AGENZIA PER LA CYBERSICUREZZA NAZIONALE

XIX legislatura - Disegno di legge - A.C. 1717

Audizione del Direttore generale
Pref. Bruno Frattasi

Commissioni riunite I e II della Camera dei deputati

- 3 aprile 2024 -

In occasione dell'audizione dello scrivente presso le Commissioni affari costituzionali e giustizia, riunite per l'esame dell'Atto Camera n. 1717 ("*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"), si consegna la presente relazione che contiene alcune riflessioni a margine delle disposizioni normative proposte, integrative della relazione illustrativa che accompagna il provvedimento.

Tali riflessioni, peraltro, si soffermano anche sulle osservazioni che, in sede di audizione, sono già state svolte da esperti appositamente convocati, tenuto conto che alcuni hanno sollevato perplessità che meritano, a parere dello scrivente, opportuni chiarimenti affinché si possa disporre di elementi informativi atti a valutarne compiutamente la portata.

Coerentemente all'impianto del provvedimento, che dedica il suo primo capo alla resilienza cibernetica del Paese, la presente relazione si soffermerà prevalentemente sulle disposizioni contenute in tale partizione del DDL, avuto riguardo alla stretta relazione che intercorre tra la missione istituzionale cui è preposta l'Agenzia per la cybersicurezza nazionale e la diffusa esigenza, avvertita in ogni ambito del Paese, di rafforzare il livello della resilienza cibernetica. Ciò, anche in considerazione del deterioramento della situazione internazionale nel contesto europeo e mondiale, che porta con sé maggiori pericoli anche dal punto di vista della sicurezza cibernetica e dell'uso della minaccia cyber per finalità di contesa geopolitica.

Passando ora alla disamina delle disposizioni contenute nel capo I, sorge la necessità di esplicitare le ragioni che hanno portato alla previsione secondo la quale anche le PP.AA. locali – o, meglio, una significativa parte rappresentativa di queste, incluse le stesse Regioni – vadano sollecitamente attratte nel "fascio di luce" della direttiva NIS 2, ossia

della direttiva (UE) 2022/2555, del dicembre 2022, con cui l'Unione europea, nel rimettere mano alla sicurezza delle reti e dei sistemi informativi, ha ritenuto, opportunamente, di ampliare il novero dei soggetti tenuti alla conformità alla direttiva medesima, includendo, tra essi, le stesse PP.AA. locali, e rimettendo, tuttavia, agli Stati membri di individuare quelle che effettivamente debbano essere ricondotte a tale disciplina.

Ed è su questa nuova base normativa europea che si è innestata la scelta del Governo di individuare, fin d'ora, alcune amministrazioni locali, particolarmente esposte sulla base dell'esperienza più recente, ai fini del loro assoggettamento ad un regime in parte simile a quello NIS, di fatto venendo ad anticipare, nei limiti di cui si è fatto cenno, l'esercizio trasposITivo che avverrà ad ottobre di quest'anno, allorché, a mente della stessa legge di delegazione europea 2022-2023 (Legge 21 febbraio 2024, n. 15), occorrerà adottare il previsto decreto legislativo di recepimento della citata direttiva (UE) 2022/2555.

Nel corso degli ultimi 12 mesi, infatti, gli attacchi cyber verso il nostro Paese, il cui numero è cresciuto considerevolmente nel 2023, hanno avuto tra i loro obiettivi privilegiati, ancorché non esclusivi, pubbliche amministrazioni locali (specie Comuni di media grandezza), aziende sanitarie locali, enti ospedalieri, società di trasporto pubblico urbano, ossia le stesse entità pubbliche prese in considerazione dall'articolo 1 del DDL a cui si aggiungono le Regioni, le Province autonome di Trento e di Bolzano, "e le rispettive società *in house*".

Come meglio si specificherà in seguito, si è trattato di intervenire su quel panorama soggettivo che, finora, non era stato destinatario di un *corpus* normativo specifico, diversamente da quegli altri soggetti (fornitori di servizi digitali, fornitori di reti e servizi di comunicazione elettronica) operanti nel settore privato, che, invece, da tempo sono destinatari di disposizioni *ad hoc* riguardanti la loro sicurezza informatica, e per i quali un'eventuale anticipazione della NIS 2 non avrebbe corrisposto a quelle stesse esigenze di immediatezza riscontrabili in ambito pubblico.

Si è fatto cenno sinora a tali entità pubbliche, e non alle PP.AA. centrali, ancorché anch'esse siano ricomprese nella platea soggettiva di riferimento dell'articolo 1, perché è proprio con riguardo alla loro inclusione nel regime NIS che sono state sollevate perplessità e obiezioni. Perplessità e obiezioni che si sono estese anche alla stessa scelta di anticipazione della NIS 2, ritenendo alcuni che sarebbe stato preferibile rimandare tale impatto normativo al successivo esercizio della delega, sicché le

amministrazioni locali avrebbero avuto un maggiore agio nel predisporsi al recepimento della direttiva in parola.

Ora, la c.d. anticipazione della NIS 2 ha voluto, invece, rappresentare un preciso e forte segnale di attenzione verso queste realtà amministrative che, proprio per la loro maggiore esposizione alla minaccia cyber, richiedono – in assenza di un quadro regolatorio specifico – prioritarie misure di intervento a fini di protezione cibernetica. Va precisato, peraltro, che tale graduale anticipazione corrisponde ad un nucleo essenziale della normativa NIS, e non a una integrale applicazione di tale normativa, concentrandosi, soprattutto, sull'obbligo di notifica degli incidenti che dovessero registrarsi a carico delle rispettive superfici digitali.

E ciò per l'essenziale e dirimente ragione che la minaccia cyber è tanto più efficacemente mitigabile e contrastabile quanto più essa viene integralmente e tempestivamente conosciuta e analizzata dall'Agenzia per la cybersicurezza nazionale; obiettivo, quest'ultimo, che può essere garantito adeguatamente proprio a partire dall'obbligo di notifica.

In altri termini, l'obbligo di notifica svolge l'imprescindibile funzione di portare a emersione una minaccia cibernetica incombente che, altrimenti, rimarrebbe non compiutamente percepita nella sua struttura e pericolosità effettiva. La notifica, a cui fa riferimento la norma, porta con sé due rilevanti conseguenze dal punto di vista sistemico: la prima consiste nel fatto che i soggetti obbligati alla medesima entrano a far parte, a pieno titolo, di quella *constituency* a cui ACN rivolge, in modo prioritario, continuativo e strutturato, la sua attività di monitoraggio della minaccia e con cui intesse una serie di relazioni proattive, rappresentate sia dalle sistematiche attività di allertamento generale, sia da puntuali segnalazioni rivolte a specifici soggetti per i quali si evidenzi una più intensa esposizione alla minaccia in ragione di rilevate vulnerabilità. La seconda conseguenza sta nell'attrarre le varie entità pubbliche indicate nell'articolo 1 in un'area di tempestiva assistenza operativa effettuata a loro sostegno da ACN tramite il CSIRT Italia (*Computer security incident response team*), il che consente un'immediata attività di *remediation* ad impatto avvenuto, onde mitigare gli effetti dello stesso impatto e riportare i servizi compromessi nella fisiologica postura cibernetica precedente all'incidente, con conseguente ritorno, il prima possibile, alla ordinaria funzionalità dei sistemi impattati.

Quanto affermato non è solo frutto di un'esigenza sistematica e di adeguamento normativo, ma trae spunto dalla stessa esperienza pratica che, come si diceva, ha visto

questa Agenzia intervenire frequentemente a sostegno di amministrazioni locali gravemente impattate, sostenendo il loro sforzo per il ripristino dei servizi. Ciò è accaduto, soltanto per citare i casi più eclatanti degli ultimi mesi, e che hanno avuto eco mediatica, in occasione degli incidenti di sicurezza cibernetica ai danni delle ASL di Matera, Modena, Torino, Alessandria e La Spezia, dell'Azienda ospedaliera Vanvitelli di Napoli, della Regione Campania, della Regione Umbria, del Comune di Ferrara, del fornitore di servizi digitali PA Digitale, ai quali si aggiungono diversi incidenti in danno di Pubbliche Amministrazioni Centrali ed operatori di servizi critici. È auspicabile, quindi, a commento degli interventi di *remediation* sopra ricordati, che la c.d. anticipazione della NIS 2, lungi dall'essere ostacolata dalla mancata corsia d'urgenza del DDL, venga concretamente assecondata dalla sollecita attenzione del Parlamento verso un tema di assoluta delicatezza per la sicurezza del Paese. Attenzione che trova concreta dimostrazione in questa lunga e fattiva sessione di audizioni per la quale lo scrivente esprime un sentito ringraziamento ai Presidenti e ai componenti tutti delle Commissioni I e II della Camera dei deputati.

Sotto altro aspetto, va sottolineato anche il criterio gradualistico cui si conforma l'articolo 1 del disegno di legge, laddove esso esprime (art. 1, commi 4 e 5) un approccio prioritariamente collaborativo verso le amministrazioni destinatarie della nuova disciplina. Trova così accoglimento un principio che si ispira alla logica della vigilanza collaborativa e che guarda alla sanzione solo come *extrema ratio* e nei casi in cui essa rappresenti effettivamente la risposta, ineludibile e necessaria, verso comportamenti reiteratamente inadempienti che possano compromettere la sicurezza cibernetica del Paese.

Tale ultima considerazione spinge anche a sottolineare come l'inclusione di tali realtà amministrative regionali e locali in un "perimetro" in parte comparabile con quello della NIS 2 risponda anche ad un'esigenza di maggiore compattezza della sicurezza cibernetica della Nazione. Tale compattezza, infatti, verrebbe seriamente compromessa nel caso in cui il vasto arcipelago delle amministrazioni regionali e locali dovesse rappresentare il "punto debole" del sistema, ossia quella parte del sistema meno protetta e più aggredibile, e, dunque, la "porta di ingresso" a potenziali rischi di compromissione di ulteriori assetti informatici, secondo una sorta di effetto domino. In questa prospettiva, la sicurezza cibernetica si presenta come espressione e particolare declinazione del concetto di sicurezza nazionale, il quale trascende l'entità statuale in quanto tale e finisce per abbracciare ogni altra entità la cui difesa cibernetica rappresenti un tassello fondamentale per la piena tutela di un bene primario del Paese.

Sembra, dunque, da questo punto di vista, riconducibile l'esercizio normativo in questione alle prerogative di esclusività predicate dall'articolo 117, comma 2, lett. d), della Costituzione.

Naturalmente tale esclusività non porta a considerare come soffocati gli spazi di autonomia legislativa e organizzativa che, rispettivamente, prima le Regioni e poi gli enti locali potranno esercitare a completamento del disegno proposto dal legislatore statuale.

Si tratta, peraltro, di significativi ambiti di manovra per i quali si potranno anche considerare tutte le opportune economie di scala, onde contenere e ridurre gli impegni finanziari legati ai necessari interventi. Si pensi soltanto, a titolo esemplificativo, alla nomina del referente per la cybersicurezza (art. 6 del DDL), che ben potrebbe coincidere con la figura del Responsabile per la transizione digitale, figura già prevista e disciplinata, peraltro come obbligatoria, dall'art. 17 del Codice dell'amministrazione digitale, e per una platea di soggetti del tutto sovrapponibile a quella destinataria delle disposizioni del DDL. Non è inconferente qui aggiungere che, a mente della stessa disposizione del CAD, spettano al Responsabile per la transizione digitale compiti afferenti alla sicurezza informatica dell'amministrazione di riferimento; sicché, una possibile concentrazione nella stessa figura soggettiva dei due compiti, oltre a una riduzione dell'impatto organizzativo, comporterebbe altresì un'intelligente razionalizzazione degli incarichi, attese le strette interazioni dei due ambiti materiali, ossia crescita digitale e sicurezza digitale, da intendersi in reciproca interdipendenza.

Riguardo alla mancanza di risorse *ad hoc* e, dunque, al rilievo che l'intervento normativo non sia sostenuto da investimenti pubblici mirati, ma avvenga, invece, a invarianza di spesa, non può non sottolinearsi come gran parte del tessuto ordinamentale e degli obblighi che ne conseguono vengano calati in realtà organizzative il cui grado di maturità cibernetica dovrebbe in linea di massima già assorbire l'impatto, in definitiva contenuto, che conseguirà all'applicazione del provvedimento una volta adottato. Impregiudicato tale aspetto, e gli eventuali possibili approdi che il confronto tra Parlamento e Governo potrà registrare, va comunque sottolineato che l'Agenzia, di recente, in corrispondenza temporale all'approvazione del DDL e pressocché "a specchio" con le sue disposizioni, ha previsto che le entità coinvolte da esso possano avere accesso alle risorse del PNRR destinate all'irrobustimento cibernetico delle Amministrazioni pubbliche.

L'avviso pubblico n. 8/2024, che l'ACN ha pubblicato di recente, dedica a tali interventi 50 milioni di euro e altri 50 milioni verranno presto messi a disposizione degli stessi potenziali beneficiari, andando così a raddoppiare il volume complessivo delle risorse finanziarie attingibili. Si tratta, in poche parole, di uno sforzo amministrativo che, per così dire, "ombreggia" e accompagna il disegno normativo, rappresentandone un significativo completamento che sembra poter andare incontro alle esigenze di sostegno finanziario da più parti sollevate nel ciclo delle precedenti audizioni.

In realtà, l'ACN è già da tempo vicina alle amministrazioni pubbliche nell'attività di accompagnamento di esse ad un maggior livello di sicurezza cibernetica. Sia con l'utilizzo del Fondo "Strategia"[1], sia con l'impiego delle risorse del Piano nazionale di ripresa e resilienza – missione n. 1, componente 1, investimento 1.5 "Cybersecurity" – l'ACN provvede da tempo ad accompagnare amministrazioni centrali, organi costituzionali, autorità amministrative indipendenti, Regioni, amministrazioni locali, ecc., nello sforzo di implementare la propria postura di sicurezza cibernetica.

Tra i principali interventi in tale settore, è bene qui ricordarne almeno due, per l'ampiezza e la significatività del loro ambito soggettivo e per l'utilità sistemica dello strumento prescelto. Si fa riferimento sia alla messa a disposizione di un tool per la valutazione e il trattamento del rischio cyber a beneficio delle PP.AA. che intendano avvalersene (170 già se ne avvalgono), che consente ad esse di effettuare operazioni di *self assessment*, sia alla realizzazione, da parte di 19 Regioni, di propri CSIRT regionali, ossia di strutture di monitoraggio della minaccia e di intervento in caso di impatto sui loro sistemi. Attività, quest'ultima – per la quale sono stati messi a disposizione, tramite l'avviso pubblico n. 6/2023, circa 30 milioni di euro a valere sui fondi PNRR – che in qualche modo viene ad integrare quella di ACN, fino a rappresentarne una forma di "demoltiplica territoriale", la quale, potendo anche estendere la protezione informatica ad altre realtà locali della stessa regione, appare suscettibile di contribuire ad un complessivo e sistemico rafforzamento della difesa cibernetica del Paese.

Con riguardo alla scelta delle PP.AA. e delle entità locali individuate dall'art. 1 si vuole ribadire, infine, che la loro individuazione, oltre che sostenuta dalle precedenti ragioni, trova fondamento nel significativo bacino d'utenza dei servizi digitali erogati al cittadino, alcuni dei quali di particolare rilevanza e delicatezza, quali i servizi relativi alla salute pubblica e alla mobilità. In questo senso, la scelta legislativa indirettamente

[1] Fondo di cui all'art. 1, comma 899, della Legge 29 dicembre 2022, n. 197 (Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025).

contribuisce all'estensione, già in atto, del principio di dignità della persona alla sua corrispondente dimensione digitale.

****

Altri aspetti sui quali intende soffermarsi la presente relazione riguardano l'impegno dell'Agenzia su alcuni fronti, presenti e futuri, della sua attività, che sono stati rimarcati in diversi interventi effettuati nella sessione di audizioni.

Il primo aspetto attiene alla formazione cyber del personale pubblico, in quanto, come rilevato in alcuni interventi, il livello formativo è considerato generalmente non all'altezza della minaccia cibernetica e richiederebbe, pertanto, un ispessimento delle competenze, sia di quelle base, sia di quelle specialistiche, onde raggiungere una maggiore maturità cibernetica anche delle risorse umane addette ai diversi livelli operativi e organizzativi. Premesso che la formazione è uno dei fattori abilitanti della Strategia nazionale di cybersicurezza, sembra necessario chiarire che ad essa sono rivolte diverse misure del Piano di implementazione (in particolare, dalla misura n. 59 alla misura n. 70), le quali, in parte, hanno già trovato una prima significativa applicazione, sia in forma diretta da parte di ACN, sia in forma indiretta, tramite iniziative di vario genere rivolte alla creazione di una *work force* nazionale che immetta nel sistema Paese maggiori e più elevate competenze.

Quanto al contributo diretto, l'ACN, in forza di un apposito accordo sottoscritto con il Presidente della Scuola Nazionale dell'Amministrazione, partecipa in prima persona ad attività formative rivolte a personale delle amministrazioni pubbliche, erogando contenuti didattici in modo frontale; inoltre, utilizzando la piattaforma Syllabus del Dipartimento della Funzione pubblica della Presidenza del Consiglio dei ministri, e sempre a valere su risorse dell'investimento 1.5 PNRR, è stato realizzato un apposito corso di formazione ("*Cybersicurezza: sviluppare la Consapevolezza nella PA*"), tramite il quale si consente, anche qui, a tutto il personale delle PP.AA. l'accesso ad attività formative online.

Riguardo, invece, a quello indiretto, incessante è lo sforzo dell'ACN di promuovere l'incremento dell'offerta formativa in materia cyber da parte di Università pubbliche e private, incoraggiando l'istituzione di nuovi percorsi accademici, pre- e post-laurea.

A tal fine, è stato nello scorso anno sottoscritto un apposito accordo con la Conferenza dei Rettori delle Università italiane (CRUI), che non preclude, peraltro, altre specifiche

forme collaborative con i singoli Atenei e consorzi interuniversitari, finalizzato alla realizzazione di mirate iniziative formative di alto livello.

Su un piano complementare, si pone poi l'attività dell'ACN volta a favorire lo sviluppo degli ITS (Istituti tecnologici superiori), onde promuovere, anche in ambito pre-universitario, un rafforzamento della cultura cyber particolarmente rivolto al tema specifico della sicurezza informatica.

Non ultimo, infine, è l'impegno di ACN ad affiancare grandi *player*, nazionali e non, nella creazione delle c.d. *e-academy*, ossia di centri di formazione digitale aperti anche alla partecipazione di privati e di professionisti che intendano, per le loro specifiche esigenze, raggiungere un maggior livello di competenza in materia cyber e di sicurezza informatica.

Questo insieme di misure – la cui ampiezza è destinata a crescere con il progressivo e graduale irrobustimento della struttura dell'Agenzia, che ha praticamente raddoppiato nel corso del 2023 la sua consistenza organica[2] – mira a creare le condizioni per le quali il processo di transizione digitale possa crescere in un ecosistema nazionale

[2] Premesso che la consistenza organica dell'Agenzia è ora di circa 300 unità e che nel triennio 2024-2026 la manovra acquisitiva porterà al raddoppio della forza lavoro in ACN, passando, dunque, a 600 unità complessive, un cenno a parte meritano alcuni strumenti che la legge istitutiva del 2021 ha messo a disposizione dell'Organismo per attrarre professionalità pregiate. A questo fine si segnalano le disposizioni che facoltizzano ACN a indire delle procedure selettive pubbliche per contratti a tempo determinato, onde acquisire specializzate figure professionali idonee a ricoprire incarichi interni la cui complessità richieda un alto valore competenziale. Inoltre, la legge istitutiva di ACN facoltizza l'Organismo ad avvalersi anche di esperti di comprovata ed elevata qualificazione provenienti da vari ambiti professionali in grado di dare un contributo significativo, sia pure *ab externo*, alla missione dell'Agenzia. Tali disposizioni concorrono a definire l'Agenzia in termini di centro amministrativo e operativo di eccellenza, termini che vanno ricondotti all'innovatività della materia cyber, al suo alto contenuto tecnologico, peraltro in continua e incessante evoluzione, e, ultimo ma non ultimo, all'eminente profilo di sicurezza nazionale che, per i motivi più volte richiamati in relazione, appare coessenziale alla stessa nascita dell'Organismo. È evidente che l'insieme di queste ragioni hanno determinato, altresì, la scelta iniziale di agganciare il trattamento economico-retributivo del personale dell'Agenzia ai più alti livelli rinvenibili nel sistema pubblico nazionale, scelta che di per sé esprime già un valore attrattivo, che si aggiunge alla leva motivazionale consistente nell'operare in un ambito di speciale tutela degli interessi nazionali. Si è posta, pertanto, particolare attenzione alla crescita professionale, prevedendo, per il personale in Agenzia, percorsi formativi di alta qualificazione che consentano il mantenimento e il perfezionamento delle capacità possedute. Naturalmente, tenuto conto del *dumping* che può comunque essere esercitato da operatori privati, come peraltro già avvenuto in questo come in altri settori, la disposizione del DDL (art. 9) sulla *retention* del personale intende rappresentare uno strumento di protezione dell'Agenzia rispetto al rischio che lo sforzo, anche economico, di sostenere il richiamato processo di crescita venga in concreto ad essere frustrato da precoci "abbandoni", che verrebbero a spogliare l'Agenzia di un patrimonio competenziale faticosamente raggiunto. La soluzione delineata nel citato articolo 9 appare, rispetto a tale rischio, un ragionevole punto di equilibrio, limitando a 2 anni la durata del vincolo e connettendolo soltanto alla frequentazione e al superamento di corsi specialistici di particolare complessità e pregio.

culturalmente maturo, ossia che abbia acquisito gli strumenti conoscitivi per affrontare adeguatamente le opportunità e i rischi che quel processo comporta.

Come dicevo, è uno sforzo, questo, innanzitutto culturale che, a parere di chi scrive, dovrà alimentare, soprattutto con riferimento alle giovani e giovanissime leve studentesche, un'attenzione e una sensibilità verso il tema cyber e l'uso corretto dei dispositivi digitali, facendone percepire i pericoli e le gravi conseguenze connesse ad un loro incauto, inconsapevole o irresponsabile utilizzo. Proprio in questa direzione sono state avviate interlocuzioni con il Ministero dell'istruzione e del merito per un accordo con ACN che valorizzi, all'interno dei vari percorsi didattici, la questione di un responsabile approccio al mondo digitale, ovviamente modulato in relazione al diverso livello scolastico e di conseguente maturità dei discenti.

Un altro rilevante punto – stavolta più prospettico – affrontato in sede di audizione attiene al cruciale tema dello sviluppo dell'intelligenza artificiale e al ruolo che l'ACN dovrebbe o potrebbe svolgere in tale strategico ambito.

La questione è stata sollevata soprattutto con riferimento all'art. 7 del DDL, in cui, intervenendo sulla legge istitutiva dell'Agenzia, si delinea uno specifico compito consistente nel curare la sicurezza informatica dei sistemi di intelligenza artificiale, con riferimento anche agli aspetti di carattere etico che attengono, soprattutto, ai loro output, in ragione delle preoccupazioni che si vanno affacciando da più parti sul rispetto dei diritti umani e della dignità della persona.

A parte ogni ragionamento, che qui per brevità si omette, sulla necessità di un approccio regolatorio al tema dello sviluppo dell'intelligenza artificiale, approccio seguito dall'Unione europea con la recente approvazione dell'AI Act, la questione che qui si vuol sottolineare è che l'uso incrementale dell'intelligenza artificiale, destinato certamente a conoscere un'espansione senza precedenti, e per certi versi dall'esito imprevedibile per gli aspetti non deterministici dei suoi algoritmi, non è scindibile dai profili di sicurezza informatica. E non lo è in quanto la sicurezza informatica, in questo ambito, non è concepibile in termini puramente di resilienza e di robustezza dei prodotti e dei servizi, ossia in un'accezione meramente tecnica o tecnologica, bensì è da intendere in un'accezione più ampia che ricomprende anche l'uso finalistico dei programmi e l'assenza, nella loro progettazione, di *bias*, cioè di pregiudizi, che influiscano in maniera discriminatoria sul già citato output. Non è altro, questo, che l'applicazione, anche nel campo della progettazione delle tecnologie di intelligenza artificiale, del principio, ormai consolidato, della *security by design*, ossia della

necessità che la sicurezza informatica dei prodotti e servizi digitali venga considerata, fin dall'inizio del loro sviluppo e per tutto il loro ciclo di vita.

La disposizione in commento del DDL non intende certo attribuire ad ACN la determinazione del quadro valoriale cui deve far riferimento l'intelligenza artificiale, derivando quest'ultimo, invece, da un *framework* eterodeterminato di regole condivise, che trova e troverà origine da fonti esterne ed estranee all'Agenzia.

Un'ulteriore riflessione va poi fatta con riferimento alla costatazione di come l'intelligenza artificiale andrà a coniugarsi con infrastrutture e tecnologie ben note alla comunità della cybersicurezza mondiale e per le quali l'ACN è già individuata dalla normativa vigente quale Autorità con compiti anche di certificazione rispetto agli schemi europei e internazionali. Ed è un contesto nel quale l'attività di certificazione assicurata dall'Agenzia ha reso possibile, esaltando la funzione preventiva dell'ACN, la scoperta e la risoluzione di molte vulnerabilità, alcune sconosciute agli stessi produttori (c.d. *0-day*), e pertanto di particolare pericolosità, specie in termini di potenziale sfruttamento da parte degli attaccanti.

Ora, la disposizione in materia di intelligenza artificiale si pone in linea di continuità con un filone legislativo, continuamente alimentato anche dopo l'istituzione dell'Agenzia, che ha collegato allo sviluppo delle c.d. tecnologie dirompenti, nel cui ambito l'intelligenza artificiale assume un ruolo quasi emblematico, la necessità di garantire il presidio della cybersicurezza, presidio di cui l'ACN è la naturale autorità di riferimento, in costante e continuo raccordo con gli omologhi organismi europei e mondiali.

Una riflessione non ultronea, sempre con riguardo ai profili di cybersicurezza, attiene alla compenetrazione dei sistemi di IA con la tecnologia del *cloud computing*, in base alla quale sarà possibile non solo la gestione efficiente delle enormi quantità di dati coinvolte, ma anche, grazie alla potenza computazionale applicata, un corrispondente ed esponenziale sfruttamento della capacità estrattiva degli stessi dati.

Non è inconferente ricordare, allora, a questo riguardo, come ACN, nello scorso anno, abbia assunto un ruolo di primaria importanza nella qualificazione dei servizi *cloud* (scrutinandone più di 1.200), affiancando il Dipartimento per la trasformazione digitale della PCM nello sforzo della transizione in sicurezza della P.A. al *cloud*.

Ai promettenti sviluppi dell'integrazione tra tecnologie dirompenti – mi preme sottolinearlo – si ispira poi l'iniziativa di ACN che denominiamo "HyperSOC", rivolta alla realizzazione, con risorse del PNRR, di una nuova infrastruttura che metterà a sistema i

dati sulla minaccia cibernetica rilevati giorno per giorno dai SOC (*Security operation centre*) di importanti soggetti nazionali operanti in ambiti strategici: quello finanziario, quello dei servizi digitali alla PA e quello energetico (altri *player* di altri settori parimenti strategici potranno aggiungersi a breve in questa iniziativa). Lo sfruttamento della capacità computazionale integrata dagli algoritmi di IA, che procederanno ad elaborare i dati provenienti da questa sorta di federazione dei SOC, metterà il Paese nelle condizioni di poter affinare, con una precisione e una rapidità notevolmente superiori a quelle attuali, la conoscenza predittiva della minaccia e, conseguentemente, anche di anticipare l'adozione delle contromisure difensive. Si sta dicendo, in altre parole, come l'IA possa rivelarsi anche un formidabile strumento di difesa cibernetica, ascrivendo, quindi, questa sua potenziale attitudine al catalogo delle maggiori opportunità che lo sviluppo di tale tecnologia potrà assicurare in un futuro non lontano.

Infine, va notato come il DPCM 15 giugno 2021, adottato in attuazione della legge istitutiva del perimetro di sicurezza nazionale cibernetica (PSNC, di cui al D.L. n. 105/2019) attribuisca già all'Agenzia il compito di valutare soluzioni di intelligenza artificiale utilizzate dai soggetti inclusi nel suddetto perimetro per la gestione di assetti informatici funzionali all'erogazione di quei servizi essenziali rilevanti per la sicurezza nazionale.

Le riflessioni che precedono sono esclusivamente volte a chiarire un aspetto – quello che attiene alla connessione tra IA e cybersicurezza – che è sembrato non immediatamente presente in tutta la sua evidenza nelle considerazioni svolte a commento dell'art. 7 del DDL. Impregiudicate, naturalmente, le scelte che Governo e Parlamento intenderanno portare avanti sull'architettura nazionale che presiederà allo sviluppo dell'intelligenza artificiale.

***

A conclusione di questa relazione, lo scrivente si sofferma brevemente sul II capo del DDL, in cui sono contenute disposizioni di carattere penale, sostanziale e processuale, ed altre che attengono anche ai rapporti tra la magistratura inquirente e questa Agenzia.

In particolare, l'art. 17 del provvedimento definisce la "linea di rispetto" tra l'attività propria di ACN, improntata alla resilienza cibernetica, di ripristino delle infrastrutture digitali critiche a seguito di un incidente, per le quali sussiste la necessità di un immediato intervento di ripristino, e quella investigativa, diretta ad accertare le

responsabilità dell'attacco, individuandone gli autori per una efficace repressione di fenomeni criminali di particolare allarme sociale e gravità. Il provvedimento raggiunge, in proposito, un punto di equilibrio tra queste due concorrenti istanze, secondo il quale viene accordato alla resilienza un rilievo del tutto adeguato rispetto alle esigenze di protezione della superficie digitale del Paese e di immediata riabilitazione dei sistemi impattati al fine di scongiurare discontinuità che potrebbero compromettere funzioni essenziali. Peraltro, la disposizione affida il bilanciamento delle due esigenze cui si è fatto cenno a una interlocuzione *post factum* tra ACN e Autorità giudiziaria competente, evitando pericolose astrazioni che potrebbero rendere difficilmente gestibile, anche in termini di responsabilità del personale operativo dell'Agenzia, il suddetto contemperamento.

Indubbiamente, l'irrobustimento delle sanzioni dei più gravi reati informatici che compromettano gli assetti maggiormente strategici dà luogo in forma indiretta a un rafforzamento anche della resilienza cibernetica in quanto il grado maggiore di deterrenza che ne deriva potrà auspicabilmente determinare una riduzione degli attacchi, svolgendo quella funzione dissuasiva propria della risposta penale.

Sotto altro ma collegato profilo, va anche ricordato come l'Agenzia abbia già avviato proficue interlocuzioni con la Direzione nazionale antimafia e antiterrorismo per la definizione di intese funzionali all'applicazione di una disposizione già vigente, quella introdotta dal decreto-legge n. 105/2023, a mente della quale ACN è tenuta a mettere a disposizione del suddetto Organo giudiziario tutti gli elementi informativi necessari all'esercizio delle funzioni di impulso e coordinamento investigativo afferenti ai reati informatici commessi in danno di infrastrutture nevralgiche per il Paese.