***03 aprile 2024***

***Audizione informale nell’ambito del disegno di legge C.1717 Governo, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, dell’Ing. Domitilla Benigni, Presidente di CY4Gate S.p.A. e CEO/COO di Elettronica S.p.A.***

Egregio Presidente, on. Pagano, Vi ringrazio per l’occasione di confronto, riflessione e approfondimento che avete voluto offrire a Cy4Gate S.p.A., tramite me, su un tema così delicato e cosi attuale quale quello della cyber sicurezza nazionale in un momento storico, peraltro, segnato da guerre in diverse aree della terra in cui la *cyber warfare* è divenuta uno degli elementi caratterizzanti e a volte decisivi nelle sorti di un conflitto c.d. “ibrido”.

Internet ha rivoluzionato il mondo in una sola generazione, trasformando il modo in cui comunichiamo e condividiamo informazioni su scala globale, creando un fiorente ecosistema digitale, interconnesso con le economie, le società e gli individui e si sono creati oramai tutti i presupposti per una collaborazione globale in tempo reale.

Se da un lato vi è oggi grande consapevolezza sul fatto che l’interconnettività sia foriera di importanti opportunità, non si è consci in maniera altrettanto capillare dei rischi che la globalizzazione digitale ha introdotto. La velocità con cui un attacco informatico oggi è in grado non solo di essere lanciato e sortire i suoi effetti, ma anche di propagarsi globalmente in ogni settore e su ogni latitudine senza che vi siano appropriate barriere tecnologiche in grado di opporvisi, è un tema che va tempestivamente affrontato e gestito, di pari passo con la poderosa “avanzata” del digitale.

Se questo è il contesto, in Italia il legislatore ha già da tempo preso consapevolezza ed è corso ai ripari con la realizzazione di un quadro normativo e di governance della cyber sicurezza che è quantomeno in linea con i Paesi Europei.

Con il mio intervento desidero, più che individuare soluzioni su una problematica complessa e che richiede un approccio olistico attraverso l’integrazione di più prospettive, dare il punto di vista di chi – dal lato dell’industria high tech già digitalizzata ed attiva nella realizzazione di prodotti per la sicurezza cibernetica – vive la tematica della resilienza tanto nella veste di potenziale target di *threat actors* che di provider di soluzioni per chi si deve difendere.

Entrando nel vivo della discussione, **plaudo al disposto normativo di cui all’art.7** in materia di **partnership pubblico-privato**. Intendo fare espresso riferimento alla disposizione con cui si riconosce all'Agenzia Nazionale per la Cyber Security il ruolo di promotore dello sviluppo di iniziative, volte a valorizzare l'IA come risorsa fondamentale per il rafforzamento della nostra sicurezza nazionale, includendo l’impiego di forme di partenariato pubblico-privato. E aggiungerei che questa forma di collaborazione vada incentivata non solo su AI ma estesa anche a tutti gli altri aspetti della cyber security.

L’attribuzione all’Agenzia per la cybersicurezza nazionale (ACN), fulcro del sistema di governance della nostra cybersecurity, di un ruolo chiave nell’azione di indirizzo e guida su iniziative in tema di AI anche tramite partenariato pubblico-privato è un primo importante segnale nella giusta direzione: coordinare e accentrare gli sforzi su un unico Ente, evitando dispendio di risorse e tempo e assicurando efficacia ed efficienza nel programmare e implementare, è il primo fondamentale tassello per migliorare le capacità di risposta alle minacce emergenti e più insidiose. E ancor più importante è poterlo fare incentivando la cooperazione tra il mondo pubblico e privato.

Si tratta di una collaborazione indubbiamente apportatrice di reciproci benefici: le Istituzioni, dal canto loro, possono indirizzare le aziende esprimendo appropriatamente le esigenze operative da tramutare in requisiti tecnici e finanziando anche parzialmente le iniziative di innovazione; le aziende, invece, sono in possesso di quelle necessarie risorse tecnologiche e umane (con sistemi di reclutamento oggi quanto meno più rapidi rispetto al settore pubblico e in grado di colmare più agevolmente gap di competenze) che si rendono fondamentali per lanciare e implementare iniziative di ricerca e sviluppo *lean* che conducano all’implementazione di soluzioni avanzate di AI per la sicurezza cibernetica e seguano anche l’evolversi della tecnologia e della minaccia colmando tempestivamente le obsolescenze che in questo settore avanzano a ritmi serrati.

Inoltre, l’intima interconnessione pubblico-privato funge da agevolatore nella gestione degli incidenti e delle crisi: mentre il ruolo dello Stato è prioritariamente quello di predisporre un quadro legislativo che aiuti nella pianificazione della resilienza (e il disegno di legge odierno ne è un esempio) e nell’individuazione di meccanismi più snelli per la condivisione delle informazioni, il settore privato può avere un impatto molto efficace nella risposta tempestiva agli attacchi, soprattutto grazie alla massiva raccolta di informazioni, rafforzata come detto dalle competenze tecnologiche avanzate e dall’AI che oggi ancora non sono cosi diffuse nel settore pubblico. Ne deriverebbe una maggiore facilità nello scambio di informazioni in tempo reale tra i due settori, indispensabile per la gestione tempestiva ed efficace di incidenti informatici.

I tempi sono maturi affinché cadano le barriere che ancor oggi si frappongono ad una strutturata e diffusa collaborazione tra le Istituzioni e le aziende e ciò sarà reso possibile se:

● vi sarà chiarezza nell’obiettivo: le parti dovranno definire sin da subito gli obiettivi attesi, che solitamente tra pubblico e privato divergono e richiedono una mediazione. Idealmente, l’obiettivo di fondo dovrebbe tendere alla protezione del cyberspace e dunque il partenariato dovrebbe affrontare tutte le questioni per la realizzazione della sicurezza informatica, sviluppare capacità di prevenzione, risposta e ripristino contro gli attacchi informatici. Oggi spesso i partenariati si sostanziano nella condivisione di informazioni e nel coordinamento della risposta agli incidenti, ma sarebbe utile allargare la portata di queste collaborazioni e ricomprendere obiettivi di più ampia portata, sia in termini di ricerca e sviluppo di strumenti tecnologici per affrontare le minacce, sia nella preparazione del personale in questo settore, che da sempre rappresenta un profondo gap da colmare. Inoltre, è importante che la collaborazione sia fondata su una base giuridica comunemente accettata dalle parti (un atto giuridico o un memorandum d’intesa). Perché il partenariato abbia successo, è necessario che tutti i partecipanti conoscano esattamente il quadro giuridico in cui muoversi;

● saranno individuati i giusti partner: la scelta dei partner è sicuramente un punto fondamentale per la realizzazione degli obiettivi dichiarati. Circa i rappresentanti della sfera pubblica, questi dovrebbero partecipare attivamente e conferire un apporto significativo in termini di conoscenze e risorse stabilmente e in via esclusiva allocate alle specifiche attività oggetto della partnership; dovrebbero essere coinvolti i rappresentanti di qualsiasi livello, dalle amministrazioni locali ai livelli più alti, perché la cybersecurity coinvolge tutti gli strati dell’amministrazione. Dal lato privato, sarebbe vantaggioso coinvolgere anche le piccole e medie imprese (PMI) che spesso non hanno la forza e la visibilità per essere chiamati a contribuire a questo tipo di collaborazioni, ma nell’ottica di aumentare il livello di protezione generale delle infrastrutture critiche digitali, sarebbe proficuo interessare anche questi attori, che possono comunque apportare un contributo importante e contemporaneamente acquisire buone pratiche da chi possiede e gestisce infrastrutture digitali ritenute asset nazionali strategici. La sfera privata dovrebbe, infine, comprendere anche stakeholders provenienti dal mondo accademico e della ricerca.

E in chiusura su questa specifica tematica, **con particolare riferimento all’AI,** mi sento di stimolare tutti noi a non voler perdere il treno della leadership tecnologica in questo settore. Siamo stati nel mondo i precursori nel disciplinare l’AI con l’**AI ACT**, il **regolamento europeo** sull’AI. Ma dobbiamo spingerci oltre, investendo e mobilitando ogni risorsa e competenza per **realizzare l’AI**, mettendo a frutto la capacità creativa di cui siamo capaci in Italia e in Europa. Non possiamo essere followers anche in questo dominio come è accaduto per le tecnologie di cyber security. E qui faccio mio il pensiero di Alec Ross, già consigliere del presidente Barack Obama per le politiche tecnologiche, il quale sul tema dell’innovazione ebbe provocatoriamente a dire che bisogna rifuggire dal paradigma consolidato per cui **gli USA innovano, la Cina copia e l’UE regolamenta**.

Un altro tema chiave che mi sta a cuore, è il **tema delle risorse umane**. Non vi può essere innnovazione avanzata, non esiste sovranità tecnologica nazionale o europea in un settore d’avanguardia come la cyber sicurezza, se non siamo in grado come sistema Paese di esprimere un potenziale di competenze in grado di colmare l’enorme gap creatosi nel dominio cibernetico a livello europeo e mondiale.

Erano 5,5 milioni i professionisti della cyber security operativi a livello globale a fine 2023, con una crescita dell’8,7% rispetto al 2022, pari a circa 440.000 posti di lavoro in più generati. E nonostante si tratti della cifra più alta mai raggiunta, a livello globale il divario tra la forza lavoro di cui il settore necessita e quella effettivamente disponibile ha toccato la soglia record di quattro milioni di lavoratori.

Ciò spiega il perché i datori di lavoro tanto nel privato quanto nel pubblico si trovino ad affrontare la c.d. “guerra dei cyber-talenti”, contendendosi risorse umane la cui scarsità è una delle concause della lentezza con cui si riesce a contrastare il crimine cibernetico.

A tal proposito, il disegno di legge in trattazione, **con l’art. 9 introduce limiti all’assunzione** per due anni da parte di aziende private di personale ACN che sia stato qualificato tramite corsi di formazione specialistica, onde porre un freno al turn-over di personale verso il mercato privato.

Si tratta a mio giudizio di un **rimedio “tattico” e di breve periodo** che non risolve una problematica di più ampia portata come sopra descritta. Per affrontare con successo la nostra sfida, servono piani strutturati e politiche di incentivazione che mirino (i) ad un ben più ampio coinvolgimento delle donne e dei giovani in questo settore e (ii) agevolino l’accesso al lavoro nel dominio cyber anche a chi risiede in aree del Paese caratterizzate da basso tasso di industrializzazione e minor presenza di Istituzioni pubbliche con esigenze di competenze cyber. Molti di questi lavori, infatti, non richiedono necessariamente l’aver completato un percorso di laurea né la prestazione di un’attività lavorativa in presenza. Idonee politiche inclusive permetterebbero quindi di allargare il bacino di reclutamento.

E se lo Stato deve fare la sua parte, anche l’iniziativa privata e su base volontaria può giocare un ruolo rilevante e mi riferisco ad associazioni che sappiano svolgere opera di awereness ed “evangelizzazione” sul tema della cyber. Mi sia permesso citare, in tal senso, l’iniziativa **“Women4Cyber Italia”,** ormai entrata nel suo terzo anno di vita operativa.

Abbiamo costituito, nel 2021, con un gruppo di colleghe e professioniste del settore, il capitolo italiano di cui sono Presidente, dell’omonima Fondazione europea Women4Cyber, nata nel 2019 in seno a ECSO (European Cyber Security Organization) con l’obiettivo di contribuire a colmare il divario di genere dei professionisti della cybersecurity a livello europeo.

Abbiamo voluto essere le prime ad incoraggiare e promuovere la formazione, il miglioramento delle competenze delle studentesse e delle professioniste verso il settore cyber, nell’ambito delle discipline STEM, quali ingegneria ed ICT, dove attualmente la presenza femminile è più bassa. Abbiamo oggi l’ambizione di rappresentare un network di riferimento anche per la riqualificazione professionale di donne specializzate nelle discipline umanistiche (psicologia, relazioni internazionali, giurisprudenza, scienze politiche, economia), che possono trovare nel cyber l’opportunità di apportare delle competenze complementari a quelle tecniche, oggi sempre più necessarie ad approcciare un dominio che assume crescente carattere di interdisciplinarietà.

Infatti, mi piace ricordare in questo contesto come la cybersecurity si sia da tempo affrancata dall'immagine stereotipata dell' "hacker" quale unico detentore del sapere di dominio; la soluzione alle tematiche cyber sin qui descritte passa necessariamente per un approccio olistico in cui la diversità di competenze in un team apporta valore ed accresce la capacità di problem solving e di contrasto al fenomeno degli attacchi cibernetici.

Un accenno infine **sull’art. 18** **che stabilisce l’"invarianza di bilancio".**

Un disegno di legge che intitola il capo I con “Disposizioni in materia di **“rafforzamento”** della cybersicurezza nazionale, **“resilienza”** delle pubbliche amministrazioni, personale e funzionamento dell’Agenzia per la cybersicurezza nazionale”, come potrà assicurare un rafforzamento e una maggior resilienza della P.A. senza dotarla di risorse finanziarie aggiuntive, considerando che quelle già stanziate sono insufficienti a colmare i fabbisogni connessi alle esigenze di tutela degli interessi strategici della nazione?

L'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano ha recentemente evidenziato un dato di rilievo: nel 2023, il mercato italiano della cybersecurity ha raggiunto un nuovo record, toccando i 2,15 miliardi di euro, con una crescita del 16% rispetto all'anno precedente.

Il rapporto tra la spesa in cybersecurity e il PIL italiano è ora dello 0,12%, in aumento rispetto al 2022 (quando era dell'0,10%). Tuttavia, nonostante questo incremento, il nostro Paese rimane ancora fanalino di coda nel G7, distante anni luce dai primi classificati come gli Stati Uniti (0,34%) e il Regno Unito (0,29%), nonché da nazioni come la Francia e la Germania (entrambe all'0,19%).

Sebbene il 62% delle grandi organizzazioni ha aumentato gli investimenti in cybersecurity, trainato dall'adozione di nuovi strumenti (68%), da una maggiore attenzione da parte dei consigli di amministrazione (62%) e dalla necessità di adeguarsi alle normative (43%), le piccole imprese, che rappresentano l’80% del tessuto imprenditoriale nazionale, stentano a realizzare investimenti concreti nella cyber, a causa delle risorse limitate e della mancanza di offerte di mercato adatte alle loro esigenze specifiche. La spesa sostenuta dalle grandi imprese rappresenta da sola infatti oltre tre quarti del mercato complessivo.

È quindi opportuno bilanciare gli obiettivi a breve termine con una visione a lungo termine, delineando chiaramente la direzione da intraprendere. Da un lato, dobbiamo proteggere i sistemi esistenti, mentre investiamo nella costruzione di un ecosistema digitale futuro intrinsecamente più difendibile e resiliente, portando a bordo le PMI che rappresentano l’anello debole della catena nel contesto della cyber security.

E questo obiettivo è perseguibile con coraggiosi investimenti pubblici in cybersecurity, complementati certamente dal settore privato delle large enterprise che hanno fatto e stanno facendo la loro parte.

**In conclusione**, il valore intrinseco di questo disegno di legge sulla cybersecurity nazionale si eleva proporzionalmente alla capacità di darsi una visione di lungo periodo e di implementare una strategia chiara, dichiarata e partecipata da tutte le forze in gioco che l’Italia può esprimere, con il pieno coinvolgimento delle proprie Istituzioni, aziende e istituti di ricerca e formazione.

Si tratterà di fare “sistema Paese”, consolidarlo attraverso una stretta collaborazione tra settore pubblico e privato che vinca ogni sorta di remora al dialogo e sappia togliere spazio a quelle componenti di burocrazia non necessarie che costituiscono un limite al fiorire dell’innovazione e della realizzazione di progetti strategici e di lungo periodo. Il tutto nella consapevolezza che in questo settore non si può essere autarchici e, fatto salvo l’interesse strategico nazionale, si dovrà sempre guardare all’Europa come la naturale sede di coordinamento e di creazione di sinergie di competenza e tecnologiche per mantenere un vantaggio competitivo e accrescere le capacità di difesa contro le minacce cibernetiche globali.

In questo contesto, il decreto rappresenta un decisivo passo in avanti di un percorso lungo e impervio, che richiederà un forte commitment di tutte le componenti della società civile per garantire un futuro digitale sicuro e prospero a tutti i cittadini e istituzioni del nostro Paese.

Il settore privato è pronto a fare la propria parte e a supportare le Istituzioni con competenza, esperienza, tecnologia e risorse, a tutela degli interessi strategici nazionali e per assicurare l’ordinato e sicuro svolgersi della vita civile.

Ringrazio tutti per l’opportunità offertami e per l’attenzione riservatami.