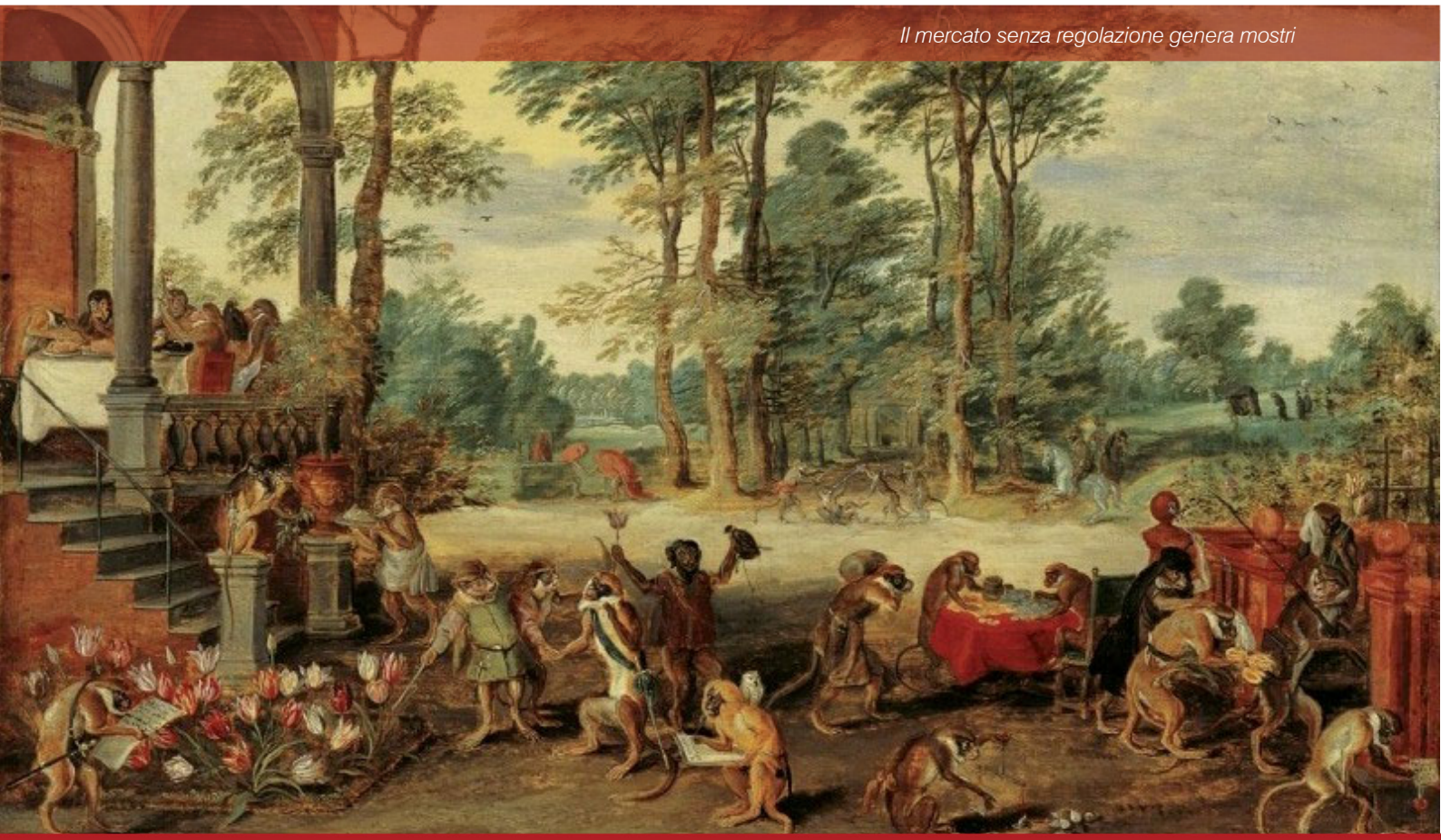
ISSN 2284-2934

Fascicolo **2** | 2023

RIVISTA DELLA
Regolazione dei mercati



Il mercato senza regolazione genera mostri

G. Giappichelli Editore

INDICE

Rivista della
Regolazione dei mercati
Fascicolo **2**| 2023

Rivista registrata presso
il Tribunale di Torino
aut. n. 31 del 25 ottobre 2013

RECENSIONI

Meta Platforms Inc., già Facebook Inc. v. Bundeskartellamt: la Corte di Giustizia dell'Unione Europea apre (finalmente) all'integrazione fra diritto antitrust e *data protection*

Meta Platforms Inc., formerly Facebook Inc. v. Bundeskartellamt: The European Court of Justice opens (finally) to the interplaybetween antitrust and data protection law

di *Anna Licastro*[*]

ABSTRACT

Il presente lavoro trae spunto dalla vicenda giudiziaria che vede confrontarsi ormai da diversi anni la società californiana Meta ed il *Bundeskartellamt*, autorità garante della concorrenza tedesca. Si propone di esaminare il percorso argomentativo che ha portato la Corte di Giustizia dell'Unione Europea ad affermare, contrariamente a quanto ritenuto da buona parte della dottrina ed anche dalla stessa Commissione Europea in varie occasioni, che è possibile far cooperare insieme il diritto della concorrenza e la normativa in materia di protezione dei dati personali al fine di arginare l'abuso di potere informativo delle grandi società della rete. Abbandonando l'idea di matrice neoliberale secondo cui il diritto antitrust persegue solo la tutela dell'efficienza economica, i giudici del Lussemburgo hanno sostenuto che non solo una violazione della *privacy* può costituire un importante indizio dal quale desumere un pregiudizio dei principi della concorrenza, ma che l'esistenza di una posizione dominante può anche essere un elemento dal quale desumere un eventuale invalidità del consenso. È evidente che le due normative non possano procedere su "binari separati" e che una loro reciproca collaborazione consenta alle autorità garanti della concorrenza di ripensare ad una nuova teoria del danno concorrenziale in cui il valore pro-competitivo della *data protection* possa sostituirsi al parametro quantitativo del prezzo.

The present work is inspired by the legal case between Meta and the Bundeskartellamt, the German competition authority. It is aimed at ascertaining the reasoning that has encouraged the European Court of Justice to support the view that antitrust and data protection law can cooperate to curb the abuse of informational power on behalf of digital platforms, as opposed to some scholars and the European Commission have declared in several occasions. Leaving behind the «law & economics approach» proposed by the neoliberal economic theory, according to which the only

[*] Dottore di ricerca in *Business, Institutions, Markets*, Università degli Studi «Gabriele d'Annunzio» di Chieti-Pescara.

goal of antitrust is barely economic efficiency, in its decision, CJEU judges have claimed that not only in the context of the examination of abuse of a dominant position by an undertaking, a privacy violation can constitute an important clue from which it can be inferred antitrust infringement but also that holding a dominant position on the social network market, it constitutes an important factor in determining whether the consent was validly and, in particular, freely given. In light of the above considerations, it is clear that antitrust and data protection law do not proceed on separate tracks as well as the integration between these two normative can foster national and supranational competition authorities to reformulate a theory of harm based on a pro-competitive value of privacy suitable to substitute the price as a quality competitive dimension in digital markets.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, SENTENZA 4 LUGLIO 2023, META PLATFORMS INC., GIÀ FACEBOOK INC., CONTRO BUNDESKARTELLAMT, C-252/21

Estratto

"[…] In tale contesto, ritenendo che la soluzione della controversia principale dipenda dalla risposta da dare a tali questioni, l'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1)

a) Se sia compatibile con gli articoli 51 e seguenti del RGPD il fatto che un'autorità garante della concorrenza di uno Stato membro, quale l'autorità federale garante della concorrenza, che non sia un'autorità di controllo ai sensi degli articoli 51 e seguenti del RGPD e nel cui Stato membro un'impresa stabilita al di fuori dell'Unione europea disponga di una filiale di supporto alla filiale principale nel settore della pubblicità, della comunicazione e delle relazioni pubbliche […] constati, nell'ambito dell'esercizio di un controllo degli abusi di posizione dominante ai sensi del diritto della concorrenza, che le condizioni contrattuali operate dalla filiale principale relativamente al trattamento dei dati e la relativa attuazione violano il RGPD, e disponga di porre fine a tale violazione.

b) In caso affermativo, se ciò sia compatibile con l'articolo 4, paragrafo 3, TUE se, nel contempo, l'autorità di controllo capofila nello Stato membro in cui si trova la filiale principale ai sensi dell'articolo 56, paragrafo 1, del RGPD sottopone a un procedimento di indagine le condizioni contrattuali per il trattamento dei dati operate da quest'ultima.

In caso di risposta affermativa alla prima questione:

2)

a) Se, nel caso di un utente di Internet che si limiti a visitare siti Internet o applicazioni("*app*") che fanno riferimento ai criteri di cui all'articolo 9, paragrafo 1, del RGPD […] ove immetta dati al fine di registrarvisi o di effettuare degli ordini, e di una (…) società, come [Meta Platforms Ireland], che raccolga i dati relativi all'accesso ai siti e alle *app* e alle informazioni ivi immesse da parte dell'utente – tramite interfacce integrate nei siti e nelle *app*, come "Strumenti di Facebook Business", o tramite marcatori temporanei ("cookies") o simili tecnologie di memorizzazione […] – li colleghi ai dati dell'account Facebook.com dell'utente e li utilizzi, la raccolta e/o il collegamento e/o l'utilizzo configurino un trattamento di dati sensibili ai sensi di detto articolo.

b) In caso affermativo: se l'accesso a tali siti e *app* e/o l'inserimento di dati e/o l'attivazione di pulsanti ("plug-in social" come "Mi piace", "Condividi" o "Facebook Login" o "AccountKit") integrati in tali siti o *app* da un fornitore come [Meta Platforms Ireland] costituiscano una modalità di rendere manifestamente pubblici i dati relativi all'accesso di per sé e/o i dati immessi da parte dell'utente, ai sensi dell'articolo 9, paragrafo 2, lettera e), del RGPD.

3)

Se un'impresa come [Meta Platforms Ireland], che gestisce un *social network* digitale finanziato dalla pubblicità e che offre, nelle sue condizioni d'uso, la personalizzazione dei contenuti e della pubblicità, la sicurezza del *network,* il miglioramento dei prodotti e l'utilizzo coerente e senza interruzioni di tutti i prodotti del gruppo, possa invocare la giustificazione della necessità per l'esecuzione di un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b), del RGPD, o la giustificazione della tutela dei legittimi interessi di cui all'articolo 6, paragrafo 1, lettera f), del RGPD, quando a tali fini essa raccoglie dati generati da altri servizi propri del gruppo e da siti e *app* di terzi tramite interfacce in essi integrate, come "Strumenti di Facebook Business", oppure tramite

cookies o simili tecnologie di memorizzazione utilizzati sul computer o sul dispositivo terminale mobile dell'utente, li collega all'account Facebook.com dell'utente e li utilizza.
4)
Se, in tal caso, possano essere considerati legittimi interessi ai sensi dell'articolo 6, paragrafo 1, lettera f), del RGPD anche
– la minore età dell'utente […];
– la fornitura di misurazioni […];
– l'offerta di comunicazioni di *marketing* destinate all'utente affinché l'impresa possa migliorare i suoi prodotti e condurre *marketing* diretto;
– ricerca e innovazione per il bene della società per far progredire lo stato dell'arte o la comprensione scientifica relativamente a importanti temi sociali e per avere un impatto positivo sulla società e sul mondo;
– informazioni alle autorità preposte all'applicazione e all'esecuzione della legge e la risposta a richieste legali […];
quando a tali fini l'impresa raccoglie dati generati da altri servizi propri del gruppo e da siti e *app* di terzi tramite interfacce in essi integrate […] li collega all'account Facebook.com dell'utente e li utilizza.
5)
Se, in tal caso, la raccolta di dati provenienti da altri servizi propri del gruppo e da siti internet e *app* di terzi tramite interfacce in essi integrate, come "Strumenti di Facebook Business", oppure tramite cookies o simili tecnologie di memorizzazione […] il collegamento con l'account Facebook.com dell'utente e l'utilizzo di tali dati, oppure l'utilizzo di dati già altrimenti e legittimamente raccolti e collegati possano essere giustificati, caso per caso, anche ai sensi dell'articolo 6, paragrafo 1, lettere c), d) ed e) del RGPD, ad esempio per rispondere ad una legittima richiesta di dati specifici [lettera c)], per contrastare comportamenti dannosi e promuovere la sicurezza [lettera d)], per ricerche a beneficio della società e per promuovere protezione, integrità e sicurezza [lettera e)].
6)
Se nei confronti di un'impresa in posizione dominante sul mercato come [Meta Platforms Ireland] sia possibile esprimere un consenso valido, e in particolare libero ai sensi dell'articolo 4, punto 11, del RGPD, in conformità con gli articoli 6, paragrafo 1, lettera a), e 9, paragrafo 2, lettera a), del RGPD.
In caso di risposta negativa alla prima questione:
7)
a) Se un'autorità nazionale garante della concorrenza di uno Stato membro, quale l'autorità federale garante della concorrenza, che non sia un'autorità di controllo ai sensi degli articoli 51 e seguenti del RGPD e che esamini una violazione del divieto di abuso diposizione dominante, ai sensi del diritto della concorrenza, da parte di un'impresa imposizione dominante, che non consista in una violazione del RGPD da parte delle sue condizioni per il trattamento dei dati e della loro attuazione, possa effettuare accertamenti, ad esempio nell'ambito del bilanciamento degli interessi, in merito alla conformità al RGPD delle condizioni per il trattamento dei dati di tale impresa e della loro attuazione.
b) In caso affermativo: se, ai sensi dell'articolo 4, paragrafo 3, TUE, ciò valga anche qualora, nel contempo, l'autorità di controllo capofila competente ai sensi dell'articolo 56, paragrafo 1, del RGPD sottoponga le condizioni per il trattamento dei dati di tale impresa ad un procedimento di indagine. Se la risposta alla settima questione è affermativa, occorre rispondere alle questioni dalla terza alla quinta per quanto riguarda i dati generati dall'utilizzo del servizio Instagram, appartenente al gruppo».

Massime

Un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso.
Nel caso in cui un utente di un *social network online* consulti siti Internet oppure applicazioni correlati a una o più delle categorie menzionate da tale disposizione e, se del caso, inserisca in essi dati, iscrivendosi oppure effettuando ordini *online*, il trattamento di dati personali da parte dell'operatore di tale *social network online* […] deve essere considerato un «trattamento di categorie particolari di dati personali», il quale è in linea di principio vietato, fatte salve le deroghe.

Un utente di un *social network online*, allorché consulta siti Internet oppure applicazioni correlati a una o più delle categorie menzionate all'articolo 9, paragrafo 1 del RGPD non rende manifestamente pubbliche, ai sensi della prima di tali disposizioni, i dati relativi a tale consultazione, raccolti dall'operatore di detto *social network online* mediante cookie o simili tecnologie di registrazione. Tale utente rende manifestamente pubblici i dati così inseriti soltanto se abbia esplicitamente espresso preliminarmente la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone.
Il trattamento di dati personali effettuato da un operatore di un *social network online* può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti, solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.
Il trattamento di dati personali effettuato da un operatore di un *social network* online – consistente nel raccogliere dati degli utenti di tale *social network* provenienti da altri servizi può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perseguito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono suddetto legittimo interesse del titolare del trattamento o di terzi.
Il trattamento di dati personali effettuato da un operatore di un *social network online* è giustificato allorché è effettivamente necessario per adempiere un obbligo legale al quale il titolare del trattamento è soggetto, in forza di una disposizione del diritto dell'Unione o del diritto dello Stato membro interessato, tale base giuridica risponde ad un obiettivo di interesse pubblico ed è proporzionata all'obiettivo legittimo perseguito e tale trattamento è effettuato nei limiti dello stretto necessario.
Il trattamento di dati personali effettuato da un operatore di un *social network online* non può, in linea di principio e ferma restando la verifica che deve essere effettuata dal giudice del rinvio, essere considerato necessario alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, ai sensi della lettera d), oppure all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi della lettera e).
La circostanza che l'operatore di un *social network online* occupi una posizione dominante sul mercato dei *social network online* non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire […] al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare.

1. Storia della vicenda giudiziaria alla base di una decisione tanto attesa

Il 4 luglio 2023 potrebbe essere uno di quei giorni da ricordare, almeno per il diritto antitrust eurounitario. L'Unione Europea, grazie alla Corte di Giustizia, prendendo la strada "meno battuta" di frostiana memoria, ha sancito l'indipen-

denza dall'idea, tanto osteggiata da una folta schiera di studiosi ed esperti del diritto della concorrenza, secondo cui diritto antitrust e protezione dei dati personali sarebbero normative non conciliabili perché nate per perseguire obiettivi diversi. La Corte, chiamata ad esprimersi sulla domanda di pronuncia pregiudiziale proposta dal Tribunale superiore di Düsseldorf in merito alla decisione del *Bundeskartellamt* (d'ora in avanti, *BKARTA*) di vietare a Meta il trattamento dei dati personali dei propri utenti alle condizioni generali d'uso della piattaforma Facebook e di darne attuazione, si è pronunciata con una sentenza "fiume" non solo sull'integrazione tra antitrust e *data protection*, ma anche su altri aspetti riguardanti l'applicazione del regolamento sulla protezione dei dati personali alle condotte delle grandi società della rete. Dirompenti potrebbero rivelarsi i suoi effetti non solo sul diritto della concorrenza eurounitario, ma anche, più in generale, sull'idea, piuttosto recente, dei regolatori di "domare" le intemperanze dell'innovazione tecnologica, mediante «una regolazione finalizzata alla predisposizione collaborativa delle regole [1]» in grado di garantire un mercato digitale equo, contendibile ed eticamente sostenibile [2].

Non c'è una controversia, tranne forse quella del caso *Google Shopping*, sulla quale negli ultimi anni gli esperti di diritto antitrust e non solo, abbiano versato fiumi di inchiostro (elettronico, letteralmente), come quella che vede affrontarsi da lungo tempo, il *Bundeskartellamt* e Meta, colosso dei *social network*. Tuttavia, se l'indagine nei riguardi di Google ha segnato la storia del diritto della concorrenza eurounitario per il tentativo, più che meritorio, di risolvere l'accesso dibattito dottrinale sulla corretta qualificazione giuridica del *self-preferencing*, quale condotta anticompetitiva tipica dei mercati *data-driven* [3],

---

[1] Sull'interazione fra regolare e regolato nella predisposizione delle regole si vedano le opportune riflessioni della studiosa L. AMMANNATI, *Regolatori e supervisori nell'era digitale: ripensare la regolazione*, in corso di pubblicazione in *Giur. Cost*., p. 12.

[2] In tal senso, le considerazioni di L. FLORIDI, *L'etica dell'Intelligenza Artificiale*, Raffaello Cortina Editore, Milano, 2022, p. 280 ss. L'Autore descrive l'Intelligenza Artificiale quale «nuova forma dell'agire che deve essere orientata al bene della società, il che significa anche far sì che gli strumenti di Intelligenza Artificiale siano usati per favorire politiche pubbliche sostenibili da un punto di vista sia etico che ambientale. Sul punto, si veda anche C.A. CIARALLI, *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, in *Federalismi*, 15, 2023, p. 76 ss.

[3] In tema di *self-preferencing* si ricorda che il Tribunale dell'Unione Europea, nel respingere il ricorso presentato dalla società californiana avverso il provvedimento della Commissione, ha sostenuto che il *self-preferencing* costituisce una categoria giuridica a sé stante dotata di una sua autonomia normativa e distinta dalle pratiche discriminatorie di cui all'art. 102 TFUE. Con riguardo alla corretta qualificazione di *self-preferencing*, fra i molti articoli si vedano: P. CARO DE SOUSA, *What shall we do about self-preferencing?*, in *Competition Policy International*, June 2020, consultabile al sito CPI, p.1.; E. IACOBUCCI-F. DUCCI, *The Google search case in Europe: tying and the single monopoly profit theorem in two-sided markets*, in *Eur. J. Law Econ.*, Vol. 47, 1, 2019, p. 18; B. VESTERDORF, *Theories of self-preferencing and duty to deal –two sides of the same coin?*, in *Competition Law & Policy Debate*, Vol. 1, 1, 2015, p. 4 ss.; N. PETIT, *Theories of self-preferencing under article 102 TFUE: a reply to B. Vesterdorf*, in *Competition Law & Policy Debate*, n. 1, 2015, pp. 7-8; P. IBÁÑEZ COLOMBO, *Self-preferencing:yet another epithet in need of limiting principles*, in *World Competition*, Vol.43, 4, 2020, pp. 5-6. Inoltre, sulle novità della pronuncia del Tribunale dell'Unione Europea sul caso *Google Shopping* si vedano: TRIBUNALE DELL'UNIONE EUROPEA, 10 novembre 2021, *Google e Alphabet/ Commissione* (*Google Shopping*), Caso T 612/17, ECLI:EU:T: 2021:763, par. 163, consultabile al sito *curia.europa.eu*; C. AHLBORN-G. VAN GERVEN-W. LESLIE, *Bronner revisited: Google Shopping and the Resurrection of Discrimination Under Article 102 TFUE*, in *Journal of European Competition Law & Practice*, Vol. 13, no. 2, 2022, p. 89; E. DEUTSCHER, *Google Shopping and the quest for a legal test for self-preferencing under article 102 TFUE, in European Papers*, Vol. 6, no.3, 2021, p. 1351. Il caso *Google Shopping* non costituisce un *unicum* perché è speculare all'oggetto dell'indagine

l'epopea tedesca, invece, la segna perché riconosce che il potere *across-markets*[4] delle grandi piattaforme può ben essere regolato mediante una strada alternativa o, quanto meno, complementare all'*ex ante regulation*, basata sull'integrazione fra il diritto antitrust e la normativa in materia di *data protection*.

Il lavoro si propone, dunque, di esaminare il percorso argomentativo che ha portato la Corte di Giustizia dell'Unione Europea a ritenere antitrust e protezione dei dati personali due normative che non possono procedere su "binari" separati perché è evidente che nel contesto dei mercati *data-driven* interagiscano fra di loro sempre con maggior frequenza. Sostenendo il contrario si commetterebbe un errore difficilmente rimediabile, visto che in gioco non c'è solo la necessità di salvaguardare il buon funzionamento del mercato, ma anche quella di tutelare il consumatore digitale dalle insidie di pratiche commerciali manipolatorie e scorrette poste in essere dai guardiani dei mercati. Seguendo, dunque, il ragionamento dei giudici del Lussemburgo, si tenterà di dimostrare come nella decisione resa sia rintracciabile un primo tentativo della Corte di Giustizia, magari neppure intenzionale, di costruire una "rinnovata" teoria del danno concorrenziale appositamente pensata per i mercati digitali, di cui le autorità garanti della concorrenza a livello nazionale e sovranazionale dovrebbero tener conto ogniqualvolta indaghino condotte commerciali anticoncorrenziali realizzate con l'intenzione di rafforzare un potere di mercato che aumenta e si rafforza in modo inversamente proporzionale alla riduzione dei livelli di *privacy* all'interno dell'ecosistema digitale.

1.1. Dal *Bundeskartellamt* al *Bundesgerichthof* passando per l'*Oberlandesgericht Düsseldorf*

Prima di analizzare la decisione della Corte di Giustizia si ritiene opportuno richiamare, almeno nei suoi termini essenziali, la storia giudiziaria che, alcuni illustri studiosi, hanno giustamente definito «saga teutonica[5]».

Dopo un'istruttoria iniziata a marzo 2016 e conclusasi a febbraio 2019, l'Ufficio federale dei Cartelli ha vietato, per abuso di posizione dominante, la condotta commerciale consistita nel trattamento illecito dei dati personali dei propri utenti messa in atto da Meta (all'epoca, ancora Facebook) nel mercato tedesco dei *social network*[6]. Veniva, infatti, contestato alla piattaforma di aver acquisito, combinato insieme e processato i dati generati dagli iscritti non solo

italiana aperta dall'AGCM a carico di Amazon nel 2019. L'istruttoria si è conclusa nel 2021 con la condanna di Amazon per abuso di posizione dominante. Il 3 ottobre 2022 il TAR Lazio ha respinto il ricorso proposto da Amazon contro la sanzione inflitta dall'AGCM in precedenza sostenendo che il provvedimento fosse viziato per effetto di vizi procedurali attinenti alla tardività nell'apertura del procedimento amministrativo. A tal riguardo, cfr. P. BOUGETTE-O. BUDZINSKI-F. MARTY, *Self-Preferencing and Competitive Damages: A Focus on Exploitative Abuses*, in *Antitrust Bull.,* Vol. 67, 2, 2022, p.191 ss. Per una disamina attenta e precisa dell'intera vicenda si vedano le riflessioni di F. GHEZZI-MAGGIOLINO, *Considerazioni intorno al provvedimento dell'Autorità garante della concorrenza nel caso FBA Amazon: nulla di nuovo sotto il sole?* in questa *Rivista*, 2, 2022, p. 513.

[4] In tal senso si vedano: G. FERRARI-M. MAGGIOLINO, *Il potere across markets delle GAFAM: come reagire?*, in *Orizzonti dir. comm*, Fascicolo Speciale, 2021, p.473. Le Autrici coniano l'espressione «ubiquità di mercato» proprio con riguardo alla capacità delle imprese digitali di conquistare mercati collegati a quello principale in cui hanno raggiunto una posizione di dominanza economica.

[5] A parlarne in questi termini R. PARDOLESI-R. VAN DEN BERGH-F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, in *Merc., conc., reg.,* 3, 2020, p. 513.

[6] Si tratta della decisione n. B6-22/16 del 6 febbraio 2019 relativa al caso *Facebook v. Bundeskartellamt*, consultabile al sito ufficiale del *BKARTA*.

nel corso dell'attività svolta all'interno dell'ecosistema digitale (c.d. dati *On-Facebook*), ma anche all'esterno, consultando pagine web e applicazioni di terze parti in grado di raccogliere tracce digitali del loro passaggio grazie all'uso di marcatori temporali (c.d. *cookies*) e strumenti progettati per la profilazione, nello specifico *plugin* e *pixel* (c.d. dati *Off-Facebook*). Grazie a questa raccolta di informazioni, la società intendeva costruire dei «super-profili» degli utenti al fine di adattare il più possibile la *user experience* alle loro preferenze, gusti, abitudini, inclinazioni e, di conseguenza, personalizzare il contenuto dei messaggi pubblicitari destinati agli utenti della piattaforma [7].

Fin qui nulla di strano. Da tempo, infatti, le autorità garanti della concorrenza sono a conoscenza dell'importanza che la pubblicità *online* assume per i giganti del digitale. Si tratta del principale strumento di finanziamento mediante cui è possibile garantire la sopravvivenza dei propri modelli di *business* [8]. L'aspetto più allarmante della condotta del *social network* ha riguardato le condizioni ed i termini d'uso di Facebook, la cui accettazione, da parte degli iscritti, risultava essenziale laddove volessero accedere ai servizi digitali offerti dalla piattaforma. Il *BKARTA* ha ritenuto che il consenso, mediante il quale gli utenti accettavano le condizioni contrattuali unilaterali ed autorizzavano Meta al trattamento dei propri dati personali, non fosse stato prestato validamente. Dirimente, in tal senso, la modalità di acquisizione del consenso presentata agli iscritti nella forma del c.d. «*take it or leave it*» che li poneva nella condizione di dover necessariamente accettare i termini di servizio proposti, pena l'esclusione dall'uso dei servizi del *social network*. È evidente che la prestazione del consenso fosse più il frutto di una «forzatura» che di una scelta volontaria.

In questa vicenda, sono, dunque, venuti a mancare i requisiti di validità del consenso, così come enucleati all'articolo 4, n.11 nonché, conseguentemente, la condizione di liceità di cui all'articolo 6, par. 1, lett. a) del regolamento Europeo per la protezione dei dati personali (d'ora in poi, GDPR) che vale a legittimare il trattamento dei dati personali. Vi è di più. È stato violato, inoltre, il dettato normativo dell'articolo 7 del GDPR e, nello specifico, il paragrafo 4 che, fra le condizioni per la valida manifestazione del consenso, pone espressamente quella di considerare se l'esecuzione di un contratto o la prestazione di un servizio digitale sia condizionata alla prestazione o meno del consenso.

Per imporre il divieto di trattamento dei dati personali così come previsto ed impedirne l'attuazione, l'autorità federale tedesca doveva, inoltre, provare che la violazione delle norme europee in materia di *data protection* da parte di Meta costituiva uno sfruttamento abusivo della posizione dominante conquistata dalla piattaforma sul mercato dei *social network*. L'Ufficio tedesco dei Cartelli compie quello che per la storia del diritto della concorrenza eurounitario può definirsi un "triplo salto carpiato" perché equipara la violazione del GDPR da parte di Facebook ad un abuso di sfruttamento non imputabile tanto all'applicazione di prezzi eccessivi, ma all'imposizione di condizioni unilaterali contrat-

[7] Si veda come si esprimeva già, nei primi anni'90, lo studioso S. RODOTÀ, *Tecnologie e Diritti*, Il Mulino, Bologna, 1995, p. 66.

[8] Fra i molti, si vedano i risultati degli studi compiuti dalla *Competition & Markets Autority*, autorità inglese della concorrenza e dell'ACCC, autorità australiana della concorrenza. Cfr. CMA, *Online Platforms and Digital Advertising Market Study Interim Report*, 2019, consultabile al sito ufficiale della CMA, p. 43 ss. nonchè ACCC, *Digital platform services inquiry. Interim report no. 5 – Regulatory reform*, September 2022, p. 31 ss.

tuali inique, fondando così le sue argomentazioni sull'articolo 19(2), n.2 del *Gesetz gegen Wettbewerbsbeschränkungen* (d'ora, in avanti Legge federale della concorrenza o GWB) che sanziona, quale abuso di posizione dominante, l'imposizione da parte dell'impresa egemone di un corrispettivo o altre condizioni negoziali ben diverse da quelle che si sarebbero previste in una situazione di concorrenza effettiva.

L'articolo 19(2), n.2 del GWB, inoltre, consentiva all'Ufficio dei Cartelli di dimostrare l'esistenza di un nesso di causalità c.d. normativa fra la condotta anticompetitiva di Meta e la posizione dominante vantata da quest'ultima nel mercato dei *social network*, senza dover passare per l'accertamento del rapporto di causalità c.d. comportamentale, certamente più rigoroso e stringente, come avrebbe richiesto l'articolo 102 del TFUE [9]. Il nesso di causalità attenuata, invece, ha permesso al *Bkarta* di dimostrare che senza il potere economico raggiunto dalla piattaforma nel mercato dei *social network*, Meta non sarebbe mai stata in grado di imporre agli utenti finali termini di servizio iniqui, lesivi del diritto all'autodeterminazione informativa.

Trascorsi tre anni dall'inizio delle indagini, il procedimento si è concluso nel 2019 con la condanna di Meta, che ha impugnato poi il provvedimento dinanzi al *Oberlandesgericht Düsseldorf* (Alta Corte Regionale di Düsseldorf) chiedendo la sospensione dell'ordine comportamentale perché sarebbe stato in grado di pregiudicare la sopravvivenza del modello di *business* della piattaforma. Il Tribunale superiore ha accolto l'istanza sospensiva considerando che due fossero le questioni in grado di dimostrare l'evidente infondatezza delle tesi avanzate dall'autorità.

La condotta adottata dalla piattaforma non poteva considerarsi un abuso di sfruttamento perché il nesso di causalità normativa non era sufficiente a dimostrare l'esistenza del rapporto fra posizione dominante e condotta anticoncorrenziale. Occorreva, al contrario, provare l'esistenza del nesso di causalità comportamentale. Difatti, la causalità normativa imponeva di provare che l'imposizione di termini d'uso iniqui fosse la causa della notevole crescita del potere di mercato di Facebook, mentre, nel secondo caso era l'abuso di posizione dominante nel mercato dei *social networks* ad aver permesso l'imposizione di condizioni negoziali inique [10]. La causalità comportamentale richiamata nel caso di specie comporta un'inversione del nesso eziologico e trasforma, così, l'uso di termini contrattuali illeciti nell'effetto piuttosto che nella causa della condotta anticompetitiva della società californiana. Deboli venivano valutate le argomentazioni relative all'abuso escludente perché, come provava la chiusura definitiva della piattaforma Google+, ideata dal motore di ricerca Google per sfidare il monopolio di Facebook, la disponibilità di una notevole base dati non costituiva necessariamente la condizione per raggiungere una posizione dominante nei mercati *data-driven*.

Interessante poi che l'Alta Corte ritenesse l'imposizione di condizioni e termini di servizio iniqui non tanto ascrivibile alla posizione di dominio economico vantata da Meta nel mercato dei *social network*, quanto semmai all'indifferenza tipica dell'utente medio della piattaforma [11]. Negava in questo modo che

---

[9] *Ivi,* punto 873 ss. Meritano, inoltre, attenzione le considerazioni sul concetto di causalità normativa di R. Pardolesi-R. Van Den Bergh-F. Weber, *Facebook e i peccati da «Konditionenmissbrauch*», cit., p. 524 ss.

[10] Cfr. A. Giannaccari, *Facebook e l'abuso da sfruttamento al vaglio del Bundesgerichtshof,* in *Merc. Conc. Reg.*, 2, 2020, p.405.

[11] Cfr. A. Giannaccari, *op. cit.*, p. 405.

fossero fondate una «perdita di controllo» sui dati da parte degli utenti ed una violazione del diritto all'autodeterminazione informativa. I giudici di Düsseldorf, dunque, hanno ritenuto che gli iscritti alla piattaforma avessero scelto liberamente di prestare il consenso al trattamento dei dati. Difatti, se solo l'avessero voluto, avrebbero potuto non iscriversi ed astenersi così dall'utilizzo di servizi digitali che non potevano considerarsi necessari.

È evidente che il procedimento cautelare dell'Alta Corte ribalta il ragionamento dell'autorità garante della concorrenza. Se quest'ultima imputava a Meta la responsabilità per aver acquisito dati personali in violazione del diritto all'autodeterminazione informativa ed aver artatamente predisposto delle informative piuttosto vaghe e difficili da comprendere al fine di rafforzare il proprio potere di mercato, l'Alta Corte, invece, facendo sue le considerazioni sul *privacy paradox* [12], addebitava all'utente la responsabilità per l'uso improprio ed iniquo dei suoi dati da parte del gigante della rete [13]. Il Tribunale regionale, infatti, riteneva che, al livello controfattuale, non era stato dimostrato che, una volta concessa agli utenti la possibilità di graduare il livello delle informazioni, questi avrebbero scelto una soluzione maggiormente rispettosa della propria *privacy* [14].

La decisione cautelare è stata nuovamente impugnata, questa volta dal *Bundeskartellamt* dinanzi al *Bundesgerichthof*, la Suprema Corte Federale tedesca, che il 23 giugno 2020, contrariamente alle aspettative di Meta, ha sconfessato il ragionamento dell'Alta Corte di Düsseldorf e avallato la tesi dell'autorità garante della concorrenza tedesca. Tuttavia, a differenza di quest'ultima, i giudici del Karlsruhe non hanno ritenuto che fosse possibile equiparare una violazione del GDPR ad un illecito antitrust, ma hanno sostenuto che le condizioni contrattuali per l'uso dei servizi della piattaforma configurassero un abuso di posizione dominante, a prescindere dalla conformità o meno delle stesse alla normativa in materia di *data protection* [15]. Il non aver offerto, all'atto dell'iscrizione, opzioni diverse e non aver consentito l'accesso a soluzioni differenti di trattamento dei dati personali, ha significato ledere la capacità degli utenti di autodeterminarsi, di «[…] decidere essenzialmente da sé circa la cessione dei propri dati personali» [16], anche quando

---

[12] In tal senso, si vedano P.A. NORBERG-D.R. HORNE-D.A. HORNE, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors,* in *J. Consum. Aff.*, Vol. 41, 1, 2007, p.1 ss. Inoltre, S. ATHEY-C. CATALINI-C. TUCKER, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, in *Nber Working Paper Series*, no.23488, 2017, p. 2; I. ADJERID-E. PEER-A. ACQUISTI, *Beyond the privacy paradox: objective versus relative risk in privacy decision making*, in *MIS Quarterly*, Vol. 42, 2, June 2018; ed ancora T. VALLETTI, *Online Platforms and Market Power Part 3: The Role of Data and Privacy in Competition*, 18 October 2019, consultabili al seguente link *<https://docs.house.gov/meetings/JU/JU05/20191018/110098/HHRG-116-JU05-Wstate-VallettiT-20191018.pdf>*, (ultimo accesso 21 agosto 2023).

[13] In tal senso, cfr. C. OSTI-R. PARDOLESI, *L'antitrust ai tempi di Facebook,* in *Merc. conc. reg.,* 2, 2019, p. 206. In senso contrario, cfr. M.BOTTA-K. WIEDEMANN, *The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy the Regulatory Dilemma in the Facebook Odyssey,* in *Antitrust Bull.,* Vol.64, 3, 2019, p. 432 ss.

[14] Cfr. E. CREMONA, *Big Data, Big Troubles: come si controlla il potere dei dati*, in E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato,* Torino, Giappichelli, 2022, p.197.

[15] Come notato giustamente da F. LAVIOLA, *Il diritto all'autodeterminazione informativa tra concorrenza e data protection, in* E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato,* Giappichelli, Torino, 2022, pp. 41-42.

[16] Si veda G. SARTOR, *Tutela della personalità e normativa per la «protezione dei dati,* in *Informatica e diritto,* XII Annata, Vol. XII, 3, 1986, p. 95 ss.

tali informazioni «[…] siano entrate a far parte della disponibilità di un altro soggetto» [17].

Il ragionamento dei giudici della Suprema Corte si spinge anche oltre. Se un operatore, come Facebook, vanta una posizione di dominanza economica che gli consente di assumere col tempo un ruolo di primo piano nel mercato dell'informazione, equiparabile a quello dei media tradizionali [18] ed abilitante ai fini della partecipazione alla vita sociale degli utenti, è evidente che, sostiene il Karlsruhe, "[…] *can be bound by fundamental rights to a similar or equal extent as the state* [19]». Pertanto, gli intermediari digitali sono tenuti, in fase di trattamento, a garantire il rispetto del diritto fondamentale all'autodeterminazione informativa inteso quale «diritto a mantenere il controllo sulle proprie informazioni [20]», la cui definitiva costituzionalizzazione è stata sancita dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea [21]. Assicurare che le operazioni di trattamento dei dati personali siano rispettose dei principi di liceità, trasparenza, correttezza, finalità, minimizzazione, esattezza ed integrità significa non solo salvaguardare la capacità di autodeterminarsi e autodefinirsi di ogni singolo utente [22], ma anche restituire autonomia decisionale al consumatore digitale ed affrancarlo dallo stato di inerzia in cui viene indotto dall'asimmetria informativa con la piattaforma [23].

Tuttavia, non è questo l'atto finale della saga. La pronuncia è stata, infatti, rinviata in via pregiudiziale dall'Alta Corte di Düsseldorf alla Corte di Giustizia dell'Unione Europea [24].

---

[17] Cfr. S. RODOTÀ, *Tecnologie e Diritti*, cit., p. 107.

[18] Sulla equiparazione fra intermediari digitali ed editori cfr. M.R. ALLEGRI, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti,* in *Informatica e Diritto,* 1-2, 2017, p. 85 ss. A proposito di Facebook come *«the largest publishing company in the world»,* cfr. E. BELL-T. OWEN, *The Platform Press: How Silicon Valley Reengineered Journalism,* in *Tow Center for Digital Journalism,* 2017, p. 59. Sul ruolo svolto dalle piattaforme nel contesto dell'informazione e, nello specifico da Facebook come «strumento di cronaca» si vedano anche le opportune considerazioni di M. MONTI, *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione,* in *Federalismi, 24, 2017, p. 22 ss.* ed inoltre sul ruolo delle piattaforme digitali come «fonte di notizie e di conoscenza» si veda G. DE GREGORIO, *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?* in *MediaLaws,* 1, 2017, p.93.

[19] Si tratta della Decisione n. KVR 69/19 del 23 giugno 2020 adottata dal *Bundesgerichtshof* relativa al caso *Facebook v. Bundeskartellamt*, punto 105, consultabile in versione inglese al sito ufficiale del *Bundeskartellamt.*

[20] Si veda S. RODOTÀ, Tecnologie e diritti, cit., pp. 101-102.

[21] Si vedano O. POLLICINO-M. BASSINI, *Commento all'articolo 8 Carta dei Diritti fondamentali dell'Unione Europea*, in *Codice della Privacy e Data Protection*, R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), Giuffrè, Milano, 2021, p. 38 ed inoltre sulla equiparazione fra il diritto della protezione dei dati personali e il diritto all'autodeterminazione informativa si veda anche G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento Europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli Editore, 2017, p.6 nonché G. CERRINA FERONI, *I dati personali come oggetto di un diritto fondamentale*, in P. STANZIONE (a cura di), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Milano, Giappichelli, 2022, p. 70.

[22] In senso, si legga la Decisione n. KVR 69/19 del 23 giugno 2020, cit., punto 105.

[23] Si vedano le quanto mai opportune riflessioni di R. PODSZUN, *The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision*, in *SSRN*, April 10, 2023, consultabile al sito *SSRN*, p. 22.

[24] In sintesi, l'Alta Corte ha sollevato sei questioni pregiudiziali fra le quali meritano particolare approfondimento la prima con cui si domanda se esista o meno la possibilità per un'autorità garante della concorrenza di esaminare la conformità del comportamento di un'impresa a nor-

1.2. Le conclusioni dell'Avvocato Generale Rantos e la pronuncia della Corte di Giustizia dell'Unione Europea

La pronuncia della Corte di Giustizia è stata preceduta dal parere, non vincolante, del 22 settembre 2022 con il quale l'Avvocato Generale Athanasios Rantos ha analizzato nel dettaglio le sei questioni pregiudiziali oggetto della controversia. L'aspetto più interessante delle sue conclusioni si rinviene nella parte in cui sostiene che l'autorità della concorrenza tedesca non ha sanzionato la violazione del GDPR di per sé, ma l'ha valutata come elemento di prova da cui desumere l'esistenza dell'abuso di posizione dominante. Se ne ricava che un'*authority* antitrust può senz'altro constatare una violazione del GDPR, anche se ciò non rientra nelle sue specifiche competenze. Tuttavia, è nell'esercizio delle medesime che può, invece, verificare se la posizione di dominanza dell'impresa indagata è stata raggiunta per meriti imprenditoriali oppure ricorrendo a mezzi che consentano di conseguire un vantaggio competitivo illecito, a discapito di concorrenti e consumatori. Nella vicenda in esame, quindi, l'Ufficio Federale dei Cartelli si sarebbe avvalso dell'accertamento circa il mancato rispetto della normativa in materia di *data protection* per provare che le condizioni ed i termini di servizio della piattaforma hanno consentito al colosso del digitale di sfruttare in modo abusivo il proprio potere economico ed alterare, di conseguenza, la concorrenza [25].

Pare, dunque, farsi sempre più concreta, l'idea secondo cui la limitazione effettiva del potere economico dei guardiani dei mercati digitali possa scaturire da un'integrazione fra due normative, antitrust e *data protection* che, nonostante le diverse competenze e prerogative delle rispettive autorità garanti, potrebbero dimostrarsi affini e per nulla distanti sul piano degli obiettivi; anche se, da una prima analisi degli stessi, sembrerebbe il contrario. Questa terza via, per la regolazione dei mercati digitali, alternativa all'approccio *laissez-faire* e per molti aspetti complementare all'approccio *ex ante regulation* del *Digital Markets Act*, come si avrà modo di vedere, emerge in maniera evidente nella decisione della Corte di Giustizia dell'Unione Europea. Quest'ultima, terminata la fase orale del procedimento, ha deliberato, infatti, sulla domanda di pronuncia pregiudiziale oggetto di controversia del 4 luglio 2023.

È bene procedere con ordine ad analizzare, le questioni pregiudiziali sulle quali i giudici, riuniti in sezione plenaria, sono stati interpellati dal Tribunale regionale di Düsseldorf, precisando sin d'ora che verranno trattate con maggior dovizia di particolari quelle che sembra avvalorino l'idea della possibile integrazione tra il diritto antitrust e la *data protection* da parte dei giudici della Corte di Giustizia.

La prima questione è stata sollevata e trattata insieme alla settima perché entrambe sono di tipo procedurale. In primo luogo, l'Alta Corte domanda alla

---

me diverse da quelle del diritto della concorrenza, come il GDPR e, nel caso ciò sia possibile, valutare se una violazione della *privacy* possa costituire un importante indizio da cui desumere una distorsione della concorrenza. La terza con cui si chiede se il trattamento dei dati effettuato da Meta possa considerarsi legittimo anche laddove sia basato su basi giuridiche diverse dal consenso, infine la sesta volta ad accertare se l'esistenza di una posizione dominante possa costituire un elemento importante per determinare se il consenso sia stato prestato validamente. In tal senso, si veda CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza del 4 luglio 2023, causa C-252/21, *Meta v. Bundeskartellamt*, punto 35, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

[25] Si veda A. RANTOS, *Presse Release, Conclusioni dell'Avvocato Generale*, September 20, 2022, Case C-252/21, *Meta Platforms e a. v. Bundeskartellamt*, punto 21, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

Corte del Lussemburgo di chiarire se un'autorità nazionale garante della concorrenza sia competente ad accertare una violazione del GDPR nel corso di un'istruttoria antitrust avviata allo scopo di provare l'esistenza di una pratica commerciale anticoncorrenziale. L'interrogativo sorge spontaneo dato che, ai sensi dell'articolo 51 del GDPR, le uniche garanti dell'effettivo rispetto delle regole europee in materia di *privacy* sono le autorità di controllo nazionali allo scopo istituite presso ogni Stato Membro [26].

Il dilemma si rafforza quando nel ragionamento del Tribunale federale si fa strada la settima questione. Qualora un'*authority* antitrust fosse competente ad occuparsi di tale accertamento, occorrerebbe considerare cosa accadrebbe se una contestazione simile fosse già stata sottoposta all'esame dell'autorità capofila competente, ai sensi dell'articolo 56, par. 1, del GDPR, per la gestione dei trattamenti dei dati personali a carattere transfrontaliero, operando in deroga al criterio dell'imputazione territoriale di cui all'articolo 55, par. 1, del GDPR [27].

È evidente che la risoluzione del primo interrogativo, cui è inscindibilmente legato il secondo, spinge la Corte di Giustizia a pronunciarsi su una questione che, solo in apparenza, può essere intesa in termini strettamente procedurali in quanto, a ben vedere, produce effetti di tipo sostanziale. Ad avviso della Corte, un'autorità garante della concorrenza, nel corso di un'indagine relativa alla sussistenza o meno di un abuso di posizione dominante, può valutare se una condotta anticoncorrenziale posta in essere dalla società indagata comporti una violazione del GDPR, a patto che da un lato «tale constatazione sia necessaria per accertare l'esistenza di un tale abuso [28]» e dall'altro venga rispettato l'obbligo di leale cooperazione con le autorità di controllo.

La prima condizione si fonda su un principio di realtà. Negare all'autorità garante della concorrenza di considerare, nel corso delle proprie istruttorie, la conformità o meno del comportamento dell'impresa in posizione dominante alle norme in materia di protezione dei dati personali vorrebbe dire negare che, nel contesto attuale dell'economia digitale, accesso ed elaborazione dei dati costituiscono la *condicio sine qua non* per permettere alle grandi piattaforme ed anche alle piccole e medie imprese, non solo di essere ora competitive, ma anche restarlo in futuro. Si badi bene, nella decisione non si sta affermando che un'autorità di controllo può essere sostituita da un'autorità della concorrenza nell'acclarare se vi sia stata una violazione del regolamento UE 2016/679, perché solo una *Data Protection Authority* è deputata a vigilare sulla corretta applicazione delle disposizioni del regolamento suddetto [29]. Al contrario, tale valutazione può effettuarsi solo quando essa sia funzionale a dimostrare che dalla continua e costante violazione della normativa in materia di protezione dei dati personali sia possibile desumere in giudizio l'esistenza di

---

[26] Cfr. Considerando 123 del Regolamento UE 679/2016.

[27] Cfr. I.M. ALAGNA *et al., Commento all'articolo 55 del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016,* n.679, in L. BOLOGNINI-E. PELINO (a cura di), *Codice della Disciplina della Privacy,* Giuffrè, Milano, 2019, p. 354 ss.

[28] Cfr. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza del 4 luglio 2023, causa C-252/21, *Meta v. Bundeskartellamt*, punto 62, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

[29] Cfr. E. GUARDIGLI, *Le Autorità di Controllo: dalla Direttiva 95/46/CE al Regolamento n.679/2016*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE N.2016/679 e d.lgs. 10 agosto 2018, n.101*, Zanichelli Editore, Bologna, 2019, p. 665 ss.

un abuso di posizione dominante [30]. Si tratta, quindi, di un accertamento abbastanza limitato e circoscritto.

La seconda condizione presuppone che la garanzia di una coerente applicazione del regolamento UE in materia di protezione dei dati personali passi per il rispetto del principio di leale cooperazione, così come sancito all'articolo 4, par. 3, TUE. Considerato in dottrina come uno dei capisaldi dell'*acquis* comunitario [31], viene elaborato dalla giurisprudenza della Corte di Giustizia a partire dall'articolo 10 del Trattato sulla Comunità europea [32], e poi successivamente abrogato dal Trattato di Lisbona [33]. Contestualmente all'abrogazione, la norma è stata sostituita con l'art. 4, par. 3, del TUE che ha innalzato il precetto della leale cooperazione a principio generale dell'intero sistema del diritto eurounitario [34].

Nella pronuncia della Corte di Giustizia, il principio della leale cooperazione viene in rilievo non tanto per l'impatto che ha nell'assicurare la salvaguardia dell'«equilibrio istituzionale [35]», quanto nel garantire una coerente ed uniforme applicazione delle norme eurounitarie in materia di protezione dei dati personali. Nel caso del GDPR, infatti, l'obbligo di leale collaborazione si esplica nella previsione di meccanismi di "cooperazione" o "coordinamento" delle funzioni delle autorità di controllo che permette loro di avere un approccio coordinato nella soluzione di un caso, evitando, di conseguenza, l'applicazione frammentata delle norme eurounitarie fra gli Stati Membri [36].

---

[30] Sul valore di accertamento incidentale di una violazione del GDPR compiuta nell'ambito della constatazione di un abuso di posizione dominante da parte di un'autorità garante della concorrenza si veda G. D'IPPOLITO, *Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata* in *Media-Laws,* 2, 2023, p. 328 ss.

[31] In tal senso, gli studiosi P. DE PASQUALE-M. CARTABIA-C. IANNONE, *Art. 4 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea,* Giuffrè, Milano, 2014, p. 28. Fra i molti, si vedano anche F. BATTAGLIA, *Il principio di leale cooperazione nel Trattato di Lisbona. Una riflessione sulle vicende legate al recesso del Regno Unito dall'Unione europea*, in *Federalismi*, 19, 2020, p. 24; A. DIRRI, *La Corte di Giustizia torna sul meccanismo di ricollocazione dei migranti tra rivendicazioni identitarie e tenuta dei valori fondanti dell'Unione europea*, in *Osservatorio AIC*, 5, 2020, p. 232 nonché G. CAGGIANO*, Il consolidamento della disciplina delle misure di esecuzione e della comitologia a Trattato invariato*, in *Studi sull'Integrazione Europea*, 3, 2006, p. 508; nonché F. CASOLARI, *The Principle of Loyal Co-Operation: A 'Master Key' for EU External Representation?*, in S. BLOCKMANS-R.A. WESSEL (eds.), *Principles and Practices of EU External Representation – Cleer Working Papers*, 5, 2012 p.13.

[32] In tal senso, cfr. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, ordinanza 13 luglio 1990, causa C-2/88, *Zwartveld e A.*, punto 17, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

[33] Cfr. U. VILLANI, Istituzioni di Diritto dell'Unione Europea, 2^ed., Cacucci Editore, Bari, p.85.

[34] A tal riguardo, si veda il dettato normativo dell'arti. 4, par.3, del TUE a mente del quale: «[…] In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati». Cfr. B. GUASTAFERRO, *Sincere Cooperation and Respect for National Identities: The Unitary and the Pluralist Twists of the European integration process*, in *New-Federalism*, *Working Papers Series*, 2, 2015, pp.3-4; inoltre si veda anche CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza 6 marzo 2018, causa C-284/16, *Slowakische Republik contro Achmea BV*, punto 34.

[35] Cfr. F. CASOLARI, *Leale cooperazione tra Stati Membri e Unione Europea. Studio della partecipazione all'Unione al tempo delle crisi*, Editoriale Scientifica, Napoli, 2020, p.28; inoltre, P. KOUTRAKOS, *Institutional Balance and Sincere Cooperation in Treaty-Making under EU Law*, in *ICLQ*, Vol. 68, 1, 2019, p. 28.

[36]A tal proposito, si veda anche l'ultima parte del Considerando 123 del GDPR ed inoltre, F. PARODO, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali*, in *Federalismi*, 25, 2021, p. 132 ss.

È bene sottolineare che, ai paragrafi 42 e 43 della pronuncia, i giudici del Lussemburgo hanno evidenziato giustamente che non vi sono norme del regolamento o strumenti del diritto eurounitario che aprono alla cooperazione fra le due autorità, ma è anche vero che non ve ne sono neppure altre che la escludono espressamente. La previsione di una possibile cooperazione pare così praticabile in virtù del rispetto del principio di leale cooperazione sancito all'art. 4, par. 3 del TUE [37]. Al fine di evitare eventuali divergenze, dovranno verificare se il comportamento indagato sia già stato deciso dal garante nazionale della protezione dei dati personali, da un'autorità capofila o dalla stessa Corte di Giustizia. Se così fosse, sarebbe necessario conformarsi a quanto già precedentemente statuito [38].

Dopo aver risposto alla seconda domanda pregiudiziale, la Corte di Giustizia, prosegue nell'analisi delle questioni rimanenti, occupandosi dalla terza alla quinta della liceità o meno del trattamento dei dati personali, laddove siano acquisiti in assenza di consenso. Le prime due della "triade" interrogano i giudici del Lussemburgo sulla concreta possibilità per un'impresa come Meta di invocare o la necessità per l'esecuzione di un contratto ai sensi dell'articolo 6, par. 1, lett. b), del GDPR o la tutela di legittimi interessi di cui all'articolo 6, par. 1, lett. f), del GDPR, quali basi giuridiche per trattare dati. L'ultima, la quinta, chiede, invece, alla Corte di Giustizia se sia possibile invocare per liceità del trattamento le ulteriori basi giuridiche previste all'art. 6 del regolamento, fra le quali sono rinvenibili l'obbligo legale di cui alla lettera c), la salvaguardia degli interessi vitali degli interessati di cui alla lettera d) ed infine, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

La questione del legittimo interesse come base giuridica in grado di legittimare il trattamento dei dati personali per finalità di pubblicità personalizzata verrà affrontata successivamente perché merita, per l'importanza che assume nel contesto dei mercati digitali, uno specifico approfondimento [39]. Con riguardo, invece, all'esecuzione di un contratto quale condizione legittimante il trattamento, la Corte di Giustizia, accogliendo fra l'altro le conclusioni dell'Avvocato Generale Rantos, ha ribadito che tale base giuridica può essere usata solo quando sia «oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere

---

[37] Sul punto, si vedano: CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza del 7 novembre 2013, causa C-518-/11, *UPC Nederland BV v. Gemeente Hilversum*, punto 59, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea ed inoltre la recente pronuncia della CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza del 1 agosto 2022, causa C-14/21 e C-15/21, *Sea Watch v. Ministero delle Infrastrutture e dei trasporti et al.*, punto 156, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

[38] Si ritiene opportuno spiegare brevemente la successiva questione pregiudiziale attinente più che altro alla natura giuridica dei dati personali raccolti dalla società californiana. I giudici sostengono che si tratti di categorie particolari di dati. Se così fosse, a detta della Corte, non sarebbe, comunque, applicabile la deroga al divieto di trattamento prevista alla lettera *e)* del secondo paragrafo dell'articolo 9 a mente della quale il trattamento di categorie particolari di dati può essere ammesso solo qualora riguardi «[…] dati personali resi manifestamente pubblici dall'interessato». La mera consultazione di siti terzi o di applicazioni, anche se collegati a quelli dell'*account* Facebook per la creazione di super-profili, non può essere considerata espressione della volontà dell'utente di rendere manifestamente pubblici i suoi dati, salvo il caso in cui gli utenti abbiano chiaramente espresso la volontà di renderli accessibili ad un numero illimitato di persone. Su questo ultimo aspetto, cfr. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, causa C-252/21, *Meta v. Bundeskartellamt*, cit., punto 82.

[39] Si rinvia al paragrafo 3 del presente contributo.

conseguito in assenza di tale trattamento [40]». Se ne deduce che non potrebbe, invece, essere usata da Meta o altri giganti del digitale per giustificare il trattamento dei dati personali per finalità di profilazione o pubblicità personalizzata perché in assenza di tali finalità il *social network* tratterebbe allo stesso modo i dati personali dei propri iscritti e sarebbe in grado di offrire loro gli stessi servizi digitali.

Fallaci, invece, si rivelano le giustificazioni dedotte a supporto della propria tesi difensiva da Meta secondo le quali sono da considerarsi indispensabili per l'esecuzione del contratto la personalizzazione dei contenuti e l'utilizzo omogeno e fluido dei servizi offerti dalla piattaforma all'interno del proprio ecosistema digitale. I giudici, pur non negando l'utilità della raccolta dati nella personalizzazione dei contenuti, non la ritengono necessaria perché l'esperienza *online* potrebbe essere adattata agli interessi dell'utente mediante soluzioni alternative che non implichino necessariamente un uso improprio della base giuridica di cui alla lettera *b)* dell'articolo 6 del GDPR. Inoltre, la Corte la esclude categoricamente in quanto la creazione di un *account* Facebook consente all'utente di usare i diversi servizi e prodotti del gruppo Meta in modo indipendente gli uni dagli altri.

Rimane, la quinta questione, con la quale la Corte di Giustizia è stata chiamata a pronunciarsi sulla legittimità di ulteriori basi giuridiche. Le condizioni di liceità di cui alle lettere *c)* ed *e)* relative all'obbligo legale e all'esecuzione di un compito di interesse pubblico, vengono trattate in modo congiunto dalla decisione proprio perché presentano aspetti comuni [41]. Tuttavia, i giudici hanno ritenuto che gli interessi indicati dal Tribunale federale – fra i quali lo svolgimento di ricerche a beneficio della società nonché la promozione di protezione, integrità e sicurezza con riguardo alla lettera *e)* dell'articolo 6 del GDPR – non siano corroborati da elementi in grado di provare la legittimità di tali basi giuridiche anche alla luce delle previsioni di cui al paragrafo 3 della medesima disposizione. Pertanto, la Corte ne ha rimesso la valutazione al giudice del rinvio.

Da analizzare, poi l'ulteriore condizione legittimante riferita alla salvaguardia di un interesse vitale. A tal proposito, la Corte esclude che possa essere ritenuto lecito il trattamento effettuato sulla base di tale presupposto in quanto sarebbero rinvenibili nessuna delle ipotesi in cui, secondo il Considerando 46 del regolamento, tutelare un interesse vitale equivale a proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Meta, dunque, non avrebbe trattato i dati personali degli utenti per prevenire minacce gravi alla salute ed all'incolumità dell'interessato o di un terzo oppure per tenere sotto controllo epidemie, emergenze sanitarie ed infine prevenire calamità naturali [42]. I giudici hanno così ritenuto inesistenti i presupposti per considerare lecito il trattamento fondato sulla salvaguardia dell'interesse vitale [43].

L'ultima, ma non meno importante, fra le questioni pregiudiziali sollevate

---

[40] Cfr. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, causa C-252/21, *Meta v. Bundeskartellamt*, 4 luglio 2023, cit., punto 125.

[41] Con riguardo alla comunanza di intenzioni delle due condizioni di liceità, si veda: D. POLETTI, *Commento all'articolo 6 del Regolamento generale sulla protezione dei dati personali*, in *Codice della Privacy e Data Protection*, R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), Giuffrè, Milano, 2021, p. 199.

[42] Sul punto si vedano le considerazioni del GRUPPO DI LAVORO ARTICOLO 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014, p. 24, consultabili al sito ufficiale del Gruppo di lavoro Articolo 29.

[43] Ivi, punti 135-139.

dal Tribunale federale è la sesta. La Corte di Giustizia viene chiamata a risolvere i dubbi del Tribunale federale in merito alla validità, alla luce dell'articolo 6, par. 1, comma 1, lett. a) e dell'art. 9, par. 2, lett. a) del GDPR, del consenso prestato a un operatore che detiene una posizione dominante sul mercato nazionale dei *social network* online, cercando, nello specifico, di comprendere se tale consenso possa dirsi effettivamente libero.

Prescindendo ora dalle specifiche delle questioni che saranno trattate a tempo debito nel corso del lavoro, pare doversi sottolineare che nel rispondere alla sesta questione, la Corte di Giustizia offra due spunti di riflessione molto importanti. Da un lato, evidenzia che la posizione dominante, pur non impedendo di per sé la prestazione di un consenso valido, può essere un chiaro indice da cui desumere se il consenso sia stato effettivamente prestato liberamente. Dall'altro, lascia al giudice del rinvio stabilire se sia opportuno prevedere una prestazione del consenso, per così dire, "granulare" di modo che siano liberi gli utenti di prestare un consenso autonomo e specifico a seconda dei dati oggetto di trattamento. Il che significa ammettere la possibilità di progettare interfacce di programmazione in cui si chieda all'utente di prestare un consenso separato per i dati raccolti *off-Facebook* tenendolo così ben distinto e separato da quello che poi verrebbe prestato con riguardo ai dati raccolti tracciando l'attività dell'utente all'interno della piattaforma [44].

Le conclusioni, dell'Avvocato Generale Rantos prima e quelle della Corte di Giustizia dell'Unione Europea poi, offrono una chiara indicazione ai regolatori sulla modalità con la quale *enforcement* antitrust e tutela dei dati personali possono cooperare fra di loro per evitare che poche grandi società si contendano il controllo dell'intero mercato *data-driven*. Nelle pagine che seguiranno si avrà modo di comprendere come sia possibile per antitrust e *data protection* muoversi all'unisono nella limitazione dell'*intermediation power* e quale sia il punto di intersezione che consente ad entrambe le normative di poterlo fare.

2. Integrazione fra diritto antitrust e *data protection*: si può fare

Dalle argomentazioni della Corte di Giustizia precedentemente esaminate si possono trarre alcune considerazioni utili sull'integrazione fra la disciplina del diritto della concorrenza e la protezione dei dati personali. Una premessa, tuttavia, è d'obbligo. In letteratura, si sono ravvisate, almeno sino ad ora, più opinioni contrarie che favorevoli ad ammettere che un coordinamento fra le due discipline fosse concretamente possibile. La ragione è da ascriversi agli obiettivi che entrambe le normative paiono perseguire. È certo, infatti, che proteggere il diritto al controllo sul flusso informativo e garantire la sicurezza del trattamento dei dati personali non siano obiettivi propri del diritto della concorrenza come, allo stesso modo, è ovvio che assicurare il buon funzionamento del mercato mediante la salvaguardia del processo competitivo non lo sia della disciplina in materia di protezione dei dati personali. L'idea della assoluta inconciliabilità fra *enforcement* antitrust e tutela dei dati personali non è diffusa solo fra numerosi studiosi ed esperti di diritto della concorrenza, ma anche fra i medesimi regolatori che in un primo momento non hanno valutato positiva-

[44] *Ivi*, punto 151.

mente l'ipotesi di usare strumenti giuridici propri del diritto antitrust per risolvere questioni legate alla violazione della *privacy* [45]. Si pensi all'allora Commissario Europeo della Concorrenza Margrete Vestager che, dinanzi alla tesi dell'integrazione, rifiutò nel 2016 categoricamente l'idea. Nel discorso introduttivo della conferenza *Digital Life Design* tenutasi a Monaco di Baviera in quello stesso anno, intervenendo in merito alla questione, si esprimeva in questo modo: «[…] *So I don't think we need to look to competition enforcement to fix privacy problems*» [46]. Ebbene, in queste parole, come in quelle pronunciate circa quattro anni più tardi a seguito dell'approvazione dell'operazione concentrativa *Google/Fit* [47], è chiaramente rinvenibile la posizione sull'opportunità di far cooperare insieme le due normative non solo del Commissario con delega alla concorrenza, ma anche della stessa Commissione Europea [48].

La contrarietà espressa all'epoca da entrambi era dovuta all'adesione da parte dell'*enforcement* antitrust europeo alle teorie della corrente di pensiero neoliberale *Chicago School* [49]. I capisaldi dell'approccio prettamente economico elaborato dalla scuola americana che, più delle altre, ha avuto negli ultimi quarant'anni un impatto notevole sulla politica economia americana, divenendo col tempo la «culla del neoliberismo» per usare le parole dell'economista Giocoli [50], possono essere riassunti in due concetti che gli studiosi di questa dottrina ripetono a mo' di mantra: la salvaguardia del «*consumer welfare*» [51] e l'efficiente allocazione delle risorse [52]. Prima che facesse la sua comparsa il pensiero neoliberista, la dottrina economica prevalente – la c.d. Scuola di Harvard – riteneva che fine ultimo della concorrenza fosse assicurare mercati aperti e contendibili, il che significava non solo salvaguardarne il buon funzionamento, ma tutelare anche la legittimazione stessa del sistema democratico [53].

---

[45] Sul fronte degli studiosi con posizioni contrarie si vedano fra le molte quelle di R. PARDOLESI-R. VAN DEN BERGH-F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit., p.532 ss., nello stesso senso R. PARDOLESI, *Piattaforme digitali, poteri privati e concorrenza*, in *Diritto Pubblico*, 3, 2021, p. 947 ss. ed inoltre G. COLANGELO-M. MAGGIOLINO, *Data accumulation and the privacy – antitrust interface: insights from the Facebook Case*, in *Int. Data Priv. Law.*, Vol. 8, 3, 2018, p. 234 ss.

[46] Cfr. M. VESTAGER, *Competition in a Big Data World*, consultabile al sito European Commission.

[47] Cfr. A. WHITE-H. ALI, *Google-Fitbit Probe Isn't for Data Watchdogs*, *Vestager Says*, in *Bloomberg*, 25 february 2020, consultabile al sito ufficiale Bloomberg, (ultimo accesso: 7 settembre 2023).

[48] Si pensi al caso *Google/DoubleClick*. Nello specifico, per approfondire si veda COMMISSIONE EUROPEA, 11 marzo 2008, case no. COMP/M.4731, *Google/ DoubleClick*, in *Official Journal of the European Union*, par. 368, consultabile al sito della Gazzetta ufficiale dell'Unione Europea.

[49] Cfr. A. GERBRANDY, *Rethinking Competition Law within the European Economic Constitution*, in *J. Common Market Stud.*, Vol. 57, 1, 2019, p. 130.

[50] Cfr. N. GIOCOLI, *La Scuola di Chicago*, IBL Libri, Milano, 2023, p.8.

[51] Nello specifico, cfr. R.H. BORK, *The Antitrust Paradox: A Policy at War with Itself*, Harper Colophon Books, 1978, p. 90. Lo studioso sostiene che la tutela del benessere del consumatore possa essere raggiunta "[…] *by requiring that any lawful products, whether skis or snowmobiles, be produced and sold under conditions most favourable to consumers*» ed ancora R. H. BORK, *Legislative Intent and the Policy of the Sherman Act,* in *J. Law Econ.*, Vol. 9, 1966, p. 26 ss.

[52] Per approfondire i concetti di efficienza allocativa e produttiva paiono esemplificative le riflessioni di E.M. FOX, *The efficiency paradox*, in R. PITOSKY (eds), *How the Chicago School Overshot the Mark: The Effect of Conservative Economic Analysis on U.S. Antitrust*, Oxford University Press, Oxford UK, 2008, p. 78.

[53] A tal proposito, pare opportuno ricordare il caso *Northern Pacific Railway Co. v. United*

Queste idee si rinvengono, seppur in parte, anche fra gli studiosi della scuola ordoliberale europea che escludevano che il mercato potesse essere "abbandonato" a sé stesso perché lo si sarebbe reso "terra di nessuno". Preferibile, dunque, riconoscere un margine di intervento ai poteri pubblici purché però fossero norme statali di rango costituzionale ad arginare eventuali "derive" del potere economico [54].

Questi principi influenzarono la disciplina della concorrenza eurounitaria sino agli anni '90 del '900 quando la Commissione Europea abbracciò la fede neoliberista di matrice chicaghiana e propose di aggiornare gli strumenti giuridici del diritto antitrust eurounitario facendo del *consumer welfare standard,* l'unico fine delle politiche di concorrenza [55]. Tuttavia, se l'esecutivo ha abbandonato l'approccio formalistico proposto a Friburgo per il modello economico neoliberale, la Corte di Giustizia dell'Unione Europea ne ha, invece, preso le distanze [56] continuando a ritenere che, nel mercato dovesse contare la salvaguardia della sua struttura pluralistica piuttosto che l'efficienza economica ed il benessere collettivo del consumatore.

È evidente che la Corte di Giustizia attribuisce alle categorie tradizionali del diritto della concorrenza eurounitario il compito di raggiungere uno scopo molto più ampio rispetto a quello previsto dai sostenitori del modello neoliberale: uno scopo che, in definitiva, consente all'antitrust di perseguire altri ed ulteriori fini rispetto alla mera tutela dell'efficienza economica [57].

Per tale ragione, sembra più che naturale che la decisione del 4 luglio abbia guardato con favore al riconoscimento della possibile integrazione fra due normative perché la Corte di Giustizia dell'Unione Europea, da sempre restia a considerare quale oggetto del diritto antitrust solo interessi prettamente economici, ha ravvisato nella tutela del consumatore digitale il loro punto di intersezione.

States del 1958 in cui il giudice federale, facendo proprie le idee della teoria strutturalista, attribuiva alla prima legge antimonopolio della storia, il perseguimento di fini ulteriori rispetto alla mera tutela del buon funzionamento del mercato: «*The Sherman Act … rests on the premise that the unrestrained interaction of competitive forces will yield the best allocation of our economic resources, the lowest prices, the highest quality and the greatest material progress, while at the time providing an environment conducive to the preservation of our democratic political and social institutions*».

[54] Per una corretta ed approfondita ricostruzione delle teorie della Scuola di Friburgo si veda, G. CONTALDI, *Diritto Europeo dell'Economia*, Giappichelli, Torino, 2019, pp. 6-8.

[55] Cfr. M. MONTI, *European Competition for the 21st Century*, in *Fordham Int. Law J.*, Vol. 24, 5, 2000, pp. 1604-1605 ed inoltre cfr. F.V OGELAAR, *Modernisation of EC competition law, economy and horizontal cooperation between undertakings*, in *Inter Econ*, Vol. 37,1, 2002, p. 20.

[56] Si veda a tal proposito CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, 23 novembre 2006, C-238/05, *Asnef-Equifax Servicios de Información sobre Solvencia y Crédito, SL v. Administración del Estado*, par. 56, consultabile al sito ufficiale della Corte di Giustizia dell'Unione Europea.

[57] Sui fini ulteriori che il diritto antitrust è in grado di perseguire, al di là dell'efficienza economica e del *consumer welfare*, si veda quanto rilevato efficacemente da F. BILANCIA, *Le trasformazioni dei rapporti tra Unione europea e Stati membri negli assetti economico-finanziari di fronte alla crisi pandemica*, in *Diritto Pubblico*, 1, 2021, p.63. L'Autore sottolinea giustamente che gli studiosi del diritto antitrust dovrebbero tener conto del fatto che le politiche della concorrenza possono perseguire anche finalità di tipo sociale. Inoltre, si veda anche R. PITOFSKY, *The political Content of Antitrust*, in *U. PA. L. REV.*, 1979, Vol. 127, p. 1051.

2.1. La violazione della *privacy* quale indice di un abuso di posizione dominante

Per comprendere in quale modo una violazione della normativa in materia di *data protection* possa costituire un «importante indizio», per usare le considerazioni della Corte, da cui desumere una distorsione delle regole della concorrenza, sembra opportuno delineare quale sia stato il "percorso" che la protezione dei dati personali ha dovuto compiere per assumere piena legittimità in un contesto in cui, per diverso tempo, la normativa antitrust si è avvalsa del prezzo quale parametro concorrenziale esclusivo.

È noto che al fine di raggiungere una determinata posizione di potere economico le imprese debbano competere fra di loro tenendo in considerazione una serie di fattori di natura quantitativa o qualitativa [58]. Se il prezzo costituisce il parametro quantitativo per eccellenza sul quale misurarsi nel mercato, fra le dimensioni concorrenziali di tipo qualitativo, invece, assumono importanza la facilità d'uso, il livello di sicurezza, il grado di innovazione del prodotto o di un determinato servizio, compreso anche più di recente il livello di protezione dei dati personali. La qualità, dunque, tende ad avere non un valore di secondo piano rispetto al prezzo, bensì equivalente ad esso.

Questo ragionamento, valido innanzitutto nel contesto dei mercati tradizionali, lo è ancora di più nel contesto economico dei mercati *zero-price* in cui sono i dati ad essere oggetto di controprestazione economica [59]. Pare evidente che le imprese dei mercati *data-driven* competano soprattutto sulla base di dimensioni concorrenziali prettamente qualitative, fra le quali anche la protezione dei dati personali [60]. Tale considerazione è tanto più vera se la si giudica a partire dalla prospettiva delle imprese concorrenti [61].

Lo dimostra la recente diatriba sul tema della tutela dei dati personali che vede confrontarsi fra loro due dei più importanti colossi del web, Facebook ed Apple [62]. Oggetto del contendere è l'applicativo *App Tracking Transparency* (in

---

[58] Cfr. A. PAPPALARDO, *Il diritto della concorrenza dell'Unione Europea*, 2^ed., Utet, Torino, 2018, pp.11-14.

[59] Sul valore economico dei dati cfr. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *Governance of/through Big Data*, Vol. II, Roma Tre Press, Roma, 2023, p. 660 ss. inoltre si vedano le corrette considerazioni di S. FRANCA, *L'intreccio fra disciplina delle pratiche commerciali scorrette e normativa in tema di protezione dei dati personali: il caso Facebook approda al Consiglio di Stato*, in questa *Rivista*, 2, 2021, p. 366 ss. Cfr. O' DONOGHUE-A. PADILLA, *The Law and Economics of Article 102 TFUE*, 3^ed., Hart Publishing, 2020, Oxford, p. 78, p.1095 ss.

[60] Cfr. MAURICE E. STUCKE-ALLEN P. GRUNES, *No mistake about it: the important role of antitrust in the era of Big Data*, in *SSNR*, april 2015, p.2, consultabile al sito Social Science Research Network (ultimo accesso: 9 settembre 2023). Sul punto, cfr. D.D. SOKOL-R COMERFORD, *Antitrust and Regulating Big Data*, in *Geo. Mason L. Rev*, Vol. 23, 5, 2016, p. 1041. Gli Autori parlano di «*data gap*» concependolo l'asimmetria informativa come un *gap* di tipo qualitativo fra le grandi piattaforme ed i loro concorrenti.

[61] Sul punto cfr. D.D. SOKOL-R COMERFORD, *Antitrust and Regulating Big Data*, in *Geo. Mason L. Rev*, Vol. 23, 5, 2016, p. 1041. Gli Autori parlano di «*data gap*» concependolo l'asimmetria informativa come un *gap* di tipo qualitativo fra le grandi piattaforme ed i loro concorrenti.

[62] Cfr. M. ISAAC-J. NICAS, *Breaking Point: How Mark Zuckerberg and Tim Cook Became Foes*, in *The New York Time*, April 26, 2021, consultabile al sito ufficiale The New York Time (ultimo accesso: 10 settembre 2023) ed inoltre si veda anche THE ECONOMIST, *Apple's long-awaited privacy policy kicks Facebook where it hurts*, in *The Economist*, February 6, 2021, consultabile al sito The Economist.

seguito, *app* ATT) che, citando testualmente dal sito ufficiale della società californiana, «[…] *consente di scegliere se un'app può tracciare le tue attività sulle app e i siti web di altre aziende per scopi pubblicitari o per condividerli con i data broker*» [63]. Secondo Apple, questo sistema, progettato per obbligare gli sviluppatori di applicazioni a richiedere previamente il consenso per tracciare l'attività digitale durante l'utilizzo dell'*app*, restituirebbe agli utenti il controllo sulla circolazione dei propri dati personali, salvaguardandoli dalla profilazione della piattaforma. L'utente potrebbe decidere in modo completamente autonomo se dare il proprio consenso al tracciamento oppure se rifiutarlo. Tuttavia, due cose sembrano sfuggire all'attenzione dell'amministratore delegato della società Tim Cook, strenuo sostenitore della nuova funzionalità [64].

In primo luogo, omette di considerare che Apple rimane pur sempre l'unica che può continuare a tracciare e monitorare in modo regolare e sistematico i propri utenti, senza chiedere loro il previo consenso al tracciamento. L'obbligo di disattivare il monitoraggio per impostazione predefinita rimane valido solo per le applicazioni degli sviluppatori terzi che in questo modo perdono un gran numero di dati da usare per profilare gli utenti per ragioni pubblicitarie. Il fine che l'ecosistema digitale vuol perseguire è, dunque, il medesimo: conseguire, per il tramite della raccolta ed il processamento dei dati, un vantaggio competitivo illecito a discapito dei propri *competitors*. Si tratta di un'ipotesi piuttosto evidente di *self-preferencing*, in cui, pare potersi sostenere, l'unico scopo della società californiana consiste nel preservare la posizione di dominanza economica conseguita nel mercato della pubblicità online col tempo [65].

In secondo luogo, l'introduzione dell'applicativo ATT non solo ha come effetto quello di escludere dal tracciamento degli utenti i concorrenti indiretti della società come gli sviluppatori delle *apps* che rivendono i propri applicativi sul negozio online di proprietà di Apple, ma anche quei concorrenti che competono direttamente con l'ecosistema nel mercato della pubblicità digitale come Meta. Restituire agli utenti la possibilità di scegliere se, concedere o meno alle *apps* di proprietà di operatori terzi l'autorizzazione al monitoraggio, vuol dire, in realtà, "colpire al cuore" un modello di *business* che sulla pubblicità mirata fonda la maggior parte dei propri introiti al solo fine estrometterla dal mercato ed occuparne la posizione di dominio economico.

Non pare possa, quindi, negarsi che la protezione dei dati personali sia divenuta col tempo un fattore qualitativo pro-concorrenziale sul quale i giganti del digitale sono chiamati a competere sempre più spesso nei mercati *data-driven*. Tuttavia, l'idea che la *privacy* potesse costituire un parametro qualitati-

---

[63] Si tenga presente che l'applicazione ATT è stata oggetto di un procedimento istruttorio aperto dall'*Autoritè de la Concurrence*, deciso il 17 marzo 2021 con il rigetto del ricorso presentato ad ottobre 2020 da un gruppo di associazioni che raccolgono media, agenzie di *marketing*, aziende informatiche ed editori. Per approfondire si rinvia a AUTORITÈ DE LA CONCURRENCE, *Targeted advertising/Apple's implementation of the ATT framework*, *Decision 21-D-07*, 17 March 2021, consultabile al sito istituzionale Autoritè de la Concurrence. Analoga la vicenda quella che ha visto l'AGCM avviare l'istruttoria sempre nei riguardi di Apple cfr. AGCM, n. A561, 11 maggio 2023, *Apple Inc.,* par. 46, consultabile al sito ufficiale dell'AGCM.

[64] Di estremo rilievo l'intervista nella quale Tim Cook annuncia il lancio della nuova funzionalità cfr. K. SWISHER, *Apple's C.E.O. is making very different choices from Mark Zuckerberg*, in *The New York Time*, April 5, 2021, l'intervista può essere ascoltata con la relativa trascrizione del contenuto al sito ufficiale de *The New York Time*, (ultimo accesso: 10 settembre 2023).

[65] In tal senso, meritevoli di considerazione le riflessioni sulla vicenda dello studioso K. WIEDEMANN, *Data protection and Competition Law enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary?* in *ICC*, Vol. 52, 2021, p. 922.

vo della concorrenza alternativo al prezzo ha incontrato molti ostacoli. Da un lato, l'influenza del pensiero neoliberale che ha impedito alle autorità garanti della concorrenza di ammettere che, nell'ambito dell'economia digitale, la *theory of harm* potesse riguardare anche l'accertamento di pregiudizi di matrice anche non strettamente economica [66], dall'altro il carattere puramente soggettivo che si accompagna ai criteri prettamente qualitativi. È ovvio che le preferenze circa il livello di tutela della protezione dei dati personali siano estremamente variabili nell'ambiente digitale perché se un consumatore può attribuire al rispetto della *privacy* un valore notevole, un altro, invece, potrebbe dimostrarsi totalmente disinteressato al livello di protezione offerto all'interno del mercato digitale. L'estrema discrezionalità con la quale si valuta la *privacy* presso i consumatori la rende un parametro concorrenziale non facilmente misurabile [67], specie all'atto della definizione del mercato rilevante. Tradizionalmente l'accertamento del mercato del prodotto rilevante che passa per la definizione del grado di sostituibilità fra due prodotti con caratteristiche simili, viene condotto avendo come punto di riferimento il c.d. *test* econometrico del monopolista perfetto in cui il prezzo, a differenza di parametri qualitativi, è precisamente determinabile [68].

Questi erano i dubbi che, al di là dell'approccio neoliberale, rendevano i regolatori e gli accademici [69] piuttosto titubanti nel riconoscere ad un eventuale peggioramento della *privacy* lo stesso valore che, nella teoria del danno concorrenziale applicata ai mercati tradizionali, aveva l'imposizione di un prezzo sovra-competitivo.

La Commissione Europea affrontò il tema in modo approfondito in due occasioni. Nel 2014, quando si trovò a dover valutare l'operazione concentrativa *Facebook/WhatApp* e successivamente nel 2016 con l'acquisizione, autorizzata in via condizionata, *Microsoft/Linkedin* [70]. Se nella prima la *privacy* viene concepita come uno fra i tanti fattori qualitativi in grado di incidere sulle scelte dei consumatori [71] è nella seconda vicenda che, per la prima volta, l'esecutivo attribuisce ad essa il valore di dimensione qualitativa della concorrenza, sep-

---

[66] Cfr. OECD, *Big Data: Bringing Competition Policy To The Digital Era*, Paris, OECD Publishing, DAF/COMP(2016)14, November 29, p. 16.

[67] Fra i molti, si vedano gli spunti di riflessione offerti da M.E. STUCKE-A.P. GRUNES, *Big Data and Competition Policy*, Oxford, Oxford University Press, 2016, pp.260-261 ed inoltre cfr. J. HAUCAP, *Data Protection and Antitrust: New Types Abuse Cases? An Economist's View in Light of the German Facebook Decision*, in *CPI Antitrust Chronicle*, February 2019, p. 3. Critici, inoltre, sulla misurabilità della *privacy* gli studiosi J. HOFFMANN-O. VÁSQUEZ DUQUE, *Can Data exploitation be properly addressed by competition law? A note of caution* in *Concurrences*, 1, 2021, p. 78 ss.

[68] Cfr. R. ALIMONTI-F. ARDUINI, *Il mercato rilevante nell'era digitale*, in A. CATRICALÀ-C.E. CAZZATO-F. FIMMANÒ (a cura di), *Diritto Antitrust*, Giuffrè, Milano, 2021, p. 98 ss.

[69] Meritevoli, anche se non condivisibili, le argomentazioni di M.K. OHLHAUSEN-A.P. OKULIAR, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, in *Antitrust Law J.*, Vol. 80, 1, 2015, p. 154. Inoltre, sempre critici sul considerare il consumatore digitale quale soggetto inerte, incapace di autodeterminarsi liberamente nello spazio digitale, gli studiosi G. COLANGELO-M. MAGGIOLINO, *From fragile to smart consumers: Shifting paradigm for the digital era*, in *CLSR*, Vol. 35, 2019, p.179.

[70] Cfr. OECD, *Quality considerations in the zero-price economy – Note by the European Union*, DAF/COMP/WD(2018)135, November 23, 2018, p.7. Sul punto, si veda anche S. VEZZOSO, *All Happy Families are alike: the EDPS' Bridges between Competition and Privacy,* in *Market and Competition Law Review*, Vol. IV, n.1, 2020, p. 48 ss.

[71] Cfr. COMMISSIONE EUROPEA, 3 ottobre 2014, case no. COMP/M.7217, *Facebook/Whats app*, consultabile al sito EUR-Lex, par. 187.

pur nella misura in cui sia percepita quale fattore importante e significativo per i consumatori [72].

Notevoli passi in avanti sono stati compiuti da allora. Tre rivelano di essere particolarmente importanti perché è grazie ad essi che le *authorities* antitrust ed i legislatori sono stati in grado di riconoscere che un eventuale pregiudizio della *data protection* da parte delle grandi piattaforme può senz'altro rivelarsi utile nel corso di un'istruttoria antitrust per accertare l'esistenza di un abuso di posizione dominante.

In primo luogo, hanno riconosciuto l'importanza che la qualità dell'esperienza *online* assume per i consumatori nella fruizione di servizi e prodotti digitali, da misurarsi non solo in termini di intensità con cui si visualizza la pubblicità online durante la navigazione [73], ma anche in termini di un notevole peggioramento della tutela dei dati personali all'interno dell'ecosistema digitale. È evidente che, trattandosi di modelli di *business* costruiti sull'abuso di potere informativo, le grandi piattaforme non abbiano alcun interesse a rispettare una normativa come il GDPR perché il loro potere di mercato cresce e si rafforza proprio nel momento in cui si abbassano, in modo significato, i livelli di tutela della *privacy* [74].

Appare chiaro quale sia, dunque, il secondo passo che le *authorities* sono chiamate a compiere nell'accertare eventuali condotte anticompetitive delle grandi piattaforme: riconoscere che la *data protection* può ben divenire il parametro qualitativo concorrenziale principale in base al quale valutare nella *theory of harm* l'esistenza di un danno al processo competitivo.

Infine, il passo senza il quale i primi due non potrebbero compiersi: superare definitivamente l'idea secondo cui antitrust e *data protection* non potrebbero collaborare in alcun modo perché perseguono obiettivi diversi. Nulla di più sbagliato, eppure per poterlo affermare occorre che le autorità antitrust ed i legislatori si assumano con coraggio l'impegno di superare la definizione di *consumer welfare* proposta, a partire dagli anni '80 del '900, dal modello economico sviluppato dalla *Chicago School* e ritornino all'idea originaria secondo cui scopo principale del diritto antitrust è la tutela del processo competitivo, il che vuol dire anche tutelare indirettamente i consumatori [75].

Se si guarda con attenzione all'ambiente virtuale costruito dalle grandi società della rete è evidente che ognuna delle infrastrutture sulle quali sono stati "edificati" gli ecosistemi digitali sia stata costruita "ad arte" per ridurre, già a partire dalle interfacce grafiche di programmazione [76], in modo costante e pro-

---

[72] Cfr. COMMISSIONE EUROPEA, 6 dicembre 2016, case M.8124, *Microsoft / LinkedIn*, consultabile al sito EUR-Lex, par. 350.

[73] Si vedano le tesi degli studiosi M. E. STUCKE-A. EZRACHI, *The Curious Case of Competition and Quality,* in *Journal of Antitrust Enforcement*, Vol. 3, 2, October 2015, p.10 ss., inoltre con riguardo alla degradazione della *privacy* nel contesto dei motori di ricerca si vedano le posizioni dei due precedenti studiosi M. E. STUCKE-A. EZRACHI, *When Competition fails to optimize quality: a look at search engines*, in *Legal Studies Research Paper Series, Research Paper #268*, May 2015, pp. 90-91.

[74] Cfr. J.C. COOPER-J.M. YUN, *Antitrust & Privacy: it's complicated*, in *George Manson University Law & Economics Reseach Paper Series*, no .21-14, June 2021, p. 3; in senso conforme, cfr. M.E. STUCKE, *Should we be concerned about data-opolies?*, in *Georgetown Law J.*, Vol. 2, 2018, p. 286.

[75] In tal senso, si veda E. BRUTI LIBERATI, *Poteri privati e nuova regolazione pubblica*, in *Diritto Pubblico*, 1, 2018, p. 286. L'Autore sottolinea giustamente che «[…] alcuni cruciali elementi costitutivi del paradigma liberista – come, ad esempio, il dogma della massimizzazione del profitto – non sono stati ancora messi seriamente in discussione».

[76] Si pensi all'uso sempre più spregiudicato dei *dark patterns* (c.d. percorsi oscuri) che, co-

gressivo l'autonomia degli utenti commerciali e finali [77]. Difatti, non è possibile negare che l'uso degli algoritmi abbia senz'altro semplificato molte delle scelte che i consumatori compiono nell'ambiente digitale [78], ciononostante dietro ai vantaggi si nascondono insidie estremamente più grandi. Come giustamente rilevato da Laura Ammannati, gli algoritmi "di nuova generazione", sono oggi in grado non solo di indirizzare, ma anche di sostituirsi alle scelte degli utenti e decidere in modo del tutto autonomo dalla volontà di questi ultimi [79]. La sostituzione può avvenire quando gli strumenti di Intelligenza Artificiale perfezionano l'acquisto per gli utenti oppure completano la transazione per loro conto avendo già registrato il codice di sicurezza della carta prepagata oppure semplificando le operazioni di pagamento online mediante una valutazione del merito creditizio in tempo reale, come accade nel caso delle c.d. piattaforme *Buy now pay later* (anche dette, piattaforme BNPL) [80].

Dietro alla semplificazione e facilitazione dei processi digitali si nasconde, dunque, la più pericolosa delle minacce: la riduzione in stato di inerzia digitale del consumatore algoritmico, [81] costretto a cedere agli «oggetti intelligenti» [82], per usare una lungimirante definizione di Rodotà, la propria capacità di autodeterminarsi [83]. Gli ecosistemi digitali costruiscono una fitta trama di suggerimenti e persuasioni, più o meno manipolative, con le quali i consumatori vengono indotti a delegare agli algoritmi il potere di assumere la maggioranza delle proprie decisioni che, invece, dovrebbero compiere personalmente [84]. È chiaro che in questo modo viene pregiudicata la capacità di decidere liberamente perché o gli algoritmi vengono progettati affinché siano in grado di sce-

---

me ben sottolineato dagli studiosi Susser, Roessler e Nissenbaum, costituiscono una forma di *hidden influence* con i quali gli ecosistemi digitali modificano artatamente il comportamento dell'utente. Si tratta, quindi, di una tipologia di *design* grafico manipolativo con cui vengono costruite le interfacce grafiche delle grandi piattaforme digitali. Sulla questione, si vedano D. SUSSER-B. ROESSLER-H. NISSENBAUM, *Technology, autonomy and manipulation*, in *Internet Policy Rev*., Vol. 8, 2, 2019, p.1 ss. Inoltre, per approfondire il tema della manipolazione *online* si veda C. R. SUSTEIN, *Manipulation as theft*, in *J. Eur. Public Policy*, Vol. 29, 12, p. 1959 ss.

[77] Cfr. H. HYDÉN, *AI, Norms, Big Data, and the Law*, in *AsianJLS,* Vol. 7, 3, 2020, p. 416.

[78] Sui vantaggi per il consumatore cfr. M.S.GAL-N. ELKIN-KOREN, *Algorithmic Consumers*, in *Harv. J. law technol.*, Vol. 30, 2, 2017, p. 318 ss. Con riguardo ai vantaggi che i processi decisionali automatizzati possono avere anche sull'attività delle pubbliche amministrazioni, si vedano le riflessioni di M. FALCONE, *Bisogni conoscitivi delle amministrazioni e principio di legalità: quale predeterminazione delle scelte conoscitive pubbliche?* in *RIID*, 2, 2022, p.60 ss.

[79] Si veda a tal proposito, L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione*, in A. CANEPA-G. GRECO-L. AMMANNATI-U. MINNECI (a cura di), *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione*, Giappichelli, Torino, 2021, pp. 147-148 ss.

[80] Su questo ultimo esempio di semplificazione delle operazioni di pagamento *online* si veda l'interessante studio di L. GOBBI, *Buy Now Pay Later, caratteristiche del mercato e prospettive di sviluppo*, in *Questioni di Economia e Finanza*, numero 730, novembre 2022, p. 5 ss.

[81] Cfr. M.S.GAL-N. ELKIN-KOREN, *Algorithmic Consumers*, in *Harvard Journal of Law & Technology*, cit., p. 313.

[82] Si veda S. RODOTÀ, *Il diritto di avere* diritti, Laterza, Bari, 2012, p. 328.

[83] Cfr. CONSIGLIO D'EUROPA, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes,* 13 febbraio 2019, p. 8, consultabile al sito del Consiglio d'Europa.

[84] Per un approfondimento in merito, si vedano le opportune riflessioni di A. CANEPA, *I mercanti dell'era digitale*. *Un contributo allo studio delle piattaforme,* Giappichelli, Torino, 2020, pp. 123-125; ed inoltre sempre della stessa studiosa si veda A. CANEPA, *Alla ricerca dell'autonomia negoziale "perduta". Consumatori e venditori in epoca di profilazione e algoritmi*, in A. CANEPA-G. GRECO-L. AMMANNATI-U. MINNECI (a cura di), *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione*, Giappichelli, Torino, 2021, p.162.

gliere per lui, spingendolo, di fatto, a sottrarsi alla decisione oppure per fargli solo credere che stia compiendo una scelta autonoma. La verità è tutt'altra: sono state ideate forme di manipolazione talmente sofisticate da indurre il consumatore digitale a compiere scelte che non avrebbe intenzione di compiere, se solo avesse modo di scegliere liberamente [85].

Ebbene, se la tutela del consumatore digitale non venisse più concepita quale massimizzazione del benessere collettivo da perseguire mediante il solo fine dell'efficienza economica, ma quale salvaguardia della sua libertà di scelta ed autonomia da raggiungersi mediante il rispetto dei principi della concorrenza e con la rigorosa osservanza della normativa in materia di *privacy*, allora sarebbe possibile per i detrattori dell'integrazione comprendere che nella tutela del consumatore digitale è rinvenibile una possibile convergenza fra le due normative.

La pronuncia della Corte di Giustizia dell'Unione Europea sul caso tedesco *Bkarta v. Facebook*, sancendo la regola secondo cui la conformità o meno di un comportamento, alle disposizioni del GDPR può costituire un importante indizio da cui desumere una violazione dei principi della concorrenza, delinea una possibile modalità di cooperazione. Da un lato, la protezione dei dati personali provvede a garantire il diritto dell'utente di decidere da sé circa l'uso e la gestione delle informazioni che lo riguardano, dall'altro il diritto della concorrenza, garantendo una leale e sana competizione fra le imprese, aumenta le opzioni a disposizione dei consumatori [86]; impendendo così che lo squilibro di potere con la piattaforma ponga questi ultimi in una posizione di "sudditanza" nei riguardi dei nuovi imperi privati.

2.2. La posizione dominante quale indice da cui desumere l'invalidità del consenso

È proprio dallo squilibrio di potere fra gli utenti, interessati dal trattamento dei dati personali, e la piattaforma che li processa in qualità di titolare del trattamento, che si può rinvenire la seconda delle novità introdotte dalla decisione. La Corte di Giustizia, infatti, è arrivata a sostenere che nel valutare la validità del consenso occorre considerare anche la posizione dominante vantata dall'operatore economico che tratta i dati.

È noto che una delle caratteristiche dei modelli di *business* delle grandi società tecnologiche sia la creazione di un sistema aziendale basato su relazioni asimmetriche fra utenti ed ecosistemi digitali [87]. Questa chiara disparità di forza consolida la posizione di superiorità economica che rende l'ecosistema digitale *partner* di mercato obbligato sia per gli utenti commerciali sia per i consumatori che, in assenza di alternative equivalenti, si rivolgono necessariamente a quella che è in grado di offrire loro servizi e prodotti tarati sulle proprie esigenze. Un maggior numero di utenti commerciali e consumatori signifi-

[85] Uno studio approfondito sulle probabili tecniche di manipolazione usate a partire dai mercati fisici è stato pubblicato dagli studiosi J.D. Kysar-D.A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, in *N.Y.U. L. Rev.*, p. 633 ss.

[86] Cfr. F. Costa-Cabral-O. Lynskey, *Family ties: the intersection between data protection and competition in EU Law*, in *Common Mark. Law Rev.*, Vol. 54,1, 2017, p.9.

[87] Su questo aspetto cfr. Commissione Europea, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, 25 maggio 2016, COM(2016) 288 final, Bruxelles, p.14; inoltre si veda fra i molti F. Pasquale, *The Black Box Society*, Harvard University Press, Harvard, US, 2015, pp. 5-7.

ca anche maggior disponibilità di informazioni, il che contribuisce a rafforzare la dinamica circolare che è alla base del potere di mercato delle grandi piattaforme.

Queste dinamiche interne alle piattaforme, come pare giustamente rilevare la Corte di Giustizia dell'Unione Europea, si pongono in palese contrasto con i presupposti deputati a garantire che il consenso sia frutto di una consapevole autodeterminazione, così come enucleati in alcuni dei Considerando e delle norme del GDPR. In primo luogo, la definizione di consenso quale manifestazione di volontà libera, specifica, informata ed inequivocabile offerta all'articolo 4 n.11 ed al Considerando 42. In secondo luogo, l'articolo 7, par.4 ed il Considerando 43 volti entrambi a stabilire quando il consenso possa definirsi effettivamente libero. Il Considerando 43, nello specifico, individua un ulteriore presupposto in base al quale il consenso può definirsi non prestato liberamente, l'esistenza di «[…] un evidente squilibrio fra il titolare del trattamento e l'interessato» nonché l'ipotesi in cui «[…] non sia possibile prestare un consenso separato a distinti trattamenti di dati personali». Con riguardo all'«evidente squilibrio», è chiaro che un rapporto non paritario fra titolare del trattamento ed interessato in cui il secondo non ha a disposizione alternative realistiche all'accettazione dei termini del trattamento non consente di concepire il consenso quale base legittima del trattamento. Con riguardo, invece, al «consenso separato», il Considerando introduce il concetto di granularità secondo il quale nel caso in cui un servizio comporti trattamenti multipli per più finalità, il consenso può presumersi non espresso liberamente, laddove non permetta all'interessato di aderire in modo separato ai distinti trattamenti dei dati personali [88].

La posizione dominante che, come ricorda la giurisprudenza comunitaria, di per sé non è illegale, viene ritenuta un indice dal quale poter desumere l'esistenza di un vizio del consenso ed in particolare della libertà del consenso prestato dall'utente del *social network* [89]. Il persistente carattere di dipendenza, come si è descritto poc'anzi, degli utenti dalla piattaforma dovuto in larga parte all'asimmetria informativa pone senz'altro gli ecosistemi digitali in una posizione economica tale da essere in grado di tenere comportamenti alquanto indipendenti dai concorrenti e dai consumatori [90]. Fra questi comportamenti, la Corte di Giustizia se ne ravvisa uno in particolare: l'impossibilità di rifiutare o revocare il consenso rispetto a particolari operazioni di trattamento dei dati personali che non sono considerate necessarie all'esecuzione del contratto fra Meta e i suoi iscritti [91], pena la rinuncia integrale al servizio digitale. Pare evidente che nessuna libertà, tuttavia, può esistere, se non si offre gli utenti la possibilità di optare per un trattamento diverso che si possa affiancare a quello previsto sino ad ora dalla società californiana [92]. È vero però che tutto que-

---

[88] Cfr. WP29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 28 novembre 2017, p. 11.

[89] Corte Di Giustizia Dell'unione Europea, sentenza del 4 luglio 2023, causa C-252/21, *Meta v. Bundeskartellamt*, cit., punto 148.

[90] Sul vincolo di dipendenza esistente fra grandi piattaforme ed utenti cfr. O. Pollicino, «Potere digitale», in *Enc. Dir.*, I Tematici, V, Giuffrè Francis Lefebvre, Milano, 2023, p. 413 ed inoltre si vedano le considerazioni di F. Esposito, *The GDPR enshrines the right to the impersonal price*, in *CLSR*, 45, 2022, p. 8 ss.

[91] *Ivi*, punti 148-149.

[92] *Ivi*, punto 150.

sto diviene possibile solo se la scelta, nei riguardi di una diversa modalità di trattamento dei dati, sia il frutto di una manifestazione di volontà "libera" nel senso che l'interessato viene posto dinanzi ad una alternativa effettiva in cui può vantare il pieno controllo sui propri dati [93]. Una soluzione quest'ultima avallata dalla stessa Corte di Giustizia che ha proposto di regolare in modo granulare il livello di informazioni da condividere, offrendo così agli utenti un'opzione alternativa consistente nella prestazione di un consenso separato col quale autorizzare la piattaforma a trattare solo i dati relativi al comportamento tenuto all'interno dell'ecosistema, ma non all'esterno (dati *Off-Facebook*), proprio nel rispetto del dettato normativo di cui al Considerando 43 del GDPR [94].

È evidente che da quest'angolazione la decisione della Corte di Giustizia possa costituire un ottimo spunto di riflessione per interrogarsi sull'efficacia dello strumento del consenso nelle dinamiche dei mercati digitali. Lo strumento consensuale sembra essere ridotto a mero simulacro di un tempo – quello coincidente con l'attuazione della Direttiva Europea 95/46/CE [95] – in cui veniva considerato massima espressione del diritto fondamentale all'autodeterminazione informativa [96].

Le modalità con le quali le grandi piattaforme hanno progettato l'ambiente digitale hanno col tempo contribuito a svuotare di efficacia il consenso [97]. Per sostenere modelli di *business* in cui la raccolta ed il processamento dei dati personali si riveli essenziale, è stato necessario costruire delle interfacce grafiche "ad uncino" in grado di rendere l'interazione degli utenti con la piattaforma continuativa. Per ottenere questo risultato le grandi società della rete hanno dovuto così mettere a punto delle particolari forme di manipolazione [98] nei riguardi degli utenti: i percorsi oscuri o schemi non trasparenti (c.d. *dark patterns*) [99]. Si tratta di veri e propri "inganni tecnologici" che, una volta implementati all'interno di pagine web ed in altre varie applicazioni, inducono gli internauti a fare scelte che paiono compiersi nel loro interesse, mentre in realtà so-

---

[93] Sulla circostanza secondo cui non vi siano al momento negli ecosistemi digitali alternative possibili al modello di trattamento dei dati personali dominante imposto dal *provider* si veda D. MESSINA, *Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent*, in *MediaLaws*, 2, 2019, p. 169.

[94] *Ivi*, punto 151.

[95] Per un approfondimento in merito al percorso normativo compiuto dall'Unione Europea nell'adozione della Direttiva 1995 si veda S. SIMITIS, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, in *Iowa L. Rev.,* Vol.80, 3, 1995, p. 445 ss.

[96] Sul punto le interessanti considerazioni di F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in FINOCCHIARO G., (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Bologna, 2019, pp. 138-138. Si veda anche D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. critica dir. priv*., 1998, pp. 350-351.

[97] Illuminanti in tal senso le riflessioni di W. HARTZOG, *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, Cambridge Massachusetts, and London, England, 2018, p. 5. Sul punto, si vedano le considerazioni di P. MASALA, *Emerging collective implications of personal da processing: challenges and responses in the European context*, in T. GROPPI-V. CARLINO-G. MILANO (edited by), *Framing and Diagnosing Constitutional Degradation: a Comparative Perspective*, Agosto 2022, p. 264 ss.

[98] Sul concetto di «*market manipulation*» si veda M. R. CALO, *Digital Market Manipulation*, in *Geo. Wash. L. Rev*., Vol. 82, n. 4, 2014, p.1004 ss.

[99] Sulla definizione di *dark patterns* H. BRIGNULL, *Dark Patterns: inside the interfaces designed to trick you*, in *The Verge*, consultabile al sito The Verge, August 29, 2013.

no compiute nell'interesse della piattaforma [100]. Sono molteplici le tipologie di percorsi oscuri predisposte dagli sviluppatori. Tuttavia, senza voler scendere in un'analisi tassonomica degli stessi, può essere senz'altro utile ricordare quelli progettati per far sì che gli utenti diano il consenso al trattamento di una quantità di dati personali maggiore rispetto a quella che sarebbe effettivamente dovuta in base alle finalità del trattamento stesso [101].

È evidente che gli schemi non trasparenti si pongano in chiaro e palese contrasto con le norme in materia di protezione dei dati personali [102]. Si pensi ad esempio, a quel particolare inganno con cui si autorizza il tracciamento mediante *cookies consent pop-ups*. Il meccanismo viene ideato per fare in modo che nell'interfaccia grafica si mostri per prima cosa il pulsante di accettazione al tracciamento (*opt-in*) e lo si renda visibile, comodo e semplice da selezionare al fine di indurre l'utente a scegliere questa opzione e liberarsi del *banner* il più velocemente possibile per accedere alle informazioni che sta cercando sulla rete. Al contrario, se decidesse di rifiutare, non avrebbe modo di selezionare così facilmente il *banner* del rifiuto (*opt-out*) perché prima di declinare definitivamente la richiesta, si aprirebbero all'utente ulteriori finestre che gli impedirebbero, in sostanza, di compiere una scelta immediata. Rinunciare ad essere tracciati si rivela essere una scelta molto più defatigante per l'utente piuttosto che accettare di esserlo. È ovvio che un'interfaccia grafica di questo tipo non consente all'utente di scegliere in modo del tutto libero ed autonomo perché è evidente che, in mancanza di tempo ed avendo la necessità di accedere ai contenuti disponibili in rete nella maniera più veloce possibile, l'utente scelga il percorso digitale più comodo e celere sebbene quest'ultimo si riveli contrario ai principi generali del trattamento dei dati personali quali *in primis* quelli di trasparenza, correttezza, finalità e minimizzazione di cui all'articolo 5 del GDPR.

È chiaro che la mera adesione al trattamento prestata mediante strategie manipolative non possa dirsi effettivamente libera [103]. Già nel 1973 Rodotà in *Elaboratori elettronici e controllo sociale*, sosteneva che il consenso fosse innanzitutto uno schema formale, «[…] una finzione», in quanto "[…] ci si rende progressivamente conto dell'impossibilità di affidare alla sola iniziativa dell'individuo isolato, dotato di un illusorio 'potere della volontà', il compito di controllare e contrastare quello che è un vero e proprio potere normativo delle imprese [104]». Queste parole, che a rileggerle avendo in mente l'attuale contesto economico sembrano quasi "profetiche", sono in grado di descrivere perfettamente lo stato nel quale oggi versa il consenso. Dinanzi all'emergere di tecnologie sempre più pervasive, il consenso non può definirsi libero almeno nel

---

[100] Per approfondire, A. Zac-Y.-C. Huang-A. Von Moltke *et al*., *Dark Patterns and Online Consumer Vulnerability*, in *Working paper CCLP(L)55*, 2023, p. 7.

[101] A tal riguardo si veda: M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, in *Notre Dame L. Rev.,* Vol, 87, 3, 2012, p. 1038.

[102] Per una panoramica esaustiva sulle varie tipologie di percorsi oscuri in palese contrasto col GDPR si veda EDPB, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, 14 marzo 2022, p. 3, consultabile al sito ufficiale EDPB.

[103] In tal senso, A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law & Security Review*, 30, 2014, p.649 ss, ed ancora cfr. C. J. Hoofnagle-A. Soltani-N. Good *et al*., *Behavioral Advertising: The Offer You Cannot Refuse* in *Harv. L. & Pol'y Rev. Harv.*, Vol. 6, 2021, p. 294 ss.

[104] Per approfondire si veda S. Rodotà, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, p. 50.

senso in cui viene inteso dalle normative in materia di *privacy* [105]. Se viene prestato per effetto di strategie manipolatorie che riducono la soglia dell'attenzione [106] o per il tramite di informative, che si rivelano tutt'altro che concise, trasparenti, intellegibili o facilmente accessibili [107], tanto da disincentivare l'utente a leggerle integralmente, è chiaro che il consenso non costituisca più il perno del sistema attorno al quale ruota la protezione dei dati personali [108].

Sul piano legislativo, paiono meritevoli di menzione i recenti sforzi di diversi legislatori che, per risolvere le problematiche connesse all'inefficacia del consenso, hanno adottato alcune soluzioni innovative sul piano regolatorio. Nello specifico, negli Stati Uniti il *California Privacy Act*, legge settoriale in tema di tutela della *privacy*, fornisce per la prima in assoluto una soluzione ai *dark patterns* prevedendo espressamente che il consenso conseguito mediante percorsi oscuri non possa essere considerato liberamente prestato [109] e ne vieta pertanto l'utilizzo sancendo la regola secondo cui, in caso di acquisizione del consenso espresso mediante *opt-in*, non debbano essere usati *dark patterns*. L'ottica del legislatore californiano è, dunque, quella volta a progettare un ambiente digitale che sia effettivamente *privacy-preserving* che ponga l'utente nella condizione di scegliere in modo del tutto consapevole se prestare o meno il consenso al trattamento, senza essere indotto a farlo sulla base di inganni tecnologici e finalità di profilazione commerciale occulta.

Sul fronte europeo, invece, sono innanzitutto meritevoli di nota le Linee guida adottate a marzo 2022 con le quali lo *European Data Protection Supervision* esorta e raccomanda, principalmente agli ingegneri informatici, di costruire interfacce grafiche prive di schemi non trasparenti e manipolatori. Alle linee guida si sono aggiunti poi il *Digital Service Act* che, al Considerando 67, menziona apertamente gli effetti pregiudizievoli che gli schemi non trasparenti possono avere sull'autonomia degli utenti ed al quale fa eco il *Digital Markets Act* (in seguito DMA). Il Considerando 37 del suddetto regolamento afferma apertamente che i *gatekeepers* «non dovrebbero progettare, organizzare o gestire le loro interfacce online in modo tale da ingannare, manipolare ovvero compromettere o falsare in altro modo, in misura rilevante, la capacità degli utenti finali di prestare liberamente il proprio consenso».

Sul piano delle possibili soluzioni si colloca anche la metodologia del *legal design* nata dalla necessità di semplificare un concetto legale attraverso l'uso di elementi testuali e para-testuali, come le icone grafiche, che ne veicolino facilmente la comunicazione e ne favoriscano la comprensione in modo chia-

---

[105] Cfr. I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale. Iniziali spunti di riflessione*, in *DIMT*, 25 gennaio 2017, p. 11.

[106] Sul punto, cfr. D. POLETTI, *Commento all'articolo 6 del Regolamento generale sulla protezione dei dati personali*, cit., p. 196.

[107] Sul punto, CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, (GRANDE SEZIONE) 1 ottobre 2019, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. Planet49 GmbH*, par.57. Sul punto per approfondire si veda T. POLVANI, *Il consenso al trattamento dei dati personali nel dialogo fra le Corti*, in E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, Giappichelli, 2022, p. 137.

[108] Cfr. F. H. CATE-V. MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in *Int. Data Priv. Law.*, Vol. 3, 2, 2013, p. 67 ss. Inoltre, si veda D. SOLOVE, *Introduction: Privacy self-management and the consent dilemma*, in *Harv. Law Rev.*, Vol. 126, 2013, p. 1885.

[109] Il testo del *California Consumer Privacy Act* è consultabile sul sito ufficiale dello *State of California Department of Justice*.

ro, efficace e trasparente [110]. La soluzione che si propone consiste nel cercare di applicare questo metodo alle informative *privacy* affinché diventino facilmente comprensibili per gli utenti, a prescindere dal loro grado di consapevolezza in merito alle norme in materia *data protection*.

Si tratta di primi tentativi che, proprio in considerazione dei metodi con i quali le grandi società influenzano la volontà degli utenti, possono senz'altro aiutare alla costruzione di un ambiente digitale in cui l'utente, nel momento in cui decide di autorizzare il trattamento, esprima un consenso libero, senza alcun previo condizionamento da parte del titolare-piattaforma perché in caso contrario sarebbe «necessitato [111]» e renderebbe il trattamento illecito.

3. Pubblicità personalizzata: il legittimo interesse non può sempre essere una via di fuga per i guardiani dei mercati digitali

La Corte di Giustizia dopo aver stabilito che l'invalidità del consenso può desumersi anche dall'esistenza di una posizione di dominanza economica nel mercato digitale, tenta di risolvere un'altra questione legata alla possibilità di rinvenire nel perseguimento del legittimo interesse da parte di Meta una base giuridica idonea a legittimare il trattamento dei dati personali per finalità di pubblicità comportamentale. In questi casi, il trattamento per essere considerato lecito deve, ai sensi dell'articolo 6, par. 1, *lett. f)*, risultare «necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

Come si evince dal dettato normativo della disposizione, questa base giuridica prevede, ai fini della sua applicazione, che il titolare sia chiamato a svolgere un vero e proprio bilanciamento tra l'interesse al trattamento vantato dallo stesso titolare o da un terzo e quelli contrapposti dei soggetti cui i dati personali ineriscono al fine di individuare quale sia quello prevalente [112]. Ad esplicitare il modo in cui questo bilanciamento di interessi differenti debba avvenire è il considerando 47 del regolamento UE 2016/679, il quale, dopo aver previsto che per finalità di *marketing* diretto la base giuridica del trattamento può essere un legittimo interesse del titolare, affida direttamente a quest'ultimo, il compito di procedere ad un'attenta valutazione degli interessi contrapposti [113], tenendo conto «delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento» nonché dell'«[…] eventualità che l'interessato, al momento e nell'ambito della raccol-

---

[110] Per approfondire questi aspetti di indubbia attualità, si veda: L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come rimedio ex ante*, in *Dir. Inform.*, 2, 2020, pp. 307-308.

[111] Sul consenso «necessitato» cfr.: S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws*, 3, 2019, p.138.

[112] Cfr. S. SCARAGLINI, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta Online*, 2, 2021, p. 503 alle cui considerazioni fanno eco quelle di I. M. ALAGNA *et al.*, *Commento all'articolo 6 del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n.679*, *Op.cit.*, p. 96.

[113] Sul punto, cfr. P. TRIGO KRAMCSÁK, *Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?* in *CLSR*, Vol. 48, 2023, p. 10.

ta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine».

Ebbene, oltre al bilanciamento fra interessi contrapposti, l'uso del legittimo interesse quale base giuridica idonea al trattamento dei dati personali richiede la sussistenza di tre imprescindibili condizioni cumulative individuate dalla stessa Corte di Giustizia dell'Unione Europea in diversi casi giurisprudenziali e richiamate al paragrafo 101 sino al 107 della decisione in commento. In primo luogo, verificare che il titolare del trattamento o un soggetto terzo perseguano un legittimo interesse; in secondo luogo, accertare che il trattamento dei dati personali debba essere effettivamente necessario a realizzare un legittimo interesse ed, infine, che gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgano sul legittimo interesse del titolare o del terzo [114].

Fra gli interessi della società californiana, quale titolare del trattamento, ne sono stati segnalati diversi, ma è la personalizzazione della pubblicità che merita maggiore approfondimento in quanto ad essa la Corte, ha dedicato particolare attenzione perché connessa alla pubblicità comportamentale [115]. I giudici hanno ritenuto che la personalizzazione dei contenuti pubblicitari non possa ritenersi un legittimo interesse in grado di giustificare il trattamento dei dati personali compiuto in assenza di consenso da parte dell'utente. Tuttavia, nel caso della pubblicità mirata sarebbe più che legittimo visto che la pubblicità, insieme alla commercializzazione diretta tradizionale o altre forme di commercializzazione di beni e servizi, è considerata una degli esempi di legittimo interesse in grado di giustificare il trattamento dei dati personali in assenza di consenso. Si tratta, infatti, di casi in cui, come ha sostenuto correttamente Federico Ferretti, il *test* di bilanciamento che accompagna l'art. 6, par. 1, *lett.f)* del GDPR consente alla norma di avere maggiore flessibilità rispetto alle altre condizioni di legittimità del trattamento [116]. È quanto si è verificato col provvedimento del Garante italiano per la protezione dei dati personali che, dopo aver bloccato la distribuzione di ChatGPT [117], ha ingiunto alla società OpenAI che lo ha sviluppato di adottare una serie di misure alle quali si è poi conformata rendendo, così, di nuovo accessibile il proprio prodotto digitale anche in Italia. Fra le varie misure proposte del Garante, anche la «modifica della base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento algoritmico» [118], con la quale viene eliminato ogni riferimento al contratto ed usata come base giuridica del trattamento il consenso o il legittimo interesse.

Sebbene la Corte sia ben consapevole di ciò, solleva dubbi in merito perché gli utenti, all'atto di iscrizione alla piattaforma, non possono ragionevol-

---

[114] Fra le molte cfr. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza 4 maggio 2017, C-13/16, *Valsts policijas Rigas c. Rigas pašvaldibas*, punto 60; CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, sentenza 17 giugno 2021, *M.I.C.M. c. Telenet BVBA*, punto 127.

[115] Sul punto le riflessioni di V. BACHELET, *Il consenso oltre il consenso*, Pacini Editore, Pisa, 2023, p. 46 ss.

[116] Cfr. F. FERRETTI, *Data Protection and the Legitimate Interest of Data Controllers Much a do about Nothing or the Winter of Rights?*, in *Common Market Law Review*, Vol. 51, 3, 2014, p. 843 ss.; inoltre P.BALDONI-D. COOPER-R. IMPERIALI *et. al*., *Legitimate Interest of Data Controller. New Data protection paradigm: legitimacy grounded on appropriate protection*, in *Int. Data Priv. Law*., Vol. 3, 4. 2013, p. 251.

[117] *Software* di Intelligenza Artificiale generativa.

[118] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento n.114 dell'11 aprile 2023*, consultabile sul sito ufficiale del Garante per la Protezione dei dati personali.

mente attendersi che, senza il loro consenso, il titolare del trattamento, nel qual caso Meta, tratti i dati per personalizzare i contenuti degli annunci pubblicitari online [119]. Viene, dunque, a mancare secondo la Corte quella ragionevole aspettativa che consente all'interessato di attendersi che, in virtù del valore economico dei dati, la raccolta ed il processamento degli stessi possa essere destinato a finalità di tipo commerciale o di *marketing* [120]. È evidente che in questa situazione i giudici del Lussemburgo abbiano voluto considerare prevalenti i diritti fondamentali e gli interessi degli iscritti rispetto all'interesse prettamente economico legato alla personalizzazione della pubblicità digitale [121].

La Corte di Giustizia, dunque, torna ad affermare come sia il consenso la sola base giuridica idonea ad autorizzare il trattamento dei dati personali degli utenti nei mercati digitali in caso di pubblicità personalizzata. Si ripropone, dunque, un orientamento emerso precedentemente nelle due decisioni vincolanti del 5 dicembre 2022 con le quali lo EDPB, dinanzi alla scelta o meglio, allo stratagemma di Meta di modificare i termini di servizio per rendere conforme al GDPR l'attività di profilazione connessa al *behavioral advertising* [122], ha statuito che, per la resa del servizio di pubblicità comportamentale, è necessario un consenso specifico e distinto degli utenti. In questo modo, lo EDPB arriva a sostenere che l'unica e valida base giuridica di questa tipologia di trattamento dei dati personali degli utenti debba essere il consenso [123].

Una rinnovata importanza del consenso è rinvenibile non solo sul piano della prassi giurisprudenziale eurounitaria, ma anche sul piano legislativo. All'articolo 5, par. 2, *lett. a)* del DMA viene introdotto un divieto generalizzato di trattamento, uso incrociato, combinazione ed accesso per fini di combinazione dei dati personali che i guardiani dei mercati digitali sono in grado di acquisire, all'interno ed all'esterno, dei propri ecosistemi digitali mediante sistemi di tracciamento, salvo il caso in cui gli utenti non abbiano espresso il proprio consenso al trattamento. È palese che la norma erediti le vicissitudini che hanno accompagnato il caso tedesco dal 2016. Non deve sorprendere, dunque, che nella disposizione confluiscano elementi attinenti sia al diritto della concorren-

---

[119] Per approfondire si veda M. MASSIMI, *Quali orizzonti per il marketing?*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, in R. PANETTA (a cura di), *Commentario al Regolamento (UE) 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, 2019, Giuffrè, Milano, pp. 619-651 ed inoltre si aggiunga sempre con riguardo al legittimo interesse il parere del WP29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014, p. 27 ss, consultabile al sito ufficiale del WP29.

[120] Cfr. G. D'IPPOLITO, *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, Torino, 2022, p. 58 ss.

[121] In tal senso, cfr. C. D'AGATA, *Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento*, in R. PANETTA (a cura di), *Commentario al Regolamento (UE) 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, 2019, Giuffrè, Milano, 2019, p. 92.

[122] Si vedano sulla questione V. MOREL-C. SANTOS *et al*., *Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls*, consultabile in arXiv:2309.11625, 2023, p. 2 ss. Per i profili più strettamente civilistici della vicenda si vedano le riflessioni di V. BACHELET, *La Corte di giustizia sul caso Meta: trattamento dei dati e "prezzo" del consenso,* in *Pactum*, 4, 2023, pp.498-499.

[123] Cfr. EDPB, *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)* consultabile al sito ufficiale dello EDPB ed inoltre EDPB, 5 dicembre 2022, *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)*, consultabile al sito dello EDPB.

za sia al diritto della protezione dei dati personali, come, tra l'altro, pare evincersi dal dettato normativo del Considerando 36 del DMA [124].

Tuttavia, anche in tal caso, il problema, o meglio – verrebbe da dire – *the elephant in the room* che i regolatori ed i legislatori si ostinano a non vedere, è legato al valore ormai meramente formale del consenso che col tempo ha finito per perdere il ruolo di baluardo dell'autodeterminazione informativa degli utenti. Pare, infatti, condivisibile la posizione di alcuni studiosi, fra i quali quella di Rupprecht Podszun, che innanzi ad una disposizione di questo genere hanno espresso dubbi e perplessità, legate non tanto al tentativo della Commissione Europea di collegare fra loro diritto antitrust e *data protection*, quanto all'indeterminatezza che accompagna il concetto di consenso ormai da tempo, il che è indubbio, sia riscontrabile anche nell'articolo 5 lett. a) del DMA in cui vengono richiamati i requisiti di validità dello stesso in mero ossequio agli artt. 4 n.11 e 7 del GDPR [125]. È scontato allora dire che qualcosa debba essere cambiato ed i tentativi di cui si è detto in precedenza potrebbero in parte risolvere il problema connesso alle «*pathologies of digital consent*» [126], come sono state definite giustamente da Richards e Hartzog.

4. Alcune considerazioni finali

Questa sentenza non passerà e, non deve passare inosservata. Soprattutto da parte di quegli studiosi di diritto antitrust che hanno escluso sin dal primo provvedimento adottato dal *BKARTA* che il diritto della concorrenza e la normativa in materia di protezione dei dati personali potessero cooperare fra loro e muoversi all'unisono non solo per arginare il potere degli ecosistemi digitali, ma anche per ripristinare l'autonomia e la libertà di scelta dei consumatori algoritmici. Tuttavia, proprio la tradizione ordoliberale, non strettamente legata all'analisi economica del diritto di matrice chicaghiana, ha consentito alla Corte di Giustizia di compiere un passo in avanti e di proiettarsi verso un possibile ripensamento della teoria del danno concorrenziale in cui le autorità garanti della concorrenza sostituiscano al prezzo sovra-competitivo l'accertamento di un'eventuale degradazione di un parametro prettamente qualitativo come quello della *privacy*, dal cui peggioramento – provato per il tramite di una violazione della *data protection* – sia possibile desumere l'esistenza del danno concorrenziale.

Alcuni studiosi, fra cui Pietro Manzini, che hanno per primi commentato la vicenda, mettono in luce alcune criticità della pronuncia. In primo luogo, sostengono che consentire alle *authorities* della concorrenza, nel corso di un'indagine, di dedurre un illecito antitrust da una violazione della *privacy* «probabilmente condizionerà in maniera significativa l'esito della decisione

[124] Cfr. W. KERBER, *Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law*, in *Antitrust Bull.*, Vol. 67, 2, p. 291 ed inoltre sempre in tal senso W. KERBER-K.K. ZOLNA, *The German Facebook case: the law and economics of the relationship between competition and data protection law*, in *Eur. J. Law Econ*, Vol.54, 2, 2022, p. 240.

[125] Cfr. R. PODSZUN, *Should Gatekeepers Be Allowed to Combine Data? Ideas for Art. 5(a) of the Draft Digital Markets Act*, in *GRUR International*, Vol. 71, 3, 2022, p. 197 ss.

[126] Per approfondire si vedano N. RICHARDS-W. HARTZOG, *The Pathologies of Digital Consent*, in *Wash. U. L. Rev.*, Vol. 96, 6, 2019, p. 1464 ss.

antitrust» [127], lasciando così intendere che il peso attribuito alle norme in materia di *data protection* potrebbe rivelarsi eccessivo, una sorta di "invasione di campo", mal tollerata in un ambito in cui la competenza a decidere spetta alle autorità garanti della concorrenza e non alle autorità di controllo. Sebbene ciò sia possibile, occorre anche notare che la Corte di Giustizia è stata piuttosto chiara nel delimitare i casi in cui una non conformità alla disciplina in materia di *data protection* potrebbe essere considerata quale indizio da cui desumere un abuso di posizione dominante. Lo si evince al paragrafo 48 della decisione in cui il riferimento alla violazione della *privacy* viene sì definito quale «importante indizio» dal quale ricavare la prova di una eventuale distorsione dei principi della concorrenza, ma la cui importanza non vale di per sé, vale solo se è in rapporto alle altre «[…] circostanze rilevanti del caso di specie».

Se ne ricavano principalmente due considerazioni. In primo luogo, l'integrazione fra le due discipline non verrà applicata in maniera generalizzata ed in secondo luogo le autorità garanti potranno far ricorso ad essa solo in una serie limitata di casi [128]. Si pensi alla vicenda giudiziaria che ha visto la FTC accusare Facebook di monopolio innanzi alla Corte Federale del Distretto di Columbia. L'agenzia governativa americana non ha soltanto dimostrato in giudizio che l'esistenza di un consolidato potere monopolistico sarebbe dovuta al peggioramento dei livelli di protezione dei dati personali per effetto della violazione delle norme in materia di *privacy* da parte della piattaforma, ma ha dato prova, inoltre, che il raggiungimento del monopolio è ascrivibile anche all'adozione di condotte anticompetitive con finalità escludenti, fra le quali rientrano le acquisizioni predatorie di Instagram e WhatsApp e l'imposizione ad *apps* terze indipendenti di condizioni anticoncorrenziali tese ad impedire l'accesso alle interfacce di programmazione della piattaforma [129]. Come è evidente in questa vicenda, la violazione della *privacy* ha sì rappresentato un elemento di prova dal quale desumere l'esistenza di una posizione di monopolio, ma non è stato l'unico elemento che la Corte Federale ha tenuto in considerazione. Lo ha valutato quale indice che insieme ad altre evidenze processuali consente di accertare la sussistenza di un pregiudizio del processo competitivo.

È anche vero che, nei mercati digitali, i regolatori potrebbero far uso maggiore della cooperazione fra antitrust e *data protection* proprio perché, come si avuto modo di vedere anche nel caso americano *FTC v. Facebook* di cui si è detto poc'anzi [130], non è possibile negare che negli ambienti digitali creati dai guardiani dei mercati il potere economico di questi operatori cresca in modo inversamente proporzionale ai livelli di tutela dei dati personali. Ricorda Neil Richards che «*information is power*» [131] per cui è ovvio che avere a disposi-

---

[127] Sul punto, si vedano le considerazioni di P. MANZINI, *Antitrust e Privacy: la strana coppia*, in *I Post di AISDUE*, V, 10, 2023, p. 219.

[128] In tal senso, A. R. MARTÍNEZ, *A threshold can take you further than a statement – the court of Justice's ruling in Meta Platforms and Others (Case C-252/21)* in *Diritti Comparati*, 13 settembre 2023.

[129] Per una disamina del caso si veda A. LICASTRO, *Facebook è un monopolio? Spunti di riflessione a partire dal caso FTC v. Facebook*, in questa *Rivista*, 1, 2022, p. 340 ss.

[130] *Ibidem*.

[131] Cfr. N. M. RICHARDS, *The dangers of Surveillance*, in *Harv. Law Rev*., Vol. 126, 2013, p. 1934 ss. Inoltre, in tal senso, si veda C. VÉLIZ, *Privacy is Power: Why and How You Should Take Back Control of Your Data*, Penguin Random House, London, 2020, p. 48. L'Autrice, in merito al rapporto fra potere e tutela della *privacy*, sostiene che "[…] *privacy matters because the lack of it gives others power over you*» in cui per «*others*» si intendono le piattaforme digitali.

zione un maggior numero di dati, ottenuti proprio grazie al mancato rispetto della normativa in materia di *data protection*, consenta alle grandi società del digitale di aumentare il proprio potere informativo, seppur a discapito del processo competitivo.

In secondo luogo, Manzini si fa portatore di un'altra eccezione del tutto legittima e legata al problema dell'inversione dell'onere probatorio che sembra porsi in contrasto con quanto previsto dal regolamento UE 679/2016 secondo cui la prova della violazione della normativa in materia di *data protection* spetta al titolare del trattamento. Tuttavia, nel caso degli illeciti antitrust è all'autorità garante che spetta dimostrare l'illiceità della condotta commerciale [132]. Per risolvere quello che Manzini definisce «cortocircuito sul piano probatorio» pare potersi ipotizzare, invece, l'introduzione *de jure condendo* di un'effettiva inversione dell'onere probatorio, definita da Tommaso Valletti in materia di concentrazioni, «*rebuttable structural presumption*» [133]. L'ecosistema digitale dovrebbe dimostrare che alla degradazione di un fattore prettamente qualitativo come la *privacy* non corrisponde l'aumento del potere economico della piattaforma e, dunque, che non è stato pregiudicato in alcun modo né l'obbligo di pressione competitiva con le imprese concorrenti e neppure il diritto del consumatore di scegliere liberamente l'alternativa commerciale di cui avvalersi fra le tante esistenti.

Pare di poter dire che la decisione della Corte di Giustizia, criticabile o meno sotto vari aspetti, compia un tentativo più che meritorio di guardare al di là dello "steccato" in cui convivono due dei principali approcci che hanno contraddistinto la storia della regolazione dei mercati digitali degli ultimi anni, *deregulation* da un lato ed *ex ante regulation* dall'altro. Prospetta così, una strada alternativa o quanto meno complementare a quella tracciata fino ad ora. Occorre, riconoscere che la *data protection* ha un compito di per sé regolatorio che non contrasta, ma si integra alla perfezione con i principi della concorrenza; sempre che le autorità antitrust, compresa la stessa Commissione Europea, siano in grado di riconoscere alla *privacy* il suo valore di dimensione qualitativa della concorrenza alternativa al prezzo.

[132] Cfr. P. MANZINI, *Antitrust e Privacy: la strana coppia*, *Op.cit*., p. 219.

[133] Cfr. T. VALLETTI, *How to Tame the Tech Giants: Reverse the Burden of Proof in Merger Reviews*, in *Promarket*, June 28, 2021, p.4, consultabile al sito Promarket.org, (ultimo accesso: 4 ottobre 2023).