INTELLIGENZA ARTIFICIALE

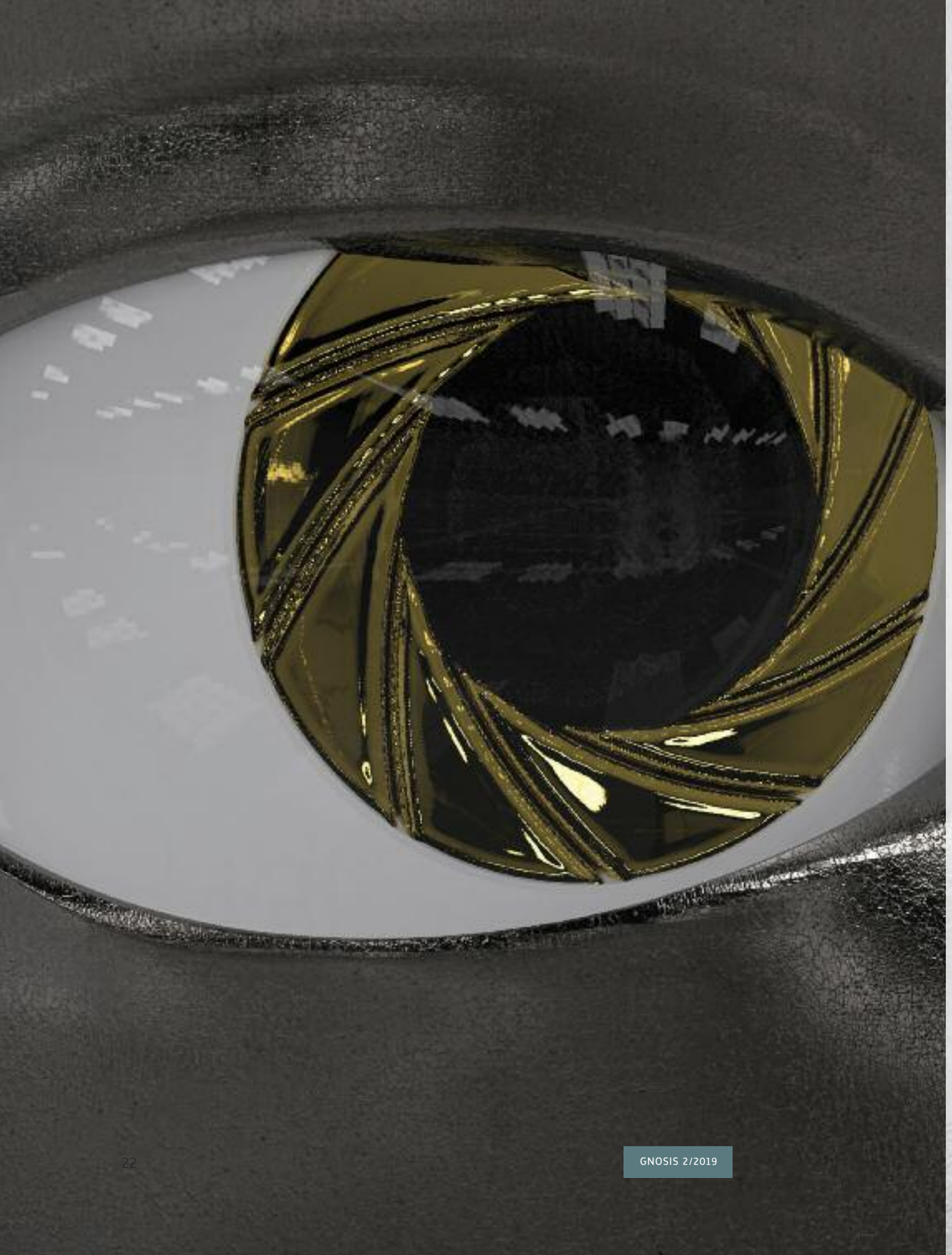
PREPARARE IL PAESE AL FUTURO

Roberto Baldoni

La digital trasformation *che permea la nostra civiltà produce molteplici effetti tanto sulla sfera psicosociale dell'individuo quanto sui driver che guidano il nostro futuro. L'articolo, che introduce una teoria di interventi sullo sviluppo tecnologico in particolare legato all'*Intelligenza Artificiale (AI) *– fattore di cambiamento ma essa stessa strumento per gestirlo – sottolinea come lo sviluppo tecnologico così avanzato imponga la sensibilità e il fattivo coinvolgimento di tutti gli attori nazionali, tra cui prioritariamente il Comparto sicurezza, per sfruttare le opportunità e circoscrivere le vulnerabilità, catalizzare le frammentarie strutture e competenze scientifiche e operative italiane, promuovere un sistema di* investiment and technology screening *per difendere l'ecosistema università-azienda e gli asset digitali strategici rilevanti ai fini della sicurezza nazionale.*

La trasformazione digitale, iniziata nella seconda metà del secolo scorso con lo sviluppo delle prime macchine ri-programmabili, ha cambiato irreversibilmente, digitalizzandoli, pezzi sempre più ampi delle nostre organizzazioni pubbliche e private, della nostra società, della nostra vita. Il processo è in costante accelerazione grazie alle capacità algoritmiche sempre più evolute, ai dati disponibili in quantità enormi, alla potenza computazionale e alla larghezza di banda in continua crescita. Questo ha dato, e darà vita, ad applicazioni più evolute con riflessi primari sull'economia di quei paesi che sapranno meglio interpretare questa trasformazione dal punto di vista sociale, normativo e tecnologico.

La trasformazione digitale, mentre rende la nostra interazione con il mondo cibernetico semplice grazie anche alla iperconnessione, nasconde un corrispettivo tecnologicamente ipercomplesso e colmo di insidie, che espone la società e i cittadini a rischi attraverso debolezze, o vulnerabilità, proprie del mondo cibernetico, che assumono forme diverse nel tempo e sovente non prevedibili a priori. Le reti sociali, ad esempio, nate per riunire amici, colleghi e persone care nel mondo virtuale, sono state modificate da abili



attori, in alcuni contesti specifici, in un sistema di manipolazione o radicalizzazione delle opinioni. Gli attacchi cyber, che sfruttano errori presenti nelle ipercomplessità del software e delle interconnessioni, mettono a repentaglio i nostri dati e la continuità di servizio delle nostre infrastrutture vitali (ormai digitalizzate). Insieme al *quantum computing* nella potenza computazionale e al 5G nelle reti, l'Intelligenza Artificiale (AI) rappresenta il pilastro fondante delle nuove applicazioni della trasformazione digitale. Per questo la AI, come il 5G, è divenuta un elemento geopolitico di rilevanza strategica. I paesi sviluppano strategie nazionali multidimensionali per pianificare un posizionamento in tale settore da cui dipende il loro futuro in termini economici e di indipendenza. È quanto hanno fatto le superpotenze Cina e Stati Uniti, e ha iniziato a fare l'Europa. L'Italia ha avviato due iniziative nazionali: la prima mirata alla ricerca in AI, condotta dal ministero dell'Istruzione, dell'Università e della Ricerca (Miur), che include posizioni di dottorato di ricerca in AI, la definizione di un nuovo Programma nazionale della ricerca che pone la AI come elemento caratterizzante e, infine, un gruppo di lavoro specifico per studiare nuove iniziative didattico-scientifiche. La seconda punta principalmente allo sviluppo e al trasferimento tecnologico, e si dipanerà attraverso una strategia definita da un gruppo di lavoro di esperti ad hoc coordinati dal ministero dello Sviluppo economico. Il Comparto intelligence e il Nucleo per la Sicurezza cibernetica nazionale, incardinato presso il Dipartimento delle informazioni per la sicurezza, analizzano da tempo il fenomeno in termini di rischi e opportunità. Nel 2018 sono state attivate alcune azioni specifiche per supportare il raggiungimento di obiettivi di sistema, come evidenziato nella *Relazione sulla politica dell'informazione per la sicurezza* al Parlamento del 2018. In particolare, ci si è concentrati su:

a. PROTEZIONE DELLA NUOVA SUPERFICIE D'ATTACCO GENERATA DA SISTEMI DI AI

I sistemi di AI, inclusi i sistemi robotici, andranno ad automatizzare funzioni e compiti sempre meno ripetitivi e più critici all'interno della nostra società. Nel futuro, forse non troppo lontano, anche parte di alcune figure professionali ad alta specializzazione, come medici, ingegneri, commercialisti e manager potrebbero seguire la sorte toccata agli operai che, nei decenni passati, sono stati progressivamente sostituiti da macchine automatiche. Il processo aumenterà drammaticamente la superficie d'attacco digitale da dover difendere da minacce di tipo cyber per assicurare il funzionamento e l'integrità dei nuovi servizi critici (e non) delle nostre società. Una politica di cybersecurity nazionale dovrà essere pronta, pertanto, per anticipare i nuovi cambiamenti e mettere in atto idonee misure di protezione di questa nuova superficie di attacco. Protezione che dovrà includere sempre più sistemi di AI per contrastare attacchi che saranno anch'essi sviluppati con sistemi di AI.

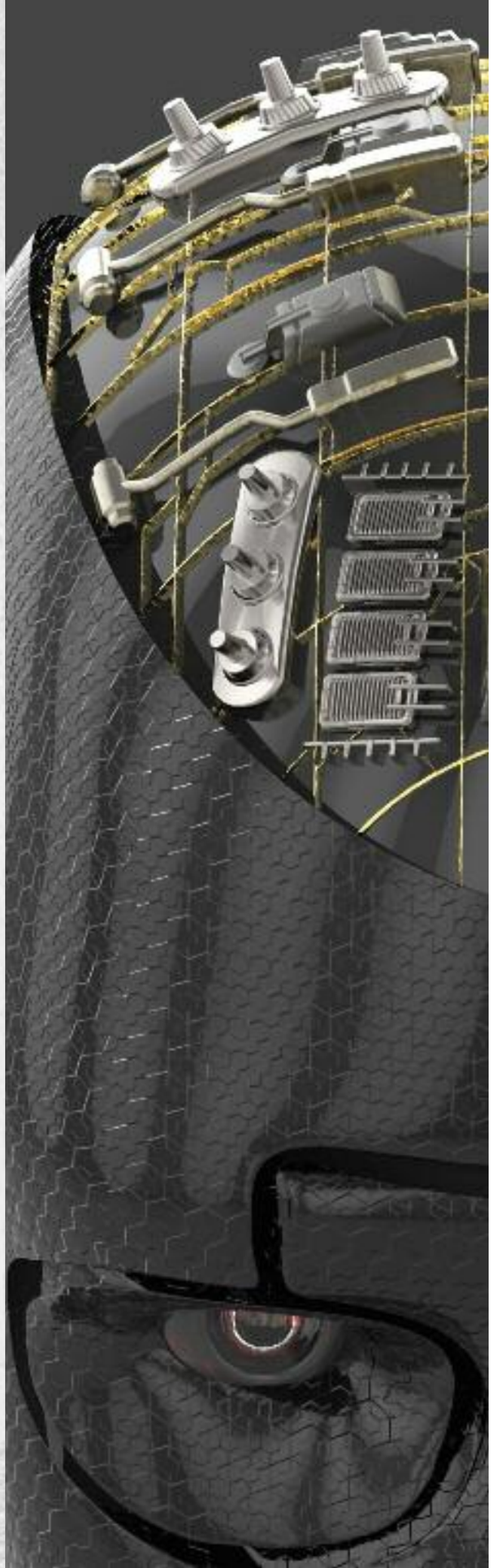
b. STRUTTURAZIONE COMUNITÀ SCIENTIFICA NAZIONALE E SVILUPPO DI KNOW-HOW NAZIONALE

La comunità scientifica nazionale in AI è una delle più attive e numerose nel panorama internazionale. Tranne in alcuni casi specifici, come il Consiglio nazionale delle ricerche, l'Istituto italiano di tecnologia e la Fondazione Bruno Kessler, la comunità è fram-

mentata tra le sessanta università nazionali. In un mondo dove i problemi diventano sempre più multiformi, ampi e intersettoriali, questa dispersione rende arduo il raggiungimento di risultati scientifici ad alto impatto, poco efficace il trasferimento tecnologico e anche gli sforzi per la difesa degli interessi nazionali di tipo scientifico in ambito europeo rischiano di diventare sterili. Il Comparto intelligence ha quindi supportato la nascita di uno strumento per connettere a rete la comunità scientifica nazionale attraverso il L*aboratorio nazionale di* I*ntelligenza artificiale e* S*istemi intelligenti* (Lab Aiis) incardinato all'interno del Consorzio interuniversitario nazionale per l'informatica (Cini). L'obiettivo è di comporre la frammentazione attraverso una piattaforma nazionale, aperta a tutti gli *stakeholder* nazionali, pubblici e privati, basata su un sistema di riferimenti scientifici di matrice anglosassone, che possa aiutare a individuare i migliori esperti in settori specifici per organizzare team in grado di affrontare la complessità dei problemi e accelerare lo sviluppo di know-how nazionale in termini di impresa e di risorse umane.

c. PROTEZIONE DEL KNOW-HOW E DELLA CATENA DI APPROVVIGIONAMENTO

Una volta sviluppato un know-how nazionale in AI e creato un ecosistema università-aziende, si pone l'esigenza di proteggere la conoscenza acquisita attraverso un ragionato sistema di *investment and technology screening*: l'*investment screening* ha lo scopo di proteggere le aziende ad alta intensità tecnologica e strategiche per la sicurezza nazionale da investimenti predatori che tendano, ad esempio, a svuotare l'azienda del suo know-how pregiato o a portare all'estero asset d'interesse nazionale. Il decreto-legge 15 marzo 2012, n. 21 (c.d. D*ecreto Golden Power*, convertito con modificazioni dalla legge 11 maggio 2012, n. 56) va in questa direzione. Il *technology screening* serve a limitare il rischio cyber legato all'utilizzo di elementi tecnologici all'interno di asset digitali strategici per la sicurezza nazionale. Il Perimetro di sicurezza nazionale cibernetica, in via di perfezionamento a livello normativo, e il Centro di valutazione e certificazione nazionale (Cvcn), incardinato nel ministero dello Sviluppo economico, costituiranno i pilastri normativi e operativi dello screening tecnologico. L'insieme delle azioni spingerà a maturare, all'interno della comunità scientifica e industriale, la necessità di nuove metodologie per assicurare l'integrità, la confidenzialità e la disponibilità dei sistemi di AI.
Certificazione, omologazione e monitoraggio di dati e algoritmi diventeranno elementi di qualità primari per tali sistemi.



Essendo legata alla trasformazione digitale della nostra società, la AI è un'affascinante tematica trasversale che ha inevitabili riflessi, ad esempio, in ambito economico, sociologico, etico e psicologico. Per avere l'ardire d'interpretare, o meglio anticipare i cambiamenti della nostra società, dobbiamo fare riferimento a un pensiero multidimensionale che includa riflessioni dalla scienza alla filosofia, alla storia, all'economia, alla geopolitica fino alla sociologia.
Questo numero di Gnosis è speciale perché rappresenta un passo verso la necessaria multidimensionalità di pensiero, raccogliendo articoli che propongono approfondimenti sulle sfide etiche di una civiltà ormai pervasa dalle macchine automatiche e sull'evoluzione della AI considerandone la storia. I contributi si concentrano sull'utilizzo della AI all'interno di verticali tecnologici specifici, segnatamente robotica, elaborazione del linguaggio naturale, reti sociali, elaborazione granulare e 5G. Considerata la matrice della Rivista, particolare attenzione è rivolta alla relazione tra AI e sicurezza in termini di evoluzione della minaccia alla sicurezza nazionale, di trasformazioni sociali e di cybersicurezza. Una sezione è dedicata ad alcune iniziative nazionali sulla AI: le attività sviluppate dal ministero dell'Istruzione, dell'università e della ricerca; quelle del Lab Aiis del Cini; quelle che coinvolgono la formazione nelle scuole superiori e infine è presentata una rassegna su come il tema della AI sia stato trattato dall'industria cinematografica e dalla letteratura, settori da sempre affascinati dal tema e, a volte, la fantasia degli autori si è rivelata ispiratrice di innovazioni tecnologiche. La qualità dei contributi, l'autorevolezza e l'eterogeneità degli autori rendono questo numero di Gnosis unico nel suo genere. La AI è una sfida enorme per la nostra società e la trasformerà in modo difficilmente predicibile. È una sfida di superiorità tecnologica con risvolti geopolitici, economici e sociali. Per un paese di medie dimensioni e limitate risorse come l'Italia, la sfida deve essere affrontata organizzandoci con il necessario anticipo a livello nazionale, cercando contemporaneamente, a livello europeo, una linea comune che sfoci in iniziative di ampio respiro scientifico con misurabili ricadute sul territorio a livello di trasferimento tecnologico. Solo se questa competizione verrà affrontata dal nostro paese in modo sistemico, ovvero coordinando e allineando il livello normativo e organizzativo, le relazioni internazionali, lo sviluppo tecnologico nazionale, la ricerca, la formazione e le campagne di consapevolezza nella società, si creeranno le condizioni per ridurre i contraccolpi di carattere sociale ed economico che, inevitabilmente, si porranno con il diffondersi di tali sistemi. Cogliendo, allo stesso tempo, le opportunità di sviluppo economico e di progresso sociale offerti dalla tecnologia. Serve un *coordinamento* rafforzato tra le varie organizzazioni che si occupano della materia con un chiaro responsabile al vertice; può essere chiamata *governance* della AI nazionale da incastonare all'interno di una *governance* della trasformazione digitale. Questo è il primo vero obiettivo da raggiungere nel nostro paese.