RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0270 • articolo sottoposto a peer review • pubblicato in anteprima il 2 apr. 2026

Arianna Fiorenza

I poteri privati digitali nell'era dell'IA: profili di concorrenza, protezione dei dati e tutela dei consumatori

Il contributo si concentra sull'intersezione tra diritto dei consumatori, protezione dei dati personali e diritto della concorrenza, promuovendo una lettura integrata e complementare di tali normative al fine di fronteggiare efficacemente i rischi connessi all'utilizzo dei sistemi di intelligenza artificiale e allo sfruttamento dei dati personali nella *data-driven economy*. Il rapido sviluppo tecnologico ha favorito, infatti, l'emersione di nuovi poteri privati, suscettibili di incidere profondamente non solo sulle dinamiche di mercato, ma anche sui diritti degli utenti. Particolare attenzione è dedicata alle nuove forme di pratiche commerciali scorrette che, attraverso meccanismi di consenso opachi e tecniche aggressive di profilazione sono suscettibili di comprimere la libertà di autodeterminazione del consumatore digitale, manipolando le sue scelte. L'analisi si sofferma, infine, sulle implicazioni concorrenziali, evidenziando come l'accesso privilegiato ai dati e alle tecnologie computazionali necessarie per elaborarli possa rafforzare le barriere all'ingresso e favorire condotte abusive non solo nel mercato digitale, ma anche nei mercati ad esso connessi, quale quello dell'intelligenza artificiale.

Intelligenza artificiale – Economia digitale – Pratiche commerciali scorrette – Libertà di autodeterminazione Concorrenza

The digital private powers in the AI era: Competition, data protection and consumer law perspectives

The article focuses on the intersection between consumer law, data protection law and competition law, highlighting the need for an integrated and complementary interpretation of these regulatory frameworks in order to effectively address the risks associated with the use of artificial intelligence systems and the exploitation of personal data in the data-driven economy. Rapid technological development has, in fact, given rise to new forms of private power capable of profoundly affecting not only market dynamics but also consumers' rights. Particular attention is devoted to new forms of unfair commercial practices which, through opaque consent mechanisms and aggressive profiling techniques, may undermine the freedom of self-determination of the digital consumer by manipulating their choices. The analysis finally addresses the competition-law implications, highlighting how privileged access to data and to the computational technologies required to process them may strengthen barriers to entry and facilitate abusive conduct not only in digital markets, but also in related ones, including the AI market.

Artificial intelligence – Digital economy – Unfair commercial practices – Right to self-determination Competition

L'Autrice è dottoranda di ricerca in discipline giuridiche privatistiche presso l'Università Roma Tre

1. IA, *Big Data* e dominio tecnologico

L'intelligenza artificiale[1] si trova oggi al centro di una profonda rivoluzione tecnologica che sta ridefinendo molteplici aspetti della nostra società, contribuendo a ridelinearne regole ed equilibri. Lo sviluppo dei sistemi di IA sta riguardando diversi settori tra i quali la medicina, il lavoro, le neuroscienze, l'economia e, persino, il diritto e la giustizia[2]. I vantaggi dell'automazione dei processi decisionali[3], l'incredibile aumento della potenza di calcolo, la crescita esponenziale delle quantità di dati disponibili – resa possibile grazie all'espansione della rete Internet - sono tra le principali ragioni della rapida diffusione dei sistemi di IA.

In particolare, l'efficace funzionamento dell'IA non può prescindere dalla disponibilità di enormi volumi di dati, i quali ne costituiscono la linfa vitale. Com'è noto, essi sono essenziali, sia in fase di addestramento degli algoritmi che nella successiva fase di concreta operatività del sistema ai fini della produzione degli output.

Negli ultimi decenni, grazie all'avanzamento dell'ICT, si è assistito ad un profondo processo di datificazione[4] della realtà, che ha portato a considerare i dati una risorsa imprescindibile per la conduzione delle più svariate attività, di interesse pubblico e privato. In tale contesto è nato il concetto di Big Data[5], definiti quale carburante[6] dell'intelligenza artificiale. Tra essi rientrano, certamente,

1. Com'è noto, la locuzione "intelligenza artificiale" comparve per la prima volta nella c.d. "proposta di Dartmouth" scritta da John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon ai fini della famosa conferenza di Dartmouth tenutasi nel 1956, evento che segna convenzionalmente l'inizio degli studi in materia di IA. L'espressione, nel tempo, è stata definita in vari modi. Un gruppo di ricercatori dell'Università di Stanford descrive l'IA come "una scienza e un insieme di tecniche computazionali che vengono ispirate – pur operando tipicamente in maniera diversa – dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire". Cfr. Stone–Calo–Brooks et al. 2016, p. 5. Una più recente definizione è contenuta nel Reg. 2024/1689 secondo cui per sistema di IA si intende: "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".
2. Battelli 2024, p. 295 ss.
3. I sistemi automatizzati sollevano gli esseri umani dal compimento di molteplici attività più o meno complesse come il ragionare, riflettere, decidere.
4. Per datificazione si intende la trasformazione delle interazioni sociali in dati digitali suscettibili di acquisire valore anche economico. Tra i principali studiosi del fenomeno si ricordano: Mayer-Schönberger–Cukier 2013.
5. "Big Data usually refer to (1) the large dimension of datasets; and (2) the need to use large scale computing power and non-standard software and methods to extract value from the data in a reasonable amount of time", OECD 2016. Sul punto, v. anche De Mauro–Greco–Grimaldi 2016.
6. Peluso 2023.

anche i dati personali. Pur non essendoci univocità su cosa debba intendersi per Big Data, le loro caratteristiche sono tradizionalmente sintetizzate nelle "5 V": volume, velocità, varietà, veridicità e valore[7].

Più nello specifico, il *volume* fa riferimento all'enorme dimensione di dati raccolti, la *varietà* alla tipologia di dati disponibili, la *velocità* riguarda la capacità delle tecnologie di generare tali dati in modo continuativo. La *veridicità*, invece, si riferisce alla qualità dei dati raccolti, i quali se errati o incompleti possono causare errori nelle risposte degli algoritmi che si basano su di essi per fare previsioni.

Il *valore*, infine, identifica la capacità dei dati di produrre valore nel momento in cui sono analizzati ed elaborati dai soggetti che li raccolgono. In particolare, sono le tecniche di intelligenza artificiale – e, più precisamente, gli algoritmi di machine learning – che consentono di estrarre valore dai Big Data. Come spiegato in alcuni recenti studi[8], dopo una preliminare fase di raccolta, interviene la vera e propria analisi dei dati la quale consente di far emergere dai dati grezzi non strutturati informazioni suscettibili di interpretazione e utilizzo pratico.

Per tale ragione riveste un ruolo centrale nell'intera "filiera dei Big Data" la fase della elaborazione, che comporta l'organizzazione dei dati grezzi non strutturati in informazioni suscettibili di essere utilizzate, ad esempio, per finalità economiche.

Ed è proprio il crescente valore acquisito – ed estratto – da tali dati che ha comportato l'emersione e l'espandersi del mercato digitale, governato da pochi attori la cui posizione dominante, però, rischia di ostacolarne una leale concorrenza[9]. Come si chiarirà in seguito, tali soggetti privati – le c.d. *Bigh Tech* – sono detentori di grandi quantità di dati posti alla base dei nuovi modelli di business delle piattaforme digitali e utilizzati prevalentemente per offrire servizi personalizzati e pubblicità mirata agli utenti, oggetto, quest'ultimi, di un'intensa e costante attività di profilazione.

Dunque, Il valore economico del dato deriva non dalla mera fornitura da parte dell'interessato, bensì dal successivo trattamento di aggregazione ed analisi[10], che si rivela essere particolarmente efficiente laddove condotto con algoritmi di autoapprendimento[11]. Ne consegue che sussiste un legame di corrispondenza biunivoca tra intelligenza artificiale e Big Data. Sebbene questi ultimi siano indispensabili per il training e il funzionamento dell'IA, allo stesso tempo la tecnologia si rivela essere uno strumento cruciale per estrarre ed attribuire, in fase di analisi, una funzione nonché un valore – anche economico – a tali dati.

Si osserva, sul punto, che lo sviluppo di nuove tecnologie per la raccolta, l'analisi e il trattamento delle informazioni sta conducendo al consolidamento della c.d. *data-driven economy*, un sistema economico basato sullo sfruttamento e la commercializzazione dei dati attraverso tecnologie automatizzate. Queste ultime consentono di creare accuratamente categorie e profili degli interessati da reimpiegare, ad esempio, nel settore della pubblicità online. Il risultato è "an economy based not on the creation of value through

7. Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la Protezione dei Dati Personali 2020, p. 8.
8. *Ivi*, p. 15.
9. Peluso 2023, p. 41.
10. D'Ippolito 2022, p. 58.
11. Inoltre, è possibile osservare che gli algoritmi di *machine learning* consentono di estrarre nuova conoscenza da questi dati. Com'è noto il sistema di IA, in quanto sistema di apprendimento autonomo, utilizza l'inferenza per acquisire informazioni non limitate al dateset iniziale. L'inferenza è quel processo che consente alla macchina di fare previsioni o prendere decisioni su dati nuovi, acquisiti sulla base dei dati noti e dei modelli di addestramento. Per questo il sistema può essere definito intelligente, in quanto raccogliendo e confrontando enormi quantità di dati e sulla base dei modelli da questi estrapolati, riesce a determinare come comportarsi in presenza di input nuovi, che vanno, cioè, al di là dei dati inizialmente somministrati dal programmatore o, meglio, dall'*addestratore*, nella fase dictraining. Per questo può dirsi che un sistema intelligente è anche un sistema "creativo", più vicino al modo di ragionare della mente umana.

production, but on values created through the flowing of information"[12].

Dunque, dati e informazioni hanno cominciato ad essere raccolti a livello globale da soggetti privati per finalità commerciali. Questo perché nell'era della datificazione, ogni istante dell'agire è, grazie alle tecnologie digitali, registrato, immagazzinato ed analizzato[13]. Si delinea, dunque, un modello di mercato in cui lo sviluppo tecnologico e i dati sono il principale oggetto di interesse delle imprese e del loro modello di business. Il legame indissolubile tra dati e IA sta ridefinendo gli equilibri economici globali, dando vita a un vero e proprio "capitalismo digitale"[14], in cui l'informazione diventa una risorsa strategica paragonabile alle materie prime del passato. In questo contesto, chi è in grado di avvalersi delle nuove tecnologie, chi detiene le maggiori quantità di dati riveste la qualità di *gatekeeper* del mercato, sviluppando un potere privato per certi versi non dissimile dal potere pubblico. Si assiste, dunque, all'emergere di nuovi poteri privati digitali con cui la dottrina identifica quei soggetti che, seppur in assenza di una qualche legittimazione democratica, rivestono una particolare forza socio-economica che permette loro di incidere unilateralmente sulle sfere giuridiche degli individui con cui entrano in contatto[15]. Essi, dunque, danno vita a nuove forme di sovranità. In particolare, gli elementi tradizionalmente posti alla base dell'autorità degli Stati sovrani – come il controllo del territorio, delle risorse e dell'informazione – sono stati significativamente ridisegnati dall'ascesa di nuovi soggetti che, esercitando un controllo sulle tecnologie su cui transitano i dati, hanno progressivamente acquisito una posizione di dominanza non solo nel mercato, ma nell'intera società[16].

Dunque, il processo di datificazione a cui si è accompagnato l'avvento e il controllo delle nuove tecnologie ha portato a ridefinire il concetto di sovranità, oggi intesa sostanzialmente quale sovranità tecnica. Infatti, a cambiare non è solo la natura del soggetto detentore del potere, ma in tale scenario un rilievo centrale è assunto dal mezzo con cui tale potere viene esercitato[17]. Tale mezzo consiste proprio nelle capacità di calcolo e di automazione delle moderne tecnologie e nel controllo dei dati – anche personali – che le alimentano. Ad ogni modo, questi nuovi centri di potere, se lasciati proliferare in assenza di regolazione, rischiano di compromettere i tradizionali valori su cui si basano le democrazie occidentali, tra i quali la libera concorrenza e la tutela dei diritti fondamentali. Sebbene, infatti, le nuove tecnologie possano contribuire alla realizzazione e all'ampliamento delle libertà fondamentali della persona, dall'altro lato possono limitarle. Questo è particolarmente importante in un tempo nel quale la tecnologia concorre alla definizione di criteri valoriali e orienta sempre più le decisioni private e pubbliche[18].

12. De Gregorio 2022, p. 80. Inoltre, in dottrina si osserva che l'incidenza di fattori tecnologici ha condotto alla diffusione della concezione del dato come *commodity*, ovvero una risorsa dalla quale è possibile trarre valore economico tanto da utilizzare il termine *consumerizzazione* della privacy. Cfr.: Alagna–Centofanti 2021, p. 127. Sul punto si tornerà successivamente.
13. Di Porto 2016.
14. Cfr. Staab 2024.
15. Cremona 2021, p. 881.
16. Il potere delle Big Tech, prive di una qualsivoglia legittimazione democratica, è in grado di influenzare la vita dei consociati in misura pari se non superiore a quella di una autorità pubblica democraticamente eletta. Sul punto, si veda Torregiani 2023, p. 132. Inoltre, alcuni autori ravvisano tra le ragioni che hanno permesso l'emergere e il consolidarsi di questi nuovi poteri il "liberalismo" degli ordinamenti democratici occidentali. De Gregorio 2022 p. 80: "New actors operating in the digital environment such as online platforms enjoy new areas of power deriving not just from a mix of business opportunities and technologies, but also from the openness of democracies oriented to digital liberalism which has left these actors accumulating powers".
17. Nell'era digitale, dunque, la sovranità deve essere intesa necessariamente in forme nuove, che non possono prescindere dal mezzo tecnico. Si rimanda a: Torregiani 2023, p. 132.
18. Come chiarito nel 2019 da Antonello Soro, allora Garante per la protezione dei dati personali nel suo intervento in occasione della giornata europea per la protezione dei dati. Egli osserva, inoltre, che le innovazioni connesse

Da questa consapevolezza sembrano muovere i recenti atti normativi dell'Unione europea, che disegnano un quadro regolatorio volto a normare lo sviluppo e l'applicazione dell'IA, nonché la gestione e la circolazione dei suoi input essenziali, i dati. In particolare, si ricordano i regolamenti in materia di *data law*[19], il Digital Markets Act[20] e il Digital Services Act[21], nonché l'AI Act[22].

Questo rapido avanzamento tecnologico impone, infatti, al diritto di adattarsi e di elaborare nuovi strumenti normativi in grado di governare rischi, opportunità e implicazioni etiche di sistemi sempre più intelligenti e pervasivi.

2. Sfruttamento dei dati personali e AI: il complementare ruolo del *data protection law* e del diritto dei consumatori

Come accennato, la raccolta e lo sfruttamento dei Big Data tramite le nuove tecnologie rappresentano il cuore della data driven economy e delle moderne attività di impresa.

Tra questi dati, rientrano anche dati personali, definiti da autorevole dottrina come il *lifeblood* per le imprese digitali[23]. Negli ultimi anni, infatti, le grandi piattaforme digitali – divenuta la sede principale per lo scambio di beni e servizi – hanno costruito modelli di business fondati sulla raccolta e l'analisi dei dati, che vengono trattati tramite sofisticati algoritmi al fine di trarne informazioni suscettibili di rilievo economico[24]. Più nello specifico, l'attività di queste imprese si basa principalmente sull'analisi continua dei comportamenti degli utenti online. Le piattaforme online, puntano, infatti, a catturare quanto più possibile l'attenzione del consumatore. Successivamente, esse mirano a far produrre il maggior numero di "azioni" (ad es. *like, scroll, search*, ecc.) all'utente in modo da immagazzinare quanti più dati possibili. Il risultato di questo meccanismo è la profilazione dell'utente, funzionale ad una proposizione selettiva di servizi e contenuti e personalizzati[25]. Com'è noto, l'art. 4 del GDPR definisce la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali" volto a valutare, analizzare e prevedere determinati aspetti personali relativi ad una persona fisica, riguardanti "il rendimento professionale, la situazione economica, la salute, le

alle tecnologie digitali sembrano scardinare le coordinate del diritto a partire dal principio di territorialità e dalla nozione di sovranità. Cfr. Garante per la protezione dei dati personali 2019-a.

19. Con tale espressione si fa riferimento alle iniziative legislative aventi ad oggetto i dati. Tra queste si ricordano: Reg. (EU) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati), 27 Aprile 2016; Reg. (EU) 2022/868 del Parlamento Europeo e del Consiglio relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Data Governance Act), 30 maggio 2022; Reg.(EU) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 relativo a norme armonizzate sull'accesso equo e l'uso dei dati (Data Act), 13 dicembre 2023.
20. Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati contestabili e equi nel settore digitale (Digital Markets Act), 14 settembre 2022.
21. Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio relativo a servizi digitali nel mercato interno e che modifica la direttiva 2000/31/CE (Digital Services Act), 19 ottobre 2022.
22. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio relativo all'intelligenza artificiale (Artificial Intelligence Act), 13 giugno 2024.
23. Cuocci 2024, p. 64.
24. Come più volte chiarito, i dati una volta organizzati ed elaborati, assumono grande rilievo in relazione alle informazioni che sono in grado di fornire e che possono essere utilizzate per scopi commerciali, sociali o politici. Sul punto si rimanda a d'Ippolito 2022, p. 58 ss.
25. Perché fortemente collegati alla propria "storia" di attività online. In particolare, il tracciamento dell'utente avviene tramite i c.d. cookie, che costituiscono la più importante modalità di acquisizione dei dati relativi all'utente, consentendone, in via successiva, una precisa profilazione. Il fenomeno è puntualmente spiegato in Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la Protezione dei Dati Personali 2020 p. 33.

preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

Tra i modelli di business più comuni vi è il c.d. *zero price*[26], che ricorre quando il servizio digitale viene offerto all'utente, senza che quest'ultimo debba pagare un corrispettivo di natura pecuniaria[27]. L'utente dovrà, invece, consentire al trattamento dei suoi dati[28], che verranno plausibilmente sfruttati dall'impresa a fini commerciali[29]. I possessori di tali dati possono, ad esempio, estrarre da essi trend di consumo dei singoli soggetti, ottenendo una serie di informazioni finalizzate ad orientare, sulla base delle preferenze espresse, le scelte commerciali dei clienti. A tal proposito, viene in rilievo il fenomeno del *targeting*, strettamente connesso alla profilazione, il quale consiste nella proposizione mirata di contenuti (ad es., pubblicità) al consumatore-utente.

Il dato personale mostra, dunque, più che mai la sua natura ambivalente: non solo attributo della personalità oggetto di un diritto fondamentale[30], ma anche un asset fondamentale nell'era dell'economia digitale e dell'IA[31].

Nel contesto descritto – mutuando il pensiero di Rodotà[32] – la persona viene ridotta ad oggetto dal quale vengono costantemente estratte, con le tecniche più disparate, tutte le possibili informazioni per costruire profili ed identità, al fine di ritagliare dalla persona ciò che interessa al mercato. Nella c.d. società della sorveglianza, l'esperienza umana viene trasformata in dati sui comportamenti[33]. In altri termini, Il trattamento di dati personali per finalità di marketing si traduce in un nuovo modo di sfruttamento commerciale della persona[34].

26. Tale modello è preso in considerazione dallo stesso legislatore europeo nella direttiva 2019/770, che attribuisce particolare valore giuridico allo scambio di dati contro servizi. Si rimanda all'art. 3 della direttiva – recepito all'art. 135 *octies* Codice del consumo –, il quale sembra codificare il fenomeno della commercializzazione dei dati personali come strumento alternativo al pagamento in denaro. La direttiva si innesta nell'ambito della *Strategia europea per il digital single market* pubblicata dalla commissione nel 2015: doc. COM(2015) 192.
27. Battelli 2022-a, p. 355 ss.
28. Si pensi ad esempio ai social o alle piattaforme di e-commerce che memorizzano i dati degli utenti per personalizzare contenuti o prodotti, ma che allo stesso tempo cedono quei dati agli inserzionisti che intendono acquistare spazi pubblicitari. Da qui la definizione di mercato digitale quale *multi-sided market*, capace di offrire più servizi a diversi gruppi di utenti.
29. Ad ogni modo il c.d. *zero price* non esaurisce i modelli di business basati sui dati. Si pensi, ad esempio, al c.d. *personal data economy model*, che implica uno scambio diretto del dato contro moneta: in questo caso alla fornitura dei dati da parte dell'utente segue la corresponsione di una somma di denaro.
30. Come tale tutelato dagli art. 8 Carta di Nizza e 16 TFUE.
31. Si ricorda la sent. TAR Lazio n. 260 del 10 gennaio 2020 secondo cui le potenzialità insite nello sfruttamento dei dati personali possono costituire un asset in senso negoziale suscettibile di sfruttamento economico ed idoneo ad assurgere alla funzione di controprestazione in senso tecnico di un contratto. Inoltre, già nel 2018, l'allora presidente dell'Autorità Garante per la protezione dei dati Antonello Soro, osservava come il dato ad oggi assume "il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale" (Discorso del Presidente Antonello Soro, *L'universo dei dati e la libertà della persona*, 2018).
32. Rodotà 2014, pp. 27-28.
33. Sul punto è significativo quanto affermato da Zuboff 2019: "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call *behavioural futures markets*".
34. Cuocci 2024 p. 65.

È evidente che la raccolta e lo sfruttamento massivo dei dati generati dall'attività *online* – ma anche *offline*[35] – degli utenti rischia di compromettere fortemente la loro libertà di determinarsi autonomamente. Infatti, anche laddove il trattamento dei dati personali sia subordinato alla prestazione di un consenso esplicito da parte dell'interessato[36], tale garanzia nella prassi si rivela essere una tutela meramente formale. Nella Risoluzione del Parlamento europeo del 25 marzo 2021[37] già si evidenziava che l'attuazione dei requisiti relativi al valido consenso è spesso compromessa dal ricorso a modelli occulti, a tracciamenti pervasivi e ad altre pratiche non etiche, soprattutto per quanto riguarda la profilazione algoritmica, il *micro-targeting* o la pubblicità online.

Vi è, infatti, un'acclarata asimmetria informativa che caratterizza i rapporti tra l'utente e la piattaforma digitale della quale egli intende usufruire per godere di un certo servizio. La scarsa consapevolezza in merito alla raccolta dei dati e alle relative modalità di utilizzo[38] rende il consumatore particolarmente vulnerabile e privo di reale autodeterminazione nel momento in cui è di fronte alla scelta di avvalersi o meno di servizi online (ancor più nell'ipotesi in cui tali servizi siano pubblicizzati come gratuiti[39]), non potendo dirsi – quasi mai - soddisfatti quei requisiti richiesti dal *data protection law* affinché la manifestazione di volontà possa dirsi realmente informata[40]. Per questi motivi, parte della dottrina sostiene che la categoria del consenso informato sia diventata una mera finzione, dovendosi piuttosto parlare di un consenso consapevolmente disinformato[41]. A ciò si aggiunge che le tecniche di *data analysys* fondate sull'intelligenza artificiale sono in grado di inferire dati personali anche da dati in astratto non riconducibili ad una persona identificata o identificabile[42]. Infatti,

35. Si pensi, ad esempio, a tutti quei dati generati dall'IoT, vale a dire da tutti quei dispositivi che, come lo smartphone, anche in assenza di un'interazione diretta con l'utente possono fornire dati rilevanti sui suoi comportamenti, abitudini e, quindi, sulle sue preferenze.
36. Com'è noto, il consenso ex art. 6 par. 1 lett. a) del GDPR, è tradizionalmente considerato uno dei principali fondamenti di liceità del trattamento, in quanto idoneo a garantire all'interessato il più ampio potere di controllo sui propri dati personali. Inoltre, la prestazione del consenso esplicito integra, ai sensi dell'art. 22, par. 2, lett. c), una delle tre eccezioni al divieto di sottoporre l'interessato a decisioni basate unicamente su trattamento automatizzato, tra cui la profilazione.
37. Risoluzione del Parlamento Europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del Regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP)).
38. Alcune indagini condotte dall'ACGM nel 2020 dimostrano che il 40% degli utenti intervistati non ha consapevolezza né del fatto che la navigazione in Internet e l'utilizzo di app e servizi online comporti la raccolta di dati personali né del fatto che tali dati possano essere ceduti dal fornitore del servizio a terzi. Cfr.: Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la Protezione dei Dati Personali 2020, p. 94. I risultati di questi studi possono considerarsi ancora rilevanti allo stato attuale.
39. Come sottolineato anche nell'indagine conoscitiva sui Big Data in particolare, l'utente viene attratto dal *claim* sulla gratuità del servizio offerto nonché dall'agevole e immediata fruibilità dello stesso per poi essere indotto a condividere in rete esperienze personali, dati e informazioni. Ad ogni modo, non sono quasi mai espressamente chiare le finalità remunerative perseguite dalle imprese, che possono ottenere il massimo sfruttamento economico dei dati attraverso la profilazione degli utenti.
40. Sul punto: considerando n. 32 GDPR.
41. Casonato 2019, p. 107.
42. Com'è noto l'art. 4 del GDPR definisce il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

l'IA utilizza una enorme mole di dati, molti dei quali rientranti nella definizione di dato personale ai sensi del GDPR, altri anonimi o anonimizzati che però l'IA potrebbe re-identificare. Si osserva, dunque, che con il progredire delle tecnologie di trattamento dei dati, muta la stessa nozione di dato personale, il quale si rivela essere un concetto fluido e cangiante essendo necessario prestare attenzione anche al contesto in cui il dato è estratto[43].

Alla luce di quanto espresso, sembra, dunque, svuotarsi di contenuto quel diritto all'autodeterminazione informativa[44], che rappresenta il punto cardine della disciplina in materia di *data protection*. In tale contesto, risulta quanto mai necessario recuperare il nucleo essenziale di tale diritto, consentendo all'utente un pieno controllo dei suoi dati. In tale scenario, riveste un ruolo centrale l'obbligo di informativa, di cui all'art 12 del GDPR, la quale deve consentire all'utente di avere piena cognizione del fatto che i dati da lui ceduti non saranno utilizzati solo per far funzionare i servizi a cui accede, ma che essi saranno sfruttati dalla piattaforma per fini di lucro.

Tuttavia, come chiarito dalla giurisprudenza attuale, una carente informazione circa le modalità di trattamento dei dati è suscettibile di integrare anche una pratica commerciale scorretta ai sensi del Codice del consumo. Infatti, il rapporto tra l'utente e l'operatore della piattaforma integra un vero e proprio rapporto di consumo, anche in assenza di una controprestazione pecuniaria[45]. Questo perché il patrimonio informativo ceduto dall'utente acquista un evidente valore economico in quanto viene usato dalla piattaforma a fini commerciali, delineandosi, solo in apparenza, un rapporto gratuito. Si ravvisa, dunque, un rapporto di scambio in cui i dati dell'utente – non più un mero interessato ai sensi del GDPR, bensì un consumatore – rappresentano la controprestazione del servizio fornito dalla piattaforma.

Alla luce di ciò, in una recente sentenza il Consiglio di Stato ha ravvisato una pratica commerciale ingannevole ai sensi dell'art 21 del Codice del consumo, consistente nell'omessa informazione sull'uso per fini commerciali dei dati personali dell'utente[46], chiarendo che non è sufficiente informare l'utente che i suoi dati saranno usati per la ricezione di comunicazioni di marketing "personalizzate", essendo una tale comunicazione del tutto inidonea a perseguire lo standard richiesto dalla normativa di protezione del consumatore. Questo in quanto la profilazione degli utenti – che è ciò che consente il miglioramento della performance di vendita delle piattaforme digitali – utilizza l'intelligenza artificiale, della quale il grande pubblico intende parlare solo da pochi anni. Nel caso di specie, non poteva dunque presumersi che il consumatore medio fosse in grado di comprendere le conseguenze della cessione dei propri dati, e cioè la profilazione, semplicemente per il fatto di essere stato avvisato che avrebbe ricevuto delle comunicazioni di marketing. Si richiede, così, una maggiore granularità e specificità delle informazioni fornite al consumatore digitale, che devono essere adeguate al concreto atteggiarsi della fattispecie e alla capacità del consumatore medio di comprendere le dinamiche commerciali in atto. Solo in questo modo il consumatore è in grado di autodeterminarsi in maniera consapevole.

Com'è noto, vi è una fisiologica debolezza contrattuale che connota il consumatore nei rapporti Business to Consumer, dovuta prevalentemente ad una asimmetria informativa tra le parti. Tale vulnerabilità risulta essere ancor di più accentuata

43. Sul punto Peluso 2023 pp. 113-114.

44. Da intendersi quale libertà positiva di controllo e di intervento in favore del soggetto a cui l'informazione è riferita. Sul punto si rimanda a Colapietro 2018, p. 13 ss. Tale principio trova la sua genesi nella sentenza della Corte Costituzionale tedesca del 15 dicembre 1983 BVerfG, BvR 209/83. La Corte delinea l'esistenza di un "diritto che garantisce la facoltà dei singoli di autodeterminarsi" e "di stabilire se divulgare e utilizzare i propri dati personali" e, quindi, di decidere "quando e entro quali limiti rivelare questioni relative alla propria vita personale": tale diritto è ritenuto corollario della dignità umana e della liberà d'agire.

45. Consiglio di Stato, 29 marzo 2021, n. 2631, il quale conferma quanto già espresso dall'AGCM nel provvedimento del 29 novembre 2018 n. 27432.

46. Consiglio di Stato, 2 dicembre 2024, n. 9614. Si trattava di un'omissione informativa posta in essere in occasione dell'attivazione del "profilo" digitale dell'utente (Apple id) circa l'utilizzo a fini commerciali dei dati personali degli utenti, elaborati tramite la profilazione durante le interazioni con il *market place* del provider.

nelle ipotesi in cui il consumatore usufruisce di servizi o prodotti digitali, cedendo come corrispettivo i propri dati personali. Questo in quanto egli non è in grado di comprendere agevolmente il funzionamento delle tecnologie di elaborazione dei dati[47], specie quando si tratta di algoritmi di autoapprendimento[48].

Nel caso in esame, il Consiglio di Stato ha, inoltre, qualificato come pratica commerciale aggressiva la scelta di Apple di preimpostare l'acquisizione del consenso al trattamento dei dati personali, rendendo particolarmente difficoltosa la procedura di opt-out per la revoca dello stesso. È, dunque, evidente lo sforzo del giudice amministrativo di attuare la disciplina consumeristica, adattandola alla luce di quelle che possono definirsi "le nuove pratiche commerciali scorrette" al fine di garantire all'utente una maggiore tutela nonché un maggiore controllo delle proprie informazioni personali. In questo senso, la disciplina della privacy e quella consumeristica non sono in rapporto antinomico, ma sono necessarie per garantire una tutela piena ed effettiva all'interessato-consumatore.

Quanto affermato si rivela essere particolarmente innovativo e prezioso nello scenario attuale in cui i grandi operatori economici utilizzano i dati degli utenti, combinati con sofisticate tecniche di intelligenza artificiale al fine di comprimere, ma anche di manipolare, la libertà di autodeterminazione del consumatore, inducendolo a scelte di consumo che altrimenti non avrebbe effettuato. Ne consegue che non solo le carenze informative, ma anche le altre condotte adottate dalla piattaforma–professionista, pur rilevanti ai fini della disciplina sulla protezione dei dati personali, possono integrare violazioni suscettibili di essere valutate anche alla luce della normativa consumeristica. Si pensi, ad esempio, al già citato fenomeno del *targeting*, consistente nella proposizione mirata di contenuti personalizzati all'utente al fine di orientare le sue decisioni commerciali[49], fino ad *indurre* nello stesso dei bisogni di acquisto. Nel *targeting*, il trattamento dei dati personali si rivela spesso opaco, potendo comportare un utilizzo dei dati per finalità ulteriori a quelle dichiarate nell'informativa che l'interessato non poteva ragionevolmente prevedere. Questo mina la capacità dell'interessato di esercitare e mantenere un controllo sui propri dati. Ad ogni modo, questo fenomeno non solleva solo problemi di contrasto con i principi del GDPR – in particolare con i principi del consenso, di minimizzazione e finalità –, ma anche in relazione ad altri diritti e libertà fondamentali. Alcune pratiche di *targeting*, infatti, grazie all'uso improprio di sofisticati algoritmi possono fortemente minare la libertà di autodeterminazione del soggetto, ad esempio inviando messaggi personalizzati idonei a sfruttare talune vulnerabilità del soggetto. Tali messaggi possono così arrivare a influenzare il processo di pensiero della persona, le emozioni e i suoi comportamenti[50] di acquisto.

Ne consegue che anche queste pratiche sono potenzialmente suscettibili di essere attratte nell'ambito di applicazione del Codice del consumo, potendo essere qualificate come pratiche commerciali ingannevoli o addirittura aggressive se idonee a determinare un indebito condizionamento del consumatore digitale ai sensi dell'art. 25 del Codice. Sul punto è utile segnalare quanto affermato dalla Commissione europea, la quale, con riguardo alle pratiche commerciali scorrette basate sui dati, ha chiarito che esse possono

47. Per questo parte della dottrina suggerisce la necessità di una alfabetizzazione digitale, in quanto solo rafforzando la consapevolezza degli utenti sull'utilizzo dei proprio dati è possibile governare il potere delle Big Tech. Cfr. Pagnanelli 2022, p. 24.

48. Il cui funzionamento può essere in parte oscuro allo stesso provider. Infatti, uno dei principali problemi dei sistemi di IA è che essi si atteggiano come una *black-box*. In altri temini, la poca trasparenza di tali sistemi non consente di prevedere ex ante il loro funzionamento né di spiegarlo *ex post*. Cfr.: Wigmore 2023.

49. Esso viene definito come veicolazione di messaggi specifici alle persone fisiche che dispongono di account sui social media. Ad oggi numerosi fornitori di social media forniscono dei servizi di *targeting*. Esso, come le altre pratiche di sfruttamento economico dei dati personali, si fonda sull'analisi e l'elaborazione delle informazioni personali fornite attivamente dagli utenti alla piattaforma o desunte sulla base di comportamenti di navigazione al di fuori della piattaforma stessa.

50. Cfr.: European Data Protection Board (EDPB), *Guidelines 8/2020 on the targeting of social media users*, 13 aprile 2021.

produrre un significativo effetto di manipolazione sui consumatori più vulnerabili[51].

Inoltre, quanto detto sembra confortato anche da quanto sostenuto dall'AGCM nel procedimento avverso la piattaforma Tik Tok[52]. In tale sede, l'Autorità ha qualificato come pratica commerciale scorretta *ex* art 25 Codice del consumo l'utilizzo da parte della piattaforma di un sistema di raccomandazione, basato su tecniche di profilazione, idoneo a generare un indebito condizionamento degli utenti. Tale sistema presenta diverse analogie con il *targeting*, in quanto entrambi i sistemi si fondano sulla profilazione algoritmica e mirano a proporre dei contenuti – di regola pubblicitari – personalizzati agli utenti, comprimendone la facoltà di scelta[53].

Alla luce di quanto espresso è dunque evidente che i rapporti tra la normativa in materia di data protection e la disciplina consumeristica debbano delinearsi sempre più in termini di una integrazione positiva, nella quale il diritto dei consumi diviene funzionale ad attuare quelle garanzie previste dal *data protection law*, contribuendo ad arginare quei fenomeni di abuso che tendono a limitare progressivamente l'autonomia informativa e decisionale dei consumatori-interessati.

3. Le dinamiche concorrenziali nell'era dei *Big Data* e dell'Intelligenza Artificiale

Alla luce di quanto chiarito nei precedenti paragrafi, emerge che, sebbene con riguardo all'illecito trattamento automatizzato di dati personali il rispetto del GDPR rimanga pur sempre centrale, esso non esclude l'applicazione di altri corpi normativi laddove il trattamento dei dati coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a presidio di altri valori ed interessi. Solo in questo modo, infatti, può essere garantita una pienezza di tutela delle persone fisiche. Del resto, già la Commissione Ue, nell'attribuire ai dati personali ceduti dagli utenti un valore economico *de facto*, aveva chiarito che una piattaforma che si qualifica come "professionista", nell'ambito delle sue pratiche commerciali deve sempre rispettare le norme dell'Ue in materia di diritto dei consumatori nonché le norme in materia di concorrenza[54].

In tale sede è opportuno focalizzare l'attenzione sulle implicazioni concorrenziali connesse all'utilizzo dei Big Data e allo sviluppo delle nuove tecnologie, la cui integrazione nel business delle imprese rappresenta la chiave per mantenere una posizione privilegiata sul mercato.

Come già accennato, l'accentramento del patrimonio informazionale nelle mani degli attori privati comporta un aumento della forza degli stessi nei confronti dei concorrenti. Dunque, dal quadro in esame si evince che la disponibilità di tali dati costituisce per le imprese non solo remunerazione della loro attività, ma anche un importante fattore competitivo nel mercato digitale e non solo. In particolare, si osserva che il possesso – o, meglio, il monopolio – dei Big Data nonché le capacità computazionali per elaborarli, permette alle Big Tech di entrare agevolmente in mercati in cui non sono ancora attive e di dominarli. Ad esempio, gli operatori che rivestono una posizione dominante nel mercato delle piattaforme digitali potrebbero estendere tale posizione di forza economica anche al mercato adiacente dell'IA, dando luogo ad eventuali abusi di posizione dominante *ex* art. 102

51. Commissione europea, *Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno* (2021/C 526/01), 29 dicembre 2021.
52. AGCM, provv. n. 31124 del 5 marzo 2024, PS12543, in "Bollettino" 11/2024.
53. Sebbene l'indagine dell'ACGM non riguardasse direttamente il targeting e la pubblicità mirata, essa evidenzia come i meccanismi di profilazione e personalizzazione propri delle piattaforme digitali possano alterare la libertà decisionale degli utenti. Con riguardo al sistema di raccomandazione usato da Tik Tok, la profilazione diventa tanto più precisa quanto più l'utente utilizza la piattaforma perché il sistema apprende in maniera più dettagliata le preferenze. Tale sistema di raccomandazione personalizzata genera nell'utente, specie nei soggetti vulnerabili, un effetto di addiction che la piattaforma riesce a monetizzare, aumentando la redditività degli introiti pubblicitari.
54. Commissione europea, *Orientamenti sull'attuazione/applicazione della Direttiva 2005/29/CE sulle pratiche commerciali scorrette (SWD(2016) 163)*, 25 maggio 2016.

TFUE[55]. Questo, in quanto essi dispongono della quantità di dati e della potenza di calcolo necessarie per la progettazione, lo sviluppo e il funzionamento dei sistemi di IA[56].

In tal senso, si può osservare che il mercato digitale e il mercato dell'IA presentano dei confini piuttosto labili, in quanto i colossi del primo ben potrebbero entrare nel secondo mercato – anche per il tramite di alleanze strategiche con aziende sviluppatrici dominanti nel settore dell'IA – offrendo ai consumatori nuovi *smart products* e servizi basati sull'intelligenza artificiale (si pensi, ad esempio, ai servizi di chatbot che usano l'IA generativa). Ne consegue che le piattaforme digitali dominanti possono sfruttare il loro potere di mercato ponendo in essere pratiche sleali (come il *self-preferencing*, il *tying* o il *bundling*) limitando le scelte dei consumatori e aumentando le barriere all'ingresso per le imprese più piccole.

Un esempio emblematico ed attuale di questa tendenza può essere individuato nella condotta di Meta, che ha integrato il servizio Meta AI all'interno di WhatsApp, imponendo di fatto il nuovo sistema di chatbot ai consumatori. Sulla questione è pendente un procedimento istruttorio dinanzi all'AGCM, al quale si è di recente aggiunto anche un procedimento cautelare[57] per presunto abuso di posizione di dominante. In particolare, si osserva che attraverso l'abbinamento di Meta AI con WhatsApp, Meta appare in grado di *trainare la propria base utenti, dal mercato in cui è già dominante* – quello digitale dei servizi di messagistica – *al nascente mercato dell'IA*, non attraverso una concorrenza basata sui meriti, ma imponendo agli utenti la disponibilità dei due servizi distinti, con potenziale pregiudizio dei servizi concorrenti. Inoltre, è significativo il passaggio del provvedimento dell'Autorità in cui si ricorda che lo sviluppo dei sistemi IA richiede la disponibilità di ampi set di dati per il training degli algoritmi. Tali dati sono input necessari a cui le grandi piattaforme come Meta hanno facilmente accesso. Nel provvedimento, non si esclude che Meta utilizzi i dati dei propri utenti al fine di allenare il suo chatbot.

In questo scenario, il rispetto delle norme sulla privacy può giocare un ruolo centrale nel contribuire a garantire la leale concorrenza tra le imprese della moderna economia[58].

Come chiarito dalla CGUE[59], la conformità alla normativa sulla protezione dei dati è un parametro significativo nella valutazione delle condotte di un'impresa dominante nei mercati digitali, soprattutto nell'ambito della valutazione di abuso di posizione dominante *ex* 102 TFUE[60].

Una efficace regolazione del trattamento dei dati personali può contribuire a rafforzare la concorrenza nel settore dell'intelligenza artificiale, assicurando maggiore fiducia da parte degli utenti[61] e condizioni paritarie di accesso ai dati, evitando che singoli operatori conseguano vantaggi

55. Il quale, come chiarito dalla giurisprudenza europea, non vieta solo l'abuso posto in essere nel mercato in cui l'impresa è dominante, ma censura anche il comportamento dell'impresa che sfrutta la sua posizione dominante in un certo mercato, per estenderla in un mercato contiguo, ma separato. CGUE, C-48/22 P, *Google LLC and Alphabet Inc. v European Commission*, 10 settembre 2024.
56. Cfr.: G7 Competition Authorities, *Digital Competition Communiqué*, 4 ottobre 2024 "The concentrated control of crucial AI inputs has the potential to place a small number of firms in key market positions".
57. AGCM, provv. n. 31634, 22 luglio 2025; ACGM, provv. n. 31728, 25 novembre 2025.
58. Pitruzzella 2016, p. 27.
59. CGUE, C252/21, *Meta Platforms Inc. and Others v. Bundeskartellamt*, 4 luglio 2023.
60. Ciò appare coerente anche con quanto già sostenuto da una parte della dottrina che propone da tempo un adattamento delle categorie tradizionali del diritto antitrust ai mercati *data-driven*. Sul punto Bagnoli 2016, secondo cui la raccolta e l'utilizzo dei Big Data inducono a ripensare la nozione di potere di mercato e di mercato rilevante.
61. In tal senso il già citato G7 Digital Competition Communiquè: "safeguarding personal data is crucial to maintaining public trust and ensuring that AI development respects individual rights". Similmente, sebbene con riguardo ai servizi digitali, v. Pitruzzella 2016 p. 27, secondo cui "Privacy is an important element of trust and trust in digital service is necessary for online markets to work smoothly and to be an engine for work and competitiveness".

anticoncorrenziali derivanti da pratiche illegittime di raccolta e uso dei dati. La stessa Commissione Ue[62] nella sua *Notice on the Definition of Relevant Market* ha individuato nella *privacy protection* garantita dal professionista un parametro da tenere in considerazione. I consumatori potrebbero, infatti, preferire soluzioni che consentano di fornire la quantità minore di dati possibile o di mantenere il maggior controllo possibile sull'utilizzo dei dati personali forniti.

Ne consegue che la protezione dei dati personali e, quindi, la garanzia di una maggiore consapevolezza da parte del consumatore sull'uso dei propri dati, possono rappresentare fattori qualitativi rilevanti per il confronto concorrenziale tra gli operatori del mercato digitale e del mercato dell'IA.

L'*European Data Protection Board* osserva che: "strengthening the link between the protection of personal data and competition can contribute to the protection of individuals and the well-being of consumers by reinforcing the common consideration of respect for their fundamental rights and the proper functioning of competitive markets"[63]. Sebbene, infatti, la normativa sulla protezione dei dati e il diritto della concorrenza perseguano differenti obiettivi, essi condividono dei tratti in comune, rinvenibili nella tutela degli individui e delle loro scelte.

È opportuno sottolineare che la protezione dei dati personali – quale diritto fondamentale – deve essere coniugata con l'esigenza di promuovere la libera circolazione di tali dati e, dunque, una maggiore apertura del mercato dell'innovazione digitale. Tale interpretazione sembra essere accolta dallo stesso GDPR, il quale già nei considerando sancisce che la protezione dei dati personali non è da intendersi quale diritto assoluto, ma deve essere contemperata con altri diritti fondamentali, compresa la libertà d'impresa, in ossequio al principio di proporzionalità. Il regolamento, infatti, unitamente alla tutela della persona, ha come obiettivo quello di assicurare la libera circolazione dei dati anche al fine di favorire il progresso economico e il rafforzamento del mercato interno[64].

Il diritto alla protezione dei dati personali non rappresenta così un ostacolo alla libera concorrenza, la quale, tuttavia, deve essere attuata nel rispetto dei valori fondamentali della persona[65].

In questo quadro, favorire una circolazione dei dati, anche personali, che sia al tempo stesso libera, ma sicura e consapevole, si rivela imprescindibile al fine di evitare una eccessiva concentrazione di quelli che sono i principali fattori di sviluppo dell'intelligenza artificiale. Infatti, l'accesso equo alle risorse – le quali comprendono i dati personali e non – è quanto mai necessario per lo sviluppo e l'implementazione dell'IA. In questo senso, garantire la portabilità dei dati e assicurare entro certi limiti una interoperabilità tra i sistemi che li trattano può favorire il leale gioco della concorrenza stimolando l'innovazione e la diversificazione dell'offerta. Come osservato dall'OECD (*Organisation for Economic Co-operation and Development*), la mancanza di portabilità e di interoperabilità può facilitare la concentrazione di dati proprietari (c.d. *data silos*[66]), determinando barriere all'entrata[67] in diversi settori di mercato nei quali l'IA già svolge (o svolgerà in futuro) un ruolo importante e sempre maggiore.

Ad ogni modo, si ribadisce che la promozione della libera circolazione dei dati e dello sviluppo delle nuove tecnologie non possono tradursi in un sacrificio dei diritti fondamentali della persona e, in particolare, del diritto alla protezione dei dati personali, che costituisce un limite invalicabile[68].

62. Commissione europea, *Notice on the Definition of the Relevant Market for the Purposes of Union competition Law* (C/2024/1645), 22 febbraio 2024.
63. Cfr.: European Data Protection Board (EDPB), *Position Paper on Interplay Between Data Protection and Competition Law*, 16 gennaio 2025.
64. Si vedano i considerando n. 2 e n. 4, nonché l'art. 1 del Regolamento.
65. Battelli 2022-b, p. 1096 ss.
66. Si tratta di dati raccolti ed utilizzati da un'unica piattaforma che non vengono resi in alcun modo accessibili a terzi o riutilizzabili da terzi.
67. OECD 2025, p. 31 ss.
68. Battelli 2022-c, p. 21 ss.

Questo è chiarito anche nell'*AI Act*, che mira allo sviluppo di un'intelligenza artificiale affidabile, antropocentrica e rispettosa dei diritti fondamentali, e tra essi il diritto alla protezione dei dati che deve essere assicurato durante l'intero ciclo di vita del sistema.

Da tali consapevolezze prendono le mosse il *Data Governance Act* e il *Data Act*, gli atti normativi complementari adottati dall'Ue che, in attuazione della *European Data Strategy*, mirano a promuovere la disponibilità dei dati – personali e non – all'interno dell'Unione e a potenziarne i relativi meccanismi di condivisione.

Tali interventi normativi devono essere interpretati in maniera coordinata e sistematica con il *Digital Markets Act*, il quale sancisce divieti e impone una serie di obblighi nei confronti dei c.d. *gatekeeper*[69] al fine di limitare un accentramento del potere di controllo sui dati, prevenendo condotte anticoncorrenziali. Sebbene tale regolamento abbia come primario ambito di applicazione i mercati digitali – costituendo un'imprescindibile strumento di regolazione *ex ante* –, la sua attuazione è idonea a produrre effetti rilevanti anche nel mercato dell'intelligenza artificiale, trattandosi di un mercato strettamente connesso a quello digitale. In particolare, le obbligazioni imposte ai *gatekeeper* sono in grado di incidere – quanto meno indirettamente – anche in questo secondo mercato in quanto gli attori destinatari del DMA sono ormai attivi nella filiera dell'AI, offrendo servizi basati su tale tecnologia. Si pensi, ad esempio, a tutti quegli obblighi di accesso ai dati e di interoperabilità previsti dall'art. 6 par. 9, 10, 11 e 12 nonché dall'art. 7 del DMA, volti a favorire la condivisione dei dati raccolti dai *gatekeeper* con imprese terze e utenti commerciali, sebbene pur sempre nel rispetto del GDPR laddove entrino in gioco dati personali[70].

È evidente che obblighi del genere sono idonei a prevenire l'accumulo di dati proprietari in capo a singole imprese, garantendo un mercato dell'IA aperto alla competitività e all'innovazione nonché più vicino al benessere del consumatore.

Infine, si aggiunge che i *gatekeeper* in quanto fornitori di servizi basati sull'IA, sono sottoposti alle regole dell'*AI Act* e saranno considerati responsabili in caso di mancata conformità agli obblighi che esso prevede[71].

4. Riflessioni conclusive

L'intelligenza artificiale e lo sfruttamento economico dei dati personali rappresentano l'avanguardia dei nuovi modelli di business.

L'analisi condotta evidenzia come la regolazione delle nuove tecnologie configura un ambito in cui la tutela dei dati personali, la protezione dei consumatori e il diritto della concorrenza sono destinati a intersecarsi in maniera sempre più stretta. Da un lato, infatti, il ruolo del *data protection law* rimane centrale, assumendo la privacy sempre più la natura di un *meta-diritto* il cui godimento è necessario per la realizzazione degli altri diritti[72]. Si pensi, ad esempio, al ruolo pro-concorrenziale della privacy nel mercato. Dall'altro lato, tuttavia, si è visto come l'applicazione di altre discipline, quale la normativa consumeristica, contribuisca a rafforzare la

69. Si rinvia alla definizione di cui all'art. 3 del DMA: "Un'impresa è designata come gatekeeper se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro". Il par. 2 prevede, poi, le condizioni in presenza della quali, si presumono soddisfatti i requisiti di cui al par. 1.

70. Questo è più volte ribadito dal DMA che si applica senza pregiudicare le norme derivanti da altri atti di diritto dell'Unione tra i quali il reg. 2016/679. Sul punto, è rilevante il considerando 61 secondo cui "Nel fornire accesso ai suoi dati di ricerca, è opportuno che il *gatekeeper* garantisca la protezione dei dati personali degli utenti finali, anche da eventuali rischi di reidentificazione, con mezzi adeguati, come l'anonimizzazione di tali dati personali, senza compromettere in maniera sostanziale la qualità o l'utilità dei dati".

71. Si rimanda a Perugini 2025, p. 71, in cui si osserva che il DMA si interseca inevitabilmente con l'AI Act.

72. Colapietro 2021, p. 832. Sul punto, si ricordano, inoltre, le parole di Antonello Soro, il quale qualifica la protezione dei dati un "requisito di tutela del consumatore e di *antitrust by design*", cfr. Garante per la protezione dei dati personali 2019-b.

tutela del (consumatore) soggetto-interessato, assicurando quel diritto all'autodeterminazione informativa alla base del GDPR.

La protezione del consumatore e, dunque, anche la protezione della sua privacy, costituiscono a loro volta uno strumento funzionale a garantire l'efficienza del mercato e il leale gioco della concorrenza. Del resto, come osserva la dottrina, regolare il mercato significa regolamentare le singole iniziative economiche che in esso trovano attuazione e, dunque, i singoli atti di autonomia privata[73], al fine di evitare che i fallimenti dell'autonomia privata si traducano in fallimenti del mercato.

Nello scenario attuale, dunque, le singole discipline non agiscono più in maniera isolata, ma si pongono in un rapporto di integrazione positiva, al fine di garantire mercati aperti e competitivi, tutelando al contempo la libertà di autodeterminazione dei singoli cittadini.

Riferimenti bibliografici

I.M. Alagna, N. Centofanti (2021), *La consumerizzazione della privacy tra California Consumer Privacy Act e GDPR*, in L. Bolognini (a cura di), "Privacy e libero mercato digitale", Giuffrè, 2021

Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la Protezione dei Dati Personali (2020), *Indagine conoscitiva sui Big Data*, 2020

V. Bagnoli (2016), *The Big Data Relevant Market*, in "Concorrenza e Mercato", 2016, n. 1

E. Battelli (2024), *La giustizia predittiva nella twin transition*, in "Tecnologie e Diritto", 2024, n. 2

E. Battelli (2022-a), *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono "gratuiti"*, in "I Contratti", 2022, n. 3

E. Battelli (2022-b), *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in "Rivista di diritto di famiglia e delle persone", 2022, n. 3

E. Battelli (2022-c), *Negoziabilità dei dati come strumento di regolazione del mercato e di protezione della persona utente di servizi digitali*, in "Rivista di diritto dell'impresa", 2022, n. 1

C. Casonato (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni,* in "Diritto pubblico comparato europeo", Numero speciale, 2019

C. Colapietro (2021), *Circolazione dei dati, automatizzazione e regolazione*, in "Osservatorio sulle fonti", 2021, n. 2

C. Colapietro (2018), *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "federalismi.it", 2018, n. 22

E. Cremona (2021), *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in "Osservatorio sulle fonti", 2021, n. 2

V.V. Cuocci (2024), *Persone vulnerabili e scelte (in)consapevoli: riflessioni su neuromarketing e protezione dei dati personali nell'era dell'intelligenza artificiale,* in S. Orlando (a cura di), "Profili giuridici del neuromarketing", Sapienza University Press, 2024

G. De Gregorio (2022), *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022

A. De Mauro, M. Greco, M. Grimaldi (2016), *A Formal Definition of Big Data Based on its Essential Features*, in "Library Review", vol. 65, 2016, n. 3

73. Sul punto Errigo 2023, p. 79.

G. d'Ippolito (2022), *Monetizzazione, patrimonializzazione e trattamento dei dati personali,* in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

F. Di Porto (2016), *La rivoluzione dei big data, un'introduzione,* in "Concorrenza e Mercato", 2016, n. 1

E. Errigo (2023), *Sulle nuove libertà economiche. Criticità e prospettive del mercato digitale tra concorrenza, nuovi beni e autonomia negoziale*, in "Diritto Costituzionale", 2023, n.1

Garante per la protezione dei dati personali (2019-a), *Discorso di apertura dei lavori del Presidente Antonello Soro*, in "I Confini del Digitale. Nuovi scenari per la protezione dei dati" (Roma, 29 gennaio 2019), 2019

Garante per la protezione dei dati personali (2019-b), *L'universo dei dati e la libertà della persona*, Relazione 2018, 7 maggio 2019

V. Mayer-Schönberger , K. Cukier (2013), *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Eamon Dolan, 2013

OECD (2025), *Artificial intelligence and competitive dynamics in downstream markets*, in "OECD Roundtables on Competition Policy Papers", OECD Publishing, 14 novembre 2025

OECD (2016), *Big Data: Bringing Competition Policy to the Digital Era*, OECD Publishing, 30 settembre 2016

V. Pagnanelli (2022), *Una "valutazione d'impatto della privacy delle Big Tech". Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

M.G. Peluso (2023), Intelligenza artificiale e tutela dei dati, Giuffrè, 2023

S. Perugini (2025), *L'AGCM di fronte all'intelligenza artificiale,* in M. Rabitti, F. Bassan (a cura di), "L'applicazione dell'IA Act in Italia e la tutela del consumatore", Roma TrE-Press, 2025

G. Pitruzzella (2016), *Big Data, Competition and Privacy. A Look From the Antitrust Perspective*, in "Concorrenza e Mercato", 2016, n. 1

S. Rodotà (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014

P. Staab (2024), *Markets and Power in Digital Capitalism*, Manchester University Press, 2024

P. Stone, R. Calo, R. Brooks et al. (2016), *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence*, Stanford University Press, 2016

S. Torregiani (2023), *Il Data Act: una versione europea del Data Nationalism?*, in "Rivista italiana di informatica e diritto", 2023, n. 2

I. Wigmore (2023), *Definition of Black Box IA*, in "Whatls.com", 2023

S. Zuboff (2019), *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, 2019