AGENZIA PER LA CYBERSICUREZZA NAZIONALE

COMMISSIONE PARLAMENTARE PER LA SEMPLIFICAZIONE

Contributo audizione del Direttore Generale
nell'ambito dell'*"Indagine conoscitiva in materia di semplificazione e digitalizzazione delle procedure amministrative nei rapporti tra cittadino e pubblica amministrazione*"

28 novembre 2024, ore 8:15

PREMESSA

- La digitalizzazione delle procedure rappresenta un fattore abilitante per la semplificazione amministrativa la quale, a sua volta, costituisce un indubbio vantaggio per migliorare il rapporto tra cittadino e Pubblica Amministrazione (PA). In questo mio intervento mi concentrerò sui profili di competenza dell'Agenzia per la cybersicurezza nazionale (ACN) relativi a questo ampio e articolato tema, approfondendo in particolare i rilevanti risvolti di sicurezza cibernetica, nonché quanto sta facendo l'ACN per contribuire allo sforzo della macchina pubblica nel senso di una digitalizzazione sicura.
- La digitalizzazione non è più una novità, ma la sua ampiezza e intensità sta aumentando progressivamente, traslando nella dimensione digitale un numero sempre maggiore di attività e processi che precedentemente erano svolti esclusivamente in maniera analogica. In questa transizione la pandemia di COVID-19 si è rivelata un fenomenale acceleratore, spingendo online realtà che non si pensava potessero essere digitalizzate, come l'istruzione.
- Se per molti versi le nostre vite sono tornate alla normalità, per altri i cambiamenti introdotte dalla pandemia sono ormai irreversibili. Anche se non utilizziamo più il green pass o l'app Immuni, i cittadini possono ormai contare su prescrizioni mediche smaterializzate e sull'impiego dell'identità digitale pubblica per l'accesso a un numero sempre maggiore di servizi pubblici, dal pagamento della TARI ai versamenti previdenziali, dalle pratiche della motorizzazione al libretto universitario.
- Questi sono solo alcuni esempi delle numerose attività che sono state semplificate grazie alla digitalizzazione. Di pari passo con la semplificazione, tuttavia, tale processo ha comportato anche un'enorme espansione della nostra superficie digitale e, quindi, dei potenziali rischi alla nostra sicurezza cibernetica. Ogni informazione o processo che si svolga in rete, infatti, è esposto a una certa misura di rischio che, purtroppo, non può essere mai eliminato del tutto. Può essere però ridotto, anche in maniera consistente, ed è questa la missione dell'Agenzia per la cybersicurezza nazionale.
- La reale semplificazione dell'attività amministrativa può essere effettivamente perseguita solo laddove vengano utilizzati sistemi sicuri e resilienti, che consentano la regolare e ininterrotta interazione tra il cittadino e la PA, nel rispetto, oltre che dei noti principi di efficienza ed

efficacia dell'azione amministrativa, anche dei diritti del cittadino, incluso quello alla riservatezza dei propri dati. Ne va del rapporto fiduciario tra cittadino e PA.

- Difatti, come lo Stato deve garantire che le strade e le città siano sicure, deve anche far sì che i cittadini possano usufruire della rete – tanto più dei servizi pubblici in rete – con il massimo grado di sicurezza possibile. Il processo di trasformazione digitale della Pubblica Amministrazione, dunque, non può prescindere da considerare la cybersicurezza delle infrastrutture tecnologiche "*by default e by design*".
- Già il Codice dell'amministrazione digitale (CAD), nella sua prima versione del 2005, aveva incluso la sicurezza dei sistemi informatici e dei dati (al fine di garantirne l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza) tra gli elementi da tenere in considerazione nella digitalizzazione dei processi della Pubblica Amministrazione.
- La sicurezza informatica è stata, inoltre, inserita tra i pilastri del Piano triennale per l'informatica nella Pubblica Amministrazione, fin dalla sua prima edizione. Alla luce delle evidenti sinergie tra quanto portato avanti da AgID nell'ambito di tale Piano e della rilevanza trasversale della cybersicurezza per tutte le aree del Piano, l'Agenzia è oggi chiamata a fornire un contributo di competenza per far sì che il Piano risponda sempre alle esigenze di supportare la trasformazione digitale del Paese in sicurezza. Questo contributo riguarda anche le modalità in cui la cybersicurezza potrà essere pienamente valorizzata nel processo di adozione dell'intelligenza artificiale (IA) da parte della Pubblica Amministrazione.
- Con l'evoluzione della digitalizzazione e della stessa minaccia cibernetica, sono stati via via adottati anche nuovi atti normativi in materia di cybersicurezza, tra cui quelli di derivazione europea (di recepimento delle direttive NIS e NIS2) e il Perimetro di sicurezza nazionale cibernetica (D.L. n. 105/2019), i quali, sotto diversi profili, hanno disposto obblighi relativi all'adozione di misure di sicurezza e alla notifica degli incidenti per i soggetti pubblici inclusi nell'ambito di applicazione.
- La vigilanza sulla sicurezza cibernetica del Paese condotta dall'ACN tramite la propria struttura tecnico-operativa CSIRT Italia ha fatto rilevare nei primi dieci mesi del 2024, infatti, una minaccia *cyber* contro soggetti nazionali che appare in crescita rispetto al 2023.
- Il cono di visibilità di cui gode l'Agenzia comprende non solo quanto disponibile sulle fonti aperte e tramite i servizi commerciali di *cyber threat intelligence*, ma anche informazioni condivise da articolazioni tecniche nazionali e da omologhi internazionali oltre a quanto notificato dai soggetti nazionali mediante le segnalazioni di incidente previste per legge. A quest'ultimo riguardo, occorre evidenziare un progressivo allargamento dell'ambito soggettivo dell'obbligo di notifica operato del legislatore proprio al fine di poter avere una migliore conoscenza situazionale.
- Alle notifiche obbligatorie si accompagnano quelle volontarie tramite le quali i soggetti che abbiano subito un incidente possono sempre far sapere all'Agenzia i dettagli della compromissione, contribuendo così a un più efficace allertamento di altri soggetti che

potrebbero incorrere nella medesima minaccia e a una più completa attività di *remediation* degli eventuali effetti avversi.

- Le Pubbliche Amministrazioni, sia centrali che locali, sono tra gli obiettivi principali degli *hacker*, anche se ciò dipende in parte dal fatto che tali soggetti sono molto spesso chiamati a notificare gli incidenti dalle normative summenzionate, anche in ragione del danno che questi possono generare. Contro la PA si sono registrati attacchi di tipo DDoS ad opera di attivisti, nonché di matrice criminale, come spesso accade nel caso dei *ransomware*. Questi ultimi, come sappiamo dalle cronache, hanno spesso effetti dirompenti sull'operatività dei servizi e, dunque, sulla fruizione da parte dei cittadini dei servizi pubblici, come nel caso di quelli ospedalieri.

RISPOSTE ACN

- È per far fronte a questa situazione che l'Agenzia è attiva su molteplici fronti, tra i quali:

1) Allertamento e supporto

- Compito essenziale del CSIRT Italia è allertare i soggetti a rischio, sia tramite canali *ad hoc* che attraverso il sito web, nonché intervenire a sostegno delle vittime per aiutarle a riattivare reti e servizi. Per questo il CSIRT Italia invia comunicazioni ai soggetti a rischio e pubblica *alert* sul proprio sito.
- Il CSIRT Italia svolge, inoltre, un'intensa attività di supporto alle Pubbliche Amministrazioni, centrali e locali, vittime di eventi *cyber*. In vari casi, opera anche presso le PA con specifiche squadre d'intervento.

2) Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente

- Il legislatore ha inteso, inoltre, consolidare quanto disposto dalle normative citate in precedenza – il Perimetro di sicurezza nazionale cibernetica e il d.lgs. di recepimento della Direttiva NIS – ampliando progressivamente, a nuovi soggetti, obblighi di cybersicurezza, aggiornandoli, altresì, all'evoluzione tecnologica. Nel 2024 sono state adottate nuove normative di settore che hanno dato un significativo impulso al rafforzamento del livello di cybersicurezza della Pubblica Amministrazione, aggiungendo nuovi obblighi e aggiornando gli *standard* di sicurezza richiesti per l'operatività delle infrastrutture digitali. Si tratta, nello specifico, della legge n. 90/2024, "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", e del decreto legislativo n. 138/2024, di recepimento della Direttiva NIS2 (Direttiva UE 2022/2555).
- In particolare, la legge n. 90/2024 è tesa ad anticipare o comunque a creare i presupposti per una efficace adozione di molte delle misure che rappresentano il cuore della disciplina della NIS2. La logica su cui si muove la legge n. 90/2024 è quella di aumentare la superficie digitale protetta delle Pubbliche Amministrazioni, anche locali, con una strategia di

accompagnamento delle stesse nell'azione di rafforzamento dei propri profili di cybersicurezza, sia con riferimento agli obblighi che alle corrispondenti sanzioni.

- Sempre in un'ottica di accompagnamento, l'ACN ha di recente pubblicato dedicate linee guida che specificano le misure di sicurezza che i soggetti individuati dalla legge n. 90/2024 devono applicare per rafforzare le proprie capacità di identificazione, protezione, rilevamento, risposta e ripristino in ambito *cyber*. A queste si aggiungono le linee guida pubblicate dall'Agenzia il 25 novembre scorso per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio, documento che va a dettagliare le misure di sicurezza, già presenti nel PSNC, e riporta esempi utili alla loro implementazione pratica.
- Nel descritto quadro di "trasferimento" di compiti e attività nella dimensione digitale, la riforma normativa operata dalla direttiva NIS2, che mira a raggiungere un livello comune elevato di cybersicurezza dei soggetti nel territorio dell'UE, e dal d.lgs. n. 138/2024 di recepimento, rappresenta un ulteriore passo fondamentale nel rafforzamento dei livelli di cybersicurezza anche della PA. La NIS2, infatti, ha ricompreso la Pubblica Amministrazione "nella sua interezza" quale nuovo settore incluso nell'ambito di applicazione della direttiva, avendo cura di prevedere meccanismi di gradualità e proporzionalità anche in relazione all'effettiva esposizione ai rischi degli specifici soggetti.
- I soggetti pubblici ai quali si applicherà la NIS2 saranno, dunque, tenuti ad adottare le nuove e più stringenti misure di gestione del rischio individuate dalla direttiva – di natura tecnica, operativa e organizzativa – tra cui quelle relative alla sicurezza della catena di approvvigionamento e alle politiche e procedure relative all'uso della crittografia, e, ove opportuno, della cifratura, oltre che a notificare gli incidenti che abbiano un impatto significativo sulla fornitura dei loro servizi.
- Oltre alle citate normative di settore, l'ACN è chiamata a emettere dei pareri in molteplici ambiti in relazione agli aspetti di cybersicurezza coinvolti nel processo di trasformazione digitale della Pubblica Amministrazione. Diversi provvedimenti hanno infatti previsto il coinvolgimento dell'Agenzia come ente chiave per garantire la sicurezza informatica nelle iniziative di semplificazione e digitalizzazione della PA.

3) Investimenti: PNRR e Fondi Strategia

- L'Agenzia è attiva, inoltre, nel sostenere con interventi concreti la digitalizzazione sicura del Paese, anche tramite l'allocazione di risorse finanziarie indispensabili a tal fine.
- Ne sono un esempio gli investimenti del PNRR che, nella sua Missione 1 Componente 1, dedica significative risorse alla digitalizzazione, innovazione e sicurezza della PA. In tale ambito, alla cybersicurezza è riservato un finanziamento specifico – l'Investimento 1.5 "Cybersecurity" dalla dotazione totale di 623 milioni di euro – di cui l'ACN è Soggetto attuatore. Tramite il finanziamento di specifiche progettualità funzionali a tale Investimento, l'ACN sta accompagnando le Pubbliche Amministrazioni verso un miglioramento della propria resilienza cibernetica, sviluppando servizi *cyber* nazionali per potenziare

monitoraggio, allertamento e risposta agli incidenti e rafforzando la rete di laboratori di scrutinio e certificazione tecnologica.

- Ad oggi l'ACN ha raggiunto tutti gli obiettivi (4 *milestone* e 1 *target*) fissati entro la scadenza del 31 dicembre 2022 e sta lavorando alacremente per poter rispettare la scadenza del dicembre 2024 entro la quale andranno completati gli ulteriori obiettivi (3 *milestone* e 1 *target*).
- Un altro primario strumento finanziario a sostegno della cybersicurezza delle Pubbliche Amministrazioni è rappresentato dal Fondo per l'attuazione della Strategia nazionale di cybersicurezza e da quello per la gestione della cybersicurezza, istituiti dalla legge di bilancio per il 2023 (legge n. 197/2022).
- Tra tali fondi e le risorse PNRR l'Agenzia, complessivamente, ha destinato alle Pubbliche Amministrazioni varie centinaia di milioni di euro. Grazie a tali risorse l'Agenzia ha potuto, tra le altre cose, coordinare numerose iniziative volte a potenziare la postura di cybersicurezza delle PA, riuscendo a produrre risultati concreti in termini di protezione e resilienza.

4) **Formazione e *awareness***

- L'ACN è molto attiva anche nel campo degli investimenti nel capitale umano, nella consapevolezza che la conoscenza è la vera protezione del Paese nel lungo periodo. Abbiamo infatti una grande necessità di professionisti ICT che possano essere impiegati dalle Pubbliche Amministrazioni, nonché dalle aziende che in Italia fanno innovazione, a partire dalle più grandi fino ad arrivare a quelle piccole e medie. Abbiamo anche necessità di rafforzare le competenze di chi è già nel mondo del lavoro e che non è in grado di cogliere appieno le potenzialità della tecnologia o – peggio ancora – costituisce l'anello debole della catena di infezione perché non adeguatamente formato alla sicurezza cibernetica. Ma è l'intera cittadinanza che deve diventare più consapevole dei rischi della rete e più resiliente, grazie a pratiche di "igiene cibernetica" che risultano orami ineludibili per chi utilizza gli strumenti digitali per piacere oltre che per lavoro.
- L'ACN sta collaborando con il Ministero dell'istruzione e del merito e con quello dell'università e della ricerca, nonché con i diversi *partner* istituzionali pubblici e privati, per dare una risposta concreta all'esigenza di maggiori conoscenze e competenze *cyber* a tutti i livelli.
- In quest'ottica si iscrive un'importante iniziativa a sostegno della formazione in materia *cyber* del personale della PA, che ha visto l'Agenzia collaborare con il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri per realizzare dei moduli formativi, fruibili in materia autonoma da tutti i dipendenti della Pubblica Amministrazione.

5) La cybersicurezza delle tecnologie innovative: *cloud*, crittografia e intelligenza artificiale

- L'ACN è a fianco della PA per supportarla nella transizione verso tecnologie sempre più innovative, in particolare, ora, attraverso la realizzazione del c.d. "*cloud* nazionale" che

prevede la migrazione su piattaforme *cloud* qualificate dei dati e dei servizi pubblici. Di recente è stato adottato, con decreto del Direttore generale dell'ACN del 27 giugno 2024, il nuovo Regolamento per le infrastrutture digitali e per i servizi *cloud* per la Pubblica Amministrazione, che stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per le Pubbliche Amministrazioni e le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi *cloud* per le Pubbliche Amministrazioni; lo stesso decreto individua, altresì, i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni.

- L'Agenzia è, quindi, coinvolta in tale trasformazione in quanto responsabile per la valutazione della conformità di infrastrutture digitali e servizi *cloud*, nell'ambito del cosiddetto processo di qualificazione. I dettagli sui servizi qualificati possono essere consultati sull'apposito catalogo, disponibile sul sito web dell'ACN, dove le Pubbliche Amministrazioni che vogliono procedere all'acquisizione di un servizio *cloud* possono trovare tutte le informazioni, incluso il livello di classificazione concesso.
- L'ACN è, inoltre, attiva sotto il profilo della promozione dell'utilizzo della crittografia per elevare gli *standard* di cybersicurezza, non da ultimo attraverso la pubblicazione di specifiche linee guida sulle soluzioni crittografiche più all'avanguardia. Alla luce dell'evidente complementarietà tra la sicurezza cibernetica e la protezione dei dati personali, uno di questi documenti è stato pubblicato congiuntamente con il Garante per la protezione dei dati personali.
- Guardando, infine, all'intelligenza artificiale, il nostro Paese sta investendo in termini di sviluppo ma anche di regolamentazione. A livello europeo è stato approvato l'*AI Act* che impatterà sulle strutture pubbliche, sia in termini di limiti e prerogative nell'utilizzo di prodotti legati all'IA sia per quanto riguarda le attività di vigilanza e di certificazione.
- È, inoltre, in corso di esame al Senato il DDL AI (A.S. 1146), il cui dettato prevede che la cybersicurezza dei sistemi e dei modelli di intelligenza artificiale dovrà essere assicurata quale precondizione essenziale, secondo un approccio proporzionale e basato sul rischio, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo.
- Sia a livello europeo che nazionale, in sostanza, si sta considerando la rilevanza della cybersicurezza in termini di garanzia per un efficace utilizzo di una tecnologia che potenzia le capacità e le competenze e, tuttavia, al tempo stesso, aumenta la superficie di rischio dei processi e dei sistemi da questa interessati. In un'ottica di semplificazione nella fruizione dei servizi, quindi, l'intelligenza artificiale pur essendo uno strumento dalle infinite potenzialità, può essere utilizzato solo a patto di aver stabilito, nella migliore delle ipotesi da principio (*security by design*), una cornice di cybersicurezza all'interno della quale assicurare il suo dispiegamento.