Le sfide per l'ecosistema digitale europeo

di Alice Bellante

15-03-2022

La ricerca della sovranità digitale è diventata una questione prioritaria all'interno dell'Unione Europea. Ciò che risulta tutt'altro che scontato, tuttavia, è cosa s'intenda di preciso con il concetto di digital sovereignty, che, a seconda delle prospettive, può indicare il controllo dei dati, le questioni relative alla sicurezza nazionale, le infrastrutture, l'autonomia tecnologica. Occorre quindi prendere in considerazione ogni variabile, per comprendere il complesso dei meccanismi di protezione dell'ecosistema digitale europeo e le politiche che incoraggiano l'innovazione.
L'aspirazione di creare soggetti alternativi alle imprese straniere che dominano il mercato europeo dei servizi digitali non è una novità e può essere fatta risalire già al 2010 in Paesi come Francia o Germania. Nel primo caso infatti Parigi, sotto il governo di François Fillon, lanciava il primo progetto di cloud sovrano e la costruzione di un grande data center finanziato con risorse pubbliche per 150 milioni di euro. Nel secondo caso, analogamente, a Berlino nel 2011 si annunciava il lancio del "Bundescloud", un cloud sovrano funzionante da piattaforma operativa centrale per il governo federale, sotto l'egida dell'allora Ministro dell'Interno, Hans-Peter Friedrich. Tuttavia, da allora sono cambiate molte cose. Nella sua "Agenda per l'Europa", Ursula von der Leyen ha affermato chiaramente che «non è troppo tardi per raggiungere la sovranità tecnologica in alcune aree tecnologiche critiche», citando l'Intelligenza Artificiale, l'informatica quantistica e la blockchain.
Occorre altresì notare che nel panorama politico e regolatorio attuale, le imprese tecnologiche non sono semplici strumenti nelle mani dei governi; al contrario, esse sono le prime a plasmare l'ambiente in cui i governi operano. Esercitano, così, un'influenza rilevante sulle tecnologie e sui servizi che guideranno la prossima rivoluzione industriale, contribuendo a determinare come i Paesi eserciteranno il proprio potere economico e militare, modelleranno il futuro del lavoro e ridefiniranno i contratti sociali.
Secondo quanto scrive Ian Bremmer su Foreign Affairs, è ora di cominciare a considerare le più grandi aziende tecnologiche come enti simili agli Stati. Esse esercitano una forma di sovranità nei confronti dello spazio digitale, un regno in rapida espansione che spesso è anche fuori dalla portata degli enti regolatori. Tuttavia, per capire come si svolgerà la dialettica tra le aziende tecnologiche e i governi, è importante comprendere la natura del potere di queste aziende. Gli strumenti a loro disposizione sono unici nel panorama globale, ed è per questo che i governi trovano così difficile tenerle a freno. La loro presenza globale oggi è pervasiva, in grado di influenzare direttamente i mezzi di sussistenza, le relazioni, la sicurezza e persino i modelli di pensiero di miliardi di persone in tutto il mondo.
Basti pensare al caso di Cambridge Analytica che, pur implicando un uso illecito di dati, risulta utile per capire fino a che punto la tecnologia è in grado di influenzare la nostra realtà quotidiana, spesso nel bene e a volte nel male. Cambridge Analytica, società fondata da Robert Mercer nel 2013, era specializzata nella raccolta e nell'elaborazione dei dati dei social network, al punto da essere arrivata a sviluppare un sistema di microtargeting comportamentale, capace di elaborare pubblicità personalizzata per ogni singolo utente. Tale meccanismo fu poi amplificato dall'interazione tra Facebook e l'app del ricercatore Aleksandr Kogan, "thisisyourdigitallife", la quale consentì l'accesso ai dati non solo degli utenti che consapevolmente si iscrivevano (acconsentendo ad un parziale uso dei propri dati), ma anche di tutti i contatti di questi utenti, i cui dati sono stati invece raccolti e utilizzati in modo illecito. A fronte di 270 mila iscritti, le stime del Guardian e del New York Times contano una raccolta di informazioni su circa 50 milioni di profili. Come noto, tali dati e i servizi di

microtargeting di Cambridge Analytica furono utilizzati per creare un software che spostò l'ago della bilancia nella campagna presidenziale di Donald Trump contro Hillary Clinton nel 2016, attraverso la creazione di account bot gestiti automaticamente per diffondere fake news e contenuti contro Clinton. Lo stesso modus operandi, seppure in un contesto più ambiguo, fu applicato alla campagna referendaria per l'uscita del Regno Unito dall'Unione Europea, la cosiddetta Brexit, con esiti ormai consolidati.
Le implicazioni di tale realtà impattano su praticamente tutti gli aspetti della vita civile, economica e privata: gli algoritmi influenzano la nostra intera esistenza. Le notifiche di Facebook e Instagram contribuiscono al rilascio di dopamina nel cervello umano, i sistemi di Intelligenza Artificiale di Google completano le nostre frasi mentre le stiamo ancora finendo di pensare, i pop-up di Amazon influenzano i nostri acquisti. In queste e altre forme, le aziende tecnologiche modificano il modo in cui le persone trascorrono il proprio tempo, quali opportunità professionali perseguono, le loro attività sociali e, in ultima analisi, il loro modo di pensare. Questo potere crescerà man mano che le istituzioni sociali, economiche e politiche continueranno a spostarsi dal mondo fisico allo spazio digitale.
In molte democrazie oggi, la capacità dei politici di ottenere seguaci su Facebook e Twitter muove il denaro e il sostegno necessari ad ottenere cariche pubbliche. Concentrarsi su questo dato aiuta a comprendere la rilevanza delle azioni delle big tech, come la decisione di Facebook, ora META, e Twitter di bannare Trump dai social network dopo la sommossa di Capitol Hill. Allo stesso modo, risulta emblematico come, per una nuova generazione di imprenditori, Amazon, Google, Microsoft 365, gli App store di Apple e gli strumenti ad-targeting di Facebook siano diventati elementi indispensabili per creare un business di successo. La futura competitività delle industrie tradizionali dipenderà da quanto efficacemente esse coglieranno le nuove opportunità create dalle reti 5G, dall'Intelligenza Artificiale e dalle tecnologie come l'Internet-of-Things, come si evince dai report e dai dati delle più grandi società di consulenza come Ernst & Young, Deloitte e KPMG.
Le aziende tecnologiche esercitano alcune funzioni fondamentali anche quando si parla di sicurezza nazionale, un ambito tradizionalmente riservato ai governi e ai relativi fornitori e appaltatori della Difesa. Non a caso, quando nel 2020 gli hacker dell'SVR - il Servizio di intelligence internazionale russo - hanno violato i server di diverse agenzie governative americane e centinaia di società private, è stata Microsoft (e non la National Security Agency o lo U.S. Cyber Command) a identificare ed estromettere gli hacker.
Ancora più di recente, il 28 febbraio 2022, il New York Times ha pubblicato un articolo sul rapporto tra pubblico e privato sul tema della cyber-security in tempi di guerra, il cui titolo è "Mentre i carri armati entrano in Ucraina, così hanno fatto i malware. Poi Microsoft è entrata in guerra". L'intervento dell'azienda si è rivelato decisivo non solo nella rilevazione e nel contrasto dei malware, ma anche nella condivisione delle strategie di difesa, ovvero i dettagli del codice, con i Paesi Baltici, la Polonia e altri Paesi europei, al fine di evitare una diffusione del virus oltre i confini dell'Ucraina. Interessante notare che il ruolo di Microsoft in questa occasione viene, dal New York Times, paragonato a ciò che la Ford Motor Company fece durante la Seconda guerra mondiale, riconvertendo le linee di produzione di automobili per assemblare carri armati Sherman.
Alla luce di ciò, occorre domandarsi se i Paesi che allontanano o reprimono l'influenza delle grandi aziende tecnologiche saranno anche in grado di cogliere le opportunità della rivoluzione digitale, oppure vedranno i propri sforzi ritorcerglisi contro.
L'Unione Europea, confrontandosi con Stati Uniti e Cina, è ormai allarmata per l'assenza di giganti tecnologici regionali ed è intenzionata a cambiare lo status quo. È dunque in prima linea nella ricerca della sovranità e del controllo del suo destino digitale.
Il 25 maggio 2018 è entrato in vigore il regolamento generale sulla protezione dei dati, in sigla GDPR, una legge che limita i trasferimenti di dati personali al di fuori del blocco dei 27 Stati membri

e minaccia pesanti sanzioni alle aziende che non si impegnano a tutelare le informazioni sensibili dei cittadini UE. Sebbene, al primo impatto, questa possa sembrare una questione di rilevanza puramente europea, è importante sottolineare che il GDPR si applica a qualsiasi organizzazione che detiene i dati personali di individui che risiedono nell'UE, indipendentemente dalla posizione dell'azienda. Secondo il regolamento, l'Unione può multare le organizzazioni fino al 4% del fatturato globale annuo o fino a 20 milioni di euro - a seconda di quale sia il valore più alto - per le infrazioni gravi e fino al 2% del fatturato globale annuo o fino a 10 milioni di euro per violazioni di obblighi in materia di protezione dei dati.
Un nuovo pacchetto normativo è attualmente in discussione a Bruxelles. Negli ultimi due anni, la Commissione europea guidata da Ursula von der Leyen ha presentato tre proposte legislative che sono state oggetto di discussione al Consiglio europeo del 21 e 22 ottobre 2021, ovvero: l'Artificial Intelligence Act, il Data Governance Act e il pacchetto Digital Services Act e Digital Markets Act. Esiste infatti la possibilità, piuttosto concreta, che la Commissione europea acquisisca la facoltà di sanzionare le piattaforme Internet per la presenza di contenuti illegali, di controllare le applicazioni di Intelligenza Artificiale ad alto rischio e di ridurre il potere di mercato delle aziende tecnologiche che le istituzioni UE ritengono troppo influenti. Oltre a ciò, gli Stati membri chiedono politiche industriali orientate allo sviluppo tecnologico, in arrivo attraverso miliardi di euro di finanziamenti pubblici, finalizzati ad incoraggiare nuovi approcci al data sharing e alle risorse informatiche. Il fine ultimo è quello di sviluppare vere e proprie alternative alle più grandi aziende tecnologiche che, a differenza delle attuali opzioni, siano radicate nei valori europei.
Alla base di tali aspirazioni vi è dunque la mentalità europea, secondo la quale la crescente influenza economica e sociale delle grandi aziende tecnologiche richiede l'applicazione di nuove regole per almeno due ragioni fondamentali. In primo luogo, per garantire la protezione e il controllo dei dati personali dei cittadini, incoraggiando la partecipazione delle imprese europee al mercato digitale. In secondo luogo, l'Unione mira a realizzare modelli normativi per la transizione digitale, al fine di stabilire uno standard di riferimento in grado di promuovere i valori, le tecnologie e gli interessi europei in tutto il mondo.
Tutto considerato, la ricerca della sovranità digitale è una scommessa enorme. L'Unione Europea, agendo da una posizione peculiare, è decisa a sfidare i giganti della tecnologia e a sprigionare una nuova ondata di innovazione tutta europea. Non è improbabile però che questi sforzi alla fine rivelino che solo le più grandi piattaforme tecnologiche possono raccogliere il capitale, i talenti e le infrastrutture necessarie per sviluppare e gestire i sistemi digitali su cui le aziende si basano. È difficile determinare se una manciata di piattaforme cloud su larga scala, con tutte le opportunità economiche e le sfide connesse, potranno continuare a guidare l'innovazione, o se sotto una maggiore supervisione governativa esse potranno ancora produrre un'infrastruttura digitale all'avanguardia, competitiva a livello globale.
Il prossimo decennio metterà alla prova l'Unione Europea nella sua ricerca per la sovranità digitale. I singoli Stati membri dovranno compiere delle scelte determinanti nel regolare le relazioni tra potere pubblico e dominio privato nella gestione dello spazio digitale e di quello fisico. I governi e le aziende tecnologiche sono pronti a competere per l'influenza su entrambi gli scenari, facendo emergere con chiarezza la necessità di un quadro regolatorio che definisca la legittimità degli obiettivi delle aziende private e il perimetro di interazione con il settore pubblico.