NAZIONE FUTURA

Dossier n. 14 / aprile 2024

TANTE REGOLE POCHE IDEE

Perché l'Europa è rimasta indietro nell'innovazione tecnologica

---

di **Maria Grazia Palluotto**, **Lucrezia Roviello** e **Jacopo Ugolini**

nazionefutura.it

SINOSSI

In un mondo in continua evoluzione, lo sviluppo e il miglioramento delle tecnologie esistenti, il progresso, alimentato dalla ricerca scientifica e dalla creatività umana, è sicuramente il motore fondamentale del cambiamento sociale. In questo dossier viene approfondita l'intricata rete di normative che sono arrivate a definire il panorama digitale europeo. Con l'espansione di Internet, i decisori europei devono implementare regolamenti per proteggere la privacy, promuovere la concorrenza e combattere la disinformazione. Dal GDPR al DSA e alla DMA, l'Europa è diventata un'importante autorità normativa, ma queste regolamentazioni sono spesso criticate per la loro complessità e il potenziale di ostacolare l'innovazione. Attraverso analisi approfondite e case studies, si esplorano gli impatti su imprese, consumatori e l'ecosistema digitale nel complesso, valutando l'efficacia delle attuali normative e identificando aree di miglioramento. Il dossier mira a informare politici, settore e pubblico sulle sfide della navigazione digitale in Europa, cercando di bilanciare i vantaggi delle nuove tecnologie con le loro implicazioni sociali, etiche e ambientali.

INDICE

Dossier n. 14 / 2024

Tante regole, poche idee. Perché l'Europa è rimasta indietro nell'innovazione tecnologica

Realizzato con il contributo di Google Italia s.r.l.

1. INTRODUZIONE

La corsa all'innovazione tecnologica è fra i più rilevanti temi globali su cui si incentra attualmente il dibattito politico, economico e sociale degli ultimi anni. In vista del prossimo mandato dell'Unione europea, e in un contesto in cui si teme l'aumentare della dipendenza dell'Europa da competitor globali ben più avanzati nell'ambito tecnologico e digitale, è necessario porre specifiche priorità tra le *policies* dedicate a tale settore, i cui sviluppi degli ultimi anni sono innanzi agli occhi dei più a differenza del lato più "pericoloso" della tecnologia, ossia quello dei rischi derivanti da sistemi sempre più digitali e quindi attaccabili in diversi e complessi modi.

Su questo fronte, non solo l'Europa è indietro rispetto agli alleati statunitensi, ma il Vecchio Continente è proprio – così sembra – sulla strada della regolamentazione eccessiva e otturante per lo sviluppo. Non è però tutto negativo: è un'ulteriore sfida per l'Unione Europea: questa preoccupazione per il gap tecnologico e delle risorse per la ricerca tra Europa e Stati Uniti potrebbe agire come leva per condurre gli stati europei a una maggiore cooperazione e persuadere l'Europa a sfidare se stessa ed essere un attore chiave nella scena dell'innovazione tecnologica globale. La suddetta corsa all'innovazione tecnologica, quindi, è "croce e delizia" per l'Europa in quanto delinea un terreno inesplorato ma al contempo fertile su cui investire e trarre benefici.

Negli ultimi anni, l'Unione europea genera dibattito nell'ambito digitale a causa dei dettami imposti a livello normativo (vedasi, ad esempio, il Digital Services Act, il Digital Markets Act, l'AI Act), che, sebbene volti a garantire sicurezza e integrità, rischiano di porre dei seri limiti alla libera espressione all'interno del web, sia per i ritardi nella progressione tecnologica (specie in campo delle AI), evidenziati nel report annuale *State of European Tech 2023*, sia per la riduzione degli investimenti – nel 2023 si è registrato un calo di 37 miliardi di investimento rispetto al 2022.

Il valore economico generato negli ultimi anni dalle big tech è molto elevato, e questo dà loro fiducia per continuare su questa linea, incrementando l'attenzione verso lo sviluppo di reti di collaborazioni. È chiaro che, intanto, a beneficiarne siano principalmente i Paesi d'origine di questi soggetti operanti nel mercato *tech*, ossia Stati Uniti e Cina. In Europa, è stato in parte grazie alla pandemia se le aziende, in risposta ai lockdown e in generale alla riduzione del lavoro, hanno investito nella digitalizzazione, così perseguendo l'obiettivo di recuperare terreno rispetto alle aziende statunitensi nell'implementazione di tecnologie digitali avanzate. Nonostante ciò, il nostro continente deve recuperare ancora un enorme *gap*, rischiando pertanto di sviluppare dipendenze in diverse tecnologie critiche e di dover fronteggiare una prospettiva di forte indebolimento nel mercato del lavoro. Rispetto agli Stati Uniti, infatti, nell'Unione europea vi è un numero elevato di piccole imprese con maggiori difficoltà nell'implementazione di sistemi digitali. Ciò determina ripercussioni direttamente sui lavoratori, in quanto le suddette imprese non sono inclini a pagare salari più alti e hanno meno probabilità di creare nuovi posti di lavoro.

La situazione che ci troviamo di fronte non è quindi delle più rosee. Ci sono certo aspetti positivi, ma l'ossessione legislativa dell'Unione Europea è di per sé fonte di rischio per lo svi-

luppo del rapporto aziende-digitalizzazione. Facendo riferimento alle normative attualmente vigenti, tale dossier ha come obiettivi quelli di fornire una panoramica sull'odierna situazione europea in ambito digitale, e di analizzare punti critici e traiettorie da definire nella corsa verso un auspicabile progresso tecnologico.

2. LA SOVRANITÀ DIGITALE DELL'UNIONE EUROPEA

Il *Digital Economy and Society Index (DESI)*, il *Digital Decade policy programme* e tutta la strategia digitale dell'Unione Europea hanno reso lo sviluppo tecnologico elemento centrale delle politiche dei Paesi europei e dei loro piani nazionali di ripresa e resilienza.

Il nuovo programma per lo sviluppo digitale dell'Europa nasce proprio all'indomani della pandemia che aveva evidenziato i limiti di cui sono caratterizzati i Paesi membri sul fronte tecnologico: vulnerabilità dello spazio digitale, dipendenza da tecnologie straniere ed effetti della disinformazione sulle nostre società dimostrano per l'ennesima volta come il grado di digitalizzazione dell'economia e della società sia un fattore primario di influenza globale ma anche di sicurezza interna/esterna.

L'obiettivo "digitale" dell'Europa per il 2030 è stato esposto mediante la documentazione *Digital Compass* ("Bussola Digitale"): questa mira a tradurre gli obiettivi UE relativi alla transizione digitale in azioni concrete, seguendo quattro linee di sviluppo, i "punti cardinali", in cui la strategia si articola. In sintesi, gli obiettivi da raggiungere sono:

- una popolazione dotata di competenze digitali e professionisti altamente qualificati nel settore digitale con l'obiettivo di conseguire l'equilibrio di genere;
- la costruzione di infrastrutture digitali sostenibili, sicure e performanti;
- la trasformazione digitale delle imprese;
- la digitalizzazione dei servizi pubblici.
-

Per realizzarli la Commissione europea si è mossa principalmente lungo tre direttrici:

1) il data sharing per lo sviluppo di sistemi di intelligenza artificiale;

2) un maggiore controllo sui *gatekeeper*, cioè sulle piattaforme digitali in grado di condizionare l'accesso al mercato, onde evitare che essi possano abusare della loro posizione dominante;

3) una maggiore responsabilizzazione degli intermediari digitali per i contenuti prodotti e diffusi dagli utenti finali dei loro servizi.

L'obiettivo del piano è di tracciare, attraverso una maggiore regolamentazione e controllo delle *tech companies*, un percorso verso la sovranità digitale dell'UE nei confronti non solo dei grandi players digitali ma anche dei suoi Stati Membri. Siamo tutti consci del fatto che impiegare tecnologie informatiche sofisticate richieda l'intervento anche dei poteri pubblici. Questo soprattutto per garantire un'adeguata tutela dei diritti fondamentali delle persone: da qui la rivendicazione da parte dell'UE del potere di disciplinare l'innovazione digitale e la tutela dei suddetti diritti.

In questo flusso di conoscenze, ricerche e scoperte in campo tecnologico, non possiamo dimenticare il fattore più importante, quello umano. Riuscirà l'uomo a mantenersi al centro di un mondo sempre più tecnologico? Per funzionare e per potersi muovere in un mondo in cui anche i servizi e la pubblica amministrazione si stanno trasformando e rischiano di diventare inaccessibili a coloro che soffrono l'assenza di adeguate competenze digitali, una società deve disporre di cittadini digitalmente capaci e responsabili e una forza lavoro digitalmente

più qualificata rispetto a oggi. Anche nella società digitale devono essere rispettati i diritti fondamentali dell'individuo: libertà di espressione, di creare e gestire imprese, accesso a informazioni affidabili e trasparenti, protezione dei dati personali e della creazione intellettuale. Il diritto alla conoscenza del web, potremmo aggiungere. Per ottenere questo risultato occorre un sistema di educazione digitale altamente performante e anche un'efficace politica internazionale in campo educativo.

Il 3 ottobre 2023 la Commissione Europea ha adottato, anche a causa delle crescenti tensioni politiche in atto con Cina e Russia, una raccomandazione sulle aree tecnologiche critiche per la sicurezza economica dell'UE. Tra quelle ritenute più a rischio ci sono i semiconduttori e le connettività avanzate, l'intelligenza artificiale, le tecnologie quantistiche, robotiche e biotecnologie. Con questa raccomandazione, l'UE intende promuovere la competitività senza eliminare i legami con i partner globali, ma semplicemente riducendo i rischi provenienti da queste relazioni. L'intreccio tra le relazioni internazionali e la sicurezza nazionale però costituisce anche un motivo di dibattito perché, a differenza di quanto appena esplicitato, molti Stati Membri mirano invece alla cosiddetta strategia "del disaccoppiamento" e quindi a una separazione più drastica con i partner globali. L'Unione Europa è, quindi, chiamata a uno sforzo di unità e lungimiranza, senza dimenticare che la tecnologia cambierà più velocemente di ogni altro aspetto e quindi la politica rischia in ogni caso di rimanere indietro, soprattutto se regolamenta eccessivamente o se priva di chiare linee direttive dalle quali non discostarsi.

3. LA BULIMIA LEGISLATIVA È UN RISCHIO

L'aspetto che andiamo ora a evidenziare, sottolineandone le conseguenze che si potrebbero con molta probabilità verificare, è quello dei regolamenti europei. La mole di produzione di atti regolatori emanati dall'Unione Europea alimenta il divario dell'Europa con altri Paesi, in particolare Cina e Stati Uniti. Con almeno quindici anni di ritardo, le istituzioni europee tramite Ursula von der Leyen, presidente della Commissione Europea, hanno riconosciuto la *issue* della sovranità tecnologica come interesse comune prioritario dei Paesi Membri UE: la volontà è la promozione di una competitività europea in grado di sfidare in futuro i monopoli delle cinque sorelle californiane e i colossi cinesi. Questa nuova attenzione per tale settore da parte delle istituzioni europee si è tradotta – in ambito politico – in una mole eccessiva di misure atte a regolamentare la tecnologia, il ruolo delle big tech e tutto ciò che concerne questo ambito.

Secondo il think tank belga Bruegel, specializzato in studi economici, le misure legislative emanate e pubblicate nella Gazzetta ufficiale dell'Unione europea fino a oggi sono circa settanta; se poi contiamo quelle che potrebbero eventualmente essere emanate durante l'attuale sessione legislativa, arriviamo a ventinove ulteriori misure legislative; infine, altre nove sono state annunciate ma non hanno ancora iniziato formalmente il proprio iter legislativo.

Oltre alla privacy e ai dati degli utenti – due temi sui quali la legislazione europea ha posto molta attenzione – gli atti già emanati prevalentemente riguardano:

- la sicurezza informatica;
- la fiducia degli utenti;
- il commercio elettronico e la tutela dei consumatori;
- la concorrenza;
- i diritti di proprietà intellettuale e media.

Guardando al lato legislativo, l'Unione Europea è intervenuta tramite l'adozione del **Digital Services Package**, diventato esecutivo dal 2023 e composto da:

- **DMA (Digital Markets Act)**, entrato in vigore il primo novembre 2022, volto a disciplinare le attività delle principali piattaforme digitali operanti nell'Unione Europea, rinominate col termine *gatekeeper*, ossia piattaforme digitali che offrono servizi di intermediazione online (tra cui motori di ricerca, social network, messaggistica e condivisione di video) e superano determinate soglie in termini di fatturato e numero di utenti;
- **DSA (Digital Service Act)**: basato sul principio "ciò che è illegale offline, è illegale online", entrato in vigore nel novembre 2022, ma la maggior parte dei suoi regolamenti hanno avuto "luce verde" dal maggio 2023. Poi, l'UE ha individuato quali piattaforme, ossia i *gatekeeper*, sono obbligate a rispettare il dettato del DSA, stabilendone un elenco ufficiale all'inizio del settembre 2023. Da quel momento i *gatekeeper* hanno avuto circa sei mesi per adottare le misure necessarie affinché fosse rispettato il dettato dell'Unione Europea, così da arrivare al prossimo 6 marzo 2024 con tutte le piattaforme in grado di rispettare quanto scritto negli atti del Digital Services Package. Guardando ai contenuti

del *DSA*, i punti cardini di questo atto sono la gestione della profilazione, il contrasto ai comportamenti scorretti online e alla disinformazione, la rimozione dei contenuti illegali e una tutela specifica per i minorenni dell'Unione Europea.

Un'altra norma – questa adottata da poco tempo da parte delle istituzioni europee – che interessa le big tech mondiali è l'*AI ACT*, il cui testo verrà approvato definitivamente il 24 aprile 2024 mentre il 2 febbraio è stato adottato il testo bozza definitivo. Al centro di questa iniziativa, la prima che a livello mondiale tenta di regolamentare l'intelligenza artificiale, vi è l'obiettivo di garantire che l'utilizzo di questa nuova tecnologia sia volto al pieno rispetto dei diritti umani e dei valori democratici. Oltre alle "belle parole", però, la realtà è ben più complicata. Regolamentare un processo in forte sviluppo, come quello riguardante l'intelligenza artificiale, rischia inevitabilmente di ridurre l'innovazione dell'AI sul suolo europeo, conducendo le principali aziende del settore verso lidi dove vi è meno regolamentazione. L'*AI ACT* entrerà in vigore il primo gennaio 2026. I produttori di sistemi basati su questa forma di intelligenza hanno tempo fino al primo gennaio 2029 per conformarsi alle nuove disposizioni.

Il settore con il più alto tasso di competitività è, appunto, quello delle *Artificial Intelligence* (AI), che fa rima con un agglomerato di conoscenze collettive in grado di comprendere, relazionarsi e restituire risultati agli esseri umani tramite realistici ragionamenti logici. Durante il 2023 tale sistema ha coperto il 19% del mercato totale (e le stime prevedono che il dato salirà al 28% entro il 2030). Una recente analisi comparsa su agendadigitale.eu, descritta da Giancarlo Vergine, racconta di un mercato, quello dell'AI, in forte sviluppo, dove gli investimenti delle *venture capitalists* nell'AI stanno crescendo esponenzialmente e dove la rapida evoluzione è guidata da USA e Cina. UE, UK e Giappone seguono le due "superpotenze tech" con notevole distacco.

Tra le risposte alle dinamiche digitali in atto, infine, è da considerare anche l'Euro digitale, concepito come motore di innovazione nel settore dei pagamenti e di cui la Commissione Europea ha presentato un progetto di proposta legislativa il 28 giugno 2023. Regolamentazioni di questo tipo potrebbero sortire un duplice effetto: se da una parte vi è la promozione dell'innovazione, dall'altra il rischio che si corre sarebbe proprio quello di allontanare l'Europa stessa dai Paesi esteri.

Ma, tornando al tema della bulimia legislativa di cui evidentemente soffre il legislatore europeo, dobbiamo chiederci quale impatto possano avere il DSA e il DMA sulle aziende statunitensi, cioè la gran parte dei cosiddetti *gatekeeper*. Queste normative non coincidono con le linee guida dei colossi esteri. Le leggi statunitensi, ad esempio, tendono a utilizzare un modello di "opt-out" (opzione per cui è possibile trasmettere comunicazioni a tutti, tranne per chi ha disdetto la propria sottoscrizione a un sito web, a un blog, a un gruppo o a qualsiasi altro servizio online), in cui in molti casi non è richiesto il consenso dell'utente alla raccolta e al trattamento dei dati personali. È necessario ottenere il consenso dei consumatori solo per condividere, vendere o utilizzare i dati personali per altri scopi commerciali.

Anche il DMA ha ricevuto critiche sin dalla sua introduzione in quanto, per impedire ai *gatekeeper* di sfruttare la loro posizione dominante nei confronti della concorrenza, impone oneri normativi e controlli eccessivi. Potrebbe così soffocare l'innovazione, danneggiare

potenzialmente le piattaforme più piccole, rallentare la crescita delle piattaforme digitali e scoraggiare gli investimenti futuri.

Ci sono, poi, preoccupazioni circa la praticità e l'applicabilità di alcune misure nel DMA. Il divieto di profilazione nella pubblicità potrebbe causare la fine dell'ecosistema pubblicitario targetizzato per come lo conosciamo, incidendo sui flussi di entrate delle piattaforme digitali e degli editori. Più in generale, dagli Stati Uniti sorgono voci critiche sulla possibilità che il DMA renda più difficile e costosa l'esportazione dei servizi digitali verso l'Europa, con conseguente minore qualità dei servizi offerti sul mercato digitale europeo. Nel complesso, il DMA ha acceso un vivace dibattito sull'equilibrio tra regolamentazione e innovazione nel mercato digitale.

L'immagine di un'Europa competitiva e "iper-regolamentata", alla luce della scadente posizione europea nel "ranking" dell'innovazione, non coinciderebbe affatto con quella di un'Europa, invece, che vorrebbe eguagliare i Paesi competitor, ma si avvicinerebbe di più a quella di un'Europa debole, impantanata in uno scenario di scarsa competitività che, a causa della sua sdoganata arretratezza, non sarebbe in grado di sostenere la sfida con i grandi competitor USA-Cina.

4. CYBERSICUREZZA: LA NUOVA SFIDA

Dopo una serie di attacchi informatici di grande entità avvenuti nel 2017, la sicurezza informatica è diventata una tematica di alta priorità per l'Europa. Come già riportato nei capitoli precedenti, da quell'anno fino a oggi sono oltre un centinaio le proposte di legge accettate o prese in considerazione dall'Unione Europea. Fra queste spiccano anche quelle riguardanti la cybersecurity. Attualmente sono entrate in vigore il *Regulation for a Cybersecurity Act* (2019), *Regulation to establish a European Cybersecurity Competence Centre* (2021) e il *NIS 2 Directive* (2022), mentre sono quattro quelle che al momento sono in fase di analisi.

Stando a tali documentazioni, le strategie pianificate dall'Europa per la sicurezza informatica riguardano principalmente due aspetti: la criminalità informatica e gli attacchi informatici. L'UE ha optato per affrontare la criminalità informatica tramite ciò che sa fare meglio: approvare leggi.

Il 30 novembre 2023 la Commissione, il Consiglio e il Parlamento Europeo hanno annunciato di aver raggiunto un accordo sul testo del *Cyber Resilience Act* ("CRA"), che introdurrà nuovi obblighi di sicurezza informatica per una gamma di prodotti digitali venduti in Europa e imporrà una serie di obblighi per i produttori e gli importatori di "prodotti con elementi digitali" ("PDE"). Si ritiene che il CRA sia il primo atto in assoluto volto a garantire che i consumatori siano meglio protetti dai produttori di hardware e software venduti all'interno dell'UE. In passato spettava al consumatore garantire che l'hardware e il software fossero sicuri, attraverso l'applicazione di patch e una corretta configurazione. Anche se questi saranno ancora richiesti, ai produttori vengono imposti maggiori controlli di sicurezza durante tutto il ciclo di sviluppo, se non vogliono incorrere in sanzioni o multe. Il *Cyber Resilience Act* è strutturato su quattro pilastri:

1. Garantire che i produttori migliorino la sicurezza informatica dei propri prodotti durante l'intero ciclo di vita;
2. Creare un quadro unico e coerente per la conformità alla sicurezza informatica nell'UE;
3. Aumentare la trasparenza delle pratiche di sicurezza informatica e delle proprietà dei prodotti e dei loro produttori;
4. Fornire ai consumatori e alle imprese prodotti sicuri pronti per l'uso.

Alcuni dettagli del *CRA* sono stati oggetto di accesi dibattiti tra le istituzioni dell'UE: in particolare l'aspetto che più di altri costituisce un ostacolo di difficile implementazione è costituito dagli obblighi di segnalazione delle vulnerabilità, nonché le categorie di PDE[1] considerate "importanti" o "critiche". Gli obblighi di segnalazione delle vulnerabilità sono di particolare interesse per l'industria, con gli esperti di sicurezza che hanno criticato il quadro proposto per la divulgazione delle vulnerabilità in quanto non al passo con gli standard internazionali e che potrebbe portare a un aumento, invece di una diminuzione, dei rischi di sicurezza informatica.

L'Europa è in ritardo rispetto alle capacità informatiche offensive di avversari come Russia e Corea del Nord: questo divario è dovuto a una serie di fattori, tra cui investimenti limitati

1. PDE sta per "prodotti con elementi digitali"

nelle capacità di difesa cibernetica, mancanza di coordinamento tra i Paesi europei e una comprensione insufficiente delle minacce informatiche emergenti.

Il concetto di "fattore deterrente" è cruciale in questo contesto. Se l'Europa non è consapevole delle minacce informatiche, continuando a rimandare le azioni necessarie per affrontarle, sta incoraggiando i "nemici globali" a perpetrare azioni offensive senza timore di conseguenze significative. In altre parole, la mancanza di una risposta tempestiva ed efficace favorisce potenziali attacchi informatici.

Per affrontare questa sfida, l'Europa dovrebbe considerare una serie di misure, tra cui:

1. Aumentare gli investimenti nelle capacità di difesa cibernetica, inclusi programmi di ricerca e sviluppo per sviluppare tecnologie avanzate per la sicurezza informatica;
2. Migliorare il coordinamento tra i Paesi europei per favorire lo scambio di informazioni e la collaborazione nella lotta contro le minacce informatiche;
3. Potenziare la formazione e l'istruzione nel campo della sicurezza informatica per garantire che ci siano abbastanza esperti in grado di affrontare le sfide emergenti;
4. Sviluppare politiche e normative efficaci per affrontare le minacce informatiche e garantire che ci siano conseguenze significative per coloro che cercano di attaccare l'infrastruttura critica o i sistemi informatici dell'Europa.

In definitiva, affrontare le sfide della sicurezza informatica richiede un impegno coordinato e a lungo termine da parte dell'Europa, insieme a una consapevolezza crescente delle minacce e alla volontà di agire in modo tempestivo ed efficace. Al momento, l'Unione Europea non dispone delle risorse per comprendere e combattere una guerra informatica. Ecco perché dovrebbe prendere in considerazione nuove proposte per facilitare la condivisione delle prove elettroniche sia all'interno che all'esterno dell'UE. I recenti piani della Commissione per consentire agli Stati membri di adottare misure *ad hoc* non risolverebbe il problema dello scambio transatlantico di dati. L'UE dovrebbe prendere in considerazione la sostituzione degli attuali accordi UE-USA con un trattato più efficiente sulle prove digitali e anche concludere accordi con altri Paesi.

L'UE dovrebbe incoraggiare gli Stati membri a investire maggiormente nella sicurezza informatica e a coordinare la loro risposta ai principali attacchi informatici, ad esempio determinando chiaramente quando possono essere consentite sanzioni economiche, chi dovrebbe essere responsabile della loro attuazione e in quali circostanze.

Altro compito di Bruxelles sarebbe quello di intensificare gli sforzi nei confronti delle minacce informatiche nell'ottica di integrare un maggior supporto per gli Stati membri nei loro tentativi di contrastarle. Per questo, la prossima Commissione Europea potrebbe istituire una task force composta da tutti i dipartimenti competenti della Commissione, così da creare un *working group* che stabilmente, anche tramite un dialogo proficuo con la società civile e i suoi rappresentanti, possa integrare le sicurezze tecnologiche dei paesi membri. Infine, l'Europa e l'Occidente dovrebbero collaborare con le aziende tecnologiche per sviluppare una serie di regole di base per definire e aiutare a vincere gli attacchi informatici.

L'UE è in svantaggio perché gli attori malevoli del mondo cibernetico – a differenza dell'Unione – conoscono approfonditamente il campo da gioco. La sfida per l'UE è imparare a sconfiggere questi criminali informatici internazionali prima che il prossimo grande attacco informatico metta a rischio l'economia europea e la sicurezza fisica dei suoi cittadini.

5. LA DIGITALIZZAZIONE DELLE IMPRESE

L'epoca che viviamo impone di affrontare senza timori la trasformazione digitale, diventata imprescindibile per le imprese di qualsiasi tipo di dimensioni. È ormai ben risaputo che dalle tecnologie digitali e il loro sviluppo possiamo ricavare effetti molto positivi per il sistema economico territoriale, regionale e nazionale. Certo, la paura della digitalizzazione e dell'automazione del lavoro è presente nell'opinione pubblica ma, se da una parte perché inevitabile e dall'altra perché possibile fautrice di positive conseguenze, l'atteggiamento col quale affrontiamo il rapporto tecnologia-lavoro dev'essere positivo e produttivo.

Queste scoperte tecnologiche offrono opportunità senza precedenti per migliorare l'efficienza operativa, raggiungere nuovi mercati e soddisfare le esigenze dei clienti in modi innovativi. Tuttavia, questa transizione non è priva di sfide, specialmente per le piccole e medie imprese (PMI), che costituiscono il cuore pulsante dell'economia europea. Le regole europee che disciplinano il digitale possono essere, indubbiamente, un prezioso strumento per garantire la protezione dei consumatori, la sicurezza dei dati e la concorrenza equa. Tuttavia, quando diventano eccessivamente stringenti, rischiano di minare la capacità delle PMI di adottare e sfruttare appieno le tecnologie digitali. Le PMI sono frequentemente oggetto di attacchi da parte di criminali informatici, principalmente a causa della loro limitata consapevolezza della sicurezza informatica e della presenza di programmi di risposta agli incidenti inadeguati. Questi fattori le rendono vulnerabili agli attacchi e facili bersagli per i cybercriminali. Contrariamente alla percezione comune secondo cui gli attacchi informatici si verificano principalmente nelle grandi organizzazioni, le PMI possono costituire componenti cruciali delle catene di approvvigionamento più vaste o fornire servizi a entità critiche.

Oltre che rischiare di essere troppo stringenti, le norme europee talvolta non sembrano provenire da legislatori consapevoli del sistema economico e produttivo degli stati membri. Vogliamo dire che spesso in ambito tecnologico l'UE ha legiferato come se i numerosi destinatari di tali norme fossero tutti al medesimo livello di digitalizzazione dei propri sistemi economici, produttivi e via dicendo. Non è così, però. Non solo l'Italia ma tutta l'Europa è prevalentemente costituita da piccolissime imprese (quelle sotto i dieci dipendenti) e da PMI. Spesso consideriamo, sbagliando, come "PMI" tutte quelle aziende che non sono multinazionali o comunque quelle aziende il cui nome, a primo impatto, non dice nulla… sbagliamo, appunto!

In Italia, delle 4,4 milioni di imprese attive, le microimprese con meno di dieci dipendenti emergono come il pilastro numerico più significativo, rappresentando il 95,13% del totale, mentre le grandi imprese costituiscono solo lo 0,09%. D'altro canto, le PMI italiane – ossia le aziende con almeno dieci dipendenti e un fatturato annuo che non va oltre i 50 milioni di euro[2] – ammontano a circa 211mila, pari al restante 4,78% del panorama imprenditoriale italiano. Tuttavia, queste PMI rivestono un ruolo cruciale nell'economia del Paese, generando da sole il 41% dell'intero fatturato nazionale, occupando il 33% della forza lavoro del settore privato e contribuendo al 38% del valore aggiunto complessivo del Paese. Sono tanto centrali nel sistema

2. Trascuriamo in questa descrizione la differenza tra piccola impresa e media impresa. La prima ha almeno 10 dipendenti e non più di 49, con un fatturato annuo massimo di dieci milioni, mentre la seconda ha tra i 50 e i 249 occupati e un fatturato annuo massimo di cinquanta milioni.

produttivo italiano quanto arretrate dal punto di vista tecnologico, come sostenuto da Webidoo Spa[3] che ha presentato al Parlamento europeo il suo rapporto sulla digitalizzazione delle PMI, secondo il quale l'Italia si posiziona al diciannovesimo posto sui ventisette Paesi membri. Andando, poi, nello specifico di quelle che sono le possibili implicazioni della digitalizzazione delle imprese, sempre Webidoo Spa porta altri dati in merito. Ad esempio, solo il 18% di PMI si avventura nell'e-commerce; unicamente il 6,9% s'avventura nel mercato transfrontaliero; andiamo peggio sul fronte dell'*AI*, dato che solo il 6% delle PMI adotta stabilmente l'utilizzo dell'intelligenza artificiale e l'8% l'analisi dei Big Data nelle loro strategie di marketing.

È chiaro che nel momento in cui, essendo chiamati tutti a rispettare le norme europee, le aziende implementano il dettato della Commissione, queste avranno più obblighi, e ciò significa più costi. Prevedere che una piccola azienda affronti senza conseguenze i costi enormi che derivano da vincoli, obblighi e restrizioni alla libera impresa, è una totale follia. Siamo tutti desiderosi di protezione dai nemici esterni – ora pensiamo particolarmente a quelli che potrebbero verificarsi nell'alveo del digitale – ma questo non può significare un aumento esponenziale dei costi per le piccole e medie, ma anche piccolissime, aziende che già per la globalizzazione dei mercati soffrono da anni.

Portiamo un semplice esempio che dimostra la scarsa attenzione dell'Unione Europea rispetto a quelle che sono le conseguenze economiche sulle imprese in seguito all'implementazione delle norme che riguardano il mondo digitale. Secondo uno studio di Swedish Enterprise, una delle principali associazioni datoriali svedesi rappresentante di oltre un milione e mezzo di dipendenti, le valutazioni di impatto proposte dalla Commissione europea in merito all'*AI ACT* non considerano l'effetto che la complessità delle norme e della loro applicazione produca in termini di costi di transazione e di oneri amministrativi. È follia pensare – come incredibilmente è scritto sempre nelle valutazioni d'impatto sull'*IA ACT* – che un'impresa investita dai nuovi adempimenti dell'*Artificial Intelligence Act* riesca a impratichirsi degli adempimenti in pochissimo tempo. Secondo lo studio svedese, quindi, l'effetto delle norme potrebbe essere quello di accrescere le difficoltà e i costi delle imprese europee.

Pensando, invece, a un altro caso, secondo gli studi condotti dalla Commissione europea per valutare l'effetto della direttiva UE sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS I) sulle entità all'interno dell'UE, solo il 27% delle piccole imprese aveva implementato una politica di cybersicurezza ICT, rispetto al 51% delle medie imprese e al 72% delle grandi imprese.

L'Alleanza Europea delle PMI Digitali[4] stima i costi per l'adozione delle soluzioni *AI* ad alto rischio intorno ai 7.000 euro. Ma introdurre un sistema manageriale adeguato alle esigenze di qualità dell'intelligenza artificiale può costare dai 193.000 ai 330.000 euro, mentre i costi della certificazione fornita da terze parti possono essere addirittura superiori.

3. Webidoo Spa è una digital company specializzata nello sviluppo di tecnologie e servizi per la digital transformation delle imprese.

4. European SME Alliance.

6. AGISCI, EUROPA!

Giunti alla conclusione, non possiamo che volgere l'attenzione a quello che accadrà dopo le elezioni europee di giugno. La coalizione di partiti che andrà a costituirsi – in assenza di sorprese – dovrebbe riprendere la medesima composizione che ha sostenuto la Commissione presieduta da Ursula Von der Leyen durante questo quinquennio. Quindi, politicamente è difficile aspettarsi grandi cambiamenti, perciò l'auspicio è piuttosto che l'Unione Europea stimoli in maniera massiccia l'adozione di nuove tecnologie da parte delle aziende nel segno della deregolamentazione legislativa. Non possono essere solo i grandi player internazionali, come ad esempio ha fatto Google, a supportare la digitalizzazione delle imprese. Il colosso americano, infatti, negli anni tramite la sua sezione filantropica (Google.org) ha fatto accordi con realtà italiane, come il progetto "Eccellenze digitali"[5] in collaborazione con Unioncamere, per supportare imprese e organizzazioni nella loro trasformazione digitale. Altro esempio virtuoso è la collaborazione[6] tra Google e Alleanza delle Cooperative italiane, data la centralità delle organizzazioni cooperative e no profit nella trasformazione digitale del Paese.

Nel contesto della crescente digitalizzazione delle imprese italiane alla luce delle normative europee, emerge chiaramente la necessità di un approccio integrato e strategico per sfruttare appieno le opportunità offerte dalle tecnologie digitali. Come evidenziato nel presente dossier, l'adozione di strumenti e processi digitali è diventata imprescindibile per rimanere competitivi sul mercato internazionale e per rispondere alle esigenze sempre più sofisticate dei consumatori. L'implementazione di normative europee mirate alla promozione della digitalizzazione, come il Regolamento Generale sulla Protezione dei Dati (GDPR) e il Digital Services Act (DSA), rappresenta una spinta significativa verso la creazione di un ambiente digitale sicuro, equo e trasparente per le imprese. Tuttavia, affinché le imprese italiane possano capitalizzare appieno su queste opportunità normative, è fondamentale un impegno continuo da parte delle istituzioni, delle imprese stesse e dei vari attori del settore per garantire una corretta applicazione e adattamento delle norme alle specifiche esigenze nazionali. È necessario, quindi, un approccio collaborativo e proattivo per garantire che la digitalizzazione diventi un motore di crescita per le imprese italiane, contribuendo così alla competitività del nostro Paese nel contesto globale dell'economia digitale, e che non sia, invece, un mero onere economicamente dispendioso.

Cosa manca all'UE quindi per stare al passo con i tempi e velocizzarsi verso la leadership tecnologica? Sicuramente urge avere a disposizione un quadro giuridico a lungo termine che lasci spazio all'innovazione, nonché di massimi investimenti e di un mercato unico digitale con

5. Si tratta di un finanziamento da 1,4 milioni di euro per promuovere la formazione dei piccoli imprenditori e dei lavoratori al fine di potenziare le loro competenze digitali. Questo finanziamento sarà particolarmente mirato a tematiche attuali, come la cybersicurezza.

6. Nel 2022, è stato avviato un progetto pluriennale dall'Alleanza delle Cooperative Italiane, supportato da un finanziamento di 3,5 milioni di euro da parte di Google.org. L'obiettivo principale del progetto è consolidare l'ecosistema dell'imprenditoria sociale in Italia. Questa iniziativa offre alle imprese cooperative e non profit beneficiarie l'accesso a servizi di innovazione digitale tramite consulenze e programmi di implementazione tecnologica forniti da oltre 40 imprese "trasformatrici" coinvolte nell'iniziativa.

standard chiari. Altrettanto sicuro è il fatto che le autorità europee non sembrano consapevoli di rappresentare in taluni casi un blocco allo sviluppo del continente: la portata delle ultime leggi imposte dalla Commissione Europea sono un deterrente alla corsa digitale europea in quanto limitano il diritto alla libera espressione e informazione, assecondando in tal modo un clima di dissimulata censura.

Affinché si possa parlare di una crescita completa, questa dovrebbe essere – oltre che sostenibile – intelligente, basata cioè sulla ricerca e sull'innovazione. Non sono poi da trascurare la carta del "fattore umano" e gli investimenti nel capitale umano: occorre formare e potenziare i futuri lavoratori nel settore, sin dalle scuole. I giovani devono essere preparati ad approdare sul mondo digitale sia da un lato social sia da un punto di vista formativo. In conclusione, l'unico modo per poter stare al passo con i tempi è l'innovazione, ecco perché l'Unione Europa dovrebbe affrettarsi e puntare ad accaparrarsi la propria posizione nel campo delle tecnologie, soprattutto nell'ambito della AI, settore che dominerà il mondo tech negli anni a venire, e cogliere la grande opportunità in serbo per le prossime elezioni per il Parlamento europeo (che si svolgeranno dal 6 al 9 giugno 2024).

NAZIONE FUTURA

Dossier n. 14 / aprile 2024

nazionefutura.it