natura giuridica sulle regole d'ingaggio di questo tipo di operazioni. In particolare bisogna chiarire se questo tipo di operazioni sono o no esclusiva dell'ambito "Cyber Defense" e quindi prerogativa delle strutture delle Forze Armate, se l'Italia offre soluzioni tecniche per portare azioni di deterrenza e reazione in dote all'Alleanza Atlantica che ha recentemente chiarito che l'attacco cyber implica la possibilità per il membro NATO attaccato di invocare l'articolo 5 del trattato, se e come i soggetti privati industriali possono operare per fornire ai soggetti istituzionalmente preposti alle iniziative di deterrenza, prodotti o servizi pensati e progettati per tale scopo.