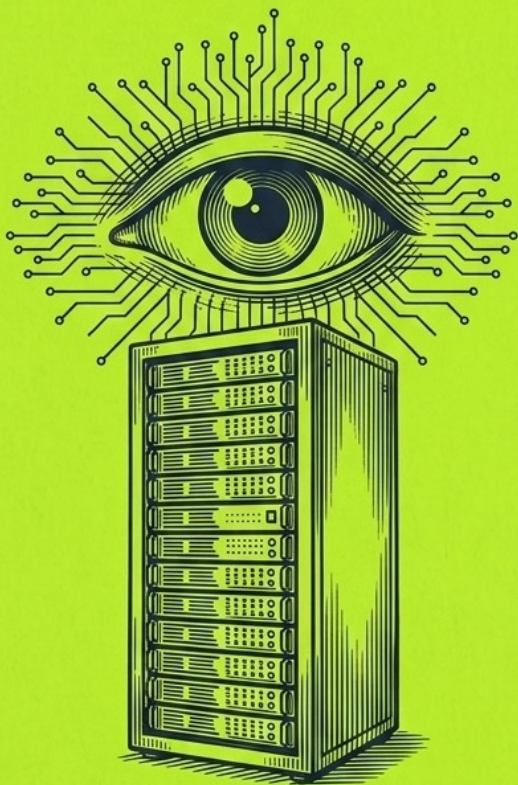


I dati che non sono più tuoi

Come le grandi piattaforme usano le tue informazioni, e perché l'Europa dipende da loro



C O N T R O P O T E R E

un libro di Alessio Farinella

I dati che non sono più tuoi

Come le grandi piattaforme usano le tue informazioni, e perché l'Europa dipende da loro

Alessio Farinella

Indice

Prefazione — Perché questo libro ti riguarda, anche se pensi di no	2
Capitolo 1 — Cosa sono davvero «i tuoi dati»	4
Capitolo 2 — Il modello di business della pubblicità mirata	7
Capitolo 3 — Come le piattaforme sono diventate così grandi	10
Capitolo 4 — Le tasse che (quasi) non pagano in Europa	13
Capitolo 5 — Il GDPR: cosa ha cambiato e cosa no .	16
Capitolo 6 — La dipendenza digitale dell'Europa . .	19
Capitolo 7 — Il Digital Markets Act e il Digital Services Act	22
Capitolo 8 — Le obiezioni, trattate con onestà	25
Capitolo 9 — Cosa si potrebbe fare	27
Capitolo 10 — Cosa puoi fare tu, adesso	30
Nota sulla trasparenza nell'uso dell'intelligenza artificiale	33

Prefazione — Perché questo libro ti riguarda, anche se pensi di no

Il prezzo di quello che sembra gratis

Quante app hai sul telefono che usi «gratis»? Cerchi su Google, guardi video, scorri i social, mandi messaggi — e per nessuna di queste cose tiri fuori il portafoglio. Sembra un affare incredibile: servizi potenti, disponibili ovunque, a costo zero.

Non è gratis. Paghi con qualcos'altro: i tuoi dati, la tua attenzione, il tempo che passi davanti allo schermo. E dietro quel «gratis» ci sono aziende tra le più grandi e redditizie della storia dell'umanità, che hanno costruito imperi economici globali su un modello che raramente viene spiegato con chiarezza a chi lo usa ogni giorno.

Non solo un problema di privacy

Questo libro non è solo un libro sulla privacy, anche se ne parleremo. È un libro su un tipo di potere diverso da quelli raccontati negli altri titoli di questa collana — non un governo, non una banca centrale, ma poche aziende private che controllano infrastrutture digitali da cui dipendono, ormai, interi paesi: la ricerca di informazioni, la comunicazione, il commercio, persino i sistemi operativi dei dispositivi che usiamo ogni giorno.

Un potere che sfugge alle regole tradizionali

Ti mostreremo, con fatti verificabili e sentenze definitive di tribunali europei, come queste aziende abbiano per anni pagato aliquote fiscali quasi nulle in Europa attraverso accordi con singoli paesi membri, e come solo di recente — dopo anni di battaglie legali — la giustizia europea abbia cominciato a imporre correzioni concrete. Vedremo anche i primi, timidi tentativi dell'Unione Europea di regolare il potere di queste aziende con nuove leggi, e quanto tempo ci vuole perché quelle leggi producano effetti reali.

Perché nessuno te lo spiega così

Il tema della tecnologia e dei dati personali viene spesso raccontato o in modo troppo tecnico, con termini che scoraggiano chi non lavora nel settore, o in modo troppo allarmistico, senza gli strumenti per distinguere i rischi reali dalle esagerazioni. Questo libro prova a stare nel mezzo: raccontare con parole semplici cosa succede davvero ai tuoi dati, chi ci guadagna, e quali strumenti reali — non teorici — hai per proteggerti.

Perché capire non è tempo perso

Come per gli altri temi di questa collana, il punto di partenza è lo stesso: capire un meccanismo è il primo passo per poterlo cambiare. Le prime sanzioni concrete contro le grandi piattaforme digitali, arrivate solo nel 2025, mostrano che le regole possono funzionare —

anche se lentamente, anche se in ritardo rispetto alla velocità con cui queste aziende sono cresciute.

Cosa troverai in questo libro

Nei capitoli che seguono ti spiegheremo, con parole semplici e dati verificabili, cosa sono davvero i tuoi dati, come funziona il modello di business della pubblicità mirata, come queste aziende sono diventate così grandi, quanto hanno pagato di tasse in Europa e con quali conseguenze legali, cosa dice davvero il GDPR, e quanto l'Europa dipenda oggi da infrastrutture digitali controllate da poche aziende straniere. L'ultimo capitolo ti dirà cosa puoi fare tu, da subito, per proteggere meglio i tuoi dati.

Buona lettura.

Capitolo 1 — Cosa sono davvero «i tuoi dati»

Più di un nome e un indirizzo

Quando senti parlare di «dati personali», probabilmente pensi a cose come il tuo nome, il tuo indirizzo, il tuo numero di telefono — informazioni che tu stesso decidi consapevolmente di condividere quando ti iscrivi a un servizio. È una parte vera, ma è solo la punta dell'iceberg.

Quello che non compili tu, ma osservano loro

Ogni volta che usi un telefono connesso a internet, generi continuamente informazioni che non hai mai scritto tu direttamente in nessun modulo: a che ora ti svegli e apri per la prima volta un'app, quanto tempo passi a guardare un video prima di scorrere al successivo, quali post ti fanno fermare il dito sullo schermo per qualche secondo in più, dove ti trovi fisicamente in ogni momento della giornata (se il GPS è attivo), quali altre app hai installato, chi sono i tuoi contatti più frequenti.

Nessuna di queste informazioni, singolarmente, sembra particolarmente sensibile. Ma messe insieme, nel tempo, costruiscono un profilo estremamente dettagliato di chi sei, cosa ti interessa, come ti comporti, e — questo è il punto centrale — cosa potresti essere convinto a comprare, votare, o credere.

Un esempio concreto

Immagina di cercare, una sera, informazioni su un problema di salute che ti preoccupa. Il giorno dopo, aprendo i social, cominci a vedere pubblicità di integratori, cliniche private, prodotti legati esattamente a quel problema. Non è una coincidenza: è il risultato di un sistema che ha collegato la tua ricerca a un profilo pubblicitario, e ha deciso che in quel momento eri

un bersaglio particolarmente ricettivo per quel tipo di prodotto.

Perché questo conta più di quanto sembri

Il punto centrale di questo libro non è che raccogliere dati sia, di per sé, un male assoluto — molti servizi utili che usiamo ogni giorno (mappe che suggeriscono il percorso più veloce, raccomandazioni di contenuti che ci interessano davvero) funzionano proprio grazie all'analisi di grandi quantità di dati. Il punto è che questo potere di conoscere in modo così dettagliato il comportamento di miliardi di persone è concentrato in mano a pochissime aziende private, con un controllo quasi nullo da parte di chi quei dati li genera ogni giorno, semplicemente vivendo la propria vita quotidiana con il telefono in tasca.

Il punto di questo capitolo

I tuoi dati non sono solo quello che scrivi consapevolmente in un modulo online: sono il sottoprodotto continuo, quasi invisibile, di ogni azione che compi con un dispositivo connesso. Capire questo è il primo passo per capire perché, nel prossimo capitolo, vedremo come un pugno di aziende sia riuscito a costruire imperi economici da centinaia di miliardi di dollari partendo da qualcosa che sembra così poco tangibile.

Capitolo 2 — Il modello di business della pubblicità mirata

Chi è davvero il cliente

C'è una frase, diventata quasi un luogo comune nel dibattito sulla tecnologia, che riassume bene il punto di questo capitolo: «se un servizio è gratis, il prodotto sei tu». Non è del tutto preciso, ma coglie qualcosa di vero: quando usi Google, Instagram, Facebook o TikTok senza pagare un abbonamento, il vero cliente che paga per far funzionare l'azienda non sei tu — sono gli inserzionisti, le aziende che vogliono mostrarti pubblicità mirata, e che pagano piattaforme come queste proprio per la loro capacità di conoscerti abbastanza bene da capire cosa potresti comprare.

Come funziona un'asta pubblicitaria in tempo reale

Quando apri un'app e ti appare una pubblicità, dietro c'è un meccanismo automatizzato molto più sofisticato di quanto sembri: nel giro di frazioni di secondo, diversi inserzionisti «fanno un'offerta» per mostrarti proprio quella pubblicità, basandosi sul tuo profilo — età, interessi, comportamento recente, luogo in cui ti trovi. Vince l'offerta più alta, e tu vedi quella specifica pubblicità, scelta per te tra migliaia di alternative possibili, in un processo che dura meno di quanto impieghi a battere le palpebre.

Perché questo modello è così redditizio

Più un'azienda conosce in dettaglio il comportamento di un utente, più può vendere agli inserzionisti la promessa di una pubblicità efficace — non uno spot generico visto da milioni di persone indistintamente, come nella pubblicità televisiva tradizionale, ma un messaggio calibrato su quella singola persona, nel momento in cui è più probabile che sia ricettiva. Questo spiega perché aziende come Google e Meta (proprietaria di Facebook e Instagram) abbiano un incentivo economico fortissimo a raccogliere quanti più dati possibile, il più dettagliati possibile, su ogni singolo utente: più dati, pubblicità più efficace, più soldi dagli inserzionisti.

Un modello che premia l'attenzione, non il tuo interesse

C'è un secondo elemento importante: queste piattaforme non guadagnano semplicemente mostrandoti pubblicità, guadagnano tenendoti sulla piattaforma il più a lungo possibile, perché più tempo passi a scorrere contenuti, più pubblicità puoi vedere. Questo crea un incentivo economico diretto a progettare le app in modo che sia il più difficile possibile smettere di usarle — notifiche calibrate per riportarti sull'app nel momento più efficace, contenuti selezionati da algoritmi che imparano esattamente cosa ti tiene incollato allo schermo, indipendentemente dal fatto che quel contenuto ti faccia bene o male.

Il paradosso del «gratis»

Il risultato di questo sistema è un paradosso interessante: aziende che offrono servizi apparentemente gratuiti sono, in realtà, tra le più redditizie della storia dell'economia mondiale — con ricavi pubblicitari misurati in centinaia di miliardi di dollari l'anno. Il «prezzo» che paghi non compare mai su una fattura, ma è reale: è il tuo tempo, la tua attenzione, e un livello di conoscenza dettagliata sulla tua vita che nessuna azienda del passato ha mai avuto su miliardi di persone contemporaneamente.

Il punto di questo capitolo

Il modello della pubblicità mirata non è, in sé, illegale o necessariamente dannoso: molte piccole aziende, che non potrebbero permettersi campagne pubblicitarie tradizionali costose, riescono a raggiungere clienti interessati proprio grazie a questi strumenti. Il problema, come vedremo nei prossimi capitoli, riguarda la scala e la concentrazione di questo potere in mano a pochissime aziende, e la scarsa trasparenza su come viene usato quello che sappiamo di ogni singolo utente.

Nel prossimo capitolo vedremo come queste aziende sono diventate così grandi, spesso acquisendo i concorrenti prima ancora che potessero diventare una minaccia reale.

Capitolo 3 — Come le piattaforme sono diventate così grandi

L'effetto rete: più utenti attirano più utenti

C'è un meccanismo economico che spiega buona parte del successo delle grandi piattaforme digitali, chiamato «effetto di rete»: il valore di un servizio aumenta all'aumentare del numero di persone che lo usano. Un social network con pochi utenti non serve a molto, perché non trovi le persone che vuoi contattare; un social network con miliardi di utenti diventa quasi indispensabile, perché è lì che si trovano tutti gli altri.

Questo effetto crea una spinta naturale verso la concentrazione: chi arriva per primo a una massa critica di utenti tende ad attrarne sempre di più, rendendo sempre più difficile per un concorrente più piccolo competere alla pari, anche offrendo un prodotto tecnicamente migliore.

La strategia delle acquisizioni preventive

Oltre alla crescita organica, un elemento chiave nella storia delle grandi piattaforme digitali è stata la strategia di acquisire aziende più piccole ma promettenti, spesso prima ancora che potessero diventare concorrenti reali. Il caso più citato è l'acquisizione di Instagram da parte di Facebook nel 2012, quando Instagram era ancora una piccola app con una manciata di dipen-

denti, o quella di WhatsApp nel 2014. In entrambi i casi, un'app che avrebbe potuto crescere come concorrente indipendente è stata invece assorbita dallo stesso gruppo che dominava già il mercato dei social network.

Perché le autorità antitrust non sono intervenute in tempo

Un tema importante da capire: al momento di queste acquisizioni, le autorità di controllo della concorrenza — sia negli Stati Uniti sia in Europa — le approvarono, perché secondo i criteri tradizionali antitrust dell'epoca, basati soprattutto su fatturato e quote di mercato al momento dell'operazione, quelle aziende sembravano troppo piccole per rappresentare un rischio concreto alla concorrenza. Solo con il senno di poi, quando quelle stesse aziende sono diventate giganti globali, si è capito che i criteri tradizionali antitrust non erano adatti a valutare il potenziale futuro di un'azienda tecnologica in rapida crescita — un errore di valutazione che ha contribuito in modo significativo alla concentrazione di potere che vediamo oggi.

Non solo acquisizioni: anche infrastrutture proprietarie

Un altro elemento di forza di queste aziende è il controllo di infrastrutture tecniche fondamentali: sistemi operativi per smartphone (Android di Google, iOS di Apple), negozi di app dove gli sviluppatori

devono passare per raggiungere gli utenti, servizi di cloud computing su cui si appoggiano migliaia di altre aziende. Controllare queste infrastrutture dà un potere ulteriore: chi le controlla può decidere le regole con cui tutti gli altri devono giocare — quali app sono ammesse, quali commissioni si pagano per vendere attraverso quei canali, quali dati possono essere condivisi con terzi.

Il punto di questo capitolo

La dimensione attuale delle grandi piattaforme digitali non è il risultato solo di prodotti migliori o di una crescita naturale del mercato: è anche il risultato di un effetto di rete che favorisce naturalmente la concentrazione, di una strategia sistematica di acquisizione dei concorrenti più promettenti prima che potessero crescere, e del controllo di infrastrutture tecniche da cui dipendono ormai migliaia di altre aziende. Le autorità di controllo, come vedremo meglio nel Capitolo 7, si stanno solo ora dotando di strumenti pensati specificamente per affrontare questo tipo di potere.

Nel prossimo capitolo vedremo un altro aspetto poco raccontato di questa storia: quanto — o meglio, quanto poco — queste aziende hanno pagato di tasse in Europa per anni.

Capitolo 4 — Le tasse che (quasi) non pagano in Europa

Un'aliquota fiscale dello 0,005%

Nel 2016 la Commissione Europea rese pubblico un dato che colpì l'opinione pubblica in tutta Europa: secondo la ricostruzione della Commissione, la controllata irlandese di Apple aveva pagato, in un anno preso a riferimento (il 2014), un'aliquota fiscale effettiva pari allo **0,005%** — praticamente nulla, su profitti enormi generati anche grazie alle vendite realizzate in tutti gli altri paesi europei, Italia inclusa.

Come funzionava il meccanismo

Il caso Apple-Irlanda, ricostruito dalla Commissione Europea, si basava su due accordi fiscali (chiamati «tax ruling») concessi dal governo irlandese ad Apple nel 1991 e nel 2007. Questi accordi permettevano a due società Apple, formalmente registrate in Irlanda ma non considerate fiscalmente residenti lì, di allocare la gran parte dei propri profitti a «sedi centrali» che esistevano solo sulla carta — senza dipendenti, senza attività reale — e che non erano tassabili né in Irlanda né in nessun altro paese.

In pratica: profitti generati vendendo prodotti e servizi in tutta Europa, incluso in Italia, finivano per essere spostati contabilmente verso un'entità che, dal punto di vista fiscale, non esisteva davvero da nessuna parte.

La decisione della Commissione

Nell'agosto 2016 la Commissione Europea stabilì che questo accordo costituiva un aiuto di Stato illegale da parte dell'Irlanda ad Apple — un vantaggio competitivo sleale rispetto alle altre aziende che pagavano le tasse normalmente — e ordinò all'Irlanda di recuperare da Apple fino a **13 miliardi di euro**. È interessante notare, come segnale di quanto fosse conveniente per l'Irlanda stessa questo tipo di accordo, che il governo irlandese si oppose alla decisione della Commissione insieme ad Apple, invece di accogliere con favore il recupero di 13 miliardi di euro nelle proprie casse pubbliche.

La sentenza definitiva, otto anni dopo

Nel settembre 2024, dopo anni di ricorsi legali, la Corte di Giustizia dell'Unione Europea — il massimo grado di giudizio, con sentenza definitiva e non più appellabile — ha confermato integralmente la decisione della Commissione: Apple deve pagare i 13 miliardi di euro. Nella stessa sentenza, la Corte ha confermato anche una multa distinta di 2,4 miliardi di euro contro Google, per abuso di posizione dominante nel mercato della ricerca online, dove per anni aveva favorito il proprio servizio di comparazione prezzi rispetto a quelli dei concorrenti in oltre una dozzina di paesi europei.

Perché ci sono voluti otto anni

Il tempo trascorso tra la decisione iniziale della Commissione (2016) e la sentenza definitiva (2024) mostra un problema strutturale importante: le grandi aziende tecnologiche, con risorse legali quasi illimitate, possono permettersi di prolungare per anni le battaglie legali contro le decisioni delle autorità europee, continuando nel frattempo a operare secondo le proprie pratiche fiscali — mentre aziende più piccole, senza le stesse risorse legali, difficilmente potrebbero permettersi strategie simili anche solo per contestare un accertamento fiscale molto più modesto.

Il punto di questo capitolo

Il caso Apple-Irlanda non è un episodio isolato, ma un esempio emblematico di come le grandi aziende tecnologiche abbiano potuto, per anni, sfruttare le differenze tra le legislazioni fiscali dei singoli paesi europei per pagare aliquote fiscali molto più basse di quelle pagate da aziende più piccole, radicate in un solo paese, senza la stessa capacità di spostare contabilmente i propri profitti. La sentenza del 2024 dimostra che la giustizia europea può intervenire — ma solo dopo anni di battaglie legali, e solo per i casi più eclatanti che arrivano fino in fondo al processo.

Nel prossimo capitolo vedremo cosa ha cambiato, e cosa no, il regolamento europeo sulla privacy — il GDPR.

Capitolo 5 — Il GDPR: cosa ha cambiato e cosa no

La legge sulla privacy più conosciuta al mondo

Se hai notato, dal 2018 in poi, che ogni sito web ti chiede il consenso ai cookie prima di poterlo visitare, hai già incontrato uno degli effetti più visibili del GDPR — il Regolamento Generale sulla Protezione dei Dati, entrato in vigore in tutta l'Unione Europea nel maggio 2018. È probabilmente la legge europea sulla tecnologia più conosciuta al mondo, citata come modello anche fuori dall'Europa.

I diritti che ti dà davvero

Il GDPR ha introdotto diritti concreti che prima non esistevano in modo così chiaro: il diritto di sapere quali dati un'azienda ha raccolto su di te, il diritto di chiederne la cancellazione (il cosiddetto «diritto all'oblio»), il diritto di ottenere una copia dei tuoi dati in un formato che puoi portare con te verso un altro servizio, e l'obbligo per le aziende di ottenere un consenso esplicito e informato prima di raccogliere ed elaborare i tuoi dati personali per scopi come la pubblicità mirata.

Le sanzioni possibili, sulla carta molto severe

Il GDPR prevede sanzioni potenzialmente enormi per le violazioni più gravi: fino al 4% del fatturato globale annuo di un'azienda, che per le grandi piattaforme digitali significa multe potenzialmente di miliardi di euro. Sulla carta, è uno degli strumenti di enforcement più severi al mondo in materia di protezione dei dati.

I limiti nella pratica

Nonostante questo impianto severo sulla carta, l'applicazione pratica del GDPR ha mostrato limiti significativi. Primo: la complessità delle indagini contro aziende multinazionali con strutture legali sofisticate rende i procedimenti lunghi, spesso anni, durante i quali l'azienda continua a operare secondo le pratiche contestate. Secondo: il sistema europeo prevede che sia l'autorità di protezione dati del paese dove un'azienda ha la propria sede europea a occuparsi dei casi che la riguardano in tutta l'Unione — un meccanismo che ha concentrato un numero enorme di casi importanti nell'autorità irlandese, dato che molte grandi piattaforme hanno scelto l'Irlanda come sede europea (anche per le ragioni fiscali viste nel capitolo precedente), sovraccaricando un'unica autorità nazionale relativamente piccola rispetto alla portata dei casi che deve gestire.

Il «cookie banner» che nessuno legge

Un effetto collaterale curioso e frustrante del GDPR è la proliferazione dei banner sui cookie che compaiono su ogni sito web. L'intenzione originaria — dare all'utente un controllo reale e consapevole sui propri dati — si è spesso trasformata, nella pratica, in un ostacolo fastidioso che la maggior parte delle persone clicca via senza leggere, semplicemente per accedere più velocemente al contenuto che cercava. È un esempio di come una buona intenzione normativa possa, nell'applicazione pratica quotidiana, perdere gran parte della propria efficacia reale.

Il punto di questo capitolo

Il GDPR rappresenta un passo avanti reale nel riconoscere formalmente diritti dei cittadini sui propri dati, con un impianto sanzionatorio potenzialmente molto severo. Ma la sua applicazione pratica mostra gli stessi limiti visti nel capitolo precedente per il caso fiscale: procedimenti lunghi, concentrazione dei casi più importanti in un'unica autorità nazionale, e un'esperienza quotidiana per l'utente — il banner dei cookie — che spesso produce l'effetto opposto a quello desiderato, l'assuefazione invece della consapevolezza.

Nel prossimo capitolo vedremo un problema più ampio: quanto l'intera Europa dipenda, per le proprie infrastrutture digitali quotidiane, da poche aziende straniere.

Capitolo 6 — La dipendenza digitale dell'Europa

Un test semplice

Prova a pensare a tutte le infrastrutture digitali che usi in una giornata normale: il sistema operativo del tuo telefono, il motore di ricerca con cui trovi informazioni, il servizio email che usi per lavoro, forse anche il cloud dove sono salvate le foto o i documenti della tua azienda. Ora prova a contare quante di queste infrastrutture sono controllate da aziende europee.

Per la maggior parte delle persone, la risposta è: quasi nessuna. Android e iOS, i due sistemi operativi che insieme coprono la quasi totalità degli smartphone al mondo, sono americani (Google e Apple). I principali servizi di cloud computing su cui si appoggiano aziende, pubbliche amministrazioni e persino ospedali in tutta Europa sono gestiti da tre aziende americane: Amazon (AWS), Microsoft (Azure) e Google (Google Cloud).

Cosa significa «dipendenza digitale» in pratica

Non significa solo che usiamo prodotti stranieri — succede in molti altri settori economici, senza che sia necessariamente un problema. Significa qualcosa di più specifico: che gran parte dell'infrastruttura su cui si basa il funzionamento quotidiano di aziende,

ospedali, scuole, uffici pubblici europei dipende da decisioni prese da poche aziende private con sede legale fuori dall'Unione Europea, soggette prima di tutto alla legislazione del proprio paese d'origine.

Questo ha conseguenze concrete: se un governo straniero impone restrizioni su un'azienda tecnologica, o se quell'azienda decide unilateralmente di cambiare le condizioni di un servizio, milioni di utenti e migliaia di aziende europee possono trovarsi coinvolti in decisioni su cui non hanno alcun potere di intervento diretto.

Il caso dei dati sanitari e pubblici

Un esempio concreto e delicato: in diversi paesi europei, Italia inclusa, sistemi sanitari pubblici e pubbliche amministrazioni hanno scelto, per ragioni di costo ed efficienza, di affidare la gestione dei propri dati — inclusi dati sanitari sensibili di milioni di cittadini — a servizi cloud di aziende americane. Questo ha sollevato interrogativi legali e politici complessi su chi abbia davvero accesso a quei dati, e sotto quale giurisdizione, specialmente dopo leggi americane che, in alcuni casi, permettono alle autorità statunitensi di richiedere accesso a dati conservati da aziende americane, anche se fisicamente immagazzinati su server situati in Europa.

Perché l'Europa non ha un proprio «gigante tecnologico»

Diverse ragioni concorrono a spiegare perché l'Europa non abbia sviluppato aziende tecnologiche di dimensioni paragonabili a quelle americane o cinesi: un mercato più frammentato in tanti paesi con lingue e regole diverse, invece di un unico grande mercato interno omogeneo come quello statunitense; minore disponibilità di capitali di rischio (venture capital) per finanziare startup tecnologiche nelle fasi iniziali, rispetto agli Stati Uniti; e, secondo alcune analisi, un approccio regolatorio più orientato a limitare i rischi che a incentivare la crescita di nuovi attori europei.

Il punto di questo capitolo

La dipendenza digitale dell'Europa non è solo un tema astratto di sovranità tecnologica: ha conseguenze concrete su chi controlla i dati di milioni di cittadini e migliaia di aziende, su chi decide le regole con cui queste infrastrutture funzionano, e sulla capacità dell'Europa di far rispettare le proprie leggi ad aziende che, in ultima istanza, rispondono prima di tutto alla legislazione di un altro continente.

Nel prossimo capitolo vedremo i primi, recenti tentativi europei di regolare questo squilibrio di potere: il Digital Markets Act e il Digital Services Act.

Capitolo 7 — Il Digital Markets Act e il Digital Services Act

Due nuove leggi, un obiettivo comune

Nell'ottobre 2022 l'Unione Europea ha approvato due regolamenti pensati specificamente per affrontare il tipo di potere descritto nei capitoli precedenti: il Digital Markets Act (DMA), che regola il comportamento delle grandi piattaforme nei confronti di concorrenti e sviluppatori, e il Digital Services Act (DSA), che regola invece i contenuti online, la moderazione, e la trasparenza degli algoritmi che decidono cosa vediamo sui social.

I «gatekeeper»

Il DMA introduce un concetto nuovo nella legislazione europea: quello di «gatekeeper» — letteralmente, «guardiano del cancello» — cioè un'azienda che controlla un punto di accesso fondamentale tra le imprese e i consumatori, tanto grande e potente da poter imporre le proprie regole a tutto un settore. Nel 2023 sono state designate sei aziende come gatekeeper: Alphabet (Google), Amazon, Apple, ByteDance (proprietaria di TikTok), Meta e Microsoft. Solo queste aziende, in base a criteri oggettivi di dimensione e diffusione, sono soggette agli obblighi più stringenti del regolamento.

Cosa vieta concretamente il DMA

Tra le regole principali: i gatekeeper non possono più impedire agli sviluppatori di app di indirizzare gli utenti verso metodi di pagamento o canali di distribuzione alternativi ai propri negozi digitali; non possono favorire i propri servizi rispetto a quelli dei concorrenti nei propri risultati di ricerca o piattaforme; devono garantire una maggiore interoperabilità tra servizi di messaggistica diversi; e devono ottenere un consenso più chiaro ed esplicito prima di combinare dati personali raccolti da servizi diversi dello stesso gruppo.

Le prime sanzioni reali, arrivate nel 2025

Per anni dopo l'approvazione del 2022, il DMA è rimasto soprattutto sulla carta, in una fase di prima applicazione. Le prime sanzioni concrete sono arrivate solo nell'aprile 2025: **Apple multata per 500 milioni di euro** per aver continuato a impedire agli sviluppatori di indirizzare gli utenti verso canali di distribuzione alternativi all'App Store, con un ordine di rimuovere queste restrizioni tecniche e commerciali. Nello stesso mese, **Meta multata per 200 milioni di euro** per non aver offerto agli utenti una scelta reale tra un servizio che usa meno dati personali e uno che ne usa di più per la pubblicità mirata.

Apple ha annunciato ricorso contro la propria sanzione — un percorso legale che, come visto nel Capitolo 4 per il caso fiscale, può richiedere anni prima di arrivare a una sentenza definitiva.

Perché ci sono voluti tre anni

Il tempo trascorso tra l'approvazione del regolamento (2022) e le prime sanzioni concrete (2025) mostra un pattern che questo libro ha già raccontato più volte: anche le regole europee più innovative e ambiziose richiedono tempo per essere applicate concretamente, tra fasi di designazione dei soggetti coinvolti, periodi di adeguamento concessi alle aziende, indagini approfondite, e la possibilità concreta di ricorsi legali che allungano ulteriormente i tempi.

Il punto di questo capitolo

Il DMA e il DSA rappresentano il tentativo più ambizioso fatto finora dall'Unione Europea per regolare il potere delle grandi piattaforme digitali, con strumenti specificamente pensati per il tipo di concentrazione di potere raccontato in questo libro. Le prime sanzioni del 2025 dimostrano che questi strumenti possono funzionare nella pratica, non solo sulla carta — ma anche che il tempo tra l'approvazione di una regola e la sua applicazione concreta resta lungo, durante il quale le aziende coinvolte continuano a operare secondo le pratiche contestate.

Nel prossimo capitolo affrontiamo, con la massima onestà possibile, gli argomenti seri di chi difende, almeno in parte, il modello attuale delle grandi piattaforme digitali.

Capitolo 8 — Le obiezioni, trattate con onestà

Perché questo capitolo conta

Fin qui abbiamo raccontato i lati problematici del potere delle grandi piattaforme digitali. Ma un libro onesto deve affrontare anche gli argomenti seri di chi difende, almeno in parte, il modello attuale.

Prima obiezione: il valore reale dei servizi gratuiti

È l'argomento più immediato e, in una certa misura, vero: servizi come la ricerca online, le mappe, la posta elettronica, i social network hanno un valore reale enorme per miliardi di persone, che non avrebbero mai potuto permettersi di pagare direttamente per servizi di questa qualità e portata. Il modello pubblicitario descritto nel Capitolo 2, per quanto abbia problemi reali, ha permesso di rendere accessibili gratuitamente strumenti che altrimenti sarebbero rimasti riservati a chi poteva permetterseli.

Seconda obiezione: il rischio di regole che soffocano l'innovazione

C'è un argomento economico serio anche a favore di una regolamentazione più leggera: regole troppo rigide, pensate per le grandi piattaforme di oggi, rischiano di scoraggiare la nascita di nuove aziende innovative, che potrebbero trovarsi soggette agli stessi vincoli

burocratici pensati per giganti da centinaia di miliardi di dollari, senza averne le risorse. Il rischio, secondo questa lettura, è che l'eccesso di regolamentazione finisca per proteggere paradossalmente le aziende già dominanti, più capaci di sostenere i costi di conformità normativa, a scapito di potenziali nuovi concorrenti più piccoli.

Terza obiezione: la complessità tecnica reale

Regolare tecnologie complesse — algoritmi di raccomandazione, sistemi pubblicitari automatizzati, infrastrutture cloud globali — richiede competenze tecniche molto specialistiche, che le istituzioni pubbliche non sempre hanno a disposizione nella stessa misura delle aziende private che devono regolare. Questo squilibrio di competenze tecniche rende, secondo questa obiezione, particolarmente difficile scrivere regole efficaci che non abbiano effetti collaterali indesiderati — come il caso del banner dei cookie, raccontato nel Capitolo 5, mostra concretamente.

Una risposta onesta a queste obiezioni

Questi argomenti contengono elementi reali che questo libro non vuole ignorare. Ma non cambiano il quadro di fondo raccontato nei capitoli precedenti: il fatto che questi servizi abbiano un valore reale non giustifica pratiche fiscali che hanno permesso per anni di pagare aliquote fiscali quasi nulle, come visto nel

Capitolo 4, né l'assenza di una vera concorrenza per anni, come visto nel Capitolo 3. Il rischio di soffocare l'innovazione con regole troppo rigide è reale, ma il DMA, raccontato nel Capitolo 7, è stato costruito proprio per colpire solo le aziende più grandi (i «gatekeeper»), lasciando le regole più leggere per le aziende più piccole — un tentativo concreto di bilanciare questi due rischi.

La domanda giusta, quindi, non è «regolare le grandi piattaforme sì o no», ma «come regolarle in modo mirato, che protegga davvero i cittadini e la concorrenza senza soffocare l'innovazione delle aziende più piccole». È quello che vedremo nel prossimo capitolo.

Capitolo 9 — Cosa si potrebbe fare

Applicare più rapidamente le regole già esistenti

La proposta più immediata non richiede nuove leggi: applicare più rapidamente quelle già esistenti. Come visto nei capitoli precedenti, il caso fiscale Apple ha richiesto otto anni per arrivare a una sentenza definitiva, e le prime sanzioni del DMA sono arrivate tre anni dopo l'approvazione del regolamento. Rafforzare le risorse e il personale delle autorità europee incaricate di questi controlli — antitrust, protezione dati, fisco — ridurrebbe questi tempi, con un effetto deterrente molto più forte su comportamenti scorretti.

Una tassazione digitale efficace a livello europeo

Diversi paesi europei, Italia inclusa, hanno introdotto negli anni tasse nazionali specifiche sui servizi digitali, proprio per intercettare almeno una parte dei profitti generati sul proprio territorio dalle grandi piattaforme, aggirando parzialmente i meccanismi di spostamento contabile dei profitti visti nel Capitolo 4. Una tassazione digitale coordinata a livello europeo, invece che paese per paese, eviterebbe che le aziende possano continuare a scegliere il paese con le condizioni fiscali più favorevoli tra i ventisette Stati membri.

Infrastrutture pubbliche o europee alternative

Per ridurre la dipendenza digitale raccontata nel Capitolo 6, diversi paesi europei stanno investendo in alternative — cloud pubblici o europei per i dati più sensibili (sanitari, di sicurezza nazionale, della pubblica amministrazione), motori di ricerca e sistemi operativi sviluppati con capitali europei. Sono progetti ancora piccoli rispetto ai giganti americani, ma rappresentano un tentativo concreto di ridurre, almeno per i settori più critici, la dipendenza da infrastrutture controllate fuori dall'Unione Europea.

Regole più semplici sull'interoperabilità

Invece di banner sui cookie che nessuno legge, come visto nel Capitolo 5, si potrebbero imporre standard

tecnici che permettano agli utenti di gestire le proprie preferenze sulla privacy una sola volta, a livello di sistema operativo o browser, invece che sito per sito — una soluzione tecnicamente più semplice e realmente più efficace per garantire un controllo consapevole, senza il fastidio quotidiano dei banner ripetuti.

Alfabetizzazione digitale diffusa

Un'ultima proposta, meno tecnica ma altrettanto importante: investire in programmi di educazione digitale nelle scuole e per gli adulti, che spieghino con parole semplici — come cerca di fare questo stesso libro — come funzionano davvero questi meccanismi. Una popolazione che capisce come funziona il modello della pubblicità mirata, chi controlla le infrastrutture che usa ogni giorno, e quali diritti ha sui propri dati, è una popolazione più difficile da sfruttare, e più capace di fare pressione politica informata su questi temi.

Il punto di questo capitolo

Nessuna di queste proposte, da sola, risolverebbe completamente lo squilibrio di potere raccontato in questo libro. Ma insieme rappresentano un cambio di approccio possibile: applicare con più forza le regole già esistenti, coordinare la tassazione a livello europeo, investire in alternative infrastrutturali, semplificare gli strumenti di controllo per gli utenti, e diffondere la conoscenza di questi meccanismi tra i cittadini.

Nell'ultimo capitolo vediamo cosa puoi fare tu, da subito, per proteggere meglio i tuoi dati.

Capitolo 10 — Cosa puoi fare tu, adesso

Piccole azioni, effetto reale

Se sei arrivato fin qui, ora sai come funziona davvero il modello economico dietro i servizi digitali che usi ogni giorno. Questo non ti dà, da solo, il potere di cambiare le regole fiscali europee o di smontare l'effetto di rete raccontato nel Capitolo 3. Ma ci sono azioni concrete, alla tua portata, che possono fare una differenza reale, sia per te sia collettivamente.

Impostazioni concrete da controllare oggi stesso

Sul tuo telefono, sia Android sia iPhone, esistono impostazioni sulla privacy che puoi controllare in pochi minuti: la possibilità di limitare il tracciamento pubblicitario tra app diverse (su iPhone si trova in Impostazioni > Privacy > Tracciamento; su Android in Impostazioni > Google > Annunci), la possibilità di rivedere e revocare i permessi concessi a ogni singola app (accesso a posizione, microfono, contatti — spesso concessi mesi o anni fa e mai più rivisti), e la possibilità di scaricare una copia di tutti i dati che un servizio ha raccolto su di te, un diritto garantito dal GDPR.

Come leggere un banner sui cookie in due minuti

Invece di cliccare automaticamente «accetta tutto» per liberarti velocemente del banner, cerca l'opzione — quasi sempre presente, anche se meno visibile — per personalizzare le preferenze, e disattiva quello che non ti serve davvero (in particolare la condivisione dei dati con «partner pubblicitari terzi», spesso la voce che comporta la raccolta più estesa e meno controllabile).

Diversificare, quando possibile

Non è sempre pratico o realistico abbandonare del tutto i servizi delle grandi piattaforme, che spesso restano i più diffusi tra amici, familiari, colleghi. Ma per singoli usi specifici — un motore di ricerca alternativo che non costruisce un profilo pubblicitario dettagliato, un'app di messaggistica con crittografia end-to-end più solida — provare alternative europee o comunque più attente alla privacy è un modo concreto per non dipendere completamente da un'unica azienda per ogni aspetto della propria vita digitale.

Segnalare abusi

Se sospetti che un'azienda stia violando i tuoi diritti sui dati personali — per esempio negandoti l'accesso ai tuoi dati o rifiutando una richiesta di cancellazione senza motivo valido — puoi presentare un reclamo gratuito al Garante per la Protezione dei Dati Persona-

li in Italia, l'autorità nazionale competente sul GDPR raccontato nel Capitolo 5.

Parlarne, senza sentirti impotente

Il tema della privacy digitale viene spesso vissuto con un misto di rassegnazione («tanto sanno già tutto di me») e distanza («è troppo tecnico per me»). Come per gli altri temi di questa collana, capire il meccanismo economico dietro queste dinamiche è il primo passo per smettere di vivere questo tema come inevitabile, e cominciare a fare scelte più consapevoli — sia individuali sia, insieme ad altri, collettive.

Condividere questo libro

Come tutti i libri della collana Contropotere, anche questo è pensato per essere condiviso liberamente e gratuitamente. Se conosci qualcuno interessato a capire meglio cosa succede davvero ai propri dati, condividi questo libro con loro.

Per finire

Il potere delle grandi piattaforme digitali non cambierà per un singolo gesto individuale. Ma la consapevolezza diffusa, come per gli altri temi di questa collana, resta la preconditione di ogni cambiamento politico reale.

Grazie per aver letto fino in fondo. Buona diffusione.

Nota sulla trasparenza nell'uso dell'intelligenza artificiale

Questo libro è stato scritto con il supporto di strumenti di intelligenza artificiale, usati per la ricerca preliminare delle fonti, la prima stesura dei testi a partire da una scaletta e da indicazioni editoriali definite dall'autore, e la revisione linguistica e strutturale.

Restano interamente umane: la scelta del tema e la tesi del libro, la verifica di ogni fatto, cifra e citazione contro una fonte primaria o istituzionale prima della pubblicazione, la decisione editoriale finale su cosa viene pubblicato o corretto, e la responsabilità editoriale dei contenuti — che resta in capo all'autore, mai allo strumento di intelligenza artificiale utilizzato.

Questa nota risponde agli obblighi di trasparenza previsti dall'art. 50 del Regolamento (UE) 2024/1689 (AI Act), applicabile dal 2 agosto 2026.

Se trovi un errore, una fonte imprecisa o un'affermazione che ritieni non verificata correttamente, scrivi a redazione@contropotere.com — ogni segnalazione fondata porta a una correzione pubblica del testo. Questo libro fa parte della collana **Contropotere**: gli altri titoli sono disponibili gratuitamente su **contropotere.com**.