(AFFARI COSTITUZIONALI, DELLA PRESIDENZA DEL CONSIGLIO E INTERNI)
26 marzo 2024

Audizione informale nell'ambito dell'esame del disegno di legge C. 1717 Governo, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, di: Luigi Garofalo, direttore responsabile di Cybersecurity Italia

Egregi Presidenti, on. Nazario Pagano e on. Ciro Maschio, grazie per l'invito. È un onore per me illustrare le mie proposte per contribuire a migliorare il disegno di legge in esame.

Un disegno di legge che dimostra che la cybersicurezza è nell'agenda del Governo, ma che è finito nell'agenda dei media solo per lo scandalo e poi l'inchiesta spionaggio nei confronti di alcuni ministri e diversi politici e personaggi famosi.
Non ci fosse stata questa inchiesta, il disegno di legge di rafforzamento della cybersicurezza nazionale e di reati informatici non avrebbe fatto notizia sui giornali e TG generalisti.

<u>Questo perché manca nel nostro Paese la cultura della cybersicurezza.</u>
Manca nei media generalisti, dove fa notizia solo "l'attacco hacker", che poi non sono hacker ma criminali informatici sempre più spesso assoldati da Stati che considerano l'Italia una Nazione ostile e cercano di sferrare cyber attacchi contro le nostre infrastrutture critiche per creare impatto rilevante, come già è avvenuto.
Manca la cultura della cybersicurezza nei cittadini, negli studenti, mentre, pian piano, sta crescendo nei lavoratori delle Pubbliche Amministrazioni e delle aziende private.
La cybersecurity è sempre più cruciale per le nostre vite, perché attiene alla sicurezza nazionale e internazionale, garantisce il business per le imprese, l'erogazione dei servizi digitali delle PA e la navigazione sicura e libera degli utenti online.

E il disegno di legge in esame non prevede nulla per alimentare sempre più la cultura della cybersicurezza nel Paese.
Che può sembrare “aria fritta”, ma invece se aumenta la cultura della cybersecurity nel Paese: in particolare, nelle PA, nelle aziende, tra voi Parlamentari, allora di sicuro aumenteranno le difese cyber dell’Italia.
Perché? Perché se si raggiunge questa consapevolezza allora il legislatore automaticamente va a prevedere fondi pubblici nuovi, ad hoc, per rafforzare la cyber-resilienza dell’Italia.
Mentre il ddl in esame è limitato dalla clausola di invarianza finanziaria. Ma come?
Il disegno di legge aumenta, giustamente, i soggetti da inserire nel perimetro di sicurezza nazionale cibernetica (dai Comuni con la popolazione superiore ai 100mila abitanti, ai Capoluoghi di Regione, alle ASL – tra le più colpite dai criminali informatici – alle in-house) ma non prevede fondi pubblici nuovi per “accompagnare” questi soggetti a conformarsi agli obblighi previsti.
Il disegno di legge in esame introduce anche, ottimamente, il Referente per la Cybersicurezza per avere una comunicazione veloce e competente tra le PA e l’Agenzia per la Cybersicurezza Nazionale. Ma senza una quota cyber ad hoc le PA faranno molta fatica ad attrarre professionisti della cybersicurezza per ricoprire questo ruolo.
Sono molto d’accordo con chi, alla recente Conferenza “CyberSec” organizzata dal giornale che dirigo, ha lanciato la seguente proposta: “Serve un PNRR della cybersicurezza”. Una provocazione? No. Fa capire l’esigenza di prevedere una quota cyber in ogni nuova norma sulla transizione digitale, ecologica e ovviamente su norme verticali sulla cybersicurezza come il Ddl in esame.
Chi può pensare di ampliare la propria villa al mare senza prevedere anche un ampliamento del sistema di allarme?
Quello che avviene offline, avviene anche online.
Basterebbe, per esempio, richiamare e concretizzare quanto previsto nella Strategia di Sicurezza Nazionale Cibernetica, a pagina dodici, che fissa i fondi nazionali in una quota annuale pari almeno all’1,2% degli investimenti pubblici.

La prima parte del provvedimento è, quindi, sostanzialmente una anticipazione della normativa di recepimento della Direttiva NIS2 all'interno dell'ordinamento italiano, con alcuni task significativi e senza dubbio positivi. Come già detto, le nuove norme infatti vanno ad individuare un "super-perimetro" che comprende al suo interno i soggetti NIS1, i soggetti del Perimetro di Sicurezza Nazionale Cibernetica ed altre entità che vengono esplicitamente elencate e che non appartengono a queste categorie. Proprio questo elemento ulteriore è molto interessante perché affronta alcune linee di presidio attualmente scoperte (anche se in prospettiva coperte dalla Direttiva NIS2): i Comuni sopra i 100.000 abitanti e le rispettive in-house e poi le società di trasporto pubblico locale con analogo bacino.
A tal proposito è necessario sottolineare, dal mio punto di osservazione, come sia necessario chiarire il tema delle in-house, anche in prospettiva NIS2.
La mera partecipazione azionaria, infatti, non è un criterio molto efficace per la definizione del perimetro di sicurezza, che invece è più influenzato dal settore di attività e dall'oggetto del servizio più che dalla "natura giuridica" che connota il rapporto tra Comune e soggetto imprenditoriale (in-house).
In particolare si dovrebbe far riferimento a tutti i servizi esternalizzati, a prescindere se essi siano esternalizzati nella formula dell'in-house providing o meno. Peraltro la dicitura "in-house" rischia di essere equivoca e non richiamare in maniera definita ad una precisa ed unica fattispecie. Meglio sarebbe riferirsi alle società affidatarie o concessionarie di servizi essenziali, escludendo invece società in-house che potrebbero essere affidatarie di servizi non particolarmente critici o comunque non inclusi nella direttiva NIS2.

La seconda parte del disegno di legge in esame, invece, è relativa all'incremento delle pene per i reati di cyber crime oltre a creare nuove fattispecie di reato.
Il Sottosegretario alla Presidenza del Consiglio dei ministri e anche Autorità delegata per la sicurezza della Repubblica **Alfredo Mantovano** durante la conferenza stampa in cui ha presentato il disegno di legge in esame ha detto, testualmente. *"La legislazione vigente prevede sanzioni penali veramente esigue, tanto che al cybercriminale conviene fare attacchi piuttosto che rubare la frutta al mercato, con il sistema delle attenuanti e dei riti abbreviati parliamo di pochi mesi di reclusioni, che non si espiano".*
Tra le nuove fattispecie di reato previste particolarmente rilevante è il tema di cui all'articolo 1, lettera p) che introduce un nuovo articolo nel Codice Penale, 635 quater.1, che introduce il reato di detenzione, installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
L'articolo in questione pone una serie di questioni di tipo interpretativo e rischia di determinare, nella sua versione attuale, alcuni paradossi.

Innanzitutto, sotto il profilo interpretativo è necessario che venga meglio chiarito e specificato il concetto espresso dall'avverbio "abusivamente". Cosa significa esattamente, quale fattispecie precisa individua? In particolare, nell'articolato è presente nella identificazione delle condotte oggetto di reato in questi termini *"…abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa…".* L'avverbio "abusivamente" è da leggersi come intrinsecamente giustapposto a ciascuna di queste singole fattispecie? Vale a dire "*abusivamente si procura, [abusivamente] detiene, [abusivamente] produce… (etc..)" ?*
Oppure esclusivamente alla fattispecie cui è esplicitamente associato "*abusivamente si procura"?* L'incertezza interpretativa potrebbe portare ad effetti pratici paradossali. Ad esempio alla non occorrenza del reato quando la pratica delittuosa sia portata attraverso uno strumento informatico detenuto legittimamente, ma usato illegittimamente.

Al contrario, è possibile, soprattutto nell'ambito di talune fattispecie, che il concetto di "abusività" sia difficilmente circostanziabile. Se ben chiaro è il significato di "abusivamente si procura" (evidentemente relativo ad una appropriazione in qualche modo indebita o in violazione di leggi vigenti), non è chiaro cosa dia vita ad una abusiva detenzione, ad una abusiva produzione (non essendo la professione di sviluppatore una professione regolata o il cui esercizio è sottoposto al possesso di un particolare titolo), "abusiva consegna" o "abusiva messa a disposizione di altri".
Sempre ragionando in tema di interpretazione, tale nuovo reato si verifica sotto la condizione che i fatti in oggetto si verifichino "allo scopo di danneggiare illecitamente un sistema informatico". Per cui la semplice occorrenza delle fattispecie prima descritte non integra da sola la dinamica delittuosa ma deve essere "asservita" all'intentum (al solo intentum, non è necessario che il danno si manifesti, basta "lo scopo di…") malevolo di "danneggiare illecitamente".
A tal proposito è necessario sottolineare, anche in questo caso, si pongano dei dubbi interpretativi nella comprensione del sintagma "danneggiare illecitamente", che indurrebbe a pensare che esista - e che quindi sia scriminata - l'ipotesi di "danneggiare lecitamente". Interpretare in questo senso è auspicabile, poiché in molti casi l'attività di cybersecurity potrebbe portare a svolgere talune delle attività sopra richiamate, ma non a scopo malevolo, bensì a scopo difensivo. Tuttavia se questo era l'intento del proponente, la formulazione non è certamente delle più chiare ed immediate, soprattutto se pensiamo al fatto che, nell'ordinamento italiano, non è prevista la legittima difesa cibernetica.
Proprio questo può essere il punto di svolta del provvedimento: il riconoscimento del legittimo ricorso all'uso del mezzo informatico per difendersi da una azione violenta che metta a rischio la sicurezza del singolo o di altri ovvero i beni ovvero il domicilio, sebbene digitale.
Come già detto quello che avviene offline, avviene anche online.

Poiché nel diritto penale non si procede per analogia è necessario intervenire in tal senso, dal mio punto di vista, per disporre esplicitamente a vantaggio dei cittadini il diritto di difesa, già previsto nella vita cinetica, anche in quella cibernetica, agendo sull'articolo 52 del Codice Penale nelle forme che il Parlamento riterrà più opportune.
Senza questo intervento, l'effetto paradossale del nuovo Art. 635 quater.1 del Codice, ma anche di molti degli altri articoli che vengono modificati con inasprimento delle pene, potrebbe essere quello di porre nella condizione gli attori malevoli di denunciare i soggetti che operano nell'ambito della cyber resilienza e che, attraverso specifiche attività, potrebbero compiere una delle azioni indicate dal nuovo articolo come delittuose.
L'esempio concreto è quello di un Red Team (difesa attiva) che agisca per far cessare un attacco informatico, potrebbe incorrere nel reato - non essendo disposta la fattispecie del "danneggiamento lecito"- per danneggiamento illecito delle capacità dell'attaccante.
Ancora, il servizio di Cyber Threat Intelligence che recupera nel dark web informazioni che consentono di sventare un attacco informatico potrebbe incorrere nella fattispecie dell' "abusivamente si procura", non essendo definito quando sia invece consentito il "procurarsi" dati, informazioni etc. E così di seguito.
Inoltre l'assetto normativo nuovo potrebbe mettere a rischio la professione e l'attività di penetration testing. Quella cioè in cui un soggetto viene ingaggiato per testare, attraverso un attacco concordato, le difese di un sistema informatico. Anche in quel caso vi sono condotte "offensive" non supportate però da un intento doloso. Certamente non si vuole vietarle, ma il rischio è quello di determinare un'inversione dell'onere della prova in relazione allo "scopo" per il quale si detiene una determinata capacità o si effettua una determinata azione.

Infine, un’osservazione su cybersicurezza e intelligenza artificiale. Il disegno di legge attribuisce all’ACN una nuova missione, la funzione di valorizzare l’intelligenza artificiale per il rafforzamento della cybersicurezza nazionale. Bene.

Siamo nell’era dell’intelligenza artificiale e l’AI può essere sì utilizzata, quindi con un approccio positivo, per rafforzare la cybersicurezza dell’Italia e dei Paesi alleati. Ma manca nel ddl la parte in cui soggetti designati lavorino in team per risolvere le vulnerabilità cyber dei sistemi di intelligenza artificiale.
Il **NIST** (National Institute of Standards and Technology), nel suo più grande lavoro di ricerca svolto per lo sviluppo dell’Intelligenza Artificiale affidabile, ha individuato i 4 tipi di cyber attacchi ai sistemi di intelligenza artificiale che possono manipolarli per causare, per esempio, incidenti delle auto connesse fino all’esfiltrazioni dei dati degli utenti che usano i chatbot basati sull’AI generativa.

L’Intelligenza Artificiale è sì il game changer.

Ma la cybersicurezza è la pre-condizione essenziale per avere l’intelligenza artificiale sicura e affidabile. E anche in questo il disegno di legge in esame può fare la sua parte.

Termino qui il mio intervento e resto a disposizione per eventuali domande da parte dei componenti delle due Commissioni.