ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
3 / 2026

LUGLIO - SETTEMBRE

Minaccia Cyber nell'era dell'A.I. generativa. I possibili strumenti di intervento normativi nel sistema del libero mercato

Nicola Scerbo

DOI: 10.13130/2723-9195/2026-3-16

I recenti sviluppi nel campo dell'intelligenza artificiale applicata hanno reso evidente la necessità d'intervento di mitigazione del rischio cyber in contesti già interessati da fenomeni di interferenza illecita nel libero mercato. E' opportuno, al riguardo, analizzare lo scenario evolutivo e le possibili criticità derivanti dall'introduzione di sistemi sofisticati ed in continuo accrescimento nelle potenziali capacità d'impiego, nell'ottica di una implementazione di mercato rispettosa dei criteri di compliance normativa, anche alla luce dei recenti interventi di adattamento del legislatore interno alla regolamentazione europea, nonché dei necessari requisiti di sicurezza gestionale contro attacchi ed interferenze esterne da parte di attori criminali. Mediante un'analisi della normativa di riferimento e delle relative proposte di intervento per il futuro, il contributo mira ad individuare vulnus e pregi di un'architettura tesa a mitigare il rischio operativo degli attori coinvolti, senza tralasciare rilievi critici funzionali ad un miglioramento del quadro di riferimento.

Cyber threats in the age of generative AI. Potential regulatory measures within the free market system

Recent developments in the field of applied artificial intelligence have emphasised the necessity of interventions to mitigate cyber risks in contexts already affected by illicit interference in the free market. In this regard, it is appropriate to analyse the evolutionary scenario and the possible critical issues arising from the introduction of sophisticated systems that are continuously growing in their potential use capabilities, with a view to a market implementation that respects regulatory compliance criteria, also in light of recent interventions by the internal legislator to adapt to European regulations as well as the necessary management security requirements against external attacks and interference by criminal actors. Through an analysis of the

actual legislation and the related proposals for future interventions, the paper aims at identifying the weaknesses and merits of an architecture aimed at mitigating the operational risk of the actors involved without neglecting critical findings that are functional to the improvement of the reference framework.

Sommario: 1. Introduzione.- 2. Le prime criticità di sistema.- 3. Qualche cenno sulla tecnologia di A.I. generativa.- 4. Il concetto di cybersecurity nell'ecosistema globalizzato.- 5. Il fenomeno Cyber nel suo dinamismo di facciata.- 6. La risposta del regolatore europeo alle esigenze di sicurezza informatica.- 7. L'A.I. come minaccia e opportunità per la sicurezza informatica.- 8. Le Direttive NIS 1 e 2 ed il Regolamento europeo sulla Cybersecurity, il frutto avvelenato di una solerzia poco focalizzata.- 9. L'architettura normativa del legislatore interno.- 10. La cybersecurity come opportunità di implementazione affidabile della tecnologia.- 11. Conclusioni.

1. Introduzione

L'impatto dell'intelligenza artificiale sul libero mercato costituisce una delle più rilevanti criticità d'impiego di moderni sistemi informatici, calibrati e concepiti ad arte, per ottimizzare ed efficientare l'operatività di meccanismi consolidati e calibrati sulle necessità delle potenzialità umane fisiche. Dall'oggi al domani è emersa la possibilità di accelerare notevolmente processi della tecnica, strutturati e concepiti sulla base di una progressione lineare attraverso le varie ere evolutive. Attori produttivi coinvolti e regolatori di ogni paese devono necessariamente interfacciarsi con la tecnologia algoritmica non solo per la necessità di assorbirne il potenziale migliorativo, ma, soprattutto, per mitigarne le spinte distorsive ed il loro affabulante potere di interferire negli equilibri relazionali di sistemi economici complessi e quanto mai soggetti a pressioni esterne[1]. Gli sviluppi della tecnica informatica e computazionale possono non essere in linea con i valori democratici di convivenza pacifica, ma tesi a condizionarne gli esiti, al fine di acquisire e perpetuare capacità e potenzialità intrusive dirimenti e spiazzanti per chi ha poca dimestichezza con le pressioni al ribasso di attori criminali. Il ruolo del legislatore, in un simile scenario, nell'ottica di una mitigazione dei rischi

connessi all'impiego delle tecnologie di intelligenza artificiale, da solo, non è sufficiente a dirimere e mitigare pressioni dal difficile inquadramento normativo e, il più delle volte, anche non perfettamente descrivibili in termini pratici, in virtù della loro intrinseca complessità tecnica, anche per professionisti ed operatori di settore. In tal caso, si pone il problema di porre un argine a fenomeni in grado di interferire con il regolare svolgimento delle più elementari attività nel libero mercato, senza, tuttavia, ridurne il grado di efficienza richiesto dalle pressioni economicistiche e di ottimizzazione dei processi tecnologici, nell'ottica di una massimizzazione del profitto. Si tratta, in verità, di equilibri non sempre facilmente raggiungibili, senza una evidente compromissione dei bisogni di realizzazione e messa in opera degli obiettivi della libera iniziativa economica, caposaldo delle economie contemporanee postbelliche. In tal caso, dinanzi alle innumerevoli sfide rappresentate dall'incalzante evoluzione informatica, con le sue pressioni efficientiste e scientiste, si pone prepotentemente il quesito sulla razionalità logica di interventi normativi tesi a confinare pulsioni ed attitudini alla semplificazione. Allo stesso tempo, però, si pone il rischio di compromettere attitudini positive di miglioramento dei sistemi sociali evoluti, sempre più bisognosi di innovazione e risposte alla maggiore richiesta di benessere e sviluppo. Riuscire a bilanciare simili necessità con il dirimente ostacolo rappresentato dalle iniziative di non trascurabili attori criminali, nelle loro elementari ed umane pulsioni al ribasso, è la principale delle sfide per chiunque voglia porsi in contrapposizione alle logiche manichee tra bene e male, al fine di consentire la convivenza pacifica[2].

2. Le prime criticità di sistema

Quando, per la prima volta, emerse la reale e concreta possibilità d'impiego, su larga scala, di tecnologie altamente sofisticate, fino ad allora ritenute più che altro concettuali e sperimentali, in grado di ottimizzare algoritmi di c.d. intelligenza artificiale generativa (*ChatGPT* e simili), molti degli addetti ai lavori, inclusi operatori specialistici e del settore informatico, sentirono immediatamente l'esigenza di segnalare i possibili elementi critici derivanti dall'impiego generalizzato di strumenti estremamente pervasivi e del tutto fuori dagli schemi classici di concepimento dell'architettura normativa sulla tutela dei diritti di

riservatezza e *privacy*. Dinanzi all'intensificazione delle esigenze di riservatezza, il legislatore euroatlantico ha immediatamente subito le pressioni della comunità sociale relative alla possibilità di vedere violato il nucleo essenziale della privata segretezza, suggerendo il possibile intervento mediante strumenti normativi idonei a confinare potenziali derive ed usi impropri degli apparati presentati alla pubblica cronaca[3]. Un misto di curiosità, tipica dell'essere umano, per l'innovazione nella tecnologia di consumo, unito alla determinazione di industrie o *startup* vecchie e nuove, ha determinato una forte propensione alla sperimentazione di applicativi soggetti a continui aggiornamenti e suscettibili, per loro intrinseca progettazione, ad agglomerare ed ingurgitare gli stilemi dell'agire quotidiano dei fruitori di servizi proposti a costi irrisori. Il mercato, inteso come insieme di comportamenti proiettati verso l'ottimizzazione di processi rivolti al profitto ed all'interscambio economico, ha, fin dall'inizio, introiettato il nucleo essenziale delle tecnologie di *A.I.,* carpendone potenzialità d'impiego e facilitandone la diffusione su larga scala. La conseguenza è stata la creazione di una simil bolla deterministicamente rivolta alla diffusione di massa dello strumento. Il processo di implementazione, infatti, è avvenuto in pochissimo tempo, incluse le sue innumerevoli criticità derivanti da una maturazione assai precaria ed in divenire, non scevra da innumerevoli ripercussioni pratiche e sollecitudini per i soggetti preposti alla regolamentazione di settore[4]. La fascinazione dello strumento in questione, come era facile ipotizzare, ha interessato non solo le parti sottoposte a stimoli positivi, ma, per ragioni statisticamente ineludibili, anche attori criminali mossi da iniziative di interferenza ed interposizione fraudolenta nei sistemi delle relazioni umane economiche e sociali. In effetti, un'architettura informatica molto complessa e di difficile comprensione, anche per soggetti dotati di una qualche capacità tecnica, si prestava facilmente ad implementazioni elusive e capziose rivolte all'aggressione dei perimetri difensivi delle innumerevoli architetture informatiche poste a tutela dell'agire sociale. Molto difficile è strutturare un equilibrio tra la garanzia delle libertà di iniziativa economica e le esigenze di tutela della sicurezza collettiva da interferenze esterne rivolte a comprometterne il legittimo affidamento. In una simile prospettiva di elementi critici, non era possibile esimersi da valutazioni di contesto e proiezioni opportunisticamente rivolte al consolidamento delle necessarie garanzie verso sistemi ben bilanciati e forieri di una serenità relazionale

senza cui è quasi impossibile stabilire una convivenza sociale ed economica pacifica e strutturalmente solida[5]. L'economia, dal suo canto, non può pretendere il "liberi tutti" ed è indispensabile immaginare un regolatore in grado di intervenire tempestivamente in funzione di garante e tutore del libero arbitrio senza interferenze malevoli o, peggio ancora, artificiali.

3. Qualche cenno sulla tecnologia di *A.I.* generativa

Basata principalmente su modelli linguistici c.d. LLM, un sofisticato sistema di reti neurali, nell'*A.I.* una innumerevole mole di dati viene processata e recuperata da ogni possibile fonte messa a disposizione degli algoritmi durante il loro addestramento. La tecnologia di intelligenza artificiale c.d. generativa, per intendersi, è quella che più delle altre ha provocato il clamore mediatico ed il *boom* commerciale dalla distribuzione su larga scala dei suoi applicativi. Il suo funzionamento simula l'agire umano mediante una articolata sintesi statistica di determinazione dei vari passaggi lessicali, cioè, scegliendo e suggerendo, sulla base della rispettiva memoria di addestramento e dello stimolo linguistico del suo interlocutore, la più probabile tra le evoluzioni semantiche tra le innumerevoli possibilità ricavate nella sua memoria[6]. Il meccanismo di elaborazione informatica dipende, *in primis*, dalla mole di dati potenzialmente fruibili e messi a disposizione del calcolo algoritmico; e tutto ciò, però, è intrinsecamente collegato, in un circolo di autoperpetuazione della tecnologia derivante dalla mole di fruitori del sistema, i quali, nella possibilità di acquisizione di facili risposte degli algoritmi, alimentano essi stessi il suo percorso di crescita e maturazione, con tutto ciò che ne consegue in termini di *bias* e pregiudizi umanamente trasmissibili[7]. Della serie che la macchina, forse, può essere concettualmente intelligente, ma il suo substrato di alimentazione è pieno di difetti. D'altro canto, i recenti progressi nella costruzione di sistemi hardware, sempre più efficienti ed in grado di supportare gli elaboratori algoritmici nel loro processo di aggregazione statistica, hanno reso più efficiente la diffusione di servizi alla portata non solo di attori specialistici, ma, soprattutto, alla mercé della comunità generalista e tutto ciò che ne consegue in termini di vizi e virtù d'impiego. Nel giro di qualche anno, l'utenza media ha suggellato l'effetto sorpresa di quella che poteva essere tranquillamente definita come una tecnologia

non del tutto sconosciuta[8]. Gli innumerevoli testi accademici, la letteratura classica, nonché il mondo dell'arte ne sono emblematici testimoni. La stessa è stata a lungo riservata a contesti di nicchia specialistici, il più delle volte avvezzi ad elucubrazioni teoriche e filosofiche, evidentemente dissociate dalla realtà fattuale. In brevissimo tempo, è esplosa in tutta la sua potenza dirimente ed efficientista, sfruttando un sistema di relazioni generalmente predisposte a pressioni esterne delle tecniche. *ChatGPT*, *Lamda*, *Copilot*, ecc., sono tutte terminologie ed acronimi espressione di sofisticati sistemi informatici, ma, nel giro di pochissimo tempo, divenuti stilemi lessicali per *millennials* e *boomers* affascinati da un sottile senso di comunitarismo d'appartenenza ad una società interessata più al potere facilitante di strumenti inverosimili, di meno a stimolare perplessità e domande legittime sui meccanismi di funzionamento degli apparati. I sistemi di *A.I.* sono stati creati ad arte per efficientare ed assecondare pulsioni massimizzanti il profitto e la semplificazione del difficilmente accessibile per le masse omologate. Ogni giorno, infatti, arrivano notizie di immaginifiche e sensazionali svolte nell'uso della tecnologia di *A.I.* in una nuova corsa all'oro del progresso scientifico. In ciò la finanza ed il mercato non rimangono inerti dinanzi alle potenziali ed esponenziali possibilità di sfruttamento[9] della tecnologia algoritmica, senza tralasciare gli aspetti legati alla lotta geopolitica per un controllo il più possibile anticipatore delle novità tecnologiche, nell'ottica di un predominio classico delle dinamiche tra attori e potenze statuali[10]. Il legislatore, mediante tentativi di approccio normativo, spesso raffazzonati ed improvvisati, forieri di una rincorsa vacua dell'evoluzione tecnologica, nel malcelato tentativo di rassicurazione della comunità sociale, ha strutturato formule regolamentari di ogni tipo. Si è impiegato l'uso di raccomandazioni, testi normativi, linee guida, codici e codicilli, senza, però, mai intercettare il nucleo essenziale del pericolo rappresentato dalla realizzazione di sistemi intrinsecamente ostici. La difficoltà non risiede nella loro natura cibernetica del sistema di riferimento, ma nel fatto che l'intelligenza artificiale è stata costruita dall'uomo per mere esigenze umane, queste ultime, spesso e volentieri, poco avvezze al rispetto del prossimo e, invece, concettualmente ed intrinsecamente destinate ad interferenze negative su chiunque possa esserne colpito, in una logica del prendere senza mai dare[11].

4. Il concetto di *cybersecurity* nell'ecosistema globalizzato

Il concetto di *cybersecurity* nasce dall'esigenza di tutela delle funzioni primarie derivanti dall'evoluzione della tecnica nel contesto informatico. Già agli albori della implementazione computazionale, per merito delle prime integrazioni di processori rudimentali e conduttori magnetici in grado di erogare potenziale di calcolo con velocità ed efficienza prima mai viste, si riteneva opportuno integrare, per via complementare, meccanismi idonei e sufficientemente affidabili di mitigazione del rischio di un uso inappropriato di apparati elettronici e derivati[12]. Nel lontano 1948, infatti, un matematico come Wiener definì la cibernetica come «*lo studio del controllo e della regolazione (e autoregolazione) della macchina tramite la trasmissione e l'elaborazione di informazioni provenienti dall'esterno*». Nel tempo, poi, il concetto ha subito numerose estensioni rivolte necessariamente al contesto del linguaggio ed alla comunicazione in senso lato. L'uso e l'implementazione della cibernetica moderna hanno determinato una evoluzione o, per meglio dire, una contaminazione ineludibile dei substrati afferenti all'agire umano tra i più variegati, *in primis*, la rete relazionale ed i suoi meccanismi di interscambio reciproco tra i differenti attori ed i loro reciproci interessi[13]. Era inevitabile interessarsi di una materia così sofisticata e raffinata nella sua logica di sistema, dando vita ad una infrastruttura soggetta a crescita esponenziale, di anno in anno, contestualmente all'evoluzione di apparati e strumenti sempre più in grado di intervenire nel naturale flusso comunicativo[14]. La sicurezza informatica, o per usare inglesismi la *cybersecurity,* nasce dall'esigenza di protezione delle reti informatiche sviluppatesi nel tempo e, soprattutto, del loro prezioso bagaglio informativo, custodito mediante *server* e memorie fisiche costruite appositamente quali organismi serventi delle costruzioni matematiche dietro ogni singolo algoritmo di funzionamento dei processi automatizzati. In soccorso, come da protocollo e terminologie enciclopediche, la stessa Treccani definisce il concetto di sicurezza informatica come «*ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti*». Si tratta, a dire il vero, di una specie di calderone in grado di agglomerare quasi ogni singolo aspetto della vita odierna, senza reale distinzione tra ciò che ha una consistenza fisica e ciò che, invece, può essere

ritenuto vacua ed effimera energia computazionale. La differenza, seppur di facile comprensione, non è scevra da ripercussioni pratiche nell'ottica della gestione appropriata di rischi e misure di mitigazione[15]. La sfida primaria deriva dalla evidenza di una pervasività tecnologica in ogni aspetto dell'agire umano, sia in termini di utilizzo tecnologico che geopolitico ed economico. La stragrande maggioranza delle attività quotidiane, oggigiorno, dipendono dall'implementazione di sistemi informatici intelligenti ed ubiquitari, come *internet*, *smartphone*, reti di comunicazione, elettrodomestici, apparecchi medicali, automobili, ecc. Ultimo, non per importanza, l'arrivo sul mercato dei sistemi di intelligenza artificiale generativa, in grado di pervadere e, per meglio dire, ottundere, il senso comune dell'affidamento nel reale[16]. Come nei sistemi fisici si tende a costruire idonee misure di sicurezza ed affidabilità, ovvero, *crash test* per automobili, test anti-fusione per centrali nucleari, vaccini contro virus e pandemie, nel contesto informatico, l'approccio degli addetti ai lavori non è poi molto diverso. Le esperienze maturate in altri contesti, infatti, possono agevolare la definizione e la strutturazione di idonei meccanismi rivolti alla salvaguardia di affidabilità delle reti informatiche globali e non solo. Possono essere create reti di salvataggio dei dati mediante configurazioni di *backup* programmati per poi recuperare il tutto mediante appropriati piani di ripristino del sistema con *recovery plan;* oppure, si possono installare appropriati sistemi antintrusione come *firewall antivirus* per evitare penetrazioni fraudolente e non volute[17]. Nel passato si vociferava, addirittura, di volontà deterministica delle case produttrici dei sistemi informatici, le quali avrebbero creato i diversi agenti virali, al solo fine di erogare idonee risposte di contenimento alla rispettiva utenza. Ora, invero, si parla addirittura di superiori intelligenze artificiali in grado di violare coscientemente, senza eterodirezione umana, ogni sistema dell'articolato mondo computazionale[18]. Difficile in tutto ciò trovare un senso del vero! Diviene inevitabile porsi alcune giuste domande in merito ai possibili rischi derivanti da banalizzazioni e generalizzazioni, quasi ai margini della superstizione d'altri tempi e non coerenti con la necessaria visione razionale ed equilibrata cui è destinato il decisore e regolatore nella sua essenziale funzione di garanzia della pacifica convivenza civile[19].

5. Il fenomeno *Cyber* nel suo dinamismo di facciata

Per effetto di convenzioni sociali e comunicative, è curioso ricordare come le prime manifestazioni documentate di attività spionistiche nel cyberspazio possano essere fatte risalire al periodo tra settembre 1986 e giugno 1987, ad opera di alcuni gruppi di *hackers* tedeschi. Mediante l'opera sistematica della violazione delle reti di appaltatori della difesa ed Università americane, durante il difficile periodo della guerra fredda, trasferirono le informazioni, estorte in maniera fraudolenta, ai nemici del tempo del KGB, i servizi secreti sovietici. Il leader del gruppo, nella figura di Markus Hess venne fortunatamente, almeno per i suoi detrattori della controparte occidentale, arrestato solo nel giugno dell'87, incriminato nell'89 e poi formalmente condannato per spionaggio nel febbraio del '90, a ridosso della caduta del muro. Mitnick, uno dei più famosi *hacker* moderni, venne arrestato dall'F.B.I. statunitense nel '95, probabilmente per le sue capacità di violare i sistemi del N.O.R.A.D. Questa breve ripetizione storica serve non tanto per rievocare episodi di elementare mitizzazione di attori relegati alla cultura *pop* e *nerd*, quanto a riconsiderare la banalizzazione ed il potenziale dirimente di attività dal notevolissimo impatto sistemico, se non perfettamente compresi e mitigati[20]. Ora, è vero che l'interventismo normativo e la repressione poliziesca degli apparati di sicurezza hanno più volte mostrato *vulnus* e perplessità spesso inaccettabili, ma è, altrettanto, vero come una indifferenza cieca alle minacce derivanti dall'implementazione delle reti informatiche, senza le idonee misure di sicurezza, avrebbe e può continuare a rappresentare un enorme rischio per qualsiasi integrazione della tecnologia nei sistemi relazionali. Siano essi di tipo istituzionale e formale, piuttosto che voluttuosamente relegati alle edonistiche suscettibilità umane di facilitazione della vita quotidiana, o, più correttamente, alla semplice e pura esigenza di supporto nella pressione emotiva della società contemporanea, complessità degli apparati tecnologici di supporto e l'innata tendenza umana alla loro sperimentazione, determinano esigenze di approfondimento degli aspetti di funzionamento delle macchine poste al servizio del progresso sociale, incluse componentistica, reti di memorizzazione delle informazioni e loro eterointegrazione nelle reti comunicative. Gli stessi concetti di sicurezza e affidabilità, così articolati e complessi nel loro nucleo essenziale, sono direttamente proporzionali alle capacità umane di saper sfruttarne

vulnerabilità e possibili meccanismi di elusione. Aumentando la superficie di attacco, aumenta, così, anche la richiesta di competenze idonee a mitigarne le criticità ed il ruolo del decisore[21]. In un simile scenario d'incertezza computazionale, il sistema di garanzie diviene dirimente per gli attori coinvolti, ma anche essenziale nel nucleo di argomentazioni concepite ad arte per i più variegati propositi, di volta in volta, posti alla base delle costruzioni di sofisticati sistemi elettronici ed informatici. All'aumentare dell'incertezza, aumenta anche la richiesta di opportune competenze per il suo contenimento e per ogni livello tecnologico, legato intrinsecamente al livello successivo. Si rende in tal senso indispensabile creare una sufficiente struttura di controllo, mediante protocolli per la gestione delle tecnologie in questione. Partendo dalla produzione del dato grezzo alla sua trasmissione e ricezione, cercando di carpirne potenziali vulnerabilità e strutturando idonee contromisure, si possono o devono sfruttare, studiare, controllare, rafforzare e gestire con altrettanti protocolli, macchine e programmi[22]. Un ruolo determinante è rappresentato, come in ogni altro settore, dall'agire umano e tutto quel che ruota intorno all'infrastruttura informatica e ai dati, ovvero persone, accessi fisici, continuità energetica ecc., apportando una distinzione, di matrice anglosassone, tra ciò che afferisce alla *security* e ciò che più propriamente determina la *safety.* È necessario difendersi da attacchi, tipologia di attacco, mezzo di attacco derivanti dall'esterno, o, più adeguatamente, serve essere consapevoli dei rischi e di quanto il fattore umano interno sia adeguatamente preparato ad affrontare simili circostanze[23]. È sufficiente, infatti, effettuare un breve *excursus* tecnico, anche per non addetti ai lavori, per comprendere quanto sia variegato l'universo delle vulnerabilità cibernetiche e quanto queste siano il più delle volte determinate da insipienze progettuali e successive implementazioni nei sistemi d'uso. Dinanzi ad un simile scenario d'incertezza funzionale, è molto difficile garantire la sicurezza assoluta dei sistemi di riferimento, anzi, è essenziale introiettare e gestire un certo margine di tolleranza, derivante da una seria analisi dei rischi. Sarà la successiva implementazione di idonee misure di mitigazione dell'impatto di buchi del sistema di sicurezza, il cui gradiente di pericolosità dipende dal potenziale distruttivo sul destinatario del servizio, sia esso finanziario, medico, culturale, infrastrutturale, mediatico, istituzionale o geopolitico a dare concretezza effettiva all'intervento di mitigazione[24]. Nell'architettura difensiva non può essere eluso il

rischio di abusi ed inefficienze di scala contro cui un legislatore, serio ed attento, dovrebbe garantire affidabilità e, soprattutto, una notevole capacità di analisi dei possibili scenari. Non sono utili alla risoluzione del problema esagerazioni di maniera, poco funzionali allo scopo o, peggio ancora, concepite al solo fine di rassicurazione ed imbonimento delle masse, preoccupate e timorate dalle meraviglie della tecnica. Professionisti e specialisti di settore meritano consapevolezza pratica e visione teorica d'insieme, con prospettiva sicura d'intervento in caso di necessità, ma con ragionato ed equilibrato tatto nel mondo del reale, senza sensazionalismi o manierismi di facciata[25].

6. La risposta del regolatore europeo alle esigenze di sicurezza informatica

Nonostante i modelli linguistici basati sulle reti neurali siano divenuti componenti essenziali dei sistemi di intelligenza artificiale, da soli, non rappresentano essi stessi l'*A.I.* nel suo complesso. Alla luce di ciò, bisogna considerare il concetto di sicurezza informatica applicato alle intelligenze artificiali generative non come strumento di compartimentazione a tenuta stagna dei singoli elementi, bensì, come approccio omnicomprensivo, rivolto agli applicativi in modo uniforme, senza tralasciare aspetti ritenuti superficiali o accessori. Al fine di garantire conformità normative ai requisiti di sicurezza, è necessario condurre una valutazione del rischio che tenga conto della progettazione dei sistemi in modo integrato e continuo, sfruttando, quando possibile, pratiche e procedure consolidate insieme ad innovative misure di mitigazione del rischio confezionate per l'uso specifico dell'*A.I.*[26]. Nonostante, allo stato dell'arte, non sia agevole garantire una sicurezza assoluta per i sistemi di intelligenza artificiale di ultima generazione, un certo margine di conformità ai requisiti di sicurezza informatica può essere garantito attraverso l'adozione di misure già sperimentate su altri apparati e non necessariamente calibrate in modo esclusivo sull'*A.I.*[27]. Un simile approccio, tuttavia, a ragion veduta, non sempre è possibile o agevole; in effetti, alcuni sistemi, considerati ad alto rischio dalla normativa europea, il cui meccanismo di funzionamento impiega tecnologie emergenti dal difficile inquadramento tecnico, potrebbero non rispettare i canoni di conformità stabiliti dal regolamento europeo 1689 del 13 giugno 2024 (c.d.

A.I. Act.). All'art. 6, vengono definiti ad alto rischio quei sistemi coerenti con alcuni requisiti critici, relativi alla sicurezza e alla conformità richiesta per la garanzia di alcune vulnerabilità afferenti alla tutela dei diritti fondamentali. Ciò che, evidentemente, il legislatore europeo ha inteso, in prima istanza, tutelare con il costrutto normativo del regolamento è costruire un certo margine di affidabilità ed affidamento nei confronti dei sistemi ritenuti più pericolosi ed innovativi, soprattutto, per l'utenza avvezza all'impiego in contesti altamente sensibili dell'agire umano. La crescente diffusione dell'*A.I.*, secondo il legislatore europeo, richiede necessariamente una particolare attenzione alla protezione di tali innovativi modelli informatici, ai dati impiegati per la loro formazione e implementazione nelle *routine* quotidiane[28]. In tal senso, gli *standards*, richiesti ed istituiti con la regolamentazione europea, possono svolgere un ruolo fondamentale nel garantire affidabilità e robustezza di sistema durante il ciclo di vita delle intelligenze artificiali. Gli stessi devono, però, essere accompagnati da una consapevolezza generale circa la fallibilità e la perfettibilità di modelli calibrati su meccanismi in continuo divenire, sottoposti a progressivi aggiornamenti ed incremento del potenziale computazionale. Gli *standards* europei, istituiti con i vari interventi normativi, sebbene costituiscano un lodevole inizio, rappresentano un primo ed importante punto di riferimento per uno sviluppo etico e responsabile dei sistemi di intelligenza artificiale. Allo stesso tempo, non sono altro che un piccolo e significativo salto nel buio sulle possibili implicazioni derivanti dalla sua applicazione in concreto[29]. La creazione di *standards* di sicurezza per apparati, da considerare essenzialmente come scatole nere imperscrutabili, rappresenta una notevole sfida per il regolatore; infatti, già nel maggio del 2023, la Commissione europea ha chiesto al Comitato europeo di normazione e al Comitato europeo di normazione elettrotecnica (CEN-CENELEC) di elaborare *standards* a supporto del regolamento. Non solo il CEN-CENELEC (gruppi JTC 13 e JTC 21), ma diverse altre organizzazioni di elaborazione, tra cui l'Istituto europeo per gli standard di telecomunicazione (ETSI) e l'Organizzazione internazionale per la normazione (ISO), stanno lavorando allo sviluppo di *standards* specifici di sicurezza per l'*A.I.* Anche se la maggior parte di quelli armonizzati e specifici non sono ancora definiti, alcuni di uso generale per la sicurezza delle informazioni, (come ISO/IEC 27001 e ISO/IEC 27002) e la gestione della qualità (come ISO/IEC 9001) sono già

disponibili per l'utenza e i gestori di servizi, potendo essere potenzialmente e parzialmente applicati anche ai sistemi di intelligenza artificiale disponibili sul mercato[30]. Nell'evidente assenza, dunque, di regole organiche in merito alla sicurezza informatica delle tecnologie in questione, le diverse Agenzie si sono mosse autonomamente nella definizione di un quadro di riferimento più preciso, al fine di garantire un certo grado di uniformità cui poter fare riferimento nelle attività operative degli attori di settore. Prima fra tutte, l'Agenzia europea per la sicurezza informatica (ENISA) si è mossa verso tale orientamento, pubblicando un quadro di sicurezza multilivello per le buone pratiche di sicurezza informatica dell'intelligenza artificiale (FAICP). Offrendo, ai potenziali fruitori dello stesso, un approccio graduale al fine di migliorare l'affidabilità e la solidità dei sistemi *A.I.* Il modello, costruito su tre differenti livelli di sicurezza, mette al primo piano la sicurezza dell'infrastruttura informatica impiegata ICT, accrescendo, via via, il grado di intervento e consapevolezza in base alla specificità dei componenti implementati nel sistema e al settore operativo di destinazione della tecnologia. Qualcosa di molto simile è rinvenibile anche nell'approccio d'oltreoceano da parte del NIST, il *National Institute of Standards and Technology* statunitense, il quale, in qualità di organo di riferimento nell'implementazione dei sistemi tecnologici ed informatici sul suolo federale, ha provveduto a pubblicare *frameworks* di gestione del rischio nell'impiego di *A.I.* per aiutare a mitigarne gli effetti e contribuire alla sua affidabilità, nonché, alla responsabilizzazione degli operatori coinvolti nei processi di sviluppo ed impiego su larga scala[31]. Si tratta di una scelta di stile, per come inteso il quadro giuridico anglosassone, normativamente poco vincolante, ma allo stesso tempo un punto di riferimento di cui tener conto anche nel contesto europeo, al fine di una migliore compliance di sistema nell'ottica di una progressiva implementazione a cascata nei diversi stati dell'unione[32]. Nel *summit* sul miglioramento del quadro di *safety*, avvenuto nel 2023, è stata diffusa una serie di raccomandazioni per gli sviluppatori relative ad ogni fase del progressivo ciclo di impiego dei sistemi *A.I.* relative a progettazione, gestione e manutenzione delle stesse[33]. Non da meno, anche i principali attori del settore privato e multinazionali come Amazon, IBM, Google, Meta ecc., nell'ottica di una ottimizzazione dei processi di affidabilità e solidità degli apparati disseminati nell'economia di mercato, hanno progressivamente pubblicato rispettivi *frameworks* di sicurezza nel rispetto dell'etica gestionale e

per la prevenzione di minacce all'immagine di affidabilità dei loro prodotti[34].

7. L'*A.I.* come minaccia e opportunità per la sicurezza informatica

Il tema della sicurezza informatica è divenuto, al tempo d'oggi, un riferimento assoluto per chiunque voglia approcciare coscientemente ai sistemi di comunicazione moderni. Non solo, il costante progredire della tecnica ha richiesto sempre più sofisticati *escamotage* ingegneristici in grado di assicurare un qualche margine di affidabilità ad apparati estremamente pervasivi e in grado di scombussolare, in pochissimo tempo, i più elementari meccanismi di condivisione delle dinamiche relazionali. Il fatto che una tecnologia come l'intelligenza artificiale possa essere interpretata ed introiettata con riserve non deve stupire! Risiede, infatti, nella natura umana approcciare a qualsiasi novità ravvisandone non solo il potenziale migliorativo per i normali processi di sviluppo della società, ma anche il grimaldello subdolo di sofisticate elusioni delle regole, sfruttandone criticità e zone grigie[35]. In generale, la tecnologia deve essere intesa come strumento il cui risultato d'impiego dipende principalmente dallo scopo e dall'uso specifico scelto dall'uomo, in una elementare delega di funzioni organiche o metafisiche inscindibilmente legate all'attitudine soggettiva del fruitore. Nell'ottica di un approccio funzionalmente critico, molti dei principali attori di sistema, come già accennato, hanno coscientemente intrapreso la strada della consapevolezza etica, approntando meccanismi specifici di mitigazione dei rischi, ma, soprattutto, sfruttando l'evidente potenziale computazionale dei progressi informatici. Tutto ciò è avvenuto nell'ottica di un miglioramento di affidabilità e garanzia dei valori di sicurezza generale, non solo tecnologica[36]. Un gruppo di multinazionali del ramo tecnologico come Google, Amazon, Microsoft ecc. ha iniziato a convertire il paradigma interpretativo dell'*A.I.* evidenziando non solo minacce e *vulnus* per la sicurezza collettiva, bensì opportunità di garanzia, mediante un impiego etico della sicurezza informatica basata su rilevazione, analisi, previsione e mitigazione dei rischi connessi all'uso dell'intelligenza artificiale. L'*A.I.,* infatti, se ben impiegata, può prevenire ipotetiche minacce, ma anche contrastare il potere distorsivo della legittima affidabilità collettiva agli apparati tecnologici derivanti dall'uso criminale degli

stessi. Le tecnologie di apprendimento automatico sono in grado di generare potenziali *malware*, ma anche di evitarne e contrastarne gli effetti pratici[37]. La stessa Google sostiene che l'intelligenza artificiale è in grado di invertire il c.d. "dilemma del difensore", il tipico dilemma etico nella scelta tra la difesa del proprio egoistico ed il giusto collettivo, aiutando professionisti della sicurezza informativa ad ampliare il loro margine d'intervento. Google afferma, inoltre, che l'*AI* generativa ha contribuito a un «*risparmio di tempo del 51% e a risultati di qualità superiore nell'output degli analisti di incidenti per le loro attività interne di rilevamento e risposta*», suggerendo, anche, come il suo specifico sistema di intelligenza generativa chiamato "*Gemini"* sia stato in grado di ampliare le capacità di rilevamento delle vulnerabilità dei sistemi analizzati. Non si tratterebbe, secondo l'azienda, solo di capacità *real time* nella gestione delle minacce, bensì di prevederne la possibile evoluzione o, addirittura, il possibile manifestarsi in un momento determinato. L'ENISA, infatti, coerentemente alla sua missione, suggerisce d'impiegare l'*A.I.* per segnalare possibili interruzioni nella fruibilità dei sistemi *IoT*. Google, inoltre, segnala come il suo sistema sia in grado di formulare modelli previsionali derivanti dall'analisi dei dati URL (U*niform Resource Locator*) ritenuti dannosi e collegati al suo servizio di navigazione[38]. Le moderne tecnologie di intelligenza artificiale sono in grado anche di analizzare interi codici sorgente al fine di rilevarne e classificare i possibili *malware* introdotti con artificio ed inganno per l'utenza media. Strumenti come "*Virus Total*", un *software* di proprietà della stessa Google, hanno già dimostrato come la scansione, sempre mediante *A.I.,* possa migliorare l'analisi dei *malware* prevenendo i c.d. falsi positivi. Migliorare l'accuratezza del rilevamento, infatti, può, determinare un efficientamento generale degli apparati, garantendo una risposta adeguata solo a minacce reali, quando le stesse si rendono realmente pericolose e laddove è richiesto effettivamente un intervento esterno di operatori specializzati, il cui impiego richiederebbe altrimenti enorme dispendio di energie e risorse. In un simile quadro d'impiego, le soluzioni di sicurezza basate sull'implementazione dell'*A.I.* possono migliorare notevolmente i tempi di risposta agli incidenti informatici dando priorità a minacce concrete, identificando tendenze o prevenendo minacce future[39]. Tuttavia, come è facile immaginare, ciò che, in linea teorica, può rappresentare una concreta opportunità di miglioramento dell'affidabilità e sicurezza informatica, può, allo

stesso tempo, determinare enormi criticità, se impiegato per attacchi da parte di malintenzionati attori criminali[40]. La stessa ENISA sottolinea come i sistemi di intelligenza artificiale stiano diventando estremamente efficaci nelle tecniche di manipolazione sociale, grazie, soprattutto, alla loro intrinseca capacità di simulare le interazioni umane[41]. I recenti modelli di LLM sono emblematicamente rappresentativi nel quadro di potenziale aggressione dei valori democratici per una equilibrata e pacifica convivenza della società civile. Bisogna poi considerare i potenziali effetti dirompenti di tecnologie come il *deepfake*, in grado, nelle forme più evolute, di riprodurre interi segmenti grafici del tutto indistinguibili dal reale se non per alcune sfaccettature di non facile comprensione per l'utenza media, anzi, molte volte in grado anche di superare il vaglio specialistico di tecnici ed operatori di settore. I *prompt* d'ingaggio, nella loro variegata e sconfinata possibilità creativa derivante dalla mente umana, determinano una consistente minaccia di ridefinizione dei consolidati canoni di riferimento tra il vero ed il falso[42]. I software di rilevamento delle minacce proposti dai principali attori sul mercato, come Microsoft e OpenAI non hanno mostrato, almeno fino ad ora, «*tecniche di attacco o abuso innovative o uniche*» basate sull'impiego dell'*A.I.* da parte degli autori delle minacce, ma le aziende in questione sottolineano come sia indispensabile garantire un continuo monitoraggio degli applicativi al fine di prevenirne usi distorsivi dell'ordine democratico. Nonostante OpenAI ritenga la sua tecnologia di punta, *ChatGPT,* un sistema con «*funzionalità limitate e incrementali per attività di sicurezza informatica dannose, oltre a quanto già realizzabile con strumenti pubblici non basati sull'A.I.*», il gruppo tecnico per lo sviluppo del modello *ChatGPT-4,* uno tra i più evoluti sul mercato, già nel 2023 ha identificato nel suo rapporto di presentazione «*comportamenti emergenti rischiosi*»[43]. Il documento, infatti, rivela come i nuovi modelli possiedano peculiari capacità di *phishing* o elusione dei sistemi di sicurezza basati sul criterio "*CAPTCHA*", con cui tutti, almeno una volta nella nostra intensa vita informatica, abbiamo dovuto fare i conti per superare barriere di accesso su siti e servizi vari. Tali capacità, ad avviso degli esperti, mostrerebbero una spiccata tendenza di potere dominante dei modelli più evoluti, a scapito, evidentemente, del necessario senso di affidabilità collettiva nei confronti dei sistemi in questione, sempre più diffusi e pervasivi. Le potenzialità d'impiego dei moderni sistemi di intelligenza artificiale non esauriscono il loro bacino di riferimento

esclusivamente in tipologie d'impiego commerciale, ma potrebbero, anche secondo quanto sostenuto dai ricercatori di Google, essere impiegati nella decriptazione di complesse chiavi di cifratura impiegate in contesti critici ed afferenti alle garanzie di sicurezza generale, difficilmente suscettibile a compromessi al ribasso nella logica di mercato[44]. Gli stessi ricercatori di Google hanno evidenziato una «*urgente necessità di ideare nuove protezioni resilienti agli attacchi di* "*deep learning*"». La ricerca e sviluppo nel settore delle intelligenze artificiali vede l'interesse e la spinta di diverse aziende del settore *tech*, tuttavia, da alcune, in particolare, sta emergendo la costruzione di modelli dai risvolti potenzialmente dirompenti nel comparto della *Cybersecurity* e della tutela di riservatezza di settori altamente sensibili per le ripercussioni pratiche ed economiche. Il modello prodotto dalla società Anthropic, chiamato "Mithos" ha sollevato l'attenzione di numerosi esperti per la sua intrinseca e dichiarata capacità di individuare le numerose vulnerabilità informatiche diffuse nei vari applicativi immessi sul mercato e, soprattutto, la capacità di strutturare ed elaborare le possibili modalità di sfruttamento. Secondo il sito di informazione Axios, la stessa amministrazione americana, già in conflitto con la società Anthropic per le richieste non accolte in merito all'impiego dei sistemi offerti dall'azienda in alcuni comparti delle attività militari e di difesa nazionale, starebbe pensando all'elaborazione di alcune linee guida federali che potrebbero consentire alle varie agenzie le classificazioni di rischio in merito all'impiego degli applicativi come Mithos. Lo stesso Donald Trump ha affermato come la società Anthropic si stia *"rimettendo in carreggiata"* agli occhi dell'amministrazione statunitense, rendendo evidente come le innovative proposte in tema di *A.I.* suscitino l'interesse degli apparati burocratici in merito al loro potenziale, temendone, però, il relativo pericolo, se non confinate entro margini sicuri e collaborativi d'impiego[45]. La caratteristica principale di Claude Mithos risiede nella possibilità del software di individuare in autonomia i c.d. *zero-day bug*, presenti fin dall'origine di progettazione dei sistemi operativi e *browser* immessi nel mercato. Nel complesso contesto di interlocuzione degli attori di settore, in un misto di *hype, fact-checking* e allarmi CERT UE il nuovo fenomeno Mithos dovrebbe interessare nel futuro il rapporto coordinato tra le capacità rappresentate dall'*A.I.* generativa *disclosure* e vari obblighi normativi (NIS2, CRA, DORA). Insomma, in un simile quadro di riferimento, è veramente

difficile riuscire a costruire un equilibrato quadro per attori e fruitori dei servizi informatici e, alla luce delle recenti evoluzioni nei modelli di intelligenza artificiale, diventa sempre complesso implementare un'architettura *Cyber* resiliente, in grado di garantire l'affidabilità informatica necessaria alle interazioni continue nel libero mercato. Il compito è notevolmente delicato non solo per chi ha una spiccata cognizione tecnica della materia, ma, soprattutto, per chi, come il decisore, si trova il più delle volte spiazzato da fenomeni esplosivi e dirompenti derivanti dall'evoluzione tecnologica. L'*A.I.,* in tutto ciò, è emblematicamente rappresentativa, ma la sua complessità intrinseca non può, allo stesso tempo, divenire elemento giustificativo di massima per pigrizie e disattenzioni del legislatore chiamato a dare certezze e porre freni a possibili derive[46].

8. Le Direttive NIS 1 e 2 ed il Regolamento europeo sulla *Cybersecurity*, il frutto avvelenato di una solerzia poco focalizzata

Il tema relativo alla sicurezza informatica, come si può ben immaginare, non riguarda esclusivamente nuclei elitari di nicchia, relegati alle loro elucubrazioni di inconciliabile definizione algebrica, ma riguarda, in un modo o nell'altro, qualsiasi attività della vita contemporanea, il cui unico interesse è ottimizzare i processi relazionali mediante strumenti ed apparati tecnici in grado di rendere la vita un po' più agevole dinanzi alle innumerevoli difficoltà e complessità quotidiane. Il ruolo del legislatore o regolatore di settore è sempre stato quello di rappresentare non tanto un ineludibile sovrapprezzo da pagare alla normale evoluzione della tecnica, bensì di un ragionevole supervisore delle potenziali distorsioni continuamente messe in evidenza dall'enorme vulnerabilità di sistemi indefiniti o difficilmente definibili per via della loro intrinseca novità o artificiosa elaborazione. Riuscire a strutturare architetture normative in grado di conciliare differenti esigenze di tutela, soprattutto, sicurezza e libertà di mercato, è compito assai difficile[47]. Alcuni tentativi di rimedio regolatorio hanno rappresentato e continuano a rappresentare il principale strumento d'intervento, al fine, evidentemente, di garantire qualche punto oggettivo di riferimento per gli operatori di settore. Allo stesso tempo, ciò può rappresentare, anche, una qualche forma di rassicurazione per l'utenza media, chiamata ad implementare la

tecnologia nella propria attività lavorativa, ricreativa e sociale[48]. Per rimanere nel contesto europeo, una prima significativa architettura o tentativo di intervento a garanzia della *cybersecurity* è stata messa in opera mediante l'introduzione della direttiva NIS 1, nel lontano 2016, quasi un'era geologica fa, se applicata al contesto *cyber.* Intesa come primo effettivo corpo normativo rivolto alla definizione di principi e quadri di riferimento per il settore, la direttiva, nella convinzione di un necessario e tempestivo intervento sul settore informatico. Anche in virtù delle spinte securitarie determinate dalla recrudescenza di particolari fenomeni di matrice criminale, come il terrorismo di matrice islamica, è strutturata in modo tale da determinare una prima importante spinta degli stati nazionali ad uniformare il quadro di riferimento, mediante il rispetto di appositi requisiti per l'operatività di alcuni settori ritenuti strategici, tra cui energia, infrastrutture, sanità, difesa, ecc.[49]. Allo stesso tempo, ha previsto una specifica *road map,* suddivisa per fasi, al fine della costruzione di appositi organismi autonomi o agenzie, in grado di apportare il necessario supporto tecnico all'implementazione degli apparati informatici o in caso di attacchi *hacker* provenienti da agenti malevoli. Il coinvolgimento del settore privato nel processo di integrazione normativa, unito alla necessaria supervisione del regolatore pubblico, ha determinato non poche difficoltà applicative, derivanti da evidenti difficoltà di conciliazione delle contrastanti esigenze, nonché dalle irrimediabili inefficienze degli apparati burocratici, afflitti da decenni di ritardi nell'aggiornamento informatico e da strutturali carenze di personale specializzato per via dei blocchi al *turnover* dei propri dipendenti. La creazione di apposite agenzie, si veda a titolo di esempio l'ACN nostrana o di organismi di risposta e raccordo, in caso di attacco informatico, come il CSIRT, non ha garantito il giusto livello di affidamento da parte degli attori coinvolti, forse impattati da novità e obblighi di conformità imposti senza un'appropriata conoscenza dello stato dell'arte e del relativo grado di maturazione del settore[50]. Un simile quadro di incertezza, anche al fine di evitare scatti in avanti o singole iniziative troppo temerarie e poco focalizzate sul problema, ha necessariamente spinto il regolatore verso altri interventi. Gli stessi sono tesi ad un maggior grado di uniformità ed integrazione europea in ambito *cyber,* da cui è uscito fuori un primo essenziale corpo normativo, generalmente applicabile in ogni sua previsione in ogni stato, sotto forma di regolamento[51]. La strategia di difesa uniforme dagli attacchi era

ormai evidente, così nel 2019 nasce il regolamento UE sulla Cybersicurezza, mediante cui si istituisce l'agenzia unica ENISA, nonché un sistema di certificazioni riconosciute sull'intero suolo europeo. Considerato l'aumento di attacchi informatici e l'emersione delle criticità relative all'implementazione di nuove tecnologie emergenti, l'UE, forse spinta da una intrinseca esigenza regolatoria, tramite varie conclusioni e linee d'indirizzo, ha cercato di indirizzare gli organi preposti verso la creazione di una legislazione di tipo orizzontale per meglio affrontare tutti gli aspetti attinenti alla cibersicurezza dei dispositivi connessi, quali la disponibilità, l'integrità e la riservatezza. Partendo dal presupposto che i c.d. dispositivi connessi e la loro sicurezza informatica svolgeranno un ruolo determinante nel plasmare l'architettura digitale dell'UE, l'insieme di un'architettura uniforme dovrebbe contribuire a tutelare il «*mercato unico digitale, anche in settori come il commercio elettronico, la mobilità intelligente e l'internet delle cose, e ad accrescere l'autonomia dell'UE nel settore della cibersicurezza*»[52]. Unite alla necessità di contrastare le minacce ibride, compresa la disinformazione, si è resa evidente, per il regolatore europeo, l'esigenza di delineare un «*quadro di resilienza per proteggere i cittadini e le imprese dell'UE dalle minacce informatiche, promuovere sistemi informativi sicuri e proteggere un ciberspazio globale, aperto, libero e sicuro*»[53]. Dopo un lungo processo di interlocuzione e verifica sul campo, anche in virtù dell'emergere di nuove minacce derivanti dai conflitti bellici sul suolo europeo e le conseguenze sull'affidabilità dei sistemi interessati da campagne di disinformazione e sabotaggio, al fine di consolidare posizioni e tesi delle parti interessate dagli scontri, generando così una nuvola di indefinita ed assoluta incertezza dimensionale, si è resa evidente la necessità di continuare nel percorso di arricchimento normativo attraverso ulteriori interventi, in grado di consolidare le posizioni securitarie già incardinate nei precedenti[54]. Dunque, «*al fine di migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo complesso*», nel novembre del 2022 nasce la Direttiva NIS 2. La stessa è destinata a sostituire la prima, stabilendo una nuova base di riferimento normativo per l'adozione di misure per la gestione dei rischi cibernetici da parte degli stati membri, unita all'imposizione di obblighi di segnalazione in caso di attacco alle infrastrutture primarie indicate e contemplate dalla direttiva[55]. Mirando ad armonizzare ulteriormente i requisiti minimi nel

comparto della cybersicurezza, mediante l'introduzione di norme minime per la cooperazione dei vari stati, la direttiva ha introdotto un elenco aggiornato dei settori ritenuti a rischio di compromissione. Ha, contestualmente, previsto mezzi idonei di segnalazione e sanzioni appropriate per garantirne l'applicazione ed il rispetto. Se dalla precedente NIS 1 emergeva la responsabilità, per gli stati, di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali, con la NIS 2 si introduce una regola di soglia dimensionale generale. La conseguenza è che tutti i soggetti di medie e grandi dimensioni, i quali operano nei settori o forniscono i servizi contemplati dalla direttiva, rientreranno nel suo ambito di applicazione. Le disposizioni rivedute con la NIS 2, mentre sono funzionali alla creazione di un adeguato meccanismo di proporzionalità e garanzia contro il rischio con criteri applicativi più chiari, allo stesso tempo, riducono il proprio margine d'intervento in settori particolarmente sensibili come la difesa o la sicurezza nazionale, la pubblica sicurezza e la relativa attività di contrasto. Anche il settore giudiziario, i parlamenti e le banche centrali sono esclusi dall'ambito di applicazione[56]. Rimane contemplato, però, il contesto delle pubbliche amministrazioni, sia di livello centrale che regionale[57]. La direttiva, inoltre, è stata, fortunatamente, allineata ed uniformata alla legislazione di settore, in particolare al regolamento relativo alla resilienza operativa digitale per il settore finanziario (DORA) e alla direttiva sulla resilienza dei soggetti critici (CER), sia per fornire chiarezza giuridica che per garantire la coerenza tra tali atti e la nuova disciplina. Il fine dovrebbe essere quello di permettere agli Stati interessati dalla sua implementazione di generare un volontario apprendimento, in condizioni di pari opportunità, accrescendo fiducia delle parti e costruzione di buone pratiche di riferimento per il settore, contribuendo a creare il giusto livello comune di affidabilità cibernetica[58]. L'eccesso di segnalazioni o falsi positivi, con ciò che ne comporta in termini di peggioramento dell'efficienza generale di sistema o ripercussioni oggettive economiche difficilmente accettabili dagli operatori privati, dovrebbe, inoltre, essere garantito dalla nazionalizzazione dell'onere sui singoli Stati. Nuove minacce e nuovi attori malevoli sono sempre dietro l'angolo e in ciò l'emersione di tecnologie come l'*A.I.* può determinare, come d'altronde già avvenuto anche in passato, fattori critici di notevole compromissione dell'architettura generale[59]. I lodevoli tentativi e la solerzia del legislatore nel cercare di seguire il passo dell'evoluzione tecnologica si scontrano

inevitabilmente con l'esigenza di garantire un appropriato margine di affidamento; senza eccedere in manierismi normativi e lessicali, mossi da esigenze definitorie non in grado di intercettare le reali circostanze concrete in cui la minaccia può divenire realmente effettiva. Bene l'attenzione costante del regolatore, ma attenzione a non superare quel sottile confine tra ciò che serve al sistema e ciò che, invece, si deve metter nero su bianco per assecondare emotività e sensazionalismo, non in linea con la complessità tecnica[60].

9. L'architettura normativa del legislatore interno

Lo stimolo all'implementazione normativa sulla sicurezza informatica dell'Unione europea, anche per mezzo del suo organo esecutivo rappresentato dalla Commissione, ha condotto il regolatore, come già detto, ad intraprendere il percorso di regolamentazione specifica sul tema. Nel tentativo di generare una armonizzazione più consistente delle regole del gioco, lo stesso si è mosso al fine di contenere e modulare i molteplici aspetti critici legati all'impiego di moderne tecnologie, in grado di rappresentare un serio pericolo per il mercato interno, soprattutto, con riferimento alla tutela delle libertà fondamentali, senza, però, tralasciare i potenziali elementi di carattere positivo. Nel caso specifico dell'impiego di *A.I.,* il regolatore europeo ha ritenuto che una concreta mitigazione dei rischi legati al suo impiego possa avvenire solo mediante una legislazione complementare con norme proporzionate e flessibili. Solo con un simile approccio normativo, dunque, l'Unione europea potrebbe divenire un punto di riferimento globale nel settore dell'intelligenza artificiale[61]. L'architettura normativa implementata con l'*A.I. Act*, basata sui differenti quattro livelli di rischio, inaccettabile, elevato, limitato e minimo, comporta una risposta graduata al notevole progresso tecnologico rappresentato dall'arrivo dell'*A.I.*; secondo una rappresentazione di sistema che la stessa Commissione, con il regolamento specifico sul tema, ha ritenuto essere lo strumento proporzionato ed equilibrato, in grado di preservare «*la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione*»[62]. Nelle Conclusioni della presidenza del Consiglio europeo n. 11481/20/2020 è stato chiarito come la vera cartina al tornasole per il rispetto dei

diritti fondamentali nell'applicazione delle norme sull'impiego dell'intelligenza artificiale sia di tenere sempre in considerazione l'opacità, la complessità, la faziosità ed un certo grado di imprevedibilità nel comportamento di taluni sistemi di *A.I*. Come specificato, anche nella relazione alla proposta di regolamento, inoltre, «*i requisiti di qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza sono strettamente necessari per attenuare i rischi per i diritti fondamentali e la sicurezza posti dall'A.I. e che non sono oggetto di altri quadri giuridici in vigore*»[63]. Dinanzi alla spinta normativa euro unitaria e, forse, anche dinanzi alle spinte del mercato di riferimento, ammantato di notizie e sensazionalismi di vario genere in merito a pericoli e potenzialità della tecnologia in questione, il legislatore interno ha subito manifestato l'idea e la volontà di una consapevole acquisizione degli elementi funzionali alla necessaria risposta dell'ordinamento nazionale nei confronti dell'innovativa tecnologia ed i rischi connessi ad un uso distorto della stessa[64]. Il disegno di legge sull'impiego dell'*A.I.* presentato nel Consiglio dei ministri il 23 aprile 2024, su proposta del Presidente Giorgia Meloni e del Ministro della Giustizia Carlo Nordio, poi tramutato nell'odierna Legge n.132 del 23 settembre 2025, ha previsto l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale. Il disegno, concepito in tempi che potremmo definire inusuali per le dinamiche della politica interna, ha «*individuato criteri regolatori capaci di riequilibrare il rapporto tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio, al loro sottoutilizzo o al loro impiego dannoso. Inoltre, vuole introdurre norme di principio e disposizioni di settore che, da un lato, promuovano l'utilizzo delle nuove tecnologie per il miglioramento delle condizioni di vita dei cittadini e della coesione sociale e, dall'altro, forniscano soluzioni per la gestione del rischio fondate su una visione antropocentrica*». In una visione d'insieme, senza pretese al rialzo o volontà di prevaricazione delle funzioni regolatorie unitarie, il Governo specifica che il DDL «*non si sovrappone al Regolamento europeo sull'intelligenza artificiale..., ma ne accompagna il quadro regolatorio in quegli spazi propri del diritto interno, tenuto conto che il regolamento è impostato su un'architettura di rischi connessi all'uso della intelligenza artificiale (A.I.)*». Si tratta di un quadro normativo snello, costruito essenzialmente intorno alla garanzia d'intervento nei cinque principali ambiti della strategia nazionale, autorità nazionali, azioni di

promozione, tutela del diritto di autore, e sanzioni penali. Nell'ambito del disegno complessivo d'intervento, il legislatore interno ritiene opportuno, allo stesso tempo, istituire un quadro di riferimento funzionale al riordino complessivo della disciplina penalistica in materia di reati informatici, strutturando un sistema normativo a garanzia dell'operatività e sicurezza degli organismi di settore, mediante la deterrenza della sanzione penale rispetto ad un uso illecito delle tecnologie di *A.I.*[65]. L'uso sostitutivo con le tecnologie di intelligenza artificiale in numerosi ambiti dell'economia di scala, mediante decisioni automatizzate, foriere di potenziali risvolti positivi in termini di oggettività, non suscettibilità a pressioni esterne ed ottimizzazione nelle tempistiche nei processi elaborativi e cognitivi, ma potenzialmente soggette ad interferenze esterne, non è esente da riserve e significative criticità per le innumerevoli conseguenze negative in termini di rispetto delle garanzie democratiche[66]. Le tecnologie di *A.I.*, allo stato dell'arte, fortemente dipendenti dalla qualità ed integrità del dato di addestramento, rendono assai complesso riuscire a definire margini assoluti di sicurezza; anzi, sono sottoposte alle dovute perplessità, afferenti a potenziali contesti applicativi per loro natura già soggetti a pressioni e condizionamenti di difficile gestione[67]. Quello che in pochissimi anni è diventato un remunerativo mercato, in settori come la giurisdizione, pone tutta una serie di domande alle quali è difficile rispondere, senza prima averne testato gli effetti d'impiego in circostanze concrete. Nel brevissimo tempo, come, d'altronde, per molte tecnologie simili, sono stati compiuti passi da gigante, con sviluppi inimmaginabili e opportunità create dai sistemi in grado di porre serissimi quesiti di natura legale ed etica, altrettanto difficili da dirimere, a cui gli addetti ai lavori sono soggetti nelle rispettive attività di implementazione professionale[68]. Il legislatore, non può esimersi dall'assunzione di una responsabilità d'intervento, generando le dovute risposte, anche se non sempre in grado di migliorare o efficientare il sistema. Il concetto di Cybersicurezza non è rimasto esente da considerazioni di questo tipo; come era immaginabile, anche in tale specifico aspetto dell'applicazione di tecnologie informatiche, è necessario strutturare misure di sicurezza che consentano una barriera contro interferenze esterne e, soprattutto, garantiscano il giusto grado di affidabilità per il libero mercato, chiamato a sfruttarne il potenziale economico. La Legge 28 giugno 2024, n. 90 contenente «*Disposizioni in materia di rafforzamento della*

cybersicurezza nazionale e di reati informatici», muove verso tale direzione. Il suo contenuto, rafforzando la cybersicurezza nazionale e aggiornando le norme contro i reati informatici, interviene soprattutto sul miglioramento della resilienza di pubbliche amministrazioni ed erogatori di servizi informatici, senza tralasciare significativi aspetti legati al coordinamento in caso di attacchi. La legge si compone di due distinti Capi, offrendo rilevanti spunti per il miglioramento degli *standards* di protezione dei sistemi informatici e informativi e, soprattutto, per chi si occupa di individuare le relative misure tecniche ed organizzative da osservare nei processi di trattamento dei dati. In tal senso, il Capo I della Legge 90 definisce e individua le necessarie misure per il rafforzamento della cybersicurezza nazionale, della conseguente resilienza delle pubbliche amministrazioni, anche per quanto attiene alla stipula e gestione di contratti pubblici di beni e servizi informatici impiegati in un contesto strettamente connesso alla tutela degli interessi nazionali, ritenuti strategici[69]. Il Capo II, invece, intervenendo sulle disposizioni del codice penale, con riferimento alla prevenzione e contrasto dei reati informatici, detta disposizioni per il coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici, un tema caro all'attività della neonata ACN o Agenzia per La Cybersicurezza nazionale, anche per come emerso dal recente Documento di «*Guida alla Notifica degli incidenti al CSIRT Italia*». Il quadro normativo è concepito sulla base di quanto previsto dall'art. 14 della legge, secondo cui la «*Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*», e che riguarda quindi le problematiche sul «*...perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*». È compito del Presidente del consiglio dei ministri, su proposta dell'ACN e previo parere del Comitato interministeriale per la sicurezza della Repubblica, emanare un Decreto tecnico che individui, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, quindi le pubbliche amministrazioni, i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse e le società a controllo pubblico, sono tenuti ad assicurare[70]. Secondo

l'architettura normativa istituita con la legge 90, i requisiti di cybersicurezza da implementare sono rappresentati da un insieme di criteri e regole tecniche la cui conformità è in grado di garantire confidenzialità, integrità e la disponibilità dei dati da trattare secondo le esigenze di tutela in materia di cybersicurezza, la protezione delle informazioni classificate, sempre nel rispetto delle esigenze di ricerca e innovazione. Secondo la novella, per l'implementazione dei servizi informatici sicuri ed affidabili, dovrà, dunque, essere incentivato anche un meccanismo premiale per stimolare l'impiego di apparati e tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO); in ogni caso di Paesi terzi che, però, sono parte di accordi di collaborazione con l'Unione europea o con la NATO[71]. Nell'acquisizione di beni e servizi, le stazioni appaltanti dovranno, inoltre, garantire che la gara non possa essere aggiudicata all'offerente al ribasso, se è accertato che non sia assicurata la presenza degli elementi essenziali di cybersicurezza**.** Non solo, il requisito della sicurezza informatica garantito dal servizio sarà criterio determinante nella misurazione del rapporto qualità/prezzo del servizio proposto dall'aggiudicatario. Ciò deve avvenire in stretta coerenza con quanto previsto dal Considerando C81 del GDPR (Regolamento (UE) 2016/679) il quale dispone che il titolare, quando affida delle attività di trattamento di dati personali a un soggetto terzo per garantire che siano rispettate le prescrizioni di legge riguardo alle mansioni che a questi saranno affidate deve ricorrere unicamente a «*...coloro che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative*» tali da assicurare la protezione dei dati personali e la loro tenuta in sicurezza[72]. Per ogni stazione appaltante, dunque, il rispetto dei requisiti introdotti dalla legge 90 sarà elemento essenziale per la garanzia di scelta dei migliori fornitori di servizi informatici sotto il piano del rispetto dei requisiti di sicurezza nella gestione dei dati nel rispetto del Regolamento (UE) 2016/679. Lo stesso, al Considerando C78, affida ai «*produttori dei prodotti, dei servizi e delle applicazioni*» l'obbligo, nel corso della fase di «*.. sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni*» di «*...tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni*»[73]. Allo stesso tempo, come sancito dall'articolo 25

del Regolamento nell'enucleare i principi di "*Privacy by design*" e di "*Privacy by default*", intesi come "Principio di protezione dei dati fin dalla progettazione" e "Principio di protezione dei dati per impostazione predefinita", sarà indispensabile che le pubbliche amministrazioni interessate dall'erogazione del servizio ed i possibili fornitori degli stessi si interessino al tema della garanzia di sicurezza informatica fin dalla fase di progettazione dei relativi sistemi. Ciò dovrebbe perpetuare un innovativo concetto di *privacy*, non come mero formalismo di maniera, ma come principio cardine nella guida all'implementazione della tecnologia nel rispetto non solo della normativa di settore europea, ma anche della relativa impostazione garantista del legislatore interno. Mediante il suo intervento, lo stesso, ha voluto assicurarsi che, fin dalla fase di progettazione e disegni dei sistemi informatici, i produttori si interessino della implementazione di misure idonee al trattamento minimo dei dati, mediante pseudonimizzazione (art. 4 GDPR) o cifrature, assicurando, così, la possibilità d'intervento alle amministrazioni titolari del trattamento per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonché, per prevenire e contenere i rischi *cyber*[74].

10. La *cybersecurity* come opportunità di implementazione affidabile della tecnologia

Il ruolo rivestito dalla tecnologia informatica, nei processi relazionali contemporanei, ha raggiunto livelli di pervasività incompatibili con un approccio pigro e poco attento alle tematiche di sicurezza gestionale degli apparati e sistemi impiegati in vari contesti del tessuto economico e sociale; a partire dalla rete comunicativa di massa, finendo per interessare aspetti critici delle dinamiche di gestione dell'ordine e della sicurezza pubblica[75]. Il legislatore ha, come si è potuto vedere, cercato sempre un approccio che tenesse conto dei molteplici fattori e scale d'interesse afferenti alle necessità del libero mercato e, contestualmente, anche delle notevoli esigenze di tenuta dei valori democratici, spesso e volentieri dal difficile inquadramento normativo. Se, da una parte, risulta difficile approcciare con assetto definitorio a circostanze della vita concreta, come l'universo digitale e la conseguente indeterminatezza materiale, è pur vero che, dall'altra, non è immaginabile acconsentire alla realizzazione di universi

relazionali asettici e privi di confini regolatori. Essi, lasciati liberi, non sarebbero in grado di attribuire un certo margine di affidabilità e rispetto generale delle regole del gioco tra le parti[76]. L'ipotesi che sistemi informatici estremamente avanzati, come le moderne tecnologie di intelligenza artificiale, possano in qualche modo agevolare fenomeni prevaricatori d'imposizione delle prospettive di singole parti, magari spinte da propositi non sempre in linea con il rispetto della osservanza normativa di contesto, rende molto persuasiva la sostenibilità di tesi descrittive al rialzo circa la necessità di contingentare pericoli e *vulnus* in grado di alterare il legittimo affidamento degli operatori coinvolti. Né, d'altro canto, è possibile sottovalutare gli innumerevoli aspetti etici e morali di una implementazione tecnologica avulsa da qualsiasi riferimento ai valori consolidati delle reti sociali, soprattutto, in contesti territoriali in cui il minimo relativo di condotta è pilastro fondamentale nella pacifica convivenza tra contrapposte pretese di valorizzazione dei rispettivi bisogni di sussistenza e sostentamento delle necessità di vita primarie[77]. Dinanzi a simili pressioni di sistema, è inevitabile strutturare sintesi e programmi d'intervento funzionali a garantire quel senso di legittimo affidamento delle parti. In un quadro di articolata complessità tecnica, la risposta più adeguata non può provenire esclusivamente da un regolatore attento e solerte, ma, soprattutto, dagli specialisti di settore e dai nuclei di pressione ed interesse dell'economia di mercato[78]. La costruzione di un'architettura informatica affidabile e sicura rappresenta un pilastro solido su cui poggiare gli elementi d'incertezza del sistema, al fine di garantire uno sviluppo integrato e sostenibile della tecnologia negli apparati di comunicazione e scambio commerciale dei destinatari di tali funzioni, volte essenzialmente all'efficientamento e ottimizzazione dei processi su cui è costruita l'intera rete relazionale del mondo digitalizzato. L'introduzione di innovazioni dirompenti e potenzialmente in grado di scardinare equilibri e pretese di affidabilità complessiva di sistema, rappresenta un quesito di cui si deve tenere conto. È importante, però, ragionare in termini non astratti ed immaginifici, ma introiettando i reali e circostanziati bisogni cui far fronte per l'ottenimento di risultati concreti e non avulsi dalla logica di umana comprensione[79]. Quando si discute di *cybersecurity*, spesso e volentieri, si viene posti dinanzi ad articolate elaborazioni teoriche e fantascientifiche di futuribile applicabilità pratica, le stesse soggette ad immediate contestazioni altrettanto immaginifiche, quasi al limite

dell'esoterismo religioso. Insomma, un approccio fideistico di accettazione *tout court* al lessico ed alla complessità imposta dalla tecnica è il principale argomento rivolto all'ascoltatore da parte dello specialista chiamato a dare risposte di significato a fenomeni da imbrigliare e circoscrivere con regole e principi di riferimento, anche per l'uomo qualunque. D'altro canto, non è colpa dell'utente se molti degli apparati strumentali, spesso immaturi ed ai primi gradi di sviluppo, vengono posti da subito, senza adeguata formazione, nella disponibilità delle masse. Grazie alle fascinazioni del potere economico, espresso mediante acquisti compulsivi ed accessi garantiti dal libero mercato, troppo intento ad ottimizzare e rimediare ad importanti investimenti con margini di rischio elevati, ottimizzando e massimizzando il profitto, il costo è sacrificare la sicurezza generale[80]. L'emanazione di direttive, regolamenti, linee guida, protocolli, discipline di settore ecc. può, dunque, essere la legittima pretesa della comunità che volontariamente ha deciso di delegare tali funzioni agli organi istituzionali preposti alla gestione dell'ordinamento democratico. Allo stesso tempo, però, non può essere l'unica risposta ai fenomeni dell'evoluzione tecnologica, se si vuole realmente costruire un argine alle possibili derive distorsive nell'impiego dei risultati di calcoli ed elaborazioni informatiche[81]. Come si è visto, emblematicamente con l'arrivo sul mercato dell'*A.I.,* è sufficiente una novità dirompente per scardinare dall'oggi al domani punti di riferimento consolidati; allora, dinanzi alle possibilità rappresentate dall'emergere di sistemi in grado di simulare il comportamento umano in modo sempre più preciso e credibile, è, probabilmente, più opportuno ragionare in termini relativi e non assoluti, determinando un sano scetticismo critico, tipico della storia evolutiva classica, in grado di veicolare il necessario tenore di consapevolezza generalizzata circa il potenziale della tecnica, ma anche del suo pericolo[82]. La *Cybersecurity*, intesa come nucleo articolato di regole consolidate e prassi circostanziate di garanzia dell'affidabilità e sicurezza dei sistemi informatici o in qualsiasi altro modo la si voglia chiamare o definire, mediante la logica del ragionamento omnicomprensivo, può e deve essere il riferimento assoluto nell'agire quotidiano. L'uomo, nei suoi valori, costruiti con fatica e processi evolutivi frutto di adattamenti e rimodulazioni conformi al contesto, deve essere punto di riferimento solido ed irremovibile anche nell'implementazione digitale. Non è possibile, allo stato attuale, strutturare definitivi criteri di consolidamento

normativo della sicurezza informatica! È ragionevole, invece, implementare meccanismi progressivi di approntamento dei sistemi cibernetici, vecchi e nuovi, in modo da garantire affidabilità ed integrità sia del dato grezzo, impiegato nei processi di elaborazione, che dei risultati specifici derivanti dal processamento di algoritmi estremamente complessi ed efficienti[83]. Il regolatore, nella sua corposa profilassi normativa non è stato veramente efficace nel dirimere perplessità e criticità derivanti dall'evoluzione della tecnica, ma i numerosi tentativi e nella volontà manifesta di non rimanere indifferente, devono comunque essere tenuti in considerazione. Forse, il migliore degli approcci non è pretendere la perfezione di sistema, semmai, una ragionevole volontà di perseguire un bene primario rappresentato dalla tutela di valori e principi fondamentali afferenti alla dignità umana, non di essere immuni dal rischio, ma di vederne ridotti il più possibile gli effetti deleteri[84].

11. Conclusioni

Il relativismo generalizzato dei tempi contemporanei porta a considerare in termini inappropriati numerosi aspetti dell'agire quotidiano, dando per scontati primari elementi critici, altrimenti ricchi di significato nelle dovute considerazioni specialistiche e tecniche. La tecnologia, infatti, unita al nucleo fondamentale di armamentari dei sistemi industrializzati odierni, rende vita facile ad un approccio qualunquista e squisitamente riduttivo del carico di complessità di fenomeni non comprensibili, senza una adeguata conoscenza della materia. Il facile accesso ai sofisticati sistemi computazionali, garantito da un libero mercato condizionato dalle dinamiche del profitto senza riserve, determina, non solo, un radicato sentimento di appartenenza ad una comunità di relazione e condivisione, ma, soprattutto, la possibilità di interferire concretamente su particolari e consolidati punti di riferimento, ritenuti essenziali alla pacifica convivenza collettiva[85]. Il ruolo di supervisore attivo del regolatore rappresenta un pilastro dell'architettura neoliberista, laddove l'esercizio legittimo di prerogative economiciste e logiche di mercato necessitano, evidentemente, di un articolato sistema di regole e protocolli, funzionali alla garanzia di legittimazione ed affidabilità tra le parti[86]. Nel momento in cui emerge, nella disponibilità del sistema, un fattore dirimente e dirompente per gli equilibri maturati in decenni di

interazioni, questo, se non ben compreso e confinato, può destabilizzare il terreno su cui poggia la macchina burocratica e normativa, oleata ed efficiente nei suoi ingranaggi di trasmissione dei valori di appartenenza, ma facilmente scardinabile con sussulti estemporanei e fuori fase. L'impatto delle tecnologie di intelligenza artificiale generativa rientra senza ombra di dubbio nei canoni di incidenza esterna in grado di ridefinire gli assetti delle logiche di scambio ed interazione nel libero mercato. Nel momento in cui il fenomeno ha impattato concretamente il sentimento comune di sicurezza ed integrità del reale, ogni individuo attivo nei processi di interscambio globale ha percepito la spinta di intervento necessaria a confinarne lo sviluppo entro margini di apprezzabile affidabilità[87]. Radicati principi, afferenti alla gestione della sicurezza informatica, subiscono la fascinazione di una applicazione per complementarità e condivisione di obiettivi, senza escludere, allo stesso tempo, adeguamenti dettagliati e ritagliati per le peculiarità del nuovo prodigio algoritmico. Nel quadro di riferimento normativo si inseriscono prepotentemente principi ritenuti fondamentali per una implementazione corretta e rispettosa della dignità umana, ma anche protocolli applicativi non eludibili e frutto di radicate esperienze nel settore dell'informatica e della sicurezza in generale[88]. La circostanza per cui algoritmi e apparati hardware subiscono continui aggiornamenti, derivanti dalle sperimentazioni e specifiche attività di ricerca di settore da parte degli attori privati e pubblici, non facilita certamente il compito di articolazione definitoria e sanzionatoria per attività interessate dal fenomeno; ciò, però, non deve costituire una scusa di rimedio per inefficienze e disattenzioni di regolatori pigri e poco reattivi dinanzi ad evidenti minacce di interferenze illecite. Il meritevole interessamento delle parti in gioco circa uno sviluppo etico, sostenibile ed affidabile della tecnologia computazionale determina pressioni che potrebbero facilmente essere evase ed eluse mediante formule stereotipate e rassicuranti, ma, al di là del rigorismo formale, è opportuno rivolgere il proprio impegno e la solerzia verso strutture regolamentari efficaci e concretamente applicabili nelle circostanze pratiche[89]. Se un simile intento sarà realmente messo in opera e se le relative conseguenze potranno sortire effetti migliorativi del sistema non è ancora dato saperlo. Bene è che concetti come *cybersecurity* ed intelligenza artificiale camminino di pari passo, senza mai compromessi al ribasso in grado di assecondare le logiche di mercato o, peggio ancora, egoismi solitari di

massimizzazione del profitto delle imprese coinvolte nel processo di implementazione della tecnologia[90].

1. B. Goertzel, Artificial General Intelligence: Concept, State of the Art, and Future Prospects, in Journal of Artificial General Intelligence, 5, 2014.
2. AA.VV., Responsible Artificial Intelligence Strategy and Implementation Pathway, DoD, 2022.
3. Per approfondimenti sul tema si rinvia a R. Curry, OpenAI Doesn't Fully Understand How GPT Works Despite Rapid Progress, in Observer, 2024.
4. V. in tal senso M. Sullivan, The frightening truth about AI chatbots: Nobody knows exactly how they won, in FastCompany, 2023.
5. Al riguardo è utile consultare S. Kumar et al., Artificial Intelligence: Revolutionizing Cybersecurity in the Digital Era, in Journal of Computers, Mechanical and Management (JCMM), 2(3), 2023.
6. Nel sistema delle reti neurali, alla base del calcolo probabilistico delle maggior parte delle A.I. generative, una rete neurale artificiale non è altro che una tipologia specifica di sistema adattivo che modifica la propria struttura sulla base delle informazioni esterne o interne che scorrono attraverso la rete stessa durante la fase di addestramento. In altri termini, le reti neurali sono delle strutture non-lineari di dati statistici organizzate come strumenti di modellazione. Esse possono essere utilizzate per simulare relazioni complesse tra ingressi e uscite che altre funzioni analitiche non riescono a rappresentare. Si veda in tal senso E. Pessa, Statistica con le reti neurali, Roma, Di Renzo Editore, 2004 e D. J. Amit, Modeling brain function, 1989 New York, NY: Cambridge University Press.
7. Si rinvia in tal senso a S. Baack, A Critical Analysis of the Largest Source for Generative AI Training Data: Common Crawl, Mozilla Foundation, 2024.
8. V. E. Ferrara, Should ChatGPT be biased? Challenges and risks of bias in large language models, University of Southern California, 2023.
9. V. S. Quintarelli, Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale, Bollati Boringhieri, Torino, 2019.
10. Significativa in tal senso è l'analisi sul tema rinvenibile in E. Gen, The tech industry can't agree on what open-source AI means. That's a problem, in MIT Technology Review, 2024. V. anche H. Jahankhani, G. Bowen, M. S. Sharif, O. Hussein, Cybersecurity and Artificial Intelligence, Transformation Strategies and Disruptive Innovation, Springer, Cham, 2024.
11. V. al riguardo D. Kahneman, Of 2 Minds: How Fast and Slow Thinking Shape Perception and Choice, in ScientificAmerican, 2012.
12. Emblematico sull'argomento J. Weizenbaum, ELIZA - a computer program for the study of natural language communication between man and machine, in Communications of the ACM, 9(1), 1966.
13. V. A. Ottolia, Big data e innovazione computazionale, Torino, Giappichelli, 2017, p. 33 ss; V. anche A. Ottolia, L'utilizzo computazionale dell'opera dell'ingegno in Internet, in

AIDA, 2014, p. 386 ss.

14. Si rinvia in tal senso a D.F. Thompson, Designing Responsibility: The Problem of Many Hands in Complex Organizations, in J. van den Hoven, S. Miller, T. Pogge, Designing in Ethics, Cambridge University Press, Cambridge, 2014.
15. V. J. Lucas et al., Fighting Fire with Fire: The Dual Role of LLMs in Crafting and Detecting Elusive Disinformation, in Proceedings of the 2023 Conference on Empirical Methods in Natural Language processing Singapore, 6-10 December 2023 Association for Computational Linguistics, 2023.
16. V. in tal senso D.L. Poole, A.K. Mackworth, Artificial Intelligence. Foundations of Computational Agents, III Ed., Cambridge University Press, Cambridge, 2023.
17. Per una ricognizione approfondita sul tema dell'implementazione di tecnologie artificiali si veda su tutti AI Index Report 2025 e precedenti – Artificial Intelligence Index, aiindex.stanford.edu.
18. Si rinvia per approfondimenti sul tema a J. Smith, Advanced Persistent Threats and AI: An Evolution in Cyber Warfare, in International Journal of Information Security, 18, 2021.
19. V. AA.VV., Universal and Transferable Adversarial Attacks on Aligned Language Models, in ArXiv abs/2307.15043, 2023 nonché, sempre sul medesimo tema, AA.VV., Indiscriminate Poisoning Attacks on Unsupervised Contrastive Learning, in Proceedings of the Eleventh International Conference on Learning Representations Kigali 1-5 May 2023, MIT, 2023.
20. V. al riguardo D.F. Thompson, Designing Responsibility: The Problem of Many Hands in Complex Organizations, in J. van den Hoven, S. Miller, T. Pogge, Designing in Ethics, Cambridge University Press, Cambridge, 2014.
21. Si rinvia in tal senso a A. Sufi, Novel Application of Open-Source Cyber Intelligence, in Electronics, 12 (17), 2023.
22. V. R. Feldmand, Corporate Strategy: Past, Present and Future, in Strategic Management Review, 1, 2020.
23. Significativo in tal senso S. Russell, P. Norvig, Artificial Intelligence. A Modern Approach, IV Ed., Pearson Higher Education, 2021.
24. V. A. Evans, M. Robles, AI-powered Malware and Polymorphic Attacks, in Journal of Cybersecurity Research, 15, 2022.
25. Sul tema si rinvia a G. Waizel, Bridging the AI Divide: The Evolving Arms Race Between AI-Driven Cyber Attacks and AI-Powered Cybersecurity Defenses, in Proceedings of the International Conference on Machine Intelligence & Security for Smart Cities. Bucharest 5 June 2024, Pro Universitaria Publishing House, 2024.
26. V. G. Weiss, Multiagent systems: a modern approach to distributed artificial intelligence, MIT press, Cambridge-London, 2013.
27. Si vedano in tal senso le Guidelines for secure AI system development, NCSC, 2023.
28. V. la "Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Creare fiducia

nell'intelligenza artificiale antropocentrica", COM/2019/168 final.

29. Vedi cosa dice il P&S Market Research. Artificial Intelligence (AI) in Cyber Security Market.
30. V. Building Security In Maturity Model (BSIMM) project.
31. V. il CIG Framework: Confidentiality, Integrity and Governance, AI RMF Framework, NIST, 2023, nonché il The NIST Cybersecurity Framework (CSF) 2.0, NIST, 2024.
32. V. in tal senso AA.VV., Large Language Models are Geographically Biased, in Proceedings of the 41st International Conference on Machine Learning, Vienna 21-27 July 2024, JMLR.org, 2024.
33. V. l'AI RMF Playbook, NIST, 2023.
34. V. su tutti il Microsoft Security Development Lifecycle (SDL).
35. V. A. Kapoor, B. Stroebl et al., AI Agents that Matter, in Transactions on Machine Learning Research, 5, 2025.
36. Si rinvia per approfondimenti a Human-Centered Artificial Intelligence Center, Stanford University, 2022. "Behavioral Insights Through AI: Evaluating Soft Skills in Digital Interactions", Stanford University Press.
37. V. in tal senso AI in 2024: McKinsey Report Reveals Value Generation & AI Adoption Spike, in 2024-gen-ai-rise-and-business-impact, 2024.
38. Sul tema si rinvia a M. Wozniak, M. Choras, The Double-Edged Sword of AI: Ethical Adversarial Attacks, in AI and Ethics, 2, 2022.
39. V. R. Thompson, K. Hughes, Cyber Warfare and Artificial Intelligence: Emerging Threats to National Security, in Defense Technology Journal, 33, 2022.
40. Sul tema si vada a vedere J. von Newmann, Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components, California Institute of Technology, 1952.
41. V. sul punto il già citato C. Castelfranchi, Modelling Social Action for AI Agent, in Artificial Intelligence, 103, 1998.
42. V. B. Patterson, The Threat of Deepfake Technology in Cybersecurity, in Cybersecurity & Digital Forensics Review, 22, 2021.
43. V. AA.VV., Provable Robust Watermarking for AI-Generated Text, in ArXiv:2306.17439, UC Santa Barbara, 2023.
44. V. AA.VV., Gone but Not Forgotten: Improved Benchmarks for Machine Unlearning, in Proceedings of the 7th deep learning security and privacy workshop. San Francisco 23 May 2024, Carnegie Mellon University, 2024.
45. La risposta operativa a fenomeno Mithos si chiama "Project Glasswing", in cui 12 Partners, (le principali Big Tech), e oltre 40 enti interessati ai software critici hanno come obiettivo di usare l'AI prodotta da Anthropic in funzione difensiva al fine mettere in sicurezza i modelli immessi sul mercato prima che relative vulnerabilità si manifestino all'utenza o possano essere impiegate con finalità malevole dai rispettivi scopritori. Per approfondimenti sul tema v. il sito ufficiale del progetto alla pagina https://www.anthropic.com/glasswing.

46. Per approfondimenti si rinvia a documento AI RMF Generative Artificial Intelligence Profile, NIST, 2024.
47. V. su tutti Executive Office of the President, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Executive Order n. 14110 of October 30, 2023.
48. Per approfondimenti si veda il Federal Information Security Modernization Act (FISMA) nonché il National Information Assurance Partnership (NIAP) Common Criteria.
49. V. in tal senso S. Del Gatto, Potere algoritmico, *digital welfare state* e garanzie per gli amministrati. I nodi ancora da sciogliere, in Riv. it. dir. pubbl. comunitario, VI, 2020, pp. 829 ss.
50. È stato il timore di un impiego «in a non-transparent and non-explainable way» dell'intelligenza artificiale «for automatic decision making» ad aver determinato l'adozione delle linee guida sull'utilizzo dell'intelligenza artificiale – incentrate su di una logica di controllo e organizzazione dell'utilizzo dell'A.I. da parte delle organizzazioni e delle istituzioni – a livello internazionale da parte della ISO e della IEC.
51. In tal senso si veda sempre la proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE e la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali).
52. Per approfondimenti vedi sempre il c.d. Data Governance Act **(**Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) (Testo rilevante ai fini del SEE), Commissione europea, Bruxelles, 25.11.2020 COM (2020) 767final e la c.d. AI Regulation (Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione {SEC(2021) 167 final} – {SWD(2021) 84 final} – {SWD (2021) 85 final).
53. Sugli imperi digitali V. A. Bradford, Digital Empires: The Global Battle to Regulate Technology, Oxford University Press, New York, 2023. In coerenza con il regolamento europeo «*un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici*» in costante aggiornamento (cfr. l'art. 9 dell'AI Act).
54. È importante ricordare le linee guida per un'A.I. affidabile elaborate dall'A.I. HLEG (High-Level Expert Group on A.I.): 1) intervento e sorveglianza umani; 2) robustezza tecnica e sicurezza; 3) vita privata e governance dei dati; 4) trasparenza; 5) diversità, non discriminazione ed equità; 6) benessere sociale e ambientale; 7) responsabilità.
55. Per approfondire la nuova disciplina si veda il d.lgs. 138/2024 che recepisce la Direttiva NIS2 all'interno dell'Ordinamento Italiano.
56. Una rigorosa interpretazione della riserva di umanità richiesta nell'utilizzo dei sistemi di IA nel settore della giustizia è condivisa da A. Punzi, *La decisione giudiziaria nell'AI Act*, in *Giurisprudenza Italiana*, 2, 2025, pp. 448 ss.

57. Com'è stato osservato in dottrina, «*resta in ogni caso molto complicato misurare se l'affidamento riposto sull'attività di IA sia legittimo oppure viziato, giacché inevitabilmente il funzionario si pone in una situazione di naturale deferenza verso un procedimento automatizzato pre-impostato e controllato ex ante*». P. Foà, *Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"?*, in *Diritto Amministrativo*, 1, 2023, p. 522.
58. V. R. Meys, Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?, in GRUR Int., 69(5), 2021, p. 459;
59. V. ad esempio, sull'implicazioni militari nell'uso di AI cosa dicono F. Morgan, B. Boudreaux, A. Lohn et al., *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*, RAND Corporation, 2020.
60. La Commissione ha avviato una consultazione per la creazione di un codice di buone pratiche per i fornitori di modelli di IA per finalità generali (GPAI). Il codice riguarderà i nodi critici rispetto all'utilizzo dell'A.I, come la trasparenza, la tutela del diritto d'autore, l'individuazione e la gestione dei rischi connessi al suo utilizzo. Accanto a tale consultazione, deve essere segnalata quella in atto (che doveva essere conclusa entro il 18 luglio 2025) sui sistemi ad alto rischio, che mira a raccogliere esempi pratici e a chiarire le questioni relative ai sistemi di IA ad alto rischio.
61. V. M. Leistner, The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A critical primer, in *Journal of Intellectual Property Law and Practice*, 16(8), 2021.
62. V. in tal senso C. Pinelli, L'*AI Act*: gestione del rischio e tutela dei diritti, in Giur. it., II, 2025, pp. 452 ss.
63. In tal senso si veda Data Governance Act **(**Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) (Testo rilevante ai fini del SEE), Commissione europea, Bruxelles, 25.11.2020 COM (2020)767final.
64. Ad esempio, le controversie in corso sul tema, specialmente negli USA, sono molto numerose. Si v. tra i casi più recenti Basbanes et al. v. Microsoft Corp., et al., U.S. District Court for the Southern District of New York, 1:23-cv-10211 (filed Jan. 5, 2024); The New York Times Co. v. Microsoft Corp., OpenAI, U.S. District Court for the Southern District of New York, 1:23-cv-11195 (filed Dec. 27, 2023); Sancton v. Microsoft Corp., OpenAI, U.S. District Court for the Southern District of New York, 1:23-cv-10211 (filed Nov. 21, 2023); Mike Huckabee v. Meta Platforms, Inc., Bloomberg L.P., Bloomberg Finance, L.P., Microsoft Corporation, and The EleutherAI Institute, U.S. District Court for the Southern District of New York, 1:23-cv-09152 (filed Oct. 17, 2023); Authors Guild v. Open AI, U.S. District Court for the Southern District of New York, 1:23-cv-8292 (filed Sept. 19, 2023); Chabon v. OpenAI Inc., U.S. District Court for the Northern District of California, 3:23-cv-04625-PHK (filed Sept. 8, 2023).
65. L'AI HLEG (High-Level Expert Group on AI) indipendente nominato dalla

Commissione nel 2019 ha elaborato sette principi etici non vincolanti per l'IA che i sistemi di IA dovrebbero soddisfare per essere considerati affidabili: 1) intervento e sorveglianza umani; 2) robustezza tecnica e sicurezza; 3) vita privata e governance dei dati; 4) trasparenza; 5) diversità, non discriminazione ed equità; 6) benessere sociale e ambientale; 7) responsabilità.

66. V. in tal senso M. Ricolfi, Il futuro della proprietà intellettuale nella società algoritmica, in Giur. it., Supplemento 2019, 10-36 e, già molto prima, allo scritto Le nuove frontiere della proprietà intellettuale. Da Chicago al cyberspazio, in G. Clerico, S. Rizzello (a cura di), Diritto ed economia della proprietà intellettuale, Cedam, Padova, 1998, 83 ss.
67. Una delle maggiori innovazioni e peculiarità dell'A.I. generativa sta nell'essere definiti sistemi "transformer", rispetto ai precedenti meccanismi. Vedi sul punto M. Sag, (nt. 2), 2023: «*one of the key differences between transformers and the prior state of the art, recurrent neural networks ("RNNs"), is that rather than looking at each word sequentially, a transformer first notes the position of the words. The ability to interpret these "positional encodings" makes the system sensitive to word order and context, which is useful because a great deal of meaning depends on sequence and context. Positional encoding is also important because it facilitates parallel processing: this in turn explains why throwing staggering amounts of computing power at LLMs works well for transformers, whereas the returns to scale for RNNs were less impressive. Transformers were also a breakthrough technology because of their capacity for "attention" and "self-attention." In simple terms, in the context of translation, this means that the system pays attention to all the words in source text when deciding how to translate any individual word. Based on the training data, the model learns which words in which contexts it should pay more and less attention to. Through "self-attention" the system derives fundamental relationships from input data and thus learns, for example, that "programmer" and "coder" are usually synonyms, and that "server" is a restaurant waiter in one context and a computer in another*».
68. V. E. Chwar, *The Ethical Implications of AI in Warfare*, Queen Mary University of London, 2020 nonché C. Geiger, V. Iaia, *The Forgotten Creator: Towards a Statutory Remuneration Right for Machine Learning of Generative AI*, in *Computer Law & Security Review*, 52, 2024.
69. In tal senso L. Mansani, Le eccezioni per estrazioni di testo e di dati, didattica e conservazione del patrimonio culturale, in AIDA, 2019, p. 13 nonché R. Ducato, A. Strowel, Ensuring text and data mining: remaining issues with the EU copyright exceptions and possible ways out, in CRIDES, Working Paper series, 1, 2021, p. 13. Secondo alcuni autori, il controllo sul rispetto della riserva da parte dell'A.I. è molto difficile (se non addirittura impossibile) per i titolari. Si v. Study on copyright and new technologies: copyright data management and artificial intelligence, SMART 2019/0038, 2022, 201. In proposito, infatti, il testo del regolamento europeo sull'A.I. (AI Act) contiene il dovere per i sistemi di A.I. di predisporre «*una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di A.I. per finalità generali*» (art. 53). Secondo alcuni autori, la disposizione normativa è volta ad agevolare

l'esercizio dell'opt-out. Si v. in tal senso C. Geiger, V. Iaia, (nt. 15), 4 ss. e J.P. Quintais, Generative AI, copyright and the AI Act, in Kluwer Copyright Blog, 9 maggio 2023.

70. V. I.B. Ørstavik, Access to data for training algorithms in machine learning – copyright law and "right-stacking", in T. Pihlajarinne, A. Alén-Savikko (eds.), Artificial Intelligence and the Media, Cheltenham, Edward Elgar, 2022, 272 ss; L'UE ha adottato un approccio più restrittivo rispetto a quello seguito da altri ordinamenti, in cui il "text and data mining" è tendenzialmente consentito anche per fini commerciali. Si v. ad es. per il caso giapponese, T. Ueno, The Flexible Copyright Exception for "Non-Enjoyment" Purposes – Recent Amendment in Japan and Its Implication, in GRUR Int., 2022. V. per una comparazione tra sistema giapponese e direttive europee: A. Derwaman, Text and data mining exceptions in the development of generative AI models: what the EU member States could learn from the Japanese "nonenjoyment" purposes?, in J. of world IP, 1, 2023. Nel Regno Unito, invece, il governo sta lavorando su un "code of practice on copyright and AI" rivolto alla elaborazione di soluzioni per semplificare l'acquisizione di licenze per fini commerciali.
71. V. R. Meys, Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?, in GRUR Int., 2021, 459 nonché A. Derwaman, Text and data mining exceptions in the development of generative Ai models: what the EU member States could learn from the Japanese "nonenjoyment" purposes?, in J. of world IP, 1, 2023.
72. V. R. Ducato, A. Strowel, Ensuring text and data mining: remaining issues with the EU copyright exceptions and possible ways out, in CRIDES, Working Paper series, 1, 2021, p. 13; per l'esame approfondito della normativa si rinvia al testo completo General Data Protection Regulation.
73. In questo senso, con riferimento alle piattaforme "peer to peer" v. CGUE, 14 giugno 2017, C-610/15, Stichting Brein, par. 36 ss.: «*le opere così messe a disposizione degli utenti della piattaforma di condivisione online TPB sono state messe online su tale piattaforma non dagli amministratori di quest'ultima, bensì dai suoi utenti. Tuttavia, detti amministratori, mediante la messa a disposizione e la gestione di una piattaforma di condivisione online, come quella di cui al procedimento principale, intervengono con piena cognizione delle conseguenze del proprio comportamento, al fine di dare accesso alle opere protette, indicizzando ed elencando su tale piattaforma i file torrent che consentono agli utenti della medesima di localizzare tali opere e di condividerle nell'ambito di una rete tra utenti (peer-to-peer). A tale riguardo* [...] *senza la messa a disposizione e la gestione da parte dei suddetti amministratori di una siffatta piattaforma, le opere in questione non potrebbero essere condivise dagli utenti o, quantomeno, la loro condivisione su Internet sarebbe più complessa. Occorre pertanto considerare che, con la messa a disposizione e la gestione della piattaforma di condivisione online TPB, gli amministratori di quest'ultima offrono ai loro utenti un accesso alle opere di cui trattasi. Si può quindi ritenere che essi svolgano un ruolo imprescindibile nella messa a disposizione delle opere in questione*». V. anche in tema di

piattaforme CGUE, 22 giugno 2021, cause riunite C-682/18 e C-683/18, Peterson.

74. Si veda in tal senso Commissione europea, Una strategia europea per i dati, 19 febbraio 2020, COM (2020) final, 1: «*i cittadini dovrebbero disporre dei mezzi per prendere decisioni migliori sulla base delle informazioni ottenute dai dati non personali, e tali dati dovrebbero essere disponibili a tutti, siano essi soggetti pubblici o privati, piccoli o grandi, start-up o colossi. In questo modo la società trarrà il massimo vantaggio dall'innovazione e dalla concorrenza e tutti beneficeranno di un dividendo digitale*».
75. Bisogna ricordare sempre l'architettura complessiva afferente alla tutela delle libertà fondamentali nel contesto europeo e non solo. La vincolatività della Carta dei diritti fondamentali è stata sancita dal Trattato di Lisbona, entrato in vigore il 1° dicembre 2009. Sulla Carta v. R. Mastroianni, O. Pollicino, S. Allegrezza, O. Razzolin (a cura di), Carta dei diritti fondamentali dell'Unione Europea, Giuffrè, Milano, 2017 e S. Peers, T. Hervey, J. Kenner, A. Ward (a cura di), The EU Charter of Fundamental Rights, Hart, Oxford-Portland, 2014.
76. V. R. Meys, Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?, in GRUR Int., 2021, p. 459.
77. V. D. Sarti, Diritti esclusivi e circolazione dei beni, Giuffrè, Milano, 1996, p. 359 ss.
78. V. I. Kuzmanov, Beyond The Illusion Of Intuition: The Mind, Society, Standardization, And The Future Of Objective Profiling In The Age Of AI, in Journal of Novel Research and Innovative Development, 3(1), 2025.
79. V. la Section 3 (b) dell'Executive order 14110 of October 30, 2023 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, adottato in USA del Presidente Biden, dove «The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action». Ad esso ha fatto seguito il Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence con l'obiettivo di rendere gli Stati Uniti un Paese leader nello sviluppo mondiale di un'IA sicura, protetta e affidabile (Section 2, "Objectives").
80. V. in tal senso G. Frosio, Why Keep a Dog and Bark Yourself? Intermediary Liability to Responsibility, in Oxford Int'l J. of Law and Information Technolog, 25, 2017, 1 ss. a 7 ss. nonché M. Taddeo, L. Floridi (a cura di), The Responsibilities of Online Service Providers, Springer, Cham, 2017.
81. In proposito si può ragionare in generale di "A.I. controllabile": secondo la ISO 22989 "controllabile" è una «*proprietà di un sistema di A.I. (3.1.4) [riguardo cui] un essere*

umano o un altro agente esterno (3.1.1) può intervenire nel funzionamento del sistema». Cfr. A. Holzinger, P. Kieseberg, F. Cabitza, A. Campagner, A.M. Tjoa, E. Weippl, Controllable AI-An Alternative to Trustworthiness in Complex AI Systems?, in International Cross-Domain Conference for Machine Learning and Knowledge Extraction, Lecture Notes in Computer Science, Springer, Cham, 2023, pp. 1 ss.

82. È stato il timore di un impiego "in a non-transparent and non-explainable way" dell'intelligenza artificiale "for automatic decision making" ad aver determinato l'adozione delle linee guida sull'utilizzo dell'intelligenza artificiale – incentrate su di una logica di controllo e organizzazione dell'utilizzo dell'A.I. da parte delle organizzazioni e delle istituzioni – a livello internazionale da parte della ISO e della IEC.
83. V. in tal senso J.B. Nordemann, J. Pukas, Copyright exceptions for AI training data – will there be an international level playing field?, in J. IP Law and Practice, 2022, p. 973, secondo il quale la grande maggioranza dei documenti che attualmente alimentano il processo di addestramento è coperta dal diritto d'autore ad eccezione delle opere cadute in pubblico dominio e quelle prive di carattere "creativo", come i testi composti da formule matematiche, i testi normativi, i manuali di istruzioni per l'uso di prodotti, ecc. Si v. sul tema M. Bertani, Diritto d'autore europeo, Giappichelli, Torino, 2011, p. 105 ss.
84. Per approfondimenti vedi sempre il c.d. Data Governance Act **(**Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) (Testo rilevante ai fini del SEE), Commissione europea, Bruxelles, 25.11.2020 COM (2020) 767 final e la c.d. AI Regulation (Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione {SEC(2021) 167 final} – {SWD(2021) 84 final} – {SWD (2021) 85 final).
85. V. P. Montalenti, L'interesse sociale: una sintesi, in Riv. soc., 2018, p. 303 ss. e F. Denozza, Logica dello scambio e "contrattualità": la società per azioni di fronte alla crisi, in Giur. comm., I, 2015, p. 5 ss.; M. Libertini, Ancora in tema di contratto, impresa e società. Un commento a Francesco Denozza, in difesa dello "istituzionalismo debole", in www.orizzontideldirittocommerciale.it e in Giur. comm., I, 2014, p. 669 ss.
86. V. R. Van Horn, Reinventing Monopoly and the Role of Corporations. The Root of Chicago Law and Economics, in Ph. Mirowski, D. Pleheve (a cura di), The Road from Mont Pèlerin. The Making of the Neoliberal Thought Collective, Harvard University Press, Cambridge-London, 2009, p. 204 ss.
87. V. D. Patterson, ChatGPT is more like an "alien intelligence" than a human brain, says futurist, in ZDNET, 2023.
88. V. J.P. Quintais, Generative AI, copyright and the AI Act, in Kluwer Copyright Blog, 9 maggio 2023.
89. V. G. Gallo, F. Wirz, G.F. Tuzzolino, The role of Artificial Intelligence in architectural design: conversation with designers and researchers, in Proceedings of S.Arch 2020, the 7th international conference on architecture and built environment. Tokyo 7-9 april 2020.
90. R. Ducato, A. Strowel, Ensuring text and data mining: remaining issues with the EU

copyright exceptions and possible ways out, in CRIDES, Working Paper series, 1, 2021, p. 13.