Poliziamoderna

Sicurezza digitale

Si stima che oggi siano oltre 30 miliardi i dispositivi connessi a Internet. Ma il numero è destinato a crescere vertiginosamente, complice la pandemia che ha reso le nostre interazioni sempre più virtuali. Secondo studi di settore il numero di apparecchi connessi nel mondo salirà a 200 miliardi nel 2030, facendoci entrare nella cosiddetta fase dell'*hyper connectivity*. Anche i sistemi statali, come le persone, sono sempre più cybernetici: Istituzioni, infrastrutture, procedure burocratiche e concorsuali, tutto viaggia alla velocità dei bit. Ma se i vantaggi offerti dalla digitalizzazione sono sotto gli occhi di tutti, non altrettanto può dirsi dei rischi a essa associati. Dalle *intelligence* straniere ostili, pronte a carpire il materiale riservato delle nostre Amministrazioni, alle organizzazioni criminali che rubano i nostri dati personali per perseguire i propri scopi illeciti, il dominio cibernetico è divenuto, negli anni, terreno di confronto e di scontro, oltre che strumento di crescita.

A rendere più pericoloso l'utilizzo delle nuove tecnologie occorre aggiungere la disinvoltura con la quale gli utenti approcciano il mondo digitale, rispetto a quanto praticato nella "vita reale". Basti pensare alla superficialità con la quale spesso prestiamo il consenso all'utilizzo dei dati personali, rispetto invece alle cautele che poniamo quando evitiamo di esporre il nostro cognome sul citofono di casa. Ed è la cronaca a riportare numerosi casi di attacchi informatici: solo per citarne alcuni possiamo ricordare quello di aprile dello scorso anno, in piena pandemia, ai server dell'Inps e quello alla Regione Lazio, che ha colpito, questa estate, il sistema delle prenotazioni vaccinali. Non è di molti giorni fa, poi, l'attacco alla Siae culminato in richieste estorsive ad alcuni artisti dei quali erano stati carpiti i dati personali.

L'esigenza di rispondere efficacemente a queste istanze di sicurezza è stata avvertita già da molti anni in diversi Paesi europei. Basti ricordare che, in Germania, l'Agenzia federale per la cybersicurezza (Bsi) è stata creata nel 1991 mentre in Francia l'Agenzia nazionale per la sicurezza dei sistemi informativi (Anssi) è stata istituita nel 2009. Con queste premesse nel nostro Paese, con il decreto legge n. 82 del 14 giugno 2021 (convertito con la legge del 4 agosto 2021, n. 109), è stata istituita l'Agenzia per la cybersicurezza nazionale (Acn). Questa dovrà definire le strategie di cybersicurezza nazionale, porre la sicurezza e la resilienza cibernetiche a fondamento del processo di digitalizzazione del Paese, promuovere la cultura della cybersicurezza e stimolare la creazione di una solida forza lavoro nazionale, nonché mantenere relazioni bilaterali e multilaterali partecipando attivamente ai processi di definizione di politiche, norme e standard internazionali. In sostanza, con la creazione di questo organismo si è voluto attribuire autonoma dignità alla sicurezza e resilienza cibernetiche, creando un quarto pilastro a completamento di quelli esistenti di *cyber-intelligence* (di competenza degli organismi di informazione per la sicurezza), *cyber-defence* (di spettanza del ministero della Difesa) e prevenzione e repressione dei reati (di competenza delle forze di polizia). È con questo spirito, dunque, che si è inteso riordinare e ridefinire la complessiva architettura nazionale cyber, che a partire dalla legge 7 agosto 2012, n. 133, ha visto l'attribuzione al Comparto intelligence e, in particolare al Dis (Dipartimento delle informazioni per la sicurezza), di compiti e funzioni pienamente rientranti nell'ambito della salvaguardia della sicurezza nazionale, ma certamente non tipici della funzione che è propria degli organismi di intelligence. L'Agenzia, in definitiva, viene a svolgere funzioni di *cybersecurity* e di *cyber-resilience* fino ad oggi espletate, in via suppletiva, dal Comparto intelligence, in assenza di un organismo a ciò specificamente deputato. Con questo intervento normativo si sono volute razionalizzare le competenze – prima distribuite tra una miriade di amministrazioni – in materia di cybersicurezza, con particolare riferimento agli ambiti della sicurezza delle reti e dei sistemi informativi (*Nis-Network and information security*), del perimetro di sicurezza nazionale cibernetica e della sicurezza delle comunicazioni elettroniche (Telco), della sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture digitali delle pubbliche amministrazioni (anche in relazione ai servizi cloud), delle certificazioni di cybersicurezza, attualmente attribuite a una pluralità di soggetti istituzionali. Ciò, anche al fine di assicurare l'unicità istituzionale di indirizzo e di azione, spesso invocata dagli operatori coinvolti, nei confronti dei soggetti pubblici e privati interessati, con particolare riferimento alla definizione di misure di sicurezza, così come alle funzioni ispettive, accertative e sanzionatorie, in un ambito connotato da un elevato livello di complessità tecnica e giuridica. Inoltre, l'Agenzia ha il compito di gestire le attività di prevenzione, preparazione e risposta alle situazioni di crisi cibernetica, coordinando, nell'ambito delle rispettive competenze, le azioni dei diversi attori che compongono l'architettura istituzionale.

Per queste finalità, nell'ambito dell'Acn è stato costituito il "Nucleo per la cybersicurezza" (che

sostituisce il Nucleo per la sicurezza cibernetica), un organismo composto dai rappresentanti delle varie amministrazioni a vario titolo interessate. L'Acn, inoltre, dovrà fornire supporto allo sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di autonomia strategica nazionale ed europea nel settore, con un forte impulso a progetti finalizzati di ricerca applicata. Per far questo potrà favorire il partenariato pubblico-privato, lo sviluppo di nuove realtà imprenditoriali, il rafforzamento delle piccole-medie imprese attraverso l'indirizzo e il coordinamento di processi di trasferimento tecnologico tra ricerca e industria assicurando anche un coordinamento europeo con enti omologhi su questi temi. Ciò, per conseguire un'autonomia tecnologica che è del resto anch'essa presupposto della sicurezza nazionale. Per svolgere i complessi compiti l'Acn avrà necessità di avvalersi di professionalità di altissimo profilo che dovranno essere costantemente reclutate con il duplice effetto virtuoso di contribuire alla creazione di nuove generazioni di esperti cyber italiani e arginare la dispersione e la fuga di capacità verso l'estero. L'Agenzia costituisce, dunque, la più recente e fondamentale pietra miliare di un lungo percorso intrapreso nel nostro Paese a partire dal 2013 (decreto del presidente del Consiglio dei ministri del 24 gennaio 2013 con il quale fu istituito, tra l'altro, il Nucleo per la sicurezza cibernetica). Attraverso una serie di interventi normativi successivi – che hanno visto nella direttiva (Ue) 2016/1148 Nis-Network information security e nel Perimetro di sicurezza cibernetica due tappe fondamentali (dl 105/2019) – il nostro Paese con l'Acn si è, finalmente, dotato di un'architettura completa in grado di fronteggiare le minacce telematiche verso i nostri asset strategici. Nel 2019, in particolare, è stato definito un "perimetro di sicurezza nello spazio cibernetico" al cui interno sono state poste le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione fondamentale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche imprescindibili per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziale, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Per le reti, i sistemi informativi e i servizi informatici di questi enti il legislatore ha previsto una particolare tutela. Infatti, da un lato ha imposto per i "responsabili della sicurezza informatica di questi enti" stringenti obblighi di notifica degli incidenti (ad esempio intrusione nelle banche dati. Dall'altro, sono state previste rigorosi parametri di valutazione, sotto il profilo tecnico, della sicurezza per l'acquisto e l'utilizzo degli apparati e dei prodotti utilizzati. In linea con tale normativa, pertanto, oggi, i citati enti dovranno comunicare i sistemi informatici di cui vogliono dotarsi, all'Acn (ed in particolare al Centro di valutazione e certificazione nazionale-Cvcn) che ove rinvenga profili di vulnerabilità, o ritenga che tali dotazioni non rispettino gli standard di sicurezza richiesti, avrà la facoltà di bloccarne l'acquisto. Il sistema così congegnato prevede una clausola di salvaguardia, con l'attivazione del cosiddetto "pulsante rosso". Si tratta, in particolare, di una disposizione che conferisce al presidente del Consiglio il potere di fronteggiare "crisi di natura cibernetica" in cui sussista un rischio grave e imminente per la sicurezza nazionale. In tali casi egli potrà disporre di disattivare, del tutto o in parte, una o più componenti impiegate nelle reti o nei sistemi, per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione.

L'Agenzia per la cybersicurezza nazionale si pone, dunque, come organismo di chiusura del sistema di protezione cibernetica e sicurezza informatica nazionale, con l'obiettivo ultimo di assicurare, oltre che la sicurezza, la resilienza informatica.

12/11/2021