Nota Verbale - D.L. 82/2021 - Disposizioni urgenti in materia di cybersicurezza

Prof. Roberto Setola

Il D.L. rappresenta un significativo intervento in tema di cyber security consentendo di:

- Effettuare una **razionalizzazione** delle competenze attualmente disperse fra più amministrazioni, razionalizzazione fortemente richiesta e sollecitata dalla totalità dei soggetti privati e già indicata come elemento fondamentale da perseguire nel Piano Nazionale per la Protezione Cibernetica (DPCM 31 marzo 2017);
- Complementare il focus della normativa introducendo, oltre agli aspetti connessi con la disponibilità, confidenzialità ed integrità del dato e dei sistemi informatici anche la dimensione della **resilienza** tesa ad assicurare, in un'ottica di tutela dei servizi essenziali erogati alla popolazione, interventi di prevenzione, protezione e **ripristino** rispetto ad eventi e minacce cyber;
- Superare l'**anomalia** legata alla collocazione all'interno del DIS della governance nazionale in tema di cyber security;

Si precisa che il DIS nel corso di questi ultimi otto anni ha svolto in maniera egregia una funzione di supplenza/coordinamento della materia, riuscendo a dare un significativo impulso ad un tema che la stratificazione di leggi aveva disperso fra diversi soggetti. Il lavoro del DIS ha consentito sia di innalzare il **livello di attenzione** nei diversi soggetti pubblici e privati, sia di delineare linee di indirizzo ed attuare una normativa che è all'avanguardia nel panorama internazionale. Purtuttavia, la collocazione della materia all'interno del DIS appare non pienamente funzionale visto che il tema della cyber-security travalica i confini propri della cyber-intelligence, coprendo ambiti che richiedono una **forte cooperazione pubblico-privata** che mal si attaglia ai meccanismi di interazione propri di una agenzia di intelligenze.

La necessità di avere una più agevole cooperazione pubblico-privato, basata su una **condivisione delle informazioni bi-direzionali,** è uno degli aspetti, infatti, maggiormente evidenziati dagli operatori di infrastrutture critiche che sono stati interessati in merito alla recente proposta di direttiva sulla resilienza dei soggetti critici (tema sul quale si tornerà oltre). Aspetto questo che appare critico in relazione all'attuale collocazione della cyber-security nell'ambito dell'intelligenze e che è testimoniato anche dalla ventesima posizione dell'Italia nel **Global Cyber Security Index 2020** del International Telecommunication Union (ITU - Nazioni Unite) in conseguenza soprattutto dal ridotto livello di sviluppo delle *Technical Measures* a partire proprio dalle attività del CIRT (Computer Incident Response Team).

Da questo punto di vista si auspica, in accordo a quanto previsto dal D.L., che la costituenda Agenzia abbia gli strumenti per favorire questa collaborazione sia in ottica **pubblico-privato** che **privato-privato** sulla falsariga di quanto ad esempio realizzato dalla associazione AIPSA (Associazione Italiana Professionisti Security Aziendale) durante il Covid, in tema di condivisione di best practice di sicurezza.

Per altro, lo stesso testo normativo, in modo apprezzabile, prefigge fra gli obiettivi della Agenzia, in parallelo al rafforzamento tecnologico, la promozione del **fattore umano** partendo dalla cultura della cyber-sicurezza anche alla luce del fatto che diversi studi indiano che una quota compresa fra il 85% e 95%, di tutte le compromissioni a livello aziendale deriva da un errore umano non intenzionale. Si auspica quindi un ampliamento dei compiti della Agenzia anche per quel che riguarda la promozione di **percorsi di formazione** specifici, sia universitari che non universitari indirizzati tanto al settore pubblico che a quello privato, ovvero favorendo l'inserimento di competenze di cyber security all'interno di quelle previste nei tradizionali percorsi formativi.

Il D.L., con l'obiettivo di razionalizzazione e semplificazione, pone in capo alla costituenda Agenzia la quasi totalità delle attività che le precedenti normativa ponevano in capo al DIS e ai Ministeri competenti in tema

di cyber security. Al tempo stesso propone una formula, quelle delle Autorità di Settore, che consente di valorizzare le competenze di settore all'interno però di un framework unitario. Restano fra le prerogative dei Ministeri (e delle Autorità di settore) l'individuazione dei soggetti da includere ai sensi della normativa NIS e del perimetro nei relativi elenchi di soggetti da tutelare. Sarebbe auspicabile prevedere che, in aggiunta al processo di identificazione effettuato dalle Autorità di settore, l'individuazione di tali soggetti **possa essere espletato anche direttamente dalla Agenzia** (dalla Autorità Nazionale Competente NIS) al fine di poter meglio gestire realtà che operano su più settori, e prevedere, in presenza di società controllate, l'inclusione nel perimetro NIS della holding di gruppo.

Quanto occorso nel mese scorso all'oleodotto Canal Pipeline negli Stati Uniti (il cui funzionamento è stato interrotto per oltre una settimana) ed altri episodi di cyber-attack occorsi negli ultimi anni in danno ad **infrastrutture critiche**, evidenzia la necessità e l'urgenza di questo D.L. per rafforzare la resilienza del Paese di fronte alle minacce cyber. Alla luce di tali eventi, si sottolinea l'opportunità che la costituenda Agenzia si strutturi in modo da poter gestire, oltre alle problematiche di cyber security dei sistemi IT, anche quelle dei così detti sistemi **OT**, ovvero delle **Operational Technology**, cioè di quei sistemi (denominati PLC, SCADA, DCS, ecc.) che sovrintendono il funzionamento delle diverse infrastrutture come energia elettrica, gas, trasporti, ecc. Questi sistemi hanno specifiche caratteristiche, essendo stati progettati per interfacciarsi direttamente con i processi fisici e con una specifica enfasi sugli aspetti di safety. Peculiarità che rendono tali sistemi significativamente diversi rispetto ai normali sistemi IT ma, al tempo stesso, proni alle medesime classi di minacce. Tali peculiarità, unitamente al possibile impatto che una loro manipolazione dolosa potrebbe comportate sul benessere della popolazione, impone che all'interno della costituenda Agenzia vengano costituite specifiche competenze di informatica e automatica per poter fornire agli operatori di infrastrutture critiche adeguati supporti e linee di indirizzo.

Estremamente apprezzabile l'aver previsto la collocazione dell'Agenzia all'interno del perimetro pubblico ponendola sotto il controllo del Presidente del Consiglio per tramite dell'Autorità Delegata, sebbene al di fuori del perimetro dell'Intelligence. Il combinato disposto della legge 124 del 2007 e di questo D.L. fa sì che il soggetto a cui il Presidente del Consiglio conferisce la delega per la sicurezza della Repubblica coordini, al fine di garantire la sicurezza nazionale, sia le attività dell'intelligence che, come una sorta di seconda gamba, anche quelle dell'Agenzia per la Cybersicurezza, realizzando in questo modo un punto di raccordo politico tra quelle che sono le attività proprie dell'intelligence e quelle che sono le iniziative e le attività nel campo della cybersicurezza.

Occorre qui sottolineare che a livello europeo, come evidenziato anche nel dossier predisposto dalla Camera, sono in fase di valutazione due nuove direttive: una in tema di sicurezza delle reti e dei sistemi informativa (la così detta **NIS 2**), l'altra in tema di "**Resilienza dei Soggetti Critici"** (**CER**), che andrà a sostituire la direttiva sulle Infrastrutture Critiche. Tali testi evidenziano e sottolineano la necessità, che si spera possa trovare adeguato riscontro anche nell'ordinamento nazionale, di sviluppare in stretta sinergia gli aspetti di sicurezza cyber con quelli connessi con la sicurezza fisica delle infrastrutture critiche nazionali. Necessità che ha indotto la Commissione Europea a far evolvere in parallelo ed in stretta sinergia i due processi legislativi, prevedendo un forte **raccordo** ed un intenso **interscambio fra i soggetti deputati a livello nazionale** (Autorità Nazionali) **alla sicurezza cyber e quelli deputati alla sicurezza fisica**. Infatti, come evidenziato anche dal rappresentante del governo canadese durante un recente trilaterale EU-US-Canada in tema di infrastrutture critiche, la dimensione fisica e quella cyber "*cannot be divided*" rappresentando ormai un unicum.

Un'ultima chiosa riguarda il termine cybersicurezza. Nonostante il neologismo, è da ritenere preferibile al termine cibernetico, che ha un significato nella lingua italiana differente da "cyber", e dalla costatazione che non esiste un effettivo sinonimo nella lingua italiano al termine "cyber" che ha assunto il significato ben più ampio del termine "informatico" (il termine "cibersicurezza" – con la "i" al posto della "y", seppur suggerito ed argomentato, non appare avere riscontri nell'uso corrente, potrebbe di converso prendersi in considerazione la possibilità di utilizzare il temine cyber-sicurezza con il "-" trattino).