Testo dell'Audizione I e II Commissione della Camera dei Deputati, A.C.n.1717 di Elisabetta Zuanelli, 27 marzo 2024

Prof. Elisabetta Zuanelli

Già Ordinario di Comunicazione digitale, Professore Emerito

Macroarea Economia, Dipartimento di Management e Diritto

Università degli Studi di Roma, "Tor Vergata"

Dal 2016, Coordinatore del partenariato per la formazione in *Cyberthreat*, *cybersecurity, privacy*

Esperto ONU in Intelligenza artificiale (Digital Transformation Roadmap)

Esperto NATO, dal 2022 Membro STO Technical Team: SAS-IST-179 on Semantic Representation to Enhance Exploitation of Military Lessons Learned

Il provvedimento in esame presenta un duplice oggetto tematico: il 'rafforzamento della cybersicurezza' e i 'reati informatici', contenuti diversi seppur tematicamente correlati.

Sui reati informatici (artt. 11, 12 e17)

Parrebbe auspicabile uno scorporo dei 'reati' informatici, segnatamente gli artt. 11, 12 e17 che prevedono modifiche al codice penale, procedura penale e tipologie dei reati. Il lavoro istruttorio contempla un auspicato inasprimento delle pene e una tipizzazione dei reati ascrivibili a soggetti persona.

Sarebbe utile una riflessione complessiva sulla **perseguibilità** del *cybercrime*, con particolar enfasi sugli attacchi che investono la sicurezza dello Stato. Attacchi *cyber* di questa natura non corrispondono, di norma, all'azione di singole persone bensì ad azioni delittuose realizzate da filiere del cyber-crimine localizzate nel mondo in aree geo-digitali nelle quali non è applicabile giurisprudenza nazionale.

Si potrebbe ipotizzare una Procura europea del *cybercrime*, analogamente a quella relativa a frodi finanziarie (EPPO), collateralmente alla quale si potrebbe immaginare una struttura europea di negoziazione a fini giudiziari sull'applicabilità di norme, come, ad esempio, fu fatto

per il GDPR. Ciò ai fini di perseguire con qualche efficacia il *cybercrime* in contesti transoceanici ed europei stessi.

Sul rafforzamento della cybersicurezza

Il **'**rafforzamento' sembra conseguirsi nell'articolato in questione mediante tre principi: obblighi di notifica, segnalazioni e adeguamento alle segnalazioni ACN

Art. 1 (Obblighi di notifica di incidenti)

Il comma 1 specifica che gli incidenti da segnalare sono quelli indicati nella 'tassonomia' di cui all'articolo 1, comma 3-bis, del decreto-legge n. 105 del 2019: la **tassonomia andrebbe aggiornata e rivista in chiave specificamente classificatoria.**

Il comma 5 individua la **sanzione amministrativa pecuniaria** per la reiterata inosservanza dell'obbligo di notifica da un minimo di 25.000 a un massimo di 125.000 euro.

Anche ammettendo che la sanzione pecuniaria operi come deterrenza per il non adempimento degli obblighi previsti verso amministrazioni periferiche, occorrerebbe valutare la **fattibilità dei controlli relativi** alla pletora di soggetti implicati. Per la procedura 'sanzionatoria' si fa riferimento a un prospettico DPCM la cui potenziale farraginosità aumenterebbe l'onere burocratico piuttosto che garantire la snellezza essenziale dei procedimenti amministrativi implicati.

Art.2 (Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale)

Nel caso specifico ovvero la previsione di:

i. **sanzioni pecuniarie per mancato o ritardato adeguamento a segnalazioni dell'ACN**
ii. **obbligo di adeguamento segnalazioni ACN**

si pone il quesito rinnovato sulla **quantità e la qualità delle risorse umane necessarie per i controlli** ma si pone un quesito più generale in relazione alla **responsabilità specifica di eventi e incidenti di *cybersecurity*.**

È noto che le grandi amministrazioni centrali e regionali, i grandi comuni e le aziende che erogano servizi essenziali, le ex infrastrutture critiche, si avvalgono regolarmente di 'consulenze' di gestione della *cybersecurity*.

Per 'consulenze', possiamo intendere sia i '*vendor'* di tecnologie di base e gestionali, sistemi operativi, app, *cloud*, ecc.; sia i '*vendor*' di Rete nonché i consulenti gestionali dei processi istituzionali, aziendali e di sicurezza dei vari SOC, SIEM, CERT e CSIRT.

Impensabile controllare o svolgere eventuali *audit* sui *vendor* di rete, i *vendor* di prodotti e servizi, la consulenza gestionale sui processi istituzionali e aziendali e l'acquisizione di tecnologie di difesa ***cybersecurity*** e **protezione dei dati**, quali, ad esempio le **tecnologie di monitoraggio degli asset, IDS, IPS, firewall, antimalware, antivirus, antispam**, ecc.

Le ragioni sono molteplici.

Non solo le ***high tech*** possiedono tutto il *know how* disponibile nel mercato ma sono talora 'certificate' da istituzioni non nazionali o autocertificate.

Del tutto inimmaginabile, dunque, l'attivazione di *team* nazionali per il 'controllo' dei 'giganti' che sono tali a ragione dell'imponenza e rilevanza globale del loro sviluppo tecnologico.

Pur tuttavia, ad oggi, come segnalato dal DoD (*Department of Defense*) statunitense, dal *Department of homeland security* e dalla MITRE Corporation **non esistono standard della cybersecurity** riconducibili all'analisi e alla potenziale classificazione degli IoC o degli IoA (rispettivamente indicatori di compromissione e attacco) segnalati dalle tecnologie di difesa della cybersicurezza.

Tipologie di dati, classificazione e analisi degli stessi sono svolte manualmente. Non esistono in commercio piattaforme ontologiche di AI per la difesa, necessarie per la rappresentazione della conoscenza, la prevenzione e la predittività degli eventi e/incidenti, i *trend* di rischio, ecc.

Piattaforme diverse in Rete danno **analisi dei dati relativi agli stessi incidenti diverse.**

A tale proposito, segnaliamo l'urgenza e l'utilità di incentivare realtà nazionali che sviluppino tecnologie prototipali di rappresentazione delle minacce, condivisione di informazioni e reportistica degli incidenti, necessarie a realizzare attività di *assessment* e valutazione del rischio nonché soluzioni preventive e predittive di attacchi, con investimenti specifici del tipo pubblico-privato. Piccole e medie imprese, accademie e centri di ricerca nazionali possono concorrere utilmente al rafforzamento della cybersicurezza, con piani anche sperimentali di applicazioni operative.

Il tema che si pone, dunque, è la **responsabilizzazione dei *vendor* di rete, dei *vendor* di sistemi operativi, di app e di *device* vari**, dal cloud ai cellulari aziendali, e dal sistema della consulenza gestionale rispetto alle 'notifiche'.

In altri termini, si tratterebbe di **distinguere** tra rischi ed incidenti connessi a errori di configurazione generati dagli operatori aziendali e istituzionali stessi, ai vari livelli, mancati aggiornamenti, errori comportamentali degli addetti da un lato; e responsabilità gestionali e consulenziali di 'beni', prodotti e servizi digitali, inclusi quelli della sicurezza, dall'altro.

Il quesito è **come integrare efficacemente ai fini del rafforzamento della sicurezza e delle notifiche** i due binari di responsabilità ovvero quello dell'istituzione, ente o azienda, e quello dei *vendor* di prodotti, servizi e consulenza di processi e tecnologie di difesa.

Una possibile soluzione sta **nell'ampliare e nel riorganizzare il perimetro delle certificazioni** e **autocertificazioni** di sicurezza dei *vendor*, della consulenza e dei *reseller*. A questi occorrerebbe chiedere **relazioni strutturate annuali di tendenza** *cybersec* da far rifluire in una piattaforma in AI di monitoraggio e di tendenza previsionale dei dati pervenuti.

Quanto agli avvisi ACN, essi dovrebbero esser già noti ai *vendor* e alle consulenze e andrebbero inserite nella suddetta piattaforma**.**

Restano fuori da questo circuito **le amministrazioni periferiche, che non dispongono né di risorse né di competenze, e le *supply chain*** che dovrebbero ricadere nella capacità di controllo **delle aziende di servizi essenziali e delle amministrazioni 'forti'.**

Per queste realtà, si potrebbe ipotizzare una **piattaforma di autocertificazione minima**, facilitando il tema dei controlli e aggiornando nel tempo la stessa, anche a fini statistici nazionali.

Un' attenzione specifica è dunque estendere le segnalazioni e le notifiche alle *supply chain* senza intenti o implicazioni sanzionatorie

Art. 5 (Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale)

"Ai sensi delle citate lettere, l'Agenzia per la cybersicurezza nazionale esercita le seguenti funzioni:

- sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il Gruppo di intervento per la sicurezza informatica in caso di incidente – CSIRT di cui all'articolo 8 del decreto legislativo 18 maggio 2018, n. 65 (cosiddetto decreto legislativo "NIS"), ed anche promuovendo iniziative di partenariato pubblico-privato (lettera n));

- nell'ambito delle funzioni appena citate, svolgere ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici (lettera n-bis)).

sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il Gruppo di intervento per la sicurezza informatica in caso di incidente –

CSIRT di cui all'articolo 8 del decreto legislativo 18 maggio 2018, n. 65 (cosiddetto decreto legislativo "NIS"), ed anche promuovendo iniziative di partenariato pubblico-privato (lettera n), "ecc.

Questo imponente elenco di competenze è oggetto di un previsto differimento di funzioni in casi particolari.

Un riordino meditato dei compiti e delle procedure in relazione al tema della sicurezza nazionale tra agenzie e strutture di intelligence e ACN dovrebbe facilitare la pronta gestione di eventi particolarmente pericolosi per la sicurezza nazionale.

Art.7 (Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di intelligenza artificiale)

L'articolo 7 inserisce tra le funzioni dell'Agenzia per la cybersicurezza nazionale – ACN la "valorizzazione dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale"**.**

Il tema dell'applicazione dell'AI Act, in corso di pubblicazione nella GUE, di complessa e globale rilevanza posto che rivoluzionerà prodotti, servizi e funzionalità di sistema nel mercato attuale e prospettico, meriterà, si immagina, **un'attenzione normativa specifica,** in particolare per le implicazioni di *compliance* che potrebbero paralizzare il mercato degli operatori, data l'inconsistenza tipologica del rischio su inesistenti analisi di scenario *ex post* e su prodotti e servizi AI valutabili in tal senso.

Per altro verso, si noti che la norma ISO 42001 sull'AI ha paradossalmente anticipato la norma AI ancora in fase conclusiva, prefigurando complesse *compliance* aziendali in materia.

Sui temi inerenti alla *cybersecurity* e all'AI, va ricordata l'indicazione ENISA, da noi discussa in un'apposita Conferenza, conferenza che l'Università di 'Tor Vergata' svolge annualmente in materia di *cybersecurity* e protezione dei dati e relata al Master interdisciplinare in Cybersecurity, protezione dei dati e privacy. La Conferenza 2021 intitolata ad **AI e cybersecurity** (www.ai4a.eu/conferenze) è visibile al sito indicato. Essa raccoglie contributi di studiosi e imprese con le visioni problematiche qui solo accennate.

Sinteticamente, il rapporto problematico AI *cybersecurity* si può riassumere in tre considerazioni sollecitate da ENISA:

1. l'allargamento del perimetro di 'insicurezza' cibernetica nell'AI, considerato il bottino potenziale di contenuti in piattaforme di milioni e miliardi di dati e relativi danni;

2. l'opportunità di sviluppo di piattaforme di rappresentazione della conoscenza ovvero di ontologie AI a scopi preventivi e predittivi degli incidenti di *cybersecurity* e per metriche efficaci di valutazione del rischio, applicazioni di *vulnerability assessment*, soluzioni di resilienza proattiva e rimediale, ecc.;

3. il rischio rappresentato dall'utilizzo da parte dei cybercriminali di modellistica AI per attacchi cyber.

Nella fattispecie AI, sappiamo che attacchi alle basi di conoscenza provocano danni quali allucinazioni della macchina, distruzione e deformazione dei dati con pericolose conseguenze applicative.

Sul tema AI e più in generale per lo sviluppo di un sistema complessivo di competenze e risorse, sarebbe opportuna l'incentivazione dell'acquisizione di personale specializzato:

- con giovani qualificati attraverso cicli di **alta specializzazione** per lo sviluppo specifico AI e applicazioni nei diversi settori e
- con **alte professionalità** provenienti dal mondo della ricerca e dello sviluppo

Il tema della carenza numerica e della qualità del personale necessario comporta per ACN una prospettiva di incentivazione delle risorse acquisibili e acquisite che contraddice quanto previsto all'Art. 9.

Su tale articolo, le professionalità acquisibili da personale delle amministrazioni dello Stato non dovrebbero inibire le carriere del personale medesimo, distaccato, chiamato e acquisito a qualunque titolo.

A tale personale dovrebbe essere garantito il mantenimento della progressione di carriera dalla quale proviene e l'eventuale ricollocazione nella stessa.

Art.8 (Procedimento sanzionatorio per le violazioni in materia di cybersicurezza di competenza dell'Agenzia)

"Le modalità di svolgimento delle ispezioni saranno disciplinate con determinazione del direttore generale dell'Agenzia pubblicata nella "Gazzetta Ufficiale". "

L'art. 8 pone i problemi già evidenziati ovvero la potenziale farraginosità del procedimento sanzionatorio da definire e l'esistenza di **addetti numericamente e qualitativamente** preposti allo scopo per i controlli a fini sanzionatori.

Art.10 (Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici)

Una sola perplessità ovvero quali sarebbero gli elementi 'essenziali' per la valutazione della cybersicurezza di beni e servizi informatici nei contratti pubblici nel contesto di tutela di interessi nazionali strategici e come sarebbero definiti?

Art.11 (Modifiche al codice penale)

Sui reati, importante la stretta delle pene.

Restano escluse le filiere di *cybercrime* **che non sono perseguibili giurisdizionalmente a ragione della dispersione geo digitale dei cybercriminali.**

Risposte ai Quesiti dei Deputati, On.li Elena Boschi e On. Le Alfonso Colucci

Sui rapporti Agenzia ACN, soggetti di intelligence e sicurezza della Repubblica (CISR, Autorità delegata, DIS, AISE, AISI, art. 4) e Magistratura va forse **rimeditato il criterio di competenza**, approfondendo la **distinzione in ordine alla notifica, alle tipologie di incidenti, ai procedimenti giudiziari inerenti reati informatici, all'interpretazione tecnologica dei fatti imputati e alla natura degli interessi nazionali strategici e ai responsabili.**

Una distinzione tipologica essenziale, inoltre, riguarda **l'uso di strumenti informatici e il danno/ impatto da attacchi** perpetrati anche da soggetti esterni al territorio nazionale.

La tipologia dei reati *cybersecurity* si può riassumere nella valutazione generale del danno apportato da un attacco ovvero **l'esfiltrazione di dati, lo spionaggio, la modifica dei dati, la distruzione dei dati, il blocco delle attività gestionali fino alla distruzione di sistemi nel caso di infrastrutture critiche quali il servizio elettrico, il bancario, le telecomunicazioni, la sanità o il nucleare ove esista, ecc.**

Non esistendo standard di analisi e classificazione dei dati a fini preventivi e predittivi se non liste parziali di indicatori e sistemi di controllo anch'essi parziali, auspicabile l'opportunità di

investire in **progetti e prodotti preventivi e predittivi**, come si riscontra in ambito internazionale, con intese progettuali pubblico-privato.

Circa l'applicazione della norma AI, il tema è di corposa rilevanza e va declinato nel biennio di acquisizione del contenuto normativo, non solo sotto il profilo della *cybersecurity* ma anche e soprattutto sull'applicabilità di norme di controllo e rischio nei prodotti e servizi offerti da *vendor* e *reseller*.

Ciò che preoccupa è l'applicabilità della norma al pregresso ovvero alle installazioni già operative di applicazioni di AI, diffuse nei contesti di alte amministrazioni e infrastrutture critiche e nei servizi delle *high tech* già in opera quali, ad esempio, motori di ricerca, *chat bot*, identificazione biometrica su pc e cellulari, ecc. ma anche sistemi di profilazione a vari fini, compresi quelli sociali e politici, ecc.

Si ricorda che il diritto alla spiegazione (*the right to explanation)* ovvero il diritto di chiedere una valutazione umana rispetto a potenziali discriminazioni automatiche era già contenuto nei considerando del GDPR 2016.

Venendo al **valore di deterrenza della sanzione pecuniaria**, non si può non ricordare la stessa irrisoria quantificazione delle sanzioni, rispetto al GDPR, inserita nel recepimento della NIS.

Quanto ai **riferimenti europei**, ricordiamo la pletora di norme alle quali il provvedimento in esame deve raccordarsi quali le normative di settore specifico e norme specifiche sulla protezione dei dati e la *cybersecurity* quali la NIS 2, il GDPR, il *Cyber act*, Dora, la *data governance*, i servizi digitali, ecc.

Problema fortemente avvertito a livello europeo è la disomogeneità di acquisizione della norma, come nel caso della NIS che ha generato la NIS 2.