377

17 marzo 2025

EPICENTER European Policy Information Center

IBL ISTITUTO BRUNO LEONI IDEE PER IL LIBERO MERCATO

IBL Focus

Vivere pericolosamente: DMA e la sfida di bilanciare concorrenza e sicurezza informatica

Di Giuseppe Colangelo

- I rischi per l'integrità e la sicurezza delle piattaforme stanno emergendo come preoccupazioni significative nell'attuazione del Digital Markets Act (DMA).
- Poiché il policy making implica necessariamente dei trade-off, la Commissione europea dovrebbe valutare se le soluzioni proposte dai gatekeeper sono in linea con l'obiettivo di promuovere la concorrenza mantenendo un adeguato livello di sicurezza, raggiungendo in definitiva un ottimo vincolato.
- Nel valutare le implementazioni tecniche dei gatekeeper, è fondamentale tenere conto delle differenze sostanziali tra i loro modelli di business.
- A causa dell'asimmetria informativa tra le autorità di regolamentazione e le aziende interessate, il raggiungimento di un corretto equilibrio tra concorrenza e sicurezza richiede il coinvolgimento attivo dei gatekeeper.
- Iniziative come l'Open Banking dimostrano che è possibile promuovere la concorrenza senza compromettere la sicurezza.

Giuseppe Colangelo è Jean Monnet Professor of European Innovation Policy e professore associato di Law and Economics presso l'Università della Basilicata.

Mentre il Digital Markets Act (DMA) entra nella sua fase di attuazione, la Commissione europea sta verificando se le soluzioni proposte dalle aziende tecnologiche dominanti (*gatekeeper*) sono conformi agli obblighi regolamentari. Tuttavia, questo processo sta facendo emergere nuove preoccupazioni su potenziali effetti collaterali e conseguenze indesiderate. Una di queste preoccupazioni è che le misure a favore della concorrenza possano indebolire l'integrità e la sicurezza delle piattaforme, esponendo gli utenti finali a violazioni dei dati, truffe e rischi per la privacy. Il tema, inoltre, è particolarmente delicato per le potenziali implicazioni geopolitiche.

Il dibattito in corso è inevitabile, dal momento che gli obblighi DMA mirano a promuovere l'accesso 'aprendo' gli ecosistemi dei gatekeeper, in particolare gli app store. A tal fine, il DMA include obblighi di *sideloading* (consentendo così agli utenti di installare le app al di fuori dell'app store), interoperabilità (promuovendo l'integrazione con i servizi di terze parti) e la rimozione delle restrizioni *anti-steering* (consentendo alle aziende di comunicare direttamente con gli utenti finali, promuovere offerte e stipulare contratti con loro, senza passare attraverso il gatekeeper).

In questo contesto, per attenuare il crescente rischio di polarizzazione - che a volte ha colpito anche le discussioni accademiche - può essere utile individuare un terreno comune e delineare principi ragionevoli per guidare i *policy maker* nella gestione di tali sfide complesse.

Navigare tra i compromessi: obiettivi primari e salvaguardie

Il punto di partenza risiede nel riconoscere che la definizione delle *policy* (nel nostro caso proconcorrenziali) si basa fondamentalmente su *trade-off*. Ciò comporta che le scelte binarie e gli appelli a un unico 'bene superiore' sono sovente inutili, se non dannosi. Il *policy making*, infatti, è l'arte di bilanciare interessi altrettanto rilevanti, sebbene contrastanti. Pertanto, i *policy maker* non dovrebbero favorire un obiettivo a scapito di un altro. In questo scenario, sarebbe ugualmente inaccettabile promuovere la concorrenza trascurando i rischi per la sicurezza o, al contrario, dare la priorità alla protezione dei consumatori trascurando la necessità di favorire la concorrenza.

Il modo in cui i *policy maker* raggiungono questo equilibrio dipende dal peso che gli interventi normativi assegnano a ciascuno degli interessi coinvolti. A tal fine, è essenziale distinguere tra le obiettivi primari che guidano l'intervento di *policy* e le garanzie che ne limitano la portata.

Nel caso della DMA, è indubbio che l'obiettivo primario sia quello di promuovere la concorrenza nei mercati digitali. Allo stesso tempo, la sicurezza degli utenti deve essere salvaguardata. Di conseguenza, ai *gatekeeper* non è vietato adottare misure necessarie e proporzionate che garantiscano l'integrità dei loro servizi e la sicurezza degli utenti finali. Analogamente, nella recente decisione su *Android Auto*, la Corte di giustizia ha stabilito che, in base al diritto antitrust, un operatore dominante è obbligato a concedere a terzi un accesso paritario alla piattaforma e a garantire l'interoperabilità quando la piattaforma - per sua natura e per il suo modello commerciale - è stata progettata per consentire a imprese terze di operare su di essa.[1] Tuttavia, tale obbligo non si applica in caso di impossibilità tecnica o quando l'accesso danneggerebbe l'integrità o la sicurezza della piattaforma.

In questo contesto, i *policy maker* sono chiamati ad individuare soluzioni che raggiungano un ottimo vincolato. Ciò significa che, come primo principio guida, nel valutare le soluzioni proposte dai *gatekeeper* al fine di rispettare gli obblighi del DMA, la Commissione europea non dovrebbe puntare al conseguimento del massimo livello di concorrenza possibile in termini assoluti. Dovrebbe, invece, cercare di ottenere il massimo livello di concorrenza possibile, garantendo al contempo un adeguato grado di sicurezza.

Il ruolo dei modelli di business

Una seconda considerazione fondamentale riguarda le differenze nei modelli di business dei *gatekeeper*. Il modello di business di una piattaforma influenza in modo significativo le sue strategie e i suoi incentivi. Inoltre, la prospettiva del modello di business aiuta a valutare correttamente il design e la governance della piattaforma nella creazione di valore. Infatti, a causa del dualismo intrinseco dei

1 CGUE, 25 febbraio 2025, causa C-233/23, *Alphabet e altri contro Autorità Garante della Concorrenza e del Mercato*, EU:C:2025:110.

mercati a più versanti, gli stessi fattori economici che guidano la crescita degli ecosistemi possono anche rappresentare rischi significativi per il loro successo. Trovare un equilibrio è essenziale per garantire che l'ecosistema rimanga vitale e non scoraggi gruppi specifici di utenti dall'impegnarsi con la piattaforma. In particolare, gli ecosistemi sono altamente vulnerabili alle esternalità negative, poiché il valore creato non è interamente sotto il controllo del gestore della piattaforma, ma dipende dalla partecipazione e dalle azioni degli utenti. La governance svolge, quindi, un ruolo cruciale per il successo di un ecosistema. Per questo motivo, i proprietari delle piattaforme regolano l'accesso e le interazioni all'interno dei loro ecosistemi per preservare il valore e l'integrità degli stessi.

Tuttavia, il DMA è stato redatto con un approccio indipendente dal modello di business interessato e, pertanto, i *gatekeeper* sono soggetti ai medesimi obblighi indipendentemente dal modello di business adottato.

Nell'attuazione del DMA e nella valutazione delle soluzioni proposte dai *gatekeeper*, la Commissione ha la possibilità di colmare tale lacuna tenendo in debita considerazione il contesto aziendale in cui tali misure saranno attuate. Questo, a sua volta, aiuterebbe la Commissione a valutare se le soluzioni proposte siano idonee a raggiungere l'ottimo vincolato, ovvero a promuovere la concorrenza garantendo al contempo un livello adeguato di sicurezza. In particolare, sia Apple che Google, nell'illustrare le misure avanzate per essere conformi ai dettami del DMA, hanno sollevato dubbi riguardo alla possibilità di garantire la sicurezza, sottolineando i notevoli investimenti fatti per costruire la fiducia degli utenti nei rispettivi app store. Nel valutare le loro soluzioni tecniche - in particolare per quanto riguarda le restrizioni *anti-steering*, il *sideloading* e le misure di interoperabilità verticale - è essenziale considerare le significative differenze tra i loro modelli di business e le modalità di accesso degli utenti ai rispettivi ecosistemi.

Su queste premesse, l'equilibrio tra concorrenza e sicurezza non dovrebbe essere lo stesso in un ecosistema chiuso, anziché aperto, in quanto l'obiettivo primario del DMA di favorire concorrenza è particolarmente difficile da raggiungere nel caso di un ecosistema come quello di Apple, spesso descritto come un *walled garden* a causa della sua architettura chiusa e strettamente integrata.

Il diavolo è nei dettagli (tecnici)

Una terza considerazione fondamentale è che il processo di *compliance* con il DMA deve essere visto come una strada a doppio senso, in cui tutte le parti cooperano e contribuiscono a trovare soluzioni appropriate e ragionevoli. Pertanto, mentre i due punti precedenti erano indirizzati alla Commissione, è altrettanto importante sottolineare che l'equilibrio tra concorrenza e sicurezza non può essere raggiunto senza il contributo dei *gatekeeper*. Ciò è particolarmente rilevante nel caso di obblighi che richiedono interventi di natura tecnica e, pertanto, destinati ad accrescere la asimmetria informativa tra le autorità di controllo e le aziende interessate, che non può essere colmata senza l'aiuto di queste ultime.

In tale scenario, e in linea con il monito iniziale contro le scelte binarie, non sarebbe possibile avere una discussione produttiva se i rischi per la sicurezza fossero prioritari rispetto alla concorrenza e utilizzati per neutralizzare completamente gli effetti degli obblighi del DMA. Ciò distorcerebbe l'equilibrio tra l'obiettivo primario

del DMA e le misure di salvaguardia. Allo stesso modo, non può essere consentito alle imprese dominanti di invocare preoccupazioni per sicurezza e privacy come scudo per proteggersi dall'applicazione delle norme antitrust.

Pertanto, è responsabilità dei *gatekeeper* sviluppare soluzioni tecniche che concilino la duplice esigenza di concorrenza e sicurezza degli utenti. A sua volta, la Commissione deve mantenere una mentalità aperta ed essere disposta a considerare le caratteristiche specifiche di ogni soluzione proposta.

A tal riguardo, l'esperienza europea dell'Open Banking fornisce un esempio prezioso. Imponendo alle banche di concedere a terzi un accesso sicuro ai dati degli utenti su richiesta di questi ultimi, l'iniziativa ha consentinto ai singoli di assumere il controllo delle proprie informazioni finanziarie. L'Europa è stata una delle prime giurisdizioni a rendere obbligatorio l'Open Banking introducendo una norma che impone alle banche di fornire i dati del conto del cliente a tutti i fornitori di servizi di pagamento terzi autorizzati e di eseguire gli ordini di pagamento.

Fin dall'inizio, l'iniziativa è stata guidata dall'obiettivo di promuovere la concorrenza nel settore. In questo scenario, le banche tradizionali sono i *gatekeeper*. E tuttavia, accanto ai vantaggi concorrenziali, sono da subito emersi rischi, in quanto l'Open Banking espone potenzialmente i consumatori a violazioni della privacy e a pericoli concernenti la sicurezza. A tal fine, è stato previsto un sistema di autenticazione forte dei clienti, ossia un'autenticazione a due fattori basata, ad esempio, su una password, sul possesso di una carta, e su un'impronta digitale. Il recente rapporto di valutazione pubblicato dalla Commissione europea ha rilevato che questa misura ha avuto successo nel ridurre le frodi bancarie e, quindi, a proteggere la sicurezza degli utenti finali.[2]

Per essere chiari, non si sta proponendo un confronto tecnico tra le misure dell'Open Banking e quelle del DMA finalizzate a garantire la protezione dei consumatori. Né si sta suggerendo che sarebbe facile definire standard tecnici di sicurezza nell'ambito del DMA per garantire un livello di protezione adeguato. Si osserva semplicemente che l'Open Banking ha affrontato problemi di sicurezza simili a quelli del DMA e la sua esperienza dimostra che è possibile trovare soluzioni per promuovere la concorrenza senza compromettere la sicurezza.

Concorrenza o sicurezza, non dovrebbe essere questo il dilemma.

La rinascita della regolamentazione ha suscitato un intenso dibattito sul valore di questo tipo di intervento rispetto alla tradizionale applicazione delle norme antitrust. Da molte parti sono stati evidenziato i potenziali aspetti negativi della (sovra)regolamentazione in termini di effetti collaterali e conseguenze indesiderate. In questo contesto, i rischi per la sicurezza sono una questione particolarmente delicata per i *policy maker*, in quanto renderebbe difficile giustificare l'obiettivo di promuovere l'apertura degli ecosistemi digitali a scapito della protezione degli utenti finali.

Coerentemente con la proposta iniziale, questo breve contributo vuole essere un appello contro le polarizzazioni e un invito ad accettare le sfide della gestione dei

2 Commissione europea, *Relazione sulla revisione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno*, COM(2023) 365.

trade-off. Si stratta di un passaggio inevitabile per quei paesi, come l'Unione europea, che hanno scelto di intervenire nei mercati digitali attraverso la regolazione.

ISTITUTO BRUNO LEONI
IDEE PER IL LIBERO MERCATO

IBL Focus

Chi Siamo

L'Istituto Bruno Leoni (IBL), intitolato al grande giurista e filosofo torinese, nasce con l'ambizione di stimolare il dibattito pubblico, in Italia, promuovendo in modo puntuale e rigoroso un punto di vista autenticamente liberale. L'IBL intende studiare, promuovere e diffondere gli ideali del mercato, della proprietà privata, e della libertà di scambio. Attraverso la pubblicazione di libri (sia di taglio accademico, sia divulgativi), l'organizzazione di convegni, la diffusione di articoli sulla stampa nazionale e internazionale, l'elaborazione di brevi studi e briefing papers, l'IBL mira ad orientare il processo decisionale, ad informare al meglio la pubblica opinione, a crescere una nuova generazione di intellettuali e studiosi sensibili alle ragioni della libertà.

Cosa Vogliamo

La nostra filosofia è conosciuta sotto molte etichette: "liberale", "liberista", "individualista", "libertaria". I nomi non contano. Ciò che importa è che a orientare la nostra azione è la fedeltà a quello che Lord Acton ha definito "il fine politico supremo": la libertà individuale. In un'epoca nella quale i nemici della libertà sembrano acquistare nuovo vigore, l'IBL vuole promuovere le ragioni della libertà attraverso studi e ricerche puntuali e rigorosi, ma al contempo scevri da ogni tecnicismo.

Istituto Bruno Leoni – Piazza Cavour 3 - 10123 Torino – Italy
T: +39 (011) 1978 1215 – F: +39 (011) 1978 1216 – www.brunoleoni.it – info@brunoleoni.it