ApertaContrada
RIFLESSIONI SU SOCIETÀ, DIRITTO, ECONOMIA

Cybersicurezza e contratti pubblici. A proposito del volume di Stefano Rossa su Cybersicurezza e pubblica amministrazione.

di *Fulvio Costantino* - 23 Dicembre 2024

L'Amministrazione Biden mette al bando il software cinese installato sulle automobili, Mossad compie una strage in Libano attraverso esplosioni simultanee di semplici cerca-persone, Edward Snowden rivela che l'*intelligence* Usa aveva manomesso i cellulari di *leader* amici, tra cui l'allora cancelliera tedesca, per intercettarne le comunicazioni, un'operazione israelo-americana entra nei comandi informatici di una centrale nucleare iraniana guastandola: Questi esempi, citati in un recente articolo giornalistico[1], segnalano per un verso come non solo grandi elaboratori informatici e strutture, ma tutti i dispositivi elettronici, anche di uso comune, possano essere soggetti ad attacco informatico; per altro verso mostrano come gli attacchi informatici siano uno strumento di guerra, peraltro utilizzabile anche in periodo di pace, anche senza alcuna formalee dichiarazione di guerra né antecedente né successiva.

Il World Economic Forum[2], in un recente rapporto, ha osservato che non basta più la "sicurezza per progettazione" (by design) delle apparecchiature informatiche, in quanto c'è una necessità di adottare un approccio di "resilienza per progettazione", oltre la protezione, per garantire che i sistemi possano resistere e riprendersi dagli inevitabili attacchi sempre più evoluti. Risulta facile comprendere che non ci si deve illudere che si riuscirà a non essere attaccati, quanto invece essere in grado di adottare risposte adeguate.

Il medesimo Forum elenca i problemi che oggi ci si trova ad affrontare: il panorama tecnologico è in espansione, con oltre 200 tecnologie critiche, oltre l'intelligenza artificiale A e l'Internet of Things; è aumentata la superficie attaccabile, dal momento che avremo entro il 2030 32 miliardi di dispositivi connessi; l'Intelligenza artificiale è in grado di produrre avvelenamento dei dati, manipolazione dei modelli; il calcolo quantistico è in grado di superare gli attuali metodi di crittografia; ci sono vulnerabilità della catena di supporto. A questo elenco sono affiancate anche le raccomandazioni, di cui si tratterà oltre.

Se questo è il quadro, l'Unione europea si sta muovendo in una direzione ben definita. Come ha evidenziato un recente studio[3], a fronte della vulnerabilità agli *shock* derivanti dall'instabilità generale le risposte che attraverso le norme relative al settore tecnologico si vogliono dare sono tre: garantire la sovranità, potenziare l'industria interna, accumulare beni fisici o dati; in altri termini, sviluppare l'economia nell'interesse della sicurezza, riducendo rischi e dipendenze esterne. In questa direzione si sta mirando all'autonomia strategica nel settore dei semiconduttori, si dispone un quadro di *governance* dei dati, si adottano requisiti di conformità

alla sicurezza informatica dell'*hardware*. Nel primo senso la sicurezza informatica dipende dalla sicurezza dei materiali, e così le catene di fornitura per la produzione di semiconduttori e le materie prime devono essere introdotte nel territorio dell'Unione o essere sotto la sua influenza normativa. Nel secondo senso, i server di dati *cloud* e gli spazi dati comuni devono essere all'interno dello spazio fisico europeo o, se basati al di fuori di esso, devono essere soggetti a regole che mirino a limitare le minacce alla sicurezza presentate da stati terzi. Nel terzo senso, l'*hardware* che non soddisfi gli *standard* di sicurezza informatica non deve essere reso disponibile nel mercato interno.

Gli attacchi hanno interessato anche le imprese italiane: 273 nel primo semestre del 2024[4]. Dal 16 ottobre è in vigore in Italia la direttiva Nis 2, e le aziende più importanti (che detengono dati personali, segreti industriali o militari) devono adottare misure di sicurezza preventive. La direttiva si occupa di aziende con almeno 250 dipendenti e fatturato annuo superiore a 50 milioni di euro o asset a bilancio per più di 43 milioni di euro, ma si applica anche ad aziende di dimensioni più ridotte nei settori dell'energia, trasporti, bancario e finanziario, sanità, acqua potabile e reflua, infrastrutture e forniture di servizi digitali, fornitura e distribuzione di alimenti, servizi postali e di corriere, gestione dei rifiuti, telecomunicazioni, cultura: attività svolte da soggetti pubblici o da concessionari. In questo caso già è emerso il timore è legato ai costi dell'adeguamento[5].

Dal punto di vista nazionale, tra i vari temi, si è osservato come vi sia il rischio di una eccessiva concentrazione di potere in capo al Presidente del Consiglio dei Ministri[6]. L'autorità NIS, cioè l'ACN (Agenzia per la Cybersicurezza Nazionale) è stata istituita presso la Presidenza del Consiglio dei ministri. Inoltre si è rilevato come il COPASIR appaia inadeguato per garantire il controllo parlamentare dell'indirizzo in materia di cybersicurezza: ciò in quanto pensato per attività di *intelligence*, per cui deve operare con un elevato livello di riservatezza (i 5 deputati, 5 senatori, Presidenti della Camera e del Senato, che ne fanno parte sono obbligati al segreto), e in quanto comunque deve chiedere al Presidente del Consiglio informazioni e copie di atti o documenti a cui sia stato opposta la "riservatezza" in ragione del pericolo che essi possono procurare alla sicurezza della Repubblica. Si sono proposti come correttivi audizioni parlamentari pubbliche semestrali o quadrimestrali dell'ACN, oppure l'istituzione di una commissione parlamentare bicamerale *ad hoc* di controllo sull'attività del Governo, con ampia rappresentatività della composizione e pubblicità dei lavori, o l'istituzione di una Autorità indipendente, che si relazioni con il ministro dell'Interno[7].

Vi è anche chi ha criticato la presenza di molteplici agenzie, dipartimenti e organismi che si occupano di sicurezza informatica, nonostante la centralizzazione e il coordinamento prodotto grazie all'Agenzia per la Cybersicurezza Nazionale dal 2021, in quanto le responsabilità operative e strategiche sono ancora parcellizzate; così come si è suggerito di adottare linee guida per l'applicazione uniforme di standard di sicurezza elevati a tutte le amministrazioni pubbliche e di creare un SOC (Security Operation Center) per la PA; rimane poi il problema di migliorare l'applicazione della disciplina sui dati personali alle amministrazioni nazionali.

Il volume per più della metà è dedicato ai contratti pubblici. La scelta è significativa: senza un accorto impiego dei corretti strumenti normativi e procedurali, non avremo un'evoluzione

adeguata del settore. L'autore accompagna il lettore per mano in mezzo a pagine del Codice dei contratti e della normativa europea purtroppo ignote a molti giuristi e amministratori italiani, con un approccio non descrittivo, ma cercando di dare un contributo reale alla soluzione di problemi, segnalando i pregi e i difetti, nonché gli ambiti di operatività, degli strumenti a disposizione (l'accordo quadro, appalto precommerciale, appalto di soluzioni innovative, l'appalto transfrontaliero, il partenariato pubblico privato, il partenariato per l'innovazione).

L'esame conduce inevitabilmente ai grandi nodi dell'amministrazione e del diritto amministrativo: il problema non è ovviamente solo nell'approccio autoritativo che si contrappone a un approccio collaborativo, perché nessuno si aspetta certamente che settori come la sicurezza di infrastrutture, sistemi, dati non siano intrisi di momenti affidati al controllo e all'operato autoritativo.

A monte i problemi sono che la velocità dei progressi tecnologici sfida la normativa, che mancano competenze adeguate nella pubblica amministrazione, che vi è un approccio burocratico difensivo, che vi è un problema di risorse. Appare inoltre chiara la necessità di recuperare un approccio pianificatorio e di assumere rischi.

Vi sono inoltre i problemi, al di là di quanto indicato dall'autore, delle ombre del nazionalismo digitale, del già citato eccessivo accentramento dei poteri presso la Presidenza del Consiglio.

Le soluzioni esposte nel volume, se le rapportiamo con quelle del più recente rapporto del *World Economic Forum*, sono dello stesso tenore: bisogna investire in ricerca e sviluppo; servono collaborazione tra governo, industria e (un aspetto sottolineato in particolare dal *Forum*) mondo accademico; è necessario un miglioramento delle competenze; le norme devono promuovere la sicurezza tramite progettazione, facilitare la cooperazione internazionale, standardizzare le pratiche di sicurezza informatica anche per migliorare l'interoperabilità tra i settori; va pianificata la resilienza informatica, con *test* di piani di risposta agli incidenti; si devono stabilire strutture di *governance* per guidare lo sviluppo e l'implementazione responsabili delle tecnologie emergenti, integrando i processi di valutazione e gestione dei rischi durante tutto il loro ciclo di vita; servono monitoraggio e adattamento continuo.

Anche un recente *paper* italiano sulle telecomunicazioni va nella stessa direzione: serve una strategia nazionale orientata alla resilienza delle reti, con il coinvolgimento dei diversi attori interessati[8] e bisogna promuovere investimenti in ricerca e sviluppo tramite partnership pubblico-private.

Serve un'attenzione costante a questo campo, e studiosi che se ne occupino in maniera duratura.

[1] Esempi menzionati da F. Rampini, *E l'America vieta il software cinese. La nuova cyber-guerra*, Corriere della sera, 24.9.2024.

[2] World Economic Forum, *Navigating Cyber Resilience in the Age of Emerging Technologies: Collaborative Solutions for Complex Challenges*, 2024.

[3] B. Farrand, H. Carrapico, A. Turobov, *The new geopolitics of EU cybersecurity: security, economy and sovereignty*, *International Affairs*, 2024 ,2379.

[4] Rapporto Clusit, 2024, https://clusit.it/rapporto-clusit/

[5] A. Longo, *Cyber sicurezza ecco le nuove regole*, *La Repubblica – Affari e Finanza*, 14.10.2024.

[6] L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, *Federalismi.it*, 2024.

[7] Moroni, cit. sulle prime due proposte; M. Ferrari, *Diritti costituzionali e cybersicurezza*, *Corriere della sera*, 3.11.2024 sulla terza.

[8] Aspen Institute Italia, *Le reti di comunicazione fra cybersicurezza, resilienza e tutela della sicurezza nazionale*, 2024.
