LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Data Protection

IL RAPPORTO TRA DATA PROTECTION E DIRITTO ANTITRUST ALLA LUCE DEL CASO "FACEBOOK GERMANY": ANALISI E PROSPETTIVE FUTURE

RELATORE
Chiar.mo Prof.
Pierluigi Congedo

CORRELATORE
Chiar.mo Prof.
Francesco Ricci

CANDIDATO
Giuseppe Filpi
Matr. 152373

ANNO ACCADEMICO 2021/2022

INDICE

CAPITOLO III

NORMATIVA VIGENTE, NUOVI STRUMENTI REGOLATORI E PREVISIONI SUL FUTURO

INTRODUZIONE

Il presente elaborato ha lo scopo di analizzare lo stato dell'arte sul rapporto tra *data protection* e diritto *antitrust,* sfociato nel recente caso "*Facebook Germany".* Questi due campi del diritto, considerati separati e distinti per decenni dalla giurisprudenza, con lo sviluppo della *data economy* hanno visto aumentare le proprie intersezioni e i casi *borderline.* L'affermarsi di grandi imprese tecnologiche che fanno della raccolta dei dati il fulcro del proprio modello di *business,* unito alle peculiarità delle piattaforme digitali e dei servizi che offrono, ha cominciato a far assottigliare la netta linea di separazione tra le due discipline, moltiplicando le zone grigie in cui le fattispecie sono rilevanti per entrambe. Con l'enorme potere economico accumulato da questi *big tech,* diversi interpreti si sono interrogati sull'efficacia degli strumenti giuridici tradizionali nel contrasto dei nuovi fenomeni, capaci di incidere pesantemente sui diritti degli individui in rete e sull'ordine democratico delle nazioni. Per questi motivi, la presente tesi avrà la seguente struttura: nel primo capitolo verranno ripercorse le tappe principali dello sviluppo di *Internet,* in modo da comprendere pienamente lo scenario digitale attuale. Analizzate le caratteristiche peculiari dei *business model* dei *tech giants,* con un *focus* su *Facebook* perché protagonista di un recente caso di diritto antitrust e di tutela dei dati personali in Germania (che chiameremo caso "*Facebook Germany*"), si metteranno in luce le grandi potenzialità, ma anche i grandi rischi, dei servizi digitali. Nel secondo capitolo, dopo aver considerato come i *Big data* stanno cambiando il panorama sociale ed economico globale, ci si concentrerà sull'analisi del caso "*Facebook Germany"* nelle sue diverse fasi, in cui il *Bundeskartellamt* (autorità garante della concorrenza tedesca) ha utilizzato il mancato rispetto delle regole della *data protection* come criterio nella sua valutazione *antitrust* sulla posizione dominante di *Facebook* nel mercato dei *social network.* Come si vedrà, la Corte Federale Tedesca ha confermato la decisione sanzionatoria dell'autorità, ma basando la sua decisione su una diversa ricostruzione più costituzionalmente orientata, auspicando la riforma del diritto *antitrust* tedesco. Si procederà così alla disamina della principale casistica europea sul tema, agli antipodi rispetto a quanto stabilito dal *Bundeskartellamt.* Sarà fatto cenno all'approccio interpretativo italiano al tema e ad un recente caso che ha interessato l'AGCM e *Facebook*, questa volta nell'alveo della tutela dei consumatori. In esso si è infatti stabilita la non gratuità della piattaforma, che ha nella raccolta e nell'utilizzo a fini

commerciali dei dati degli utenti il proprio corrispettivo. Nel terzo capitolo verranno considerate le attuali normative europee a tutela dei dati personali e della concorrenza, nell'ottica di valutare elementi comuni, differenze e possibili intersezioni. Terminata l'analisi dei diversi strumenti giuridici, si passerà allo studio delle proposte regolatorie più recenti in entrambi i campi in questione. Esempi emblematici sono il *Digital Markets Act (DMA)* ed il *Digital Service Act* (*DSA*), proposte di regolamento che puntano ad innovare profondamente la metodologia attuale sul controllo dei giganti del *web*. Si approfondirà il tema della tutela dei diritti costituzionalmente garantiti degli individui *online,* fondamento giuridico e filosofico del pacchetto di riforme europee, messi in pericolo dalle condotte abusive dei giganti digitali e dal *laissez-faire* delle istituzioni, come apparso negli scandali degli ultimi anni. Infine si analizzerà lo scenario internazionale, prendendo in considerazione l'approccio ai *big tech* ed alla rivoluzione digitale di grandi *player* quali gli Stati Uniti, la Cina e la Russia. Alla luce di tutto ciò, si tenterà di fare previsioni sui *trend* del prossimo futuro, proponendo soluzioni per la migliore interpretazione del rapporto tra *data protection* e diritto *antitrust,* la lotta allo strapotere dei giganti del *web* e la creazione di un sistema multilivello di tutela, adeguato all'era digitale, che abbia al centro i diritti della persona, poiché su questi temi si giocherà il futuro delle democrazie mondiali.

CAPITOLO I

PANORAMICA DEL MONDO DIGITALE E CONSIDERAZIONI INTRODUTTIVE SU FACEBOOK, SOCIAL NETWORK PROTAGONISTA DEL CASO TEDESCO

"The coronavirus crisis has demonstrated how crucial it is for citizens and businesses to be connected and to be able to interact with each other online. We will continue to work with Member States to identify areas where more investment is needed so that all Europeans can benefit from digital services and innovations."- Margrethe Vestager, Commissario europeo per la concorrenza[1].

1. Scenario digitale in cui viviamo e considerazioni preliminari sui *social network*

Sono trascorsi poco più di cinquant'anni dalla nascita di *Internet.* La sua forma embrionale, *ARPANET*, fu realizzata durante gli anni Sessanta negli Stati Uniti, nei pesanti anni della Guerra fredda, con lo scopo di connettere varie università americane, così da portare avanti e potenziare la ricerca tecnologica, soprattutto nel campo delle telecomunicazioni. Successivamente, a causa del difficile clima politico e dell'ombra sempre presente di un nuovo conflitto, questa volta atomico, le istituzioni americane decisero di sfruttare l'infrastruttura anche per scopi militari, perché, grazie al suo modello resiliente, sarebbe stata in grado di continuare a funzionare perfino in caso di distruzione parziale ad opera dei sovietici. All'epoca era impossibile prevedere l'impatto incredibile che quella limitata rete di reti avrebbe avuto sul mondo e sulla società e, infatti, quando le acque internazionali iniziarono a calmarsi e l'anima militare del progetto andò scomparendo (con la separazione definitiva da ARPANET di MILNET nel 1983, una rete unicamente con scopi militari, su decisione del Dipartimento della Difesa americano), questo potè finalmente mostrare tutte le sue potenzialità. Dopo anni di utilizzo sempre maggiore della rete e lo smantellamento

[1] Margrethe Vestager, *Press Release: New Commission report shows the importance of digital resilience in times of crisis,* (11 giugno 2020). L'ultimo accesso a tutti i siti è stato effettuato il 28 febbraio 2022.

definitivo dell'originaria ARPANET, ormai divenuta obsoleta, la svolta epocale si ebbe nel 1991 con la creazione del *World Wide Web (WWW)* ad opera degli informatici Robert Cailliau e Tim Berners-Lee (quest'ultimo pubblicò il primo sito *web* il 6 agosto 1991 presso il CERN di Ginevra)[2] e la successiva pubblicazione della stessa tecnologia da parte del CERN, nel 1993. A partire da quel momento, *Internet* smise di essere un *network* utilizzato unicamente da studiosi ed istituzioni e si tramutò in un universo vibrante e in continua espansione, grazie anche alla forte diffusione dei *personal computer,* che negli ultimi anni dello scorso secolo permisero ad un numero sempre maggiore di persone di connettersi[3]. Inizialmente, data anche la non grandissima capacità di calcolo delle macchine e la tecnologia da migliorare, le azioni degli utenti erano limitate e i contenuti accessibili prevalentemente passivi, rendendo le pagine *web* molto simili ad un'enciclopedia in formato digitale. Questo stadio "statico" di *Internet* è ciò che viene definito "Web 1.0", qualcosa di molto lontano dal mondo del Web 2.0 in cui viviamo oggi, uno spazio virtuale in cui le persone possono non solo cercare e inviare informazioni, bensì un ecosistema dinamico, veloce e innovativo, dove gli utenti interagiscono tra loro, generando dati e contenuti in quantità sempre crescente, contribuendo a plasmare il *network*[4]. Questo mondo digitale, prima qualcosa di parallelo e separato dal mondo "reale", ha finito per fondersi con esso e con ogni aspetto della vita delle persone[5], supportato dal progresso tecnologico e dai nuovi *device* in grado di restare sempre connessi, portando gli studiosi a teorizzare perfino un Web 3.0 ancor più automatizzato (il cosiddetto *Internet of things)*[6]. Ogni attività umana è stata contaminata dal digitale o è interamente migrata in esso (basti pensare al grande numero di attività

---

[2] È possibile visualizzare la versione originaria del primo sito web al seguente link: https://web.archive.org/web/20150717103715/http://info.cern.ch/hypertext/WWW/TheProject.html

[3] Editori dell'Encyclopedia Britannica, *Foundation of the Internet,* Encyclopedia Britannica.

[4] Varie istituzioni europee, *Manuale sul diritto europeo in materia di protezione dei dati,* (ed. 2018, Ufficio pubblicazioni UE, 2018), 405.

[5] Perfino l'ONU è giunta ad affermare l'accesso alla rete come un diritto civile centrale, seguita dal Parlamento Europeo (Parlamento Europeo, *Risoluzione del Parlamento europeo dell'11 dicembre 2012 Una strategia di libertà digitale nella politica estera dell'UE (2012/2094 (INI)), 11 dicembre 2012)* e le altre istituzioni. Il parlamento italiano ha approvato il 14 luglio 2015 la *Dichiarazioni dei diritti in Internet* ed è sempre più al centro del dibattito politico e pubblico l'introduzione nella Costituzione italiana del diritto ad *Internet,* proposta per la prima volta dall'illustre giurista Stefano Rodotà nel 2010 (Flavia Cerquozzi, *"Diritto di accesso ad Internet" e Costituzione,* Iusinitinere (24 ottobre 2020)).

[6] Cfr. Commissione europea, *Advancing the Internet of Things in Europe,* SWD/2016/0110 final, [2016].

commerciali fisiche che hanno una pagina *web* per la vendita dei prodotti e di quelle che si basano solo sull'*e-commerce),* e questa "rete di rete" di fatto ora costituisce l'impalcatura che regge la nostra società, con tutti i vantaggi ed i rischi che ne derivano[7].

Nell'era del Web 2.0, tra le applicazioni e i servizi di maggior successo che hanno cambiato la vita delle persone, troviamo senza dubbio i *social network* (d'ora in poi "*SN*"), piattaforme che permettono agli utenti di crearsi una rete di persone e collegamenti o entrare a farne parte[8]. Questi costituiscono la rappresentazione e l'effetto più alti del processo di fusione tra il reale e il virtuale, perché non si tratta più di un mero mezzo di comunicazione come può essere stato il telefono o la posta elettronica, bensì di un'effettiva dimensione alternativa in cui le persone, consapevolmente o meno, si ritrovano a vivere. I *social* sono ormai molti e diversi, ma tutti hanno l'effetto di creare uno spazio digitale, una sorta di agorà 2.0, dove le persone possono conoscersi, rimanere in contatto, pubblicare e condividere i propri pensieri e i propri contenuti, creando un doppione digitale della propria vita sociale e del proprio io in grado, in ultima analisi, di influenzare non solo ciò che accade in rete, ma anche il mondo reale. Tutto questo diventa ancora più concreto se consideriamo ciò che è avvenuto durante i mesi iniziali della pandemia. Quando il mondo intero è stato costretto a ricorrere alla misura di pubblica sicurezza dei *lockdown* totali (alternati con coprifuoco, prerogativa delle due guerre mondiali), le persone, non potendo più uscire dalle proprie abitazioni per evitare di diffondere il *virus* e vedendo la propria "vita reale" quasi annichilita, si sono trovate costrette a rifugiarsi nella propria vita virtuale e ad affollare gli spazi digitali, sempre accessibili, aperti e sicuri. Questo "esodo di massa" non è stato solo dei

---

[7] Per comprendere e visualizzare numericamente questa tendenza in continua espansione consideriamo che si è passati da soli 10.000 computer connessi ad Internet nel 1989, su una popolazione mondiale di circa sei miliardi di persone, a ben cinque miliardi di utenti della rete su un totale di quasi otto miliardi di persone (il 65%) nel Marzo 2021. Il tasso di crescita dal 2000 ad oggi è del 1.331,9 % e non accenna a diminuire, anche per effetto della pandemia che nell'ultimo anno e mezzo ha accelerato e forzato il processo di digitalizzazione, con paesi in cui la media di utenti in rete rispetto alla popolazione totale sfiora il 100%. Fonti: internetworldstats.com (Marzo 2021) (https://www.internetworldstats.com/stats.htm); wearesocial.com (Gennaio 2021) (https://wearesocial.com/digital-2021); Filippo Mastroianni, *Come è cambiata la geografia del Web (dal 1995 al 2015),* IlSole24Ore (9 luglio 2017).

[8] Gruppo di lavoro articolo 29 (2009), *Parere 5/2009 sui social network on-line*, WP 163, (12 giugno 2009), 4.

comuni cittadini, ma anche di istituzioni, università e professionisti che hanno sfruttato le opportunità del mondo digitale per tentare di continuare la vita precedente all'emergenza, avvalendosi, soprattutto, dei *social network*. Per la prima volta dalla nascita di *Internet* il digitale ha prevalso sul reale e considerando i difficili tempi che l'umanità dovrà affrontare (tra condizioni climatiche sempre più estreme e epidemie purtroppo sempre più ricorrenti[9]) questo *trend* non potrà che rafforzarsi, rendendo queste piattaforme un'infrastruttura sempre più centrale e fondamentale. Considerato questo scenario e l'importanza indiscutibile dei *social network* per la società, è fondamentale analizzare le caratteristiche di successo di queste piattaforme. Dal punto di vista tecnico le caratteristiche che rendono i *SN* vincenti e di successo sono principalmente tre: lo sfruttamento dell'effetto *network* (diretto e indiretto); un modello di *business* ad alto potenziale in grado di massimizzare i profitti, connettendo soggetti da entrambi i lati del mercato (cosiddette *multi-sided platforms);* assenza di limitazioni spaziali e temporali , poiché basta una connessione ad *Internet* ad un *device* per usufruire dei servizi in ogni luogo e momento[10]. Partendo dall'effetto *network,* questo può essere di due tipi, diretto ed indiretto. Grazie all'effetto *network* diretto più utenti partecipano alla rete e più vi è un incentivo ad entrare a farne parte, creando un circolo virtuoso che porta alla crescita esponenziale della piattaforma. Oltre ad incentivarne l'entrata, questo effetto "di rete" rende anche più difficile la scelta di lasciare la stessa, perché si perderebbe il beneficio derivante dalla presenza su quella determinata piattaforma di una varietà di utenti e collegamenti, non rinvenibili in altre piattaforme concorrenti[11]. L'effetto *network* indiretto, invece, è leggermente diverso perché il risultato cui si vuole tendere è sempre la crescita della rete, ma, questa volta, l'incentivo

---

[9] Sam Fleming, *EU must prepare for 'Era of pandemics', Von der Leyen says,* Financial Times (28 febbraio 2021).

[10] Wei Cui, *The Digital Services Tax: A Conceptual Defense* (22 aprile 2019). 73(1) Tax Law Review 69-111 (2019), disponibile su SSRN:
https://ssrn.com/abstract=3273641 o http://dx.doi.org/10.2139/ssrn.3273641

[11] La prova evidente di questa affermazione la si è avuta nei mesi scorsi, quando i cambiamenti dei termini e delle condizioni del servizio di messaggistica Whatsapp, collegato a Facebook, ha generato preoccupazione negli utenti per i possibili effetti negativi alla loro *privacy.* Si è così tentato di migrare su una piattaforma concorrente, Signal, molto simile alla prima ma con un occhio più attento alla *privacy* e alla sicurezza degli utenti, e si è scoperto il grande limite di dover convincere i propri contatti Whatsapp a trasferirsi per poter continuare a comunicare. In questo modo la maggior parte delle persone, seppur preoccupate per la propria sicurezza e riservatezza, sono state costrette a rimanere su Whatsapp.

per entrare a farne parte è costituito dalla presenza di utenti appartenenti al versante opposto del mercato (da qui, la formula di "*two-sided markets*" o "mercati a due versanti"). Si ottengono in questo modo le cosiddette esternalità di rete, dove il valore aggiunto di un prodotto o di un servizio è direttamente proporzionale al numero di utenti che lo utilizzano[12]. L'esempio è il caso di *Facebook (FB)* che unisce il mercato dei *social network* con quello dell'*advertising*: gli appartenenti al *SN* usufruiscono "gratuitamente" dei servizi della piattaforma e i fornitori di pubblicità, interessati a raggiungere il maggior numero possibile di persone, hanno un vasto bacino di utenti verso cui dirigere i loro annunci[13]. Proprio per questo motivo i *social,* nonostante le loro particolarità e diversità, sono *multi-sided platforms,* e giungiamo, qui, al loro secondo punto di forza, il modello di business, strettamente collegato all'effetto *network*. Partendo da quanto già accennato con l'esempio di *FB* possiamo comprendere cosa si intenda per "piattaforma a più versanti": sono piattaforme con due o più gruppi di utenti dipendenti tra loro che utilizzano la piattaforma come strumento di incontro per creare valore aggiunto[14]. La piattaforma assume, così, il ruolo di catalizzatore, facilitando l'interazione tra i diversi gruppi di utenti che, altrimenti, sarebbe difficile da raggiungere[15]. Per aumentare questo processo e rendere ancor più dirompente l'effetto *network* indiretto, nella quasi totalità dei casi il servizio offerto è gratuito sul lato consumatori (non è proprio così, come a breve si vedrà) per incentivarli ad entrare. Strettamente collegati ai concetti appena richiamati ci sono quelli di economie di scala e scopo. Si hanno economie di scala quando, all'aumentare della produzione, si ha una diminuzione dei costi medi di produzione, mentre quelle di scopo nel caso in cui, producendo più tipologie di prodotti, a parità di fattori di produzione, si ottiene lo stesso effetto di diminuzione dei costi (come avviene ad esempio con *Microsoft,* che è produttrice sia dei componenti *hardware* che dei *software* a parità di fattori)[16]. Questo

[12] Nicholas Economides, *Network Externalities, Complementarities, and Invitations to Enter*, (1997), disponibile su SSRN: https://ssrn.com/abstract=2237.

[13] Yun, John M., *Overview of Network Effects & Platforms in Digital Markets* (11 novembre 2020), 1-10. The Global Antitrust Institute Report on the Digital Economy, 2.

[14] ibidem *10-12.*

[15] Lapo Filistrucchi, Damien Geradin, Eric van Damme, Eric Affeldt, *Market Definition in Two-Sided Markets: Theory and Practice*, Journal of Competition Law and Economics, vol. 10 (2), 2014, 293-339. Ancora, Andrei Hagiu, Julian Wright, *Multi-Sided Platforms*, International Journal of Industrial Organization, Vol. 43, 2015, (19 marzo 2015).

[16] Cfr. John Sloman, Dean Garratt, *Microeconomia,* Il Mulino (2014), 128- 130.

significa che più un soggetto economico è in grado di aumentare la propria produzione e affermare la propria posizione nel mercato, e più si otterrà un "effetto valanga" che renderà sempre maggiori i risultati. Quanto analizzato permette di comprendere i fenomeni di *market tipping* che interessano i *SN*. Grazie all'effetto *network,* ai diversi servizi offerti a costo zero e alla mole enorme di dati in possesso, queste piattaforme d'attenzione (che quindi sfruttano il tempo e l'attenzione che gli utenti vi dedicano per mostrargli pubblicità, principalmente mirate[17]) riescono a sbaragliare la concorrenza, creando barriere d'entrata al loro mercato rilevante[18]. Gli *switching costs* degli utenti verso altre piattaforme concorrenti sono molto elevati e impediscono la migrazione perché si perderebbero i benefici del *network,* ed anche in casi di *multi-homing,* utenti iscritti a più servizi concorrenti, il pericolo di chiusura del mercato non diminuisce molto se questi sono controllati o fanno parte del gruppo della piattaforma dominante (come succede con *Facebook*, che contiene sotto la sua egida i *social* concorrenti *Instagram* e *Snapchat).* Se aggiungiamo a tutto ciò il fatto che è possibile iscriversi ai *social* senza vincoli di tempo e spazio sfruttando la fluidità e la velocità di *Internet* e le strategie commerciali delle società che le gestiscono, orientate verso la crescita più che ai profitti nel breve termine, ne deriviamo la progressiva mutazione di tali piattaforme in veri e propri giganti del *web* (c.d. "*Big Tech*") che detengono un potere di mercato grandissimo e un'influenza decisiva sulla vita di miliardi di persone. Oltre a queste ragioni tecniche ed economiche, dietro il successo dei *SN* vi è anche la conoscenza e lo sfruttamento del funzionamento del cervello umano e degli inconsci meccanismi che lo regolano. Grazie agli enormi progressi delle neuroscienze sappiamo che le informazioni viaggiano tra i neuroni sotto forma di impulsi elettrochimici e che ogni parte del cervello ha il proprio ruolo[19]. Un'interessante teoria che tenta di spiegare proprio quest'ultimo punto è quella del "cervello trino" elaborata Paul D. MacLean negli anni Sessanta, secondo cui l'attuale struttura del nostro cervello conserva in sé le tracce del proprio passato evolutivo. La parte più antica (comparsa circa 500 milioni di anni fa),

---

[17] David Evans, *Attention Platforms, the Value of Content, and Public Policy*, Review of Industrial Organization (2019), 54.

[18] Özlem Bedre-Defolie, Rainer Nitsche, *When Do Markets Tip? An Overview and Some Insights for Policy*, Journal of European Competition Law & Practice, Volume 11, Issue 10, (dicembre 2020), Pagg. 610–622,

[19] Intesa Sanpaolo Innovation Center, IMT School for Advanced Studies Lucca, *Neuroscience Impact,* 40-50.

composta da tronco cerebrale e cervelletto, costituisce il cervello rettiliano (così chiamato perché presente anche nei rettili) ed è adibito alle funzioni fondamentali del corpo insieme agli istinti di sopravvivenza. Poi troviamo il sistema limbico, formato da ippocampo, amigdala, bulbo olfattivo, ipotalamo, gangli basali e corteccia cingolata, responsabile della memoria, dell'apprendimento, delle emozioni e di tutti i nostri comportamenti sociali ma anche reattivi alle stimolazioni primarie (amigdala e cingolato sovrintendono all'istinto di 'lotta o fuga' ("*fight or flight*"), nel linguaggio delle neuroscienze). Infine la parte più "recente", la corteccia cerebrale, è alla base della razionalità, del pensiero critico e analitico e di tutte quelle capacità superiori caratteristiche della specie umana[20]. I *social* sono programmati per andare a colpire proprio le parti più istintive e poco razionali del nostro cervello, le più "silenziose" ma allo stesso tempo influenti, per coinvolgerci e farci compiere inconsciamente le azioni che gli sviluppatori delle piattaforme desiderano, facendo leva sui nostri desideri e i nostri istinti più profondi: il desiderio di essere parte di un gruppo e sentirsi da esso accettati, la paura di essere esclusi e soli, il bisogno di conferme e sempre nuovi e maggiori stimoli, l'egocentrismo. Istinti primari e potentissimi, già noti nel settore della pubblicità e della moda dove notoriamente si fa leva su di essi[21]. È stato inoltre provato che più un comportamento viene ripetuto nel tempo e più nel nostro cervello si consolidano determinati percorsi neuronali, cristallizzando le sensazioni provate e generando un'abitudine[22]. Questi meccanismi vengono ampiamente sfruttati dalle piattaforme per attirare l'attenzione degli utenti e rendere la loro esperienza più stimolante, ma negli ultimi anni ciò ha dato origine al nuovo, preoccupante, fenomeno della dipendenza dai *social network.* Si tratta di una dipendenza comportamentale caratterizzata dall'uso compulsivo e non più controllabile di queste piattaforme, tale da causare effetti psicofisici simili a quelli osservabili nella ludopatia e nel tabagismo, come aumento di ansia e stress, diminuzione dell'attenzione e sbalzi d'umore, che a

[20] Paul D. MacLean, *Evoluzione del cervello e comportamento umano. Studi sul cervello trino*, Einaudi (1984).

[21] Thabani Nyoni, Wellington Garikai Bonga, *Neuromarketing: No Brain, No Gain!* (28 febbraio 2017), Dynamic Research Journals' Journal of Economics and Finance (DRJ-JEF), Volume 2, Issue 2, pp 17-29., disponibile su SSRN: https://ssrn.com/abstract=2925857.

[22] Julie Hani, (Fit4D), *The Neuroscience of behavior change,* StartupHealth, 8 agosto 2017. (https://healthtransformer.co/the-neuroscience-of-behavior-change-bcb567fa83c1). Si ricordi la celebre frase di Horace Mann: *"le abitudini sono come una fune. Ne intrecciamo un trefolo al giorno e ben presto non riusciamo più a spezzarla".*

lungo andare possono sfociare in vera e propria depressione[23]. Sono stati compiuti molti studi sul punto ed è emerso che l'utilizzo eccessivo dei *SN* porta all'attivazione delle stesse aree del cervello interessate nell'assunzione di sostanze stupefacenti, i gangli della base, molto importanti per i meccanismi di ricompensa grazie alla loro elevata capacità di produrre dopamina[24]. Questi processi sono fondamentali perché su di essi si basano i sistemi di apprendimento degli esseri umani, sfruttando il rilascio di dopamina per associare comportamenti ed esperienze a sensazioni di piacere, in modo da fissare e rafforzare quelle che portano beneficio al corpo[25]. Confrontandosi con sempre nuovi stimoli, il cervello seleziona le azioni che comportano maggiori ricompense, portandoci a ripeterle e ricercarle per accrescere il benessere[26]. Le piattaforme di attenzione come i *social network* si avvalgono di questo sistema, sfruttando le loro funzionalità per fornire continui stimoli e "ricompense" agli utenti, che spesso sono inferiori nella vita quotidiana, causando il rilascio di elevati quantitativi di dopamina. Nel breve termine questa sensazione di benessere è positiva per l'umore e la motivazione, ma a lungo andare, considerando che le piattaforme sono realizzate in modo da adattarsi ad ogni utente per fornirgli una migliore esperienza, si rischia di diventarne dipendenti[27]. I sopracitati effetti negativi a livello fisico e mentale sono ancora più dirompenti in soggetti fragili, come gli adolescenti, che trovano nei *social* interazioni e partecipazione che nella vita manca loro, diventando il loro rifugio sicuro. In essi sono stati osservati effetti mentali e sociali negativi, come il peggioramento dei risultati scolastici e il

---

[23] Jena Hilliard, Theresa Parisi, *What is social media addiction?,* Addiction Center, (8 ottobre 2020). (https://www.addictioncenter.com/drugs/social-media-addiction/)

[24] Ad esempio, Yubo Hou, Dan Xiong, Tonglin Jiang, Lily Song, Qui Wang, *Social media addiction: Its impact, mediation, and intervention*. Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13*(1), (2019) Articolo 4.

Ancora, Cecilie Schou Andreassen, *Online social network site addiction: A comprehensive review.* Current Addiction Reports*, 2*, (2015) 175–184.

[25] Oscar Arias-Carrión, Maria Stamelou, Eric Murillo-Rodríguez, Manuel Menéndez-González, Ernst Pöppel, *Dopaminergic reward system: a short integrative review,* Int Arch Med. 2010; 3: 24, (6 ottobre 2010).

[26] Marcus Stephenson-Jones, , Kai Yu, Sandra Ahrens, Jason M. Tucciarone, Aile N. van Huijstee, Luis A. Mejia, Mario A. Penzo, Lung-Hao Tai, Linda Wilbrecht, Bo Li, *A basal ganglia circuit for evaluating action outcomes*. Nature 539, 289–293 (2016). (https://doi.org/10.1038/nature19845).

[27] Vikram Bhargava, Manuel Velasquez, *Ethics of the Attention Economy: The Problem of Social Media Addiction*. Business Ethics Quarterly*, 31*(3), (2021). 321-359.

persistere di stati d'animo negativi, in maggior misura rispetto ad altre fasce d'età, generando la preoccupazione di famiglie ed istituzioni[28]. Nelle persone che soffrono di questi disturbi e sono caduti nella dipendenza, è risultato che limitando e razionalizzando l'utilizzo dei *SN* si giunge, fin da subito, a sorprendenti effetti positivi, con un aumento dell'attenzione, un maggior controllo delle proprie emozioni e un risanamento dei rapporti sociali [29]. Naturalmente non possiamo demonizzare queste piattaforme perché come osservato esse hanno portato alla società innumerevoli benefici, però è giusto avere la piena consapevolezza del loro funzionamento.

Dopo questo veloce spaccato del variegato contesto digitale odierno, il passo successivo sarà concentrarsi sul più diffuso e "popolato" tra i *social network, Facebook*, per analizzarne la storia ed il funzionamento e carpire i segreti e le criticità in esso racchiusi, così da poter poi meglio comprendere i motivi che hanno spinto le istituzioni di tutto il mondo, soprattutto nel campo della concorrenza e della protezione dei dati personali, a muovere le contestazioni nei confronti di talune condotte (in ipotesi, illecite) dallo stesso poste in essere, come avvenuto in Germania col *Bundeskartellamt*.

2. *Facebook:* modello di *business*, ruolo centrale dell'*advertising* e rilevanza per i campi della *data protection* e del diritto *antitrust*

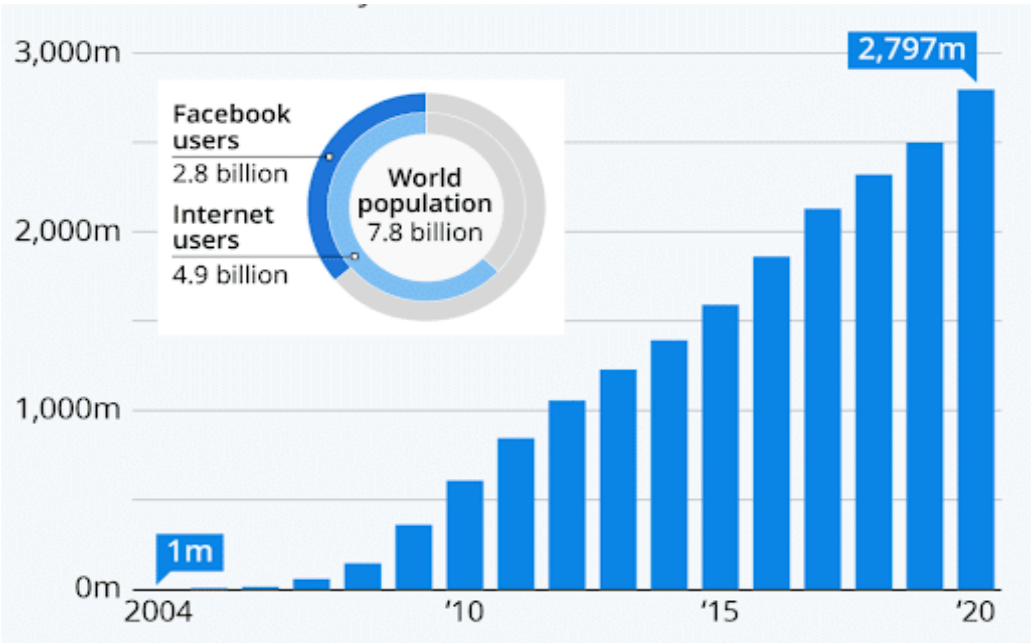
Con quasi tre miliardi di utenti su un totale di 4.9 miliardi di persone online (di cui 4.3 utenti attivi sui *social)* ad aprile 2021 (+12% rispetto all'anno precedente)*, Facebook* è di diritto il *social network* più importante ed utilizzato, tanto da essere l'unica piattaforma *social* a far parte delle proverbiali "GAFAM" (*Google, Amazon, Facebook,*

[28] Judita Habermann, *Self-Control and Social Media Addiction (Facebook): A Quantitative Analysis* (26 giugno 2021). Disponibile su SSRN: https://ssrn.com/abstract=3875633.

A riprova di quanto questo fenomeno rischi di diventare sistemico è utile ricordare alle parole di Chamath Palihapitiya, ex vicepresidente di *Facebook,* il quale ha affermato: " The short-term dopamine-driven feedback loops we've created are destroying how society works... . I feel tremendous guilt... . I think ... we kind of knew something bad could happen" (Amy B. Wang, *Former Facebook VP says social media is destroying society with 'dopamine-driven feedback loops',* The Washington Post, (12 dicembre 2017).

[29] Melissa G. Hunt, Rachel Marx, Courtney Lipson e Jordyn Young, *No More FOMO: Limiting Social Media Decreases Loneliness and Depression Read More,* Journal of Social and Clinical Psychology, (2018).

Apple e *Microsoft*, appunto), i *tech-giants* che stanno cambiando il mondo e dominando i mercati [30]. Non solo *FB* è la piattaforma sociale con più utenti attivi, l'app per dispositivi mobili più scaricata e tra i siti *web* più visitati, ma grazie alla strategia adottata negli anni dalla società la maggioranza dei *social* concorrenti sono stati acquisiti dalla stessa, creando un impero digitale che ogni giorno assorbe la vita di miliardi di persone[31].



Il grafico mostra l'aumento degli utenti di Facebook negli anni.

Fonte: Statista.com

Prima di diventare il gigante tecnologico che conosciamo oggi, *Facebook* ha dovuto affrontare una lunga strada ed una corsa che, per quanto veloce ed inarrestabile, ha avuto diversi ostacoli da superare[32]. Nel giro di pochi anni vengono introdotte e

[30] Wearesocial.com (https://wearesocial.com/blog/2021/04/60-percent-of-the-worlds-population-is-now-online).

[31] ibidem.

[32] La nascita di Facebook infatti risale al 4 febbraio 2004 quando fu messo in rete il sito web "Thefacebook.com" sviluppato e programmato dall'allora diciannovenne Mark Zuckerberg con l'aiuto dei *co-founder* Dustin Moskovitz, Chris Hughes ed Eduardo Saverin. Sin dall'inizio la storia di Facebook fu abbastanza travagliata, già a partire dal suo predecessore "Facemash", un sito web in cui era possibile votare le foto degli studenti di Harvard per stabilire il più *cool,* perché per ottenere le foto degli studenti Zuckerberg accedette ad aree ed informazioni protette della rete universitaria e dopo la messa online la

migliorate le varie funzionalità della piattaforma per renderla sempre più attraente per gli utenti, raggiungendo i 500 milioni di utenti attivi nel 2010. Nel 2011 viene introdotto *Messenger,* un servizio che permette di inviare messaggi agli altri utenti del *network,* mentre nel 2012 viene acquisito Instagram, *social* di condivisione di foto e video, per un miliardo di dollari. Nel 2014 vengono acquisite *Whatsapp* (per ben 19 miliardi), *app* di messaggistica istantanea, e *Oculus,* società produttrice di visori per la realtà aumentata, mentre sempre nuovi e più innovativi servizi vengono sviluppati per la piattaforma "madre" e le collegate, potenziando e rafforzando la propria posizione di *social network* "*over the top".* Nel 2017 viene superato il traguardo dei 2 miliardi di utenti mensili attivi (soltanto di FB, senza considerare le app collegate) e nel 2019 è annunciato il progetto di una *stablecoin,* una valuta digitale agganciata al valore del dollaro, di nome "*Libra"* in grado di permettere agli utenti del *social* di ricevere e inviare denaro istantaneamente (lanciando, per questo fine, nel 2020 un portafoglio digitale chiamato Novi)[33]. Il progetto di *Libra*, per via delle varie opposizioni a più livelli da parte delle istituzioni americane, che vedevano questa mossa come un tentativo della società di aumentare talmente tanto la propria potenza economica da sfidare quella di banche e nazioni, si è andato ridimensionando nel corso dei mesi, giungendo alla vendita degli asset tecnologici e avviando la chiusura del consorzio dedicato. Questo fa comunque ben intravedere quale sarà la direzione che la società e la piattaforma stanno seguendo. Come infatti testimoniano le dichiarazioni durante questi ultimi mesi del CEO Mark Zuckerberg ed il *rebranding* da *Facebook* in "*Meta"*[34]*,* l'obiettivo che avrà *il SN* nei prossimi anni è quello di diventare sempre più un "metaverso", un ecosistema ibrido tra

---

popolarità del sito mandò in *crash* il sistema, facendogli rischiare l'espulsione. Dopo soli sei giorni dalla pubblicazione del sito tre studenti della stessa università, Cameron e Tyler Winklevoss e Divya Narendra, accusarono Mark di aver rubato la loro idea e di averli truffati fingendo di volerli aiutare nella creazione di "HarvardConnection.com", un *social network* (molto simile a *FB* come funzionalità) che avrebbe permesso agli studenti di Harvard di connettersi e rimanere in contatto, al solo fine di sfruttare ciò che stavano creando per migliorare la proprio piattaforma#. Inizialmente Facebook era aperto solo agli studenti di Harvard ma il suo grande e immediato successo (a fine 2004 gli utenti attivi erano già 1 Milione) lo fece espandere prima alle altre università vicine, poi ad altre istituzione e compagnie americane e infine, da settembre 2006, fu possibile per tutti accedervi ed iscriversi. Entro la fine del 2004 venne fondata la società *"Facebook Inc."* e nel 2005 acquistato il nome a dominio attuale per 200.000 dollari.

[33] Company Info di Facebook. (https://about.facebook.com/company-info/)

[34] https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ .

reale e digitale in cui le persone possono accedere sfruttando le tecnologie a realtà aumentata, acquistare beni e servizi digitali utilizzando moneta elettronica basata sulla tecnologia Blockchain e interagire tra loro, rendendo ancora più sottile il confine tra ciò che è reale e ciò che è virtuale[35]. Questo progetto ambizioso potrebbe rivoluzionare ancora una volta il nostro stile di vita, ma molti mettono in guardia dal rischio di creare un mondo distopico e centralizzato nelle mani di pochi[36]. Per gli utenti iscriversi ed utilizzare la piattaforma di *Facebook* è gratuito. Guardando però le cifre dei bilanci della società (29 miliardi di fatturato solo nel secondo trimestre del 2021) e i costi sostenuti per acquisire *Instagram, Whatsapp* e le altre piattaforme ora nella galassia *FB*, sembra un paradosso che una società che offre servizi gratuiti sia tra le più ricche e in crescita a livello mondiale. Il segreto di questi immensi guadagni sta nel modello di *business* della società basato sulla pubblicità e sui dati. *Facebook* è infatti una *multi-sided* platform capace di connettere i consumatori, da un lato, e i fornitori di pubblicità dall'altro. Come già illustrato, i primi vengono attratti dalle funzionalità della piattaforma, ormai una vera e propria finestra sul mondo, e dal non dover pagare per utilizzarne i servizi, i secondi dalla grande presenza dei primi, pagando alla piattaforma il prezzo per mostrare i propri *ads*. Quella di ottenere i propri introiti dalla pubblicità non è una novità, infatti le televisioni private e le radio utilizzano questo modello di finanziamento da molto prima dei *social network,* ma *Facebook* aggiunge un tassello in più al sistema: l'utilizzo dei dati degli utenti. Mentre nelle televisioni, nelle radio e perfino nei cartelloni lungo le strade gli annunci vanno praticamente "a vuoto", messi lì sperando di fare effetto ma senza ulteriori capacità, qui l'utente, dal momento in cui si iscrive e ogni volta che utilizza la piattaforma, fornisce informazioni su se stesso, sui suoi gusti e le sue preferenze, rendendo possibile una profilazione sempre più accurata. L'intero *social* è progettato per questo, infatti al momento dell'iscrizione viene chiesto di accettare i termini e le condizioni della piattaforma che prevedono di fornire il consenso alla raccolta dei dati generati dal suo uso. A tal riguardo, tra le "armi" più efficienti nell'arsenale di *Facebook* troviamo il *contextual advertising* ed il *remarketing advertising.* Il primo consiste nel mostrare pubblicità che riguardano lo stesso argomento o contesto della pagina *web* visitata (ad esempio se si visita una pagina che

[35] Hannah Towey, *Mark Zuckerberg said he wanted to transform Facebook from a social-media company into 'a metaverse company',* Businessinsider (22 luglio 2021).

[36] John Mac Ghlionn, *The metaverse: Mark Zuckerberg's Brave New World,* Cointelegraph, (11 agosto 2021).

tratta di auto e motori verranno mostrati *ads* contenenti annunci per le polizze auto), mentre nel secondo vengono mostrati annunci di prodotti già visualizzati[37]. "*Non è più il petrolio la risorsa più preziosa al mondo, ma i dati*" recita il titolo di un articolo dell'*Economist* pubblicato nel 2017, e questo ne è l'esempio lampante[38]. Il fine dichiarato di questa continua raccolta è di migliorare le funzionalità della piattaforma e donare un'esperienza di più alto livello ai consumatori, ma *FB* si finanzia con la pubblicità e le funzionalità che offre sono solo un incentivo per entrare e restare nel *network*, mentre i reali interlocutori della piattaforma sono gli *advertiser* interessati ad acquistare a caro prezzo il reale prodotto della piattaforma: i suoi utenti[39]. Seguendo ogni attività con algoritmi sempre più sofisticati e perfezionati grazie al *machine learning*, mettendo insieme ed aggregando le piccole "impronte" lasciate in giro dagli utenti come pezzi di un puzzle, vengono creati *database* così ricchi di informazioni da competere con la reale conoscenza che ognuno ha di sé. Queste preziose informazioni vengono così vendute agli inserzionisti in modo da poter mostrare annunci sempre più pertinenti e allineati con le preferenze che i dati rivelano. Oltre alle informazioni che gli utenti acconsentono a cedere è interessante notare che *Facebook* è in grado di ottenere dati perfino da coloro che ancora non sono iscritti al *social network.* Può sembrare strano e paradossale, soprattutto dal punto di vista della base giuridica di questa operazione, ma già la Corte di Giustizia dell'Unione Europea ("CGUE") ha preso atto e dichiarato questa possibilità nella sentenza del caso "*Fashion ID*" del 2019[40], in cui si discuteva sulla titolarità del trattamento dei dati personali nell'ambito di una pagina web che conteneva l'iconico pulsante *"Like"* di *FB* in modo che le persone potessero cliccare e farlo risultare direttamente anche sul *social,* senza bisogno di dover aprire la piattaforma. In particolare è stato osservato come i dati personali dei visitatori della pagina *web*, per quanto ignari e senza aver dato il loro consenso, venissero trasmessi a *Facebook* semplicemente visualizzando il sito, anche senza cliccare il *Like.* Le informazioni trasmesse sono quelle dei *cookie,* piccoli *file* contenuti nel device utilizzato per navigare in rete e che permettono di usufruire di molti servizi che le

[37] Asuncion Esteve, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA,* International Data Privacy Law (2017, Vol. 7, No. 1), 40.

[38] "*The world's most valuable resource is no longer oil, but data*", The Economist, (6 Maggio 2017).

[39] Come d'altronde affermò il famoso informatico Jaron Lanier, "*Se il servizio è gratis, il prodotto sei tu*".

[40] C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, 29 febbraio [2019], ECLI:EU:C:2019:629, para 98.

pagine *web* offrono, che per quanto limitate possono comunque essere associate alle altre già in possesso, creando valore aggiunto. Visitando un sito in cui è stato posto il pulsante *Like,* i *cookie* vengono inviati a *Facebook* e nel caso l'utente sia già iscritto al *social* saranno inseriti nel *database* a lui associato. Se invece il visitatore del sito non è ancora iscritto alla piattaforma verrà creata un'apposita banca dati con un nuovo codice identificativo a cui sarà collegato il profilo dell'utente nell'eventualità questo decida di iscriversi. In questo modo *Facebook* riesce a tracciare perfino i suoi futuri e possibili utenti e, visto l'elevatissimo numero di siti *web* che presentano i pulsanti ad esso collegati, è concreto il rischio di vedere assottigliarsi il confine tra gli utenti di *Internet* e quelli iscritti al *social,* visto che anche senza essere iscritti *Facebook* raccoglie informazioni su di noi[41]. Questo è uno dei profili critici che hanno portato le autorità *antitrust* europee e statunitensi ad interrogarsi sulla legittimità di queste condotte e del potere di mercato con esse conquistato, poiché i dati sono alla base del funzionamento della piattaforma e delle sue entrate. Per i motivi sopra esposti si comprende la rilevanza del fenomeno per il diritto *antitrust* e la *data protection,* oltre che le ragioni che hanno portato le autorità competenti ad agire. Questo tema verrà trattato nel prossimo capitolo ma è già possibile valutare, a questo stadio della trattazione, come, nonostante le innovazioni, l'incredibile crescita e i benefici offerti da *Facebook* e le altre piattaforme digitali, molteplici siano le criticità che si celano dietro al funzionamento e all'articolazione pratica di tale *business.*

3. Criticità della piattaforma e scandali negli anni

I giganti del web non sono andati esenti da scandali di portata planetaria e guardando alla storia di *Facebook*, si è assistito all'insorgere di controversie di indubitabile risonanza mediatica. Per quanto è di interesse in questa sede, occorre far menzione di un caso che ha disvelato tutti i pericoli che i *social network* nascondono e che molti hanno sottovalutato, vale a dire lo scandalo di *Cambridge Analytica (CA). CA* è stata una società di consulenza politica inglese che grazie all'analisi dei dati e la profilazione

[41] Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!* (November 30, 2010), Tilburg Law School Legal Studies Research Paper Series No. 03/2011, pag. 5. Disponibile su SSRN: https://ssrn.com/abstract=1717563

psicometrica era in grado di spingere le persone a votare in un determinato modo in base alle pubblicità mostrate[42]. Fondata nel 2013 da SCL, compagnia di comunicazione strategica, e parte del suo gruppo, *CA* è divenuta famosa dopo aver partecipato alle campagne elettorali di Ted Cruz e Donald Trump e al referendum della Brexit (oltre che ovviamente al suo scandalo con *Facebook*). La società si rivolse al *data scientist* Aleksandr Kogan, ricercatore presso l'Università di Cambridge, nel 2014 interessata dai dati su *Facebook* a disposizione del progetto che stava portando avanti col suo team di ricerca. Disposta a pagare i ricercatori per i dati, non raggiunto un accordo solo Kogan si disse disposto a lavorare con loro, offrendosi di creare un'apposita applicazione per raccogliere i dati di cui *CA* aveva bisogno. La società accettò e aiutò Kogan a creare una nuova e separata società, la *Global Science Research,* allo scopo di raccogliere i dati che sarebbero poi stati passati a *CA*.

Venne così creata l'app "*This is your digital life*" contenente un test della personalità con un determinato numero di domande in grado di mettere in luce le caratteristiche principali della personalità degli utilizzatori (secondo i cinque parametri del modello OCEAN: *Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism)* e a cui bisognava accedere con le proprie credenziali ed il proprio profilo *Facebook*. Non solo usando l'app si accettava di cedere i propri dati presenti su *FB*, ma perfino le informazioni dei propri amici (punto questo molto problematico vista la mancanza del loro consenso). Per rendere più veloce il processo, gli utenti che hanno partecipato hanno ricevuto come incentivo una somma di denaro tra i 2 e i 4 dollari e alla fine sono state ottenute informazioni su circa 87 milioni di persone grazie alle 300.000 che hanno partecipato al quiz[43]. Grazie a questo ampio *database* a disposizione, *CA* ha potuto preparare, nei mesi precedenti le elezioni presidenziali americane del 2016, un'aggressiva campagna pubblicitaria per convincere le persone a votare per il partito repubblicano ed il candidato presidente Donald Trump sfruttando le informazioni psicometriche ottenute in modo da mostrare ad ognuno *ads* in linea con la propria personalità (questa strategia pubblicitaria è chiamata "*micro-targeting"* poiché va a

---

[42] La psicometria è la scienza che si prefigge di misurare i tratti della personalità di ciascuno così da categorizzarli.

[43] Dave Smith, *Weapons of Micro Destruction: How our 'Likes' hijacked democracy,* Towardsdatascience.com (17 ottobre 2018). Accessibile al sito: https://towardsdatascience.com/weapons-of-micro-destruction-how-our-likes-hijacked-democracy-c9ab6fcd3d02

colpire gli utenti in modo incredibilmente preciso, segmentandoli in piccoli gruppi omogenei con comuni caratteristiche). Tali annunci pubblicitari mostravano solo ciò che l'utente voleva vedere, estremizzando sempre di più la sua posizione politica o facendogli cambiare idea in base a quale fosse l'obiettivo perseguito dalla campagna. Per analizzare tutti i dati ottenuti dall'*app* sono stati utilizzati algoritmi di *machine learning* in grado di estrarre le informazioni più rilevanti e prevedere i comportamenti e le personalità dei partecipanti, rivelandosi molto più accurati delle analisi compiute dagli esseri umani (è stato dimostrato che basta un numero limitato di *Like* su *Facebook* per permettere ai modelli matematici di prevedere le caratteristiche non solo dell'utente, ma anche delle persone a lui più prossime[44]). Dopo l'effettiva elezione di Donald Trump *CA* ha utilizzato la notizia come prova dell'efficacia dei suoi modelli e della sua azione, ma per quanto non ci sia nessuna prova effettiva bisogna ammettere che l'utilizzo massivo della pubblicità mirata può, comunque, costituire un fattore importante quando il risultato di una consultazione politica dipende da pochi voti di scarto come nel caso in esame. In ogni caso lo scandalo è venuto alla luce solo nel 2018 grazie alle rivelazioni dell'ex-dipendente e *whistleblower* Christopher Wylie generando scalpore per l'ammontare di dati personali utilizzati senza il consenso degli utenti di *Facebook*. Per quanto i termini e le condizioni dell'app utilizzata da *CA* fossero poco trasparenti e al limite della legalità[45], essendo *FB* la piattaforma responsabile dei dati in questione ci sarebbe dovuta essere maggiore attenzione da parte della società. Questo *data breach* non è stato causato da attacchi *hacker* o azioni esterne di soggetti malintenzionati, bensì dal permesso di *Facebook* dato a Kogan (e quindi *CA)* per utilizzare i dati della piattaforma e degli utenti per fini di studio e ricerca e dal consenso degli utenti allo sfruttamento dei dati propri e dei propri amici, rendendo il fatto ancora più grave. Le richieste e le dichiarazioni di *CA* erano false e in malafede ma questo non assolve il *social* dalle proprie colpe in quanto garante della sicurezza e segretezza dei dati contenuti. Infatti la *Federal Trade Commission* ha sanzionato *Facebook* con una multa di 5 miliardi di dollari (misura non troppo pesante per la società visto che le entrate medie ogni anno sono di circa 55 miliardi) ma per *CA* non c'è stato nessun

[44] Wu Youyou, Michal Kosinski, David Stillwell, *Computer-based personality judgments are more accurate than those made by human,* PNAS, 112 (4), (27 gennaio 2015), 1036-1040.

[45] Una parte di essi recitano: *"*If you click "OKAY" or otherwise use the Application ora accept payment , you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data".

provvedimento penale. Questo scandalo non è stato l'ultimo che ha interessato la piattaforma. Nel 2018 infatti *Facebook* ha dovuto riconoscere le proprie colpe per quel che è accaduto nel Myanmar, dove il *social network*, spesso unico o principale mezzo di comunicazione e informazione delle persone, ha assunto il ruolo di catalizzatore dell'odio che ha finito per esplodere in un'ondata di violenza in tutto il paese, soprattutto ai danni della minoranza musulmana Rohingya. In particolare il suo ruolo è stato quello di non riuscire a (o a non voler) evitare il clima pesante e pieno di discriminazione che dal mondo reale si è trasferito sul *social* e ne ha aggravato le conseguenze. Stessa situazione e stesso risultato si sono avuti con il barbaro assalto al Campidoglio americano del 6 gennaio 2021 da parte dei sostenitori dell'uscente presidente Donald Trump, fatto che ha portato il suo *ban* dalla piattaforma[46]. Anche in questo caso la colpa di *Facebook* è stata quella di non riuscire a controllare, nonostante gli strumenti di controllo e di sorveglianza di ciò che avviene sul *network,* un'ondata ampiamente preannunciata di violenza e devastazione.[47] Ciò che si può sintetizzare da questi tre casi è la posizione passiva della società nei confronti dei pericoli che possono interessare gli utenti sia in rete che nel mondo virtuale, spesso fenomeni collegati e che si accrescono a vicenda. La novità di queste piattaforme digitali rende difficile il controllo da parte delle autorità, perché sono fenomeni ancora poco compresi e spesso sottovalutati. Come abbiamo potuto osservare, i *social network* sono e diventeranno sempre più fondamentali nel panorama globale come infrastruttura essenziale per la vita delle persone, così come aumenterà il valore e la quantità dei dati delle persone presenti su di essi, ed è paradossale che allo stato attuale non esista una normativa precisa che li regoli in modo dettagliato alla luce delle loro particolarità, lasciando tutto alla loro autoregolazione e al controllo limitato delle istituzioni in forza delle regole "tradizionali". Pensare che basti il consenso degli utenti per rendere tutto regolare come

[46] Mike Isaac, Sheera Frenkel, *Facebook Says Trump's Ban Will Last at Least 2 Years,* New York Times (7 giugno 2021).

[47] Le recenti rivelazioni della *whistleblower* Frances Haugen riguardo la consapevolezza di *Facebook* sugli episodi negativi che stavano avvenendo sulla piattaforma e dei loro ancor peggiori effetti che avrebbero avuto sul mondo, ma che non ha portato all'adozione di nessuna contromisura, privilegiando i profitti invece che la sicurezza, oltre a destare preoccupazione hanno portato le istituzioni di tutto il mondo ad interrogarsi sul migliore approccio da seguire nei confronti di questi giganti del *web.* La recente scelta della società di cambiare il nome in *Meta* appare probabilmente più motivata dal *marketing,* creando un'immaginaria rottura col *brand "Facebook"* macchiato da scandali e problemi, che da un reale cambiamento del *modus operandi*, della struttura sociale o degli obiettivi da questa perseguiti.

nel caso di *Cambridge Analytica* o che non sia pretendibile un'azione *ex ante* se sulla piattaforma soffiano funesti venti di guerra e odio sarà sempre meno giustificato, in particolare se il *SN* si tramuterà sempre di più in un metaverso. Quelli che agli albori erano punti interrogativi, ora che l'importanza dei *social* è aumentata, si sono tramutati in criticità non più affidabili alla diligenza autonoma di società private, rendendo necessario un maggior controllo esterno e maggiori regole per creare un ecosistema sano nel breve e lungo periodo.

CAPITOLO II

L'EVOLUZIONE DEL RAPPORTO TRA DATA PROTECTION E DIRITTO ANTITRUST NELLA CASISTICA EUROPEA. IL CASO "FACEBOOK GERMANY"

"Today data are a decisive factor in competition. In the case of Facebook they are the essential factor for establishing the company's dominant position. On the one hand there is a service provided to users free of charge. On the other hand, the attractiveness and value of the advertising spaces increase with the amount and detail of user data. It is therefore precisely in the area of data collection and data use where Facebook, as a dominant company, must comply with the rules and laws applicable in Germany and Europe"- Andreas Mundt, Presidente Bundeskartellamt[48]

1. La rivoluzione dei *Big data*

La forte crescita del vibrante ecosistema digitale, che fin qui si è tentato di analizzare, ha posto le basi per la fiorente economia dei dati, delineando il ruolo sempre più centrale di questi come risorsa insostituibile e preziosa[49]. La dinamica società dell'informazione in cui oggi viviamo, plasmata dal repentino sviluppo delle tecnologie informatiche e di comunicazioni elettroniche, ha nei dati, e nelle informazioni che questi contengono, il fulcro ed il principale fattore di crescita sociale ed economica[50]. Con il

[48] Andreas Mundt, *Press Release del Bundeskartellamt per il caso Facebook Germany,* (7 febbraio 2019).

[49] Bundeskartellamt (Autorità della concorrenza tedesca), Autorité de la concurrence (Autorità della concorrenza francese), *Competition Law and Data, joint report,* (10 maggio 2016), 4-12, accessibile al *link* *https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html* .

[50] Hiranya K. Nath, *The Information Society* , The Information Society. Space and Culture, India, [S.l.], v. 4, n. 3, p. 19-28, mar. 2017, (31 marzo 2017). Disponibile al link: https://ssrn.com/abstract=3077759.
Per una definizione di "società dell'informazione": https://www.treccani.it/enciclopedia/societa-dell-informazione_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/ .

miglioramento delle tecniche di estrazione, elaborazione e conservazione, unite alla mole, in aumento esponenziale[51], delle informazioni generate da dispositivi ed utenti, questa *new economy* ha visto mutare le regole su cui si fondavano interi settori economici, oltre che lo stile di vita delle popolazioni di tutto il mondo, con l'emersione nel mercato globale di nuovi *player* che hanno basato il proprio modello di *business* sullo sfruttamento dei dati e l'utilizzo di tecniche di analisi e *data mining*[52]. Come affermato da Wojciech Wiewiórowski, Garante Europeo della Protezione dei Dati (per il periodo 2019-2024), nel suo discorso in occasione del *Data Protection Day* 2020 tenuto a Zagabria, in Croatia, "*è in atto un movimento delle placche tettoniche*", dove la forte digitalizzazione degli ultimi decenni, unita all'affinarsi delle tecniche di analisi dei dati e alla loro centralità nell'economia contemporanea, ha portato società private a fornire servizi innovativi sotto costo o secondo il modello *"freemium",* dove il prezzo pagato dagli utenti non è monetario ed il sinallagma consiste nel consenso alla raccolta dei propri dati, per essere poi conservati, analizzati e monetizzati (come avviene nel caso, già trattato, di *Facebook* e i *social network)* [53]. In questa epoca di grandi cambiamenti, caratterizzata da un livello senza precedenti di raccolta, circolazione ed elaborazione

---

Il riconoscimento del cambiamento epocale che sta plasmando la società e la grande attenzione che, sin dall'inizio, le istituzioni europee hanno dedicato alla comprensione di questo fenomeno, per favorirlo in modo da accrescere i suoi benefici sull'economia ed i cittadini, si possono trovare nelle molteplici iniziative a livello europeo che hanno caratterizzato i decenni passati. In particolare, è interessante osservare l'accento posto sullo sviluppo informatico e tecnologico come strumento da valorizzare per aumentare il benessere di cittadini, lavoratori e imprese, nell'iniziativa dell'UE "*eEurope- Una Società dell'Informazione per tutti*" (https://cordis.europa.eu/programme/id/IS-EEUROPE/it) lanciata all'inizio degli anni duemila e confermata da successivi progetti ed interventi.

[51] Nel 2018 la quantità totale di dati in rete è stata di circa 28 zettabyte, dove ogni zettabyte equivale a circa un trilione di gigabyte, e si prevede che nel 2025 si raggiungeranno i 168 zettabyte. Fonte: Reinsel, John Gantz, John Rydning, "Data Age 2025: *The Evolution of Data to Life-Critical. Don't Focus on Big data; Focus on the Data That's Big*". *IDC Report*, (2018).

[52] *Cfr.* William J. Magnuson, *A Unified Theory of Data*, Harvard Journal on Legislation (8 settembre 2020), Vol. 58, Iss. 1,(2021), Texas A&M University School of Law Legal Studies Research Paper No. 20-38, Consultabile su: https://ssrn.com/abstract=3688687 .

[53] Wojciech Wiewiórowski, *Data Protection Day 2020: Facing New Challenges,* discorso in occasione della conferenza della presidenza croata al Consiglio Europeo di Zagabria, (16 gennaio 2020), consultabile al *link* *https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/data-protection-day-2020-facing-new_en* .

delle informazioni, reso possibile dalla rivoluzione tecnologica inarrestabile e destinato ad una ancora maggior espansione grazie all'utilizzo di nuove applicazioni come la rete 5G, l'*Internet of Things* ed il *Web 3.0,* stiamo assistendo al mutamento dei rapporti di forza a livello internazionale e al sempre maggior potere delle grandi imprese tecnologiche[54]. I "*Big data",* cioè grandi quantità di dati che non è possibile gestire con normali sistemi *hardware* e *software* e in tempo trascurabile, contraddistinti dalle cosiddette "4 V" (volume, velocità, varietà e valore), sono diventati uno strumento di fondamentale rilevanza strategica ed economica, grazie alla possibilità di razionalizzare e rendere più efficienti i processi organizzativi e produttivi con il loro utilizzo, ottenendo forti vantaggi competitivi[55]. Sfruttando i potenti algoritmi di *machine learning* e di intelligenza artificiale, le organizzazioni, agendo sui loro *database,* sono in grado di individuare *trend* e correlazioni tra eventi e variabili, prendendo decisioni con molta più velocità e anticipando i possibili scenari futuri, capacità inestimabile nel mondo globalizzato, complesso e interconnesso[56]. Per questo motivo il possesso di

---

[54] Atti del Convegno presso il Garante per la protezione dei dati personali italiano,, "*Big data e Privacy. La nuova geografia dei poteri*", (30 gennaio 2017), 11-25, accessibile al *link* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5846360.

[55] Cfr. David Bollier, *The Promise and Peril of Big data*, Washington, 2010.

AGCOM, *Big data- Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/ CONS,* (giugno 2018), 17-25.

Non vi è una definizione normativa di "*Big data"* e gli studiosi offrono, con le diverse definizioni, tutte comunque corrette, sfaccettature dello stesso fenomeno. Per questo motivo si è optato per la descrizione ampia qui proposta, in modo da cogliere e illustrare il fenomeno nei suoi fondamentali. Inoltre, anche le "quattro V" che caratterizzano questi dati sono dibattute, potendo imbattersi in articoli che ne individuano tre, sette o perfino quarantadue (Orie T.Shafer, *The 42 V's of Big data and Data Science*", Elder Research – Data Science & Predictive Analytics, , (2017)). Per un interessante approfondimento sul tema, si consulti anche M. Delmastro, A. Nicita, *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna (2019).

[56] Un progetto che destò molto interesse fu "*Google flu",* avviato dal gigante *tech* nel 2009 con l'avveniristico obiettivo di prevedere e stimare l'arrivo dell'influenza stagionale, a livello mondiale, basandosi sulle ricerche compiute sul motore di ricerca. Per quanto lo scopo fosse ambizioso e i dati mostrassero una sincronia tra le ricerche relative all'influenza e l'effettiva diffusione della stessa, il progetto fu interrotto per la poca accuratezza dei risultati e la loro discrepanza rispetto l'effettivo perdurare della malattia. Questo fu un chiaro esempio di come i *Big data,* oltre alle grandissime opportunità che offrono, portano con sé il problema della qualità dei dati che vengono sottoposti ad analisi e i possibili *bias* ed errori che essi nascondono. (Mike Wheatley, *Google Flu Trend: A case of Big data gone bad?,* Silicon Angle (24 marzo 2014),

maggiori informazioni, intrinsecamente di poco valore ma che lo acquistano una volta elaborate ed organizzate, diventa un obiettivo di primo piano per i *player* che operano nel mercato e che garantisce spiccata capacità innovativa ed un miglior *decision making* delle aziende, soprattutto considerando che gli algoritmi utilizzati per estrarre *insight* dai dati "grezzi" e non strutturati necessitano di essere impiegati su grandi banche dati[57]. Questa corsa ai dati pone però molti interrogativi. In *primis* c'è da considerare, dal punto di vista tecnico, il rischio informatico che discende dal massivo utilizzo e *storage* dei dati, principalmente in sistemi centralizzati, dunque virtualmente più fragili, che attraggono l'attenzione di criminali ed *hacker.* La *cybersecurity* è una necessità sempre più sentita e delicata nella nostra società digitalizzata, retta e dipendente da infrastrutture informatiche: per questo motivo le istituzioni nazionali ed europee stanno concentrando i loro sforzi per cercare di contrastare il *cybercrime* in continua espansione, e sventare così *data breach* che possono mettere in pericolo i dati dei cittadini e delle pubbliche amministrazioni[58]. Come risulta dai *report* e dagli studi dell'ENISA, l'Agenzia europea per la cybersicurezza, le minacce informatiche sono tutte in costante aumento, così come il numero e la gravità dei furti di dati, peraltro accentuato durante i mesi della pandemia, con attacchi più frequenti, complessi e difficili da evitare, che impongono uno sforzo sempre maggiore da parte del settore ICT

---

https://siliconangle.com/2014/03/24/google-flu-trends-a-case-of-big-data-gone-bad/.

[57] AGCOM (53), *27-42.*

La tendenza attuale, inoltre, appare il passaggio dalle classiche *data warehouse,* composti da dati strutturati e organizzati, a veri e propri *data lake,* composti da dati conservati senza essere previamente ordinati, molto meno costosi ma che allo stesso tempo permettono di avere a disposizione maggiori dati pronti per essere analizzati con meno sforzo

(https://aws.amazon.com/it/big-data/datalakes-and-analytics/what-is-a-data-lake/).

[58] "*Oggi il mondo sta diventando un computer. L'informatica sta diventando connessa al mondo, in ogni parte della nostra vita quotidiana*", ha dichiarato il CEO di *Microsoft* Satya Nadella ad un incontro presso l'Università Bocconi di Milano con studenti e *start-up,* evidenziando la stretta connessione tra il mondo digitale e quello reale e tutti i rischi che ciò comporta.

(https://www.corriere.it/tecnologia/19_maggio_30/ceo-microsoft-satya-nadella-italia-oggi-mondo-sta-diventando-computer-73d22f50-82ae-11e9-93b3-f04c99d00891.shtml)

Nel PNRR (Piano nazionale di ripresa e resilienza) italiano la *cybersecurity* rappresenta uno dei pilastri su cui fondare la ripartenza economica del sistema paese. Inoltre nell'agosto 2021 è stata creata l'Agenzia per la cybersicurezza nazionale , autorità volta a tutelare lo spazio *cyber* italiano e coordinare gli sforzi a livello nazionali su questa direzione, prima frammentati nell'operato di una costellazioni di autorità differenti.

e delle istituzioni[59]. Oltre a questo rischio definibile come "intrinseco", ciò che preoccupa maggiormente e che ha attivato il monitoraggio delle varie autorità di settore e delle istituzioni internazionali è senza dubbio l'enorme vantaggio, non solo economico, che si sta consolidando nelle mani di poche multinazionali *tech,* insieme al potere di influenzare fortemente la società e minare le basi della democrazia e della libertà individuale dei singoli cittadini, creando un "grande fratello" capace di sorvegliare ogni persona e prevederne i comportamenti, soprattutto adesso che i *tech giants* stanno volgendo i loro sforzi verso la creazione di un vero e proprio "metaverso", una realtà mista tra reale e virtuale dove le persone sono rappresentate da avatar[60]. Sulla possibilità che le grandi società si auto-regolino da diversi anni è stato lanciato l'allarme da eminenti studiosi e professori universitari di tutto il mondo: si tenga presente che negli ultimi 50 anni le principali università occidentali hanno seguito l'insegnamento dell'economista premio Nobel Milton Friedman (Scuola di Chicago), in base al quale pensare ed aspettarsi che una società privata abbia una "responsabilità sociale", un interesse filantropico ed ulteriore a quello economico nei confronti di cittadini e comunità, è pura utopia[61]. Una conferma in questo senso è stata senz'altro data dallo scandalo di *Cambridge Analytica* e gli ulteriori che hanno interessato *Facebook.* Con l'utilizzo di grandi quantità di dati è inevitabile che possano essere processati dati

---

[59] ENISA, *Analisi delle minacce settoriali / tematiche*, (Da gennaio 2019 ad aprile 2020); ENISA, *L'anno in Rassegna*, (da gennaio 2019 ad aprile 2020). Per approfondimenti e report ulteriori si veda: https://www.enisa.europa.eu/ .

[60]Si è già constatato che le piattaforme e le applicazioni digitali riescono ad ottenere informazioni da ogni singola azione degli utenti, come se i nostri *device* fossero "un questionario che compiliamo ogni volta che li accendiamo" (Prof. Pierluigi Congedo). L'ombra di una società distopica in stile Orwelliano sembra sempre più vicina con l'avvento del metaverso, uno spazio dove per la prima volta non è possibile distinguere il reale dal virtuale, che le società private stanno cercando di conquistare. La letteratura sul metaverso è ancora agli inizi poiché questo *trend* è molto recente. Per dei primi spunti: *Quanto dobbiamo prendere sul serio il metaverso?,* IlPost (12 novembre 2021), https://www.ilpost.it/2021/11/12/metaverso-facebook-meta/ .

[61] Milton Friedman, *A Friedman doctrine-- The social responsibility of business is to increase its profits,* New York Times (13 settembre 1970), accessibile al link: https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html .

personali[62], una particolare categoria di dati tutelata dal Regolamento generale sulla protezione dati personali 679/2016 (GDPR), normativa unitaria europea e pietra miliare della *data protection*, che li definisce, all'art. 4, "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*"[63]. Lo stesso GDPR considera "identificabile", sempre all'art. 4, "*qualsiasi persona fisica che può essere identificata"*[64]*,* attraverso informazioni identificative come il nome o caratteristiche fisiche, e per "trattamento" "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*[65]*,* dunque un ambito di applicazione molto ampio, capace di coprire la maggioranza delle operazioni che hanno ad oggetto l'uso di dati[66]. La protezione dei dati personali, proiezioni virtuali delle persone, acquista sempre maggiore importanza, considerando l'espansione tecnologica e della *data economy,* in cui il principale strumento di pagamento sono proprio i dati personali, e rappresenta la primaria e potente garanzia degli utenti nella nostra società dell'informazione, fissando confini allo sfruttamento che di questi possono farne i *service provider* e le società informatiche. Il corpo di norme volto alla tutela dei dati personali costituisce un enorme passo in avanti, ma risente della grande frammentarietà a livello internazionale della disciplina, che ha come effetto il rallentamento o il blocco della circolazione transfrontaliera dei dati. Se in Europa è presente il GDPR, strumento legale con efficacia orizzontale identica in tutta l'Unione che garantisce certezza e unitarietà delle regole applicabili, ma nel resto del mondo molti paesi hanno solo normative settoriali o, peggio ancora, nessuna

[62] Nonostante sia difficile risalire alle singole informazioni che compongono i *Big data,* con gli algoritmi sempre in miglioramento, l'IA ed il *machine learning* si può arrivare a segmentare i dati personali in categorie molto ristrette o perfino profilare gli interessati.

[63] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88, Art. 4.

[64] ibidem.

[65] ibidem.

[66] ibidem.

disciplina, creando rilevanti vuoti di tutela che inficiano il sistema complessivo e l'operato dei paesi virtuosi, insieme alla sicurezza dei loro dati[67]. Sono stati adottati strumenti tecnici e giuridici per permettere il trasferimento in sicurezza, ma ciò non sempre basta a cancellare i rischi che possono interessare i dati di cittadini ed imprese, come è stato dimostrato nei due celebri casi *Schrems* I e II .

2. (*Segue:)* I casi *Schrems* I e II: i dati sono davvero al sicuro?

Il trasferimento dei dati personali tra i paesi europei viene garantito, quale fattore di rilevante sviluppo economico e sociale, vietando restrizioni alla libera circolazione che potrebbero limitarlo[68]. Per i trasferimenti verso paesi terzi, invece, il diritto Ue richiede la presenza di condizioni che garantiscano un livello di protezione adeguato, permettendoli in due casi: in forza di una decisione di adeguatezza della Commissione Europea o, in mancanza, mediante garanzie appropriate fornite dal titolare o dal responsabile del trattamento.

L'art. 45 GDPR comma 1 stabilisce infatti che

> "*Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione*

[67] Si veda Michael Goodyear, *A Rising Tide Lifts All Consumers: Penumbras of Foreign Data Protection Laws in the United States*, Richmond Journal of Law and Technology (7 luglio 2020), Accessibile al link: https://ssrn.com/abstract=3645085.
Per una mappa aggiornata delle normative di *data protection* nel mondo: https://www.dlapiperdataprotection.com/ . Esempio eclatante sono gli Stati Uniti, dove manca una legge federale omnicomprensiva e i singoli stati garantiscono la protezione dei dati personali mediante leggi di settore.

[68] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88, Art. 1, par. 3.

internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche"[69],

specificando al comma successivo che nella valutazione dell'adeguatezza sono rilevanti criteri come la tutela dei diritti umani in quel determinato paese, la presenza di autorità di controllo indipendenti a cui ricorrere in caso di violazioni e gli impegni internazionali assunti dallo stesso, fattori ed elementi che dovranno essere costantemente monitorati ed accertati dalla Commissione per evitare vuoti di tutela per i cittadini Ue.

Relativamente invece al secondo caso, il successivo art. 46 dello stesso Regolamento afferma che

"*in mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*"[70].

Questi meccanismi giuridici sono estremamente importanti e proprio le decisioni di adeguatezza della Commissione, fattispecie sicuramente più rilevante tra le due, sono state al centro dei casi *Schrems* I e II, in cui la giurisprudenza ha potuto fissare

---

[69] *ibidem,* art. 45.

[70] Tra le garanzie adeguate il comma 2 dell'art 46 GDPR prevede "*a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;b) le norme vincolanti d'impresa in conformità dell'articolo 47;c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.*

fondamentali punti fermi sul tema e su cosa bisogna intendere per "livello di protezione adeguato".

Maximillian Schrems, cittadino austriaco, attivista e protagonista di questi due casi giudiziari, si è iscritto a *Facebook* nel 2008, acconsentendo contrattualmente, per utilizzare la piattaforma, al trasferimento dei suoi dati personali nel server centrale del *social network,* negli Stati Uniti. Dopo le rivelazioni dell'ex agente CIA Edward Snowden[71], concernenti le pratiche dei servizi segreti americani ed, in particolare, della *National Security Agency (NSA),* nel 2013 Mr. Schrems adì l'autorità di vigilanza irlandese (poiché in Irlanda è la sede legale della sussidiaria di *Facebook* responsabile della raccolta e del trattamento dei dati personali dei cittadini europei) lamentando l'inadeguatezza della protezione negli Stati Uniti e chiedendo di vietare il trasferimento dei suoi dati personali. L'autorità respinse la richiesta, ritenendola infondata alla luce della decisione 2000/520/CE della Commissione europea (che ha istituito il regime del cd. "*Safe Harbour")*, dove questa accertò un livello di protezione adeguato nel Paese . Al tempo della vicenda non era ancora entrato in vigore il GDPR e la disciplina applicabile era la direttiva 95/46/CE, in cui la previsione sulle decisioni di adeguatezza, oggi nell'art. 45 GDPR, era contenuta nell'art. 25 ("*Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva")*[72]. Il signor Schrems fece così ricorso dinanzi all'*High Court* irlandese che, dopo aver constatato l'eccessività delle condotte dell'*intelligence* americana alla luce delle dichiarazioni di Edward Snowden e aver affermato che l'accesso senza limiti e in massa ai dati personali dei cittadini costituisce una chiara violazione dei principi cristallizzati nella Costituzione irlandese, rimise la questione alla Corte di Giustizia dell'Unione Europea (CGUE) tramite rinvio pregiudiziale *ex* art. 267 TFUE, poiché

---

[71] Glenn Greenwald, Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others,* The Guardian, (7 giugno 2013), Accessibile al *link*: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data .

[72] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, [1995],

OJ L 281, 23.11.1995, p. 31–50.

vertente sull'attuazione del diritto dell'Unione Europea e la validità della decisione 2000/520/CE della Commissione. La Corte avviò la sua disamina considerando l'importante ruolo attribuito attribuito dalla direttiva 95/46/CE all'art. 28, alle autorità nazionali di controllo del trasferimento dei dati personali verso paesi terzi, con diversi poteri e facoltà ed il compito di vigilare, in totale indipendenza, il rispetto delle regole relative al trattamento dei dati personali e dei diritti garantiti ai cittadini europei. In presenza di una decisione di adeguatezza della Commissione naturalmente l'autorità non potrà andare contro quanto in essa stabilito, ma neppure abdicare al proprio compito di controllore indipendente sui trasferimenti dei dati, ove sia investita di un ricorso. Per questo motivo per la Corte UE la decisione di adeguatezza ('*Adequacy decision*') 2000/520/CE non ostava all'esame della domanda da parte dell'autorità nazionale competente. La problematica che subito venne analizzata fu la definizione dell'adeguatezza che deve caratterizzare il livello di protezione dei dati in un paese terzo, definizione che manca a livello legislativo. Nell'art. 25 della direttiva 95/46/CE erano tuttavia previsti diversi criteri per valutare lo standard di protezione, come la normativa vigente nel paese destinatario e il rispetto degli impegni internazionali e dei diritti fondamentali. In questo modo la valutazione della Commissione risultava vincolata in sede di approvazione di una decisione di adeguatezza, decisione che ove non rispondente ai criteri e principi enunciati dalla direttiva sarebbe potuta essere dichiarata invalida dalla CGUE. Lo *standard* di protezione dei dati personali che il paese terzo era, dunque, chiamato ad assicurare doveva, per la Corte, essere "sostanzialmente equivalente" a quello europeo. Osservando quanto stabilito dalla decisione della Commissione europea n. 2000/520/CE, veniva comunque sancito il primato delle "*esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]*"[73] rispetto alle garanzie fornite dal cosiddetto *Safe Harbour,* permettendo così alle autorità americane di porre in essere condotte poco rispettose della *privacy* sui dati personali trasferiti dall'UE nei *server* statunitensi, senza che fosse approfondita e prevista una tutela giuridica per i cittadini europei lesi. Risultarono in questo modo violati l'art. 7[74], sul rispetto della vita privata e personale,

[73] Decisione della Commissione 2000/520/CE [2000], OJ L 215, 25.8.2000.

[74] Art 7 CDFUE, "*Rispetto della vita privata e della vita familiare*": "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni"*.

della Carta dei diritti fondamentali dell'UE e l'art. 47[75], sul diritto ad un ricorso effettivo dinanzi ad un giudice imparziale, determinandosi una chiara lesione del diritto alla tutela dei dati personali sancito all'art. 8 della stessa Carta[76]. Inoltre bisogna notare come la Commissione non analizzò questa prassi e la legislazione statunitense sul punto, e neppure affermi che gli *USA* effettivamente garantiscano una tutela adeguata nel rispetto dei principi della direttiva. Per tali motivi la CGUE concluse che l'art 25, paragrafo 6, della direttiva Direttiva 95/46/CE, dovesse essere letto nel senso di permettere all'autorità nazionale di controllo, ove venga adita da una persona per valutare il livello di protezione di un paese terzo che potrebbe inficiare il suo diritto alla tutela dei dati personali, di esaminare la domanda. Essa inoltre stabilì che la "decisione di adeguatezza" n. 2000/520/CE fosse invalida[77].

Dopo la dichiarazione di invalidità del *Safe Harbour* previsto dalla decisione di adeguatezza UE 2000/520, la Commissione Europea ha adottato una nuova decisione di adeguatezza, denominata *Privacy Shield,* a seguito di una più attenta valutazione del contesto normativo degli Stati Uniti. Con questa si attesta nuovamente l'adeguatezza della tutela dei dati personali trasferiti per fini commerciali[78]. In base al nuovo regime è

---

[75] Art 47 CDFUE, *"Diritto a un ricorso effettivo e a un giudice imparziale":* " "*Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato, qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia".*

[76] Art 8 CDFUE, "*Protezione dei dati di carattere personale":* "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."*

[77] C-362/14, *Maximilian Schrems c. Data Protection Commissioner,* [2015], ECLI:EU:C:2015:650, para 37-104.

[78] Infatti, al para 65 della decisione, e affermato sul punto: "*La Commissione ha valutato le limitazioni e le garanzie cui la normativa statunitense subordina la facoltà delle autorità pubbliche statunitensi di accedere e usare i dati personali trasferiti nell'ambito dello scudo per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico. Il governo statunitense ha altresì comunicato alla Commissione, tramite l'Ufficio del direttore dell'intelligence nazionale (ODNI) (56), le dichiarazioni e gli impegni particolareggiati riportati nell'allegato VI della presente decisione.*

stato introdotto un sistema di autocertificazione volontaria, secondo cui le aziende statunitensi che aderiscono al *Privacy Shield* si impegnano a rispettare i dati personali dei cittadini europei e la normativa Ue, mentre le autorità americane vigilano sul rispetto delle regole stabilite dalla decisione, assicurando maggior controllo e trasparenza, senza accessi abusivi da parte delle agenzie nazionali. Tra le misure più rilevanti, vengono previsti obblighi di protezione più stringenti in capo delle aziende, la possibilità di ricorso per gli europei, rivolgendosi direttamente all'impresa o all'autorità garante della protezione dei dati personali competente, in collaborazione con quelle *USA,* la creazione di sistemi di *ADR (Alternative Dispute Resolution)* per la risoluzione celere ed efficace delle controversie ed una revisione annuale per verificare l'attuazione ed il rispetto del nuovo regime[79].

Rispetto al *Safe Harbour* questo regime è molto più ponderato e con maggiori garanzie, ma è abbastanza per assicurare la protezione dei dati personali contro le possibili condotte ingiustificate delle agenzie statunitensi? Il caso *Schrems II* prende le mosse e si svolge proprio intorno a questo punto[80]. Dopo che la CGUE ha dichiarato invalido il *Safe Harbour e* la *High Court* irlandese ha annullato il rigetto della denuncia da parte del Commissario a protezione dei dati irlandese, Mr. Schrems ha formulato il 1° dicembre 2015 la sua istanza argomentando che negli Stati Uniti il diritto europeo avrebbe imposto a *Facebook,* così come alle altre società che importassero dati personali europei in America, di mettere a disposizione delle autorità, come l'*NSA* e

---

Con lettera firmata dal segretario di Stato, acclusa alla presente decisione come allegato III, il governo degli Stati Uniti si è impegnato altresì a creare un nuovo meccanismo di vigilanza sulle ingerenze per motivi di sicurezza nazionale, indipendente dai servizi di intelligence: il Mediatore dello scudo. Infine, la dichiarazione del Dipartimento della Giustizia degli USA, riportata nell'allegato VII della presente decisione, espone le garanzie e limitazioni relative all'accesso delle autorità pubbliche ai dati per finalità di contrasto e di interesse pubblico. Ai fini della trasparenza e per rispecchiare la natura giuridica di questi impegni, ciascuno dei documenti elencati e allegati alla presente decisione è pubblicato nel Registro federale degli USA.". C/2016/4176*,* Decisione di esecuzione della Commissione 2016/1250 [2016], OJ L 207, 1.8.2016, p. 1–112.

[79] Varie istituzioni europee, *Manuale sul diritto europeo in materia di protezione dei dati,* (ed. 2018, Ufficio pubblicazioni UE, 2018), 286-288. Per ulteriori informazioni si veda: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5306161 .

[80] Già il Gruppo di lavoro articolo 29, sì favorevole allo *Shield*, aveva mostrato alcune perplessità nella sua *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision* (13 aprile 2016), come la non sufficiente indipendenza delle autorità chiamate a vigilare negli US e la mancanza di chiarezza di alcuni punti del sistema.

l'*FBI,* i dati personali contenuti nei loro *server,* compresi quelli trasferiti dall'UE, senza operare un'adeguata verifica della tutela dei dati personali ai sensi del GDPR. Anche in questo caso Schrems solleva dubbi sulla seconda decisione di adeguatezza. Secondo Schrems i dati personali vengono utilizzati in diversi programmi di sorveglianza di massa, come i programmi PRISM e UPSTREAM, incompatibili con gli artt. 7, 8 e 47 della CDFUE, e dunque Schrems chiede di bloccare il trasferimento dei suoi dati operato da *Facebook.* Il Commissario, con una bozza di decisione pubblicata il 24 maggio 2016, ha condiviso la visione del ricorrente sul rischio per i dati personali e la non conciliabilità della prassi delle autorità americane con i diritti affermati dalla CDFUE, ritenendo le clausole tipo ("*standard clauses*") della decisione di adeguatezza n. 2016/1250 non sufficienti a garantire anche in questo secondo caso la protezione dei dati personali, sia dell'appellante, Sig. Schrems, che dei cittadini europei *lato sensu*. Per questi motivi, alla richiesta di sollevare la questione sulla validità del *Privacy Shield* disciplinato dalla seconda decisione di adeguatezza, il Commissario della Privacy irlandese ha adito l'*High Court* irlandese e questa, il 4 maggio 2018, ha rimesso nuovamente la questione alla CGUE, competente per l'interpretazione delle norme UE. La Corte UE chiarisce subito che, a differenza del primo caso *Schrems,* questa volta la normativa applicabile è il GDPR, non la direttiva 95/46/CE, ed il trattamento dei dati trasferiti rientra perfettamente nel suo campo di applicazione, non essendo applicabili le eccezioni dell'art 2 comma 2. L'art 44 del GDPR fissa i principi che devono essere rispettati per trasferire i dati personali dei cittadini Ue verso paesi terzi e l'art. 45, riguardo alle decisioni di adeguatezza della Commissione, prevede la necessaria presenza di "*un livello di protezione adeguato",* senza definirlo, ma che deve intendersi come un livello di protezione equivalente a quello unionale, come confermato anche nel caso *Schrems I.* Sulla questione della possibilità per l'autorità di controllo di sospendere o impedire il trasferimento dei dati, ove richiesto, basato su clausole standardizzate, se queste vengono ritenute non adeguate, la Corte ritiene che il compito fondamentale delle autorità, argomentando alla luce del considerando 116 del Regolamento[81], è quello

[81] Il considerando 116 del GDPR contempla infatti che " *Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri*

di verificare l'effettiva applicazione delle regole contenute nel GDPR e dunque anche in presenza di una decisione di adeguatezza non è possibile svuotarla di questo ruolo. Quando vengono utilizzate "clausole standardizzate" o "tipo" (cosiddette *standard clauses*), come nel caso di specie, per permettere il trasferimento dei dati *ex* Art 46, commi 1 e 2, del GDPR al di fuori della UE, per quanto i titolare o il responsabile si impegnino a garantire la protezione dei dati trasferiti, tali clausole non vincolano le autorità nazionali del paese di destinazione. Se esse non si dimostrino sufficienti per assicurare la protezione dei dati personali, deve essere possibile il ricorso alla Corte UE per verificarne la compatibilità con i trattati, i regolamenti o le direttive applicabili. Nella decisione di adeguatezza n. 2016/1250, al punto I.5 dell'allegato II, viene previsto che

> "*l'adesione ai principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione, oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando, nelle rispettive politiche in materia di tutela della sfera privata, in quali casi saranno regolarmente applicate le eccezioni ammesse dalla lettera b).*

---

per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento."

Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata",

perciò anche nel regime del *Privacy Shield,* così come nel precedente, abrogato, regime stabilito dalla decisione di adeguatezza UE "*Safe Harbour*", sarebbe stato stabilito il primato degli interessi nazionali statunitensi su quello della protezione dei dati dei cittadini UE, rendendo così perfettamente possibili ingerenze delle autorità *USA* mediante condotte che destano di fatto seri dubbi sul livello di "adeguatezza" del livello di protezione garantito ai dati dei cittadini europei. Nonostante, dunque, il *Privacy Shield* offra maggiori garanzie rispetto al regime precedente e vi sia l'impegno delle istituzioni americane a rendere più effettiva la tutela dei dati dei cittadini europei trasferiti nei server degli *States,* la CGUE dichiarò ugualmente invalida la decisione 2016/1250 poiché, alla luce delle risultanze e delle previsioni che permettono l'accesso alle informazioni da parte delle autorità del paese, non viene rispettato il principio di adeguatezza della tutela e dei diritti sanciti dagli artt. 7, 8 e 47 della CDFUE[82].

A seguito dell'importante sentenza *Schrems II* e del suo grande impatto sul trasferimento dei dati, l'*European Data Protection Board (EDPB)* ha pubblicato delle importanti raccomandazioni sulle misure supplementari da adottare da parte delle imprese con sede in paesi terzi che esportano dati dall'UE, al fine di garantire un adeguato livello di protezione[83]. Queste hanno lo scopo di aiutare e guidare le aziende esportatrici dei dati nel complesso compito di valutazione dello *standard* di protezione effettivo nel paese di destinazione e di scelta delle concrete misure da adottare, attraverso una lista di attività progressive da realizzare e di esempi. Il presidente dell'*EDPB,* Andrea Jelinek, ha infatti messo in luce, in sue dichiarazioni, come l'effetto della suddetta sentenza non sia da sottovalutare e che i flussi internazionali di dati, data

[82] C-311/18, *Maximilian Schrems c. Data Protection Commissioner,* [2020], ECLI:EU:C:2020:559, para 80-196.

[83] EDPB, *recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2,* (18 giugno 2020). Per un approfondimento sulle singole misure visitare: https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_it . La versione originaria è stata aggiornata successivamente alla sentenza *Schrems II,* nell'ottica di una più ponderata valutazione del contesto generale del paese terzo riguardo la protezione dei dati personali.

la loro importanza e delicatezza, necessitano di maggiore controllo. In questo modo le raccomandazioni realizzano l'importante compito di aiutare gli esportatori di dati, allo stesso tempo garantendo la protezione degli stessi[84]. Loquace è al riguardo l'affermazione contenuta nell'ultimo *report* annuale di *Meta (ex Facebook)* alla *Securities and Exchange Commission (SEC),* autorità di vigilanza americana del mercato mobiliare e della borsa, sulla possibilità che le diverse piattaforme della società non offrano più i loro servizi in Europa. Questa è solo l'ultima di una lunga serie di "minacce" dell'impresa alle istituzioni del vecchio continente, ma la prima ad essere formalizzata in un documento ufficiale[85]. Nel *report* di quasi centocinquanta pagine sulle attività e gli obiettivi societari, le giustificazioni su cui si fonda la dichiarazione sono il quadro normativo europeo in continua evoluzione, in materia di protezione dei dati personali, e le limitazioni da questo poste sul trasferimento dei dati nei *server* statunitensi. Dopo l'invalidamento del *Privacy Shield,* infatti, *Meta,* attiva nello sviluppo di sistemi a realtà aumentata, il futuro dei *social network*[86]*,* ha continuato il trasferimento transfrontaliero secondo il regime delle clausole contrattuali standardizzate, ricevendo però una bozza di decisione dell'*Irish Data Protection Commission,* nell'agosto 2020, che ha asserito la non adeguatezza della protezione in base a dettami del GDPR e ha proposto la sospensione di ogni suo trasferimento. La società ha così lamentato la negatività degli effetti economici, generati dalle stringenti regolo europee sui risultati e gli obiettivi dell'azienda. In seguito *Meta* ha chiarito le sue posizioni, fonte di preoccupazione degli utenti residenti nell'UE, dichiarando l'inesistenza di un programma di ritiro delle piattaforme digitali dai mercati europei e la mera ipoteticità dello scenario[87]. Questa vicenda permette di cogliere quali sono, in concreto, i rischi e le difficoltà relative al trasferimento transfrontaliero dei dati, fenomeno di fondamentale importanza nel mondo globalizzato e interconnesso, che nasconde complessità spesso sottovalutate e che possono sfociare in gravi violazioni dei dati personali.

---

[84] *ibidem.*

[85] *Report* consultabile al *link* https://www.sec.gov/ix?doc=/Archives/edgar/data/1326801/000132680122000018/fb-20211231.htm# .

[86] Per ulteriori notizie ed approfondimenti su *Meta:* https://about.facebook.com/meta/ .

[87] Michela Rovelli, *Facebook e Instagram lasciano l'Europa? Cosa c'è dietro le parole di Meta in un documento ufficiale,* Corriere della Sera (7 febbraio 2022).

3. Introduzione al rapporto tra *data protection* e diritto *antitrust*

L'effetto totalizzante della *data economy,* con la sua catena di valore in continua espansione grazie alla raccolta massiva di dati da parte delle imprese, unita alla possibilità di riutilizzo degli stessi per sempre nuovi utilizzi, ha originato fenomeni economici e sociali non limitati al campo della protezione dei dati personali[88]. I cittadini e le imprese, anche quelle operanti in settori tradizionali, fanno ormai largo uso di servizi digitali e piattaforme, diventandone spesso dipendenti, sia come strumenti d'uso quotidiano che per finalità di *business,* grazie ai benefici dati dalla loro rapidità, potenza, utilità e capacità di adattamento ad ogni singola esigenza del consumatore. Per quanto questo sistema si fondi sui dati e dunque le prime esigenze siano proprio quelle legate alla *data protection,* avendo l'innovazione digitale fatto breccia in ogni settore sociale ed economico, diversi sono i bisogni di tutela e i settori giuridici interessati, come dimostrano varie iniziative e studi portati avanti da istituzioni ed autorità, tra cui spicca l'indagine conoscitiva sui *Big data,* nata dagli sforzi congiunti di AGCM, AGCOM e Garante per la protezione dei dati personali[89]. Da questa analisi, risultato di una lunga serie di collaborazioni e di *report*, emergono le questioni e le criticità discendenti dall'accentramento dei *Big data* nelle mani di poche *big tech* a livello internazionale, fenomeno che le istituzioni europee e nazionali stanno da tempo cercando di fronteggiare. A tale scopo sono in fase di preparazione ed attuazione nuove misure legislative, soprattutto a livello UE, rivolte a regolamentare in maniera più dettagliata, precisa ed al passo coi tempi, le piattaforme digitali ed il comportamento delle grandi aziende dietro di esse, come il *Digital Service Act* ed il *Digital Markets Act.* La consapevolezza di fondo è che le piattaforme e lo sfruttamento dei *Big data* possono, e nella maggior parte dei casi riescono ad influenzare le scelte dei singoli consumatori e dei mercati, con ripercussioni sulla concorrenza tra imprese ed il benessere dei consumatori[90]. In particolare, gli effetti che incidono maggiormente sulle dinamiche concorrenziali ed il funzionamento dei mercati sono i già citati effetti di rete, le economie di scala e di scopo e la presenza di *switching costs* che possono portare ad un

---

[88] AGCOM, *Big data, Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS,* (10 febbraio 2020), 15-22, Accessibile al sito: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9264204 .

[89] ibidem.

[90] ibidem, 70-102.

lock-in degli utenti ed un conseguente consolidamento della posizione di mercato della piattaforma (cd. *market tipping).* Inoltre estremamente rilevanti sono la possibile configurazione dei dati come barriere all'entrata, con scarsa presenza del *multi-homing* (la situazione in cui, in presenza di diverse piattaforme, i consumatori scelgono di utilizzarne contemporaneamente più di una)[91], e l'integrazione verticale ed orizzontale delle strutture societarie dietro le piattaforme (rafforzata dalle cosiddette *killer acquisitions* volte ad assorbire sul nascere possibili e futuri concorrenti), fenomeni che possono portare all'emersione di posizioni dominanti, difficilmente attaccabili per le particolarità dei mercati digitali, dove il vincitore della concorrenza "prende tutto". In essi le *big tech* svolgono un ruolo da *gatekeepers,* controllando l'accesso ai servizi ed il rapporto tra imprese e consumatori[92]. La base giuridica principale su cui si basa il trattamento dei dati, prezzo e merce di scambio della *data economy,* è il consenso degli utenti. Risulta tuttavia logicamente difficile ritenerlo libero, effettivo, o comunque sufficiente, vista lo squilibrio di forza tra le posizioni delle piattaforme e dei consumatori. Questa sproporzione viene considerata, dalla dottrina, alla base del fenomeno conosciuto in letteratura come "*privacy paradox",* il comportamento degli utenti che si dichiarano attenti alla loro *privacy* ma che in concreto, nell'utilizzo dei servizi digitali, realizzano condotte che poco la tutelano, come la mancata lettura dei termini e delle condizioni delle piattaforme, poiché in ogni caso difficilmente si rinuncerebbe ai benefici di questi[93]. Queste incongruenze, unite alla complessità degli strumenti tecnologici, la mancanza di trasparenza nei termini dei servizi e le misure insufficienti poste in essere dalle società *tech* per rispondere alle richiesta di tutela della privacy avanzate dagli utenti, possono sfociare in *market failures* di difficile

---

[91] Kyeonggook Park, Robert Seamans, Feng Zhu, *Multi-Homing and Platform Strategies: Historical Evidence from the US Newspaper Industry*, Harvard Business School Technology & Operations Mgt. Unit Working Paper No. 18-032, (1 dicembre 2018), 5-7.

[92] ibidem*,* 42-83*,* ma anche, Bundeskartellamt (Autorità della concorrenza tedesca), Autorité de la concurrence (Autorità della concorrenza francese), *Competition Law and Data, joint report,* (10 maggio 2016), 11-29.

[93] Susanne Barth, Menno D.T. de Jong, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,* Telematics and Informatics, Volume 34, Issue 7, (2017), 1038-1058, https://doi.org/10.1016/j.tele.2017.04.013.

quantificazione e portata[94]. In questo contesto, piuttosto complesso anche per interpreti, legislatori ed *enforcers,* si apre un "*regulatory dilemma"* su quali siano le regole applicabili e in quale ambito ricada la singola condotta dannosa tra la normativa a tutela dei dati personali, quella *pro*-consumatori ed il diritto *antitrust*. Per quanto queste normative puntino tutte ad aumentare e tutelare il benessere degli individui all'interno della società e del mercato, i loro obiettivi sono simili ma differenti. La *data protection* "*protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali",* come recita l'art. 1, comma 2 del GDPR, con un campo di applicazione limitato ai dati personali. Il diritto *antitrust,* invece, ha lo scopo di garantire e promuovere la concorrenza effettiva all'interno del mercato (il più astrattamente vicina al modello ideale della concorrenza perfetta), proteggendo, di riflesso, l'interesse aggregato dei consumatori grazie al perseguendo le eventuali condotte anticompetitive delle imprese. Diversamente la normativa consumeristica tutela direttamente l'interesse dei singoli consumatori, disciplinando le relazioni contrattuali *business to consumer,* la cui applicabilità dipende dalla qualifica del soggetto come "consumatore" (ad esempio, definito dall'art. 3 del Codice del Consumo italiano, Dlgs 206/2005, come "*la persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta")*[95]. Nonostante le similitudini, queste tre branche del diritto hanno le loro particolarità che le rendono insostituibili, ma con l'avanzare dei mercati digitali sono sempre più frequenti i casi di zone grigie e di possibile sovrapposizione delle discipline. Diventa in questo modo possibile inquadrare le fattispecie secondo più regole appartenenti a settori differenti. Negli ultimi anni, in particolare, il rapporto tra *data protection* e diritto *antitrust* è diventato un tema molto discusso e controverso, con casi giurisprudenziali o *mergers* che hanno avuto come protagoniste le GAFAM (le principali e più importanti imprese tecnologiche, cioè *Google, Amazon, Facebook, Apple e Microsoft*), portando le istituzioni europee ad interrogarsi su quali fossero gli strumenti giuridici da utilizzare per far fronte a situazioni nuove e suscettibili di incidere

[94] Marco Botta, Wiedemann, Klaus, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, Antitrust Bulletin (2 ottobre 2019), 428-430. Consultabile su: https://ssrn.com/abstract=3462983 .

[95] ibidem*,* 434-438.

sugli interessi e i diritti di innumerevoli utenti e cittadini europei[96]. Nella già menzionata indagine congiunta sui *Big data* tra AGCM, AGCOM e Garante *privacy,* viene messo in rilievo come "*esiste una possibile tensione tra diritto alla protezione dei dati e concorrenza"*[97]*,* in un equilibrio molto delicato da mantenere tra *enforcement* antitrust e tutela dei dati personali. Un approccio restrittivo, diretto alla maggiore tutela dei dati, potrebbe avere effetti negativi sui mercati, aumentando le barriere all'entrata e danneggiando maggiormente i consumatori, mentre un approccio più permissivo rafforzerebbe le posizioni dominanti, peraltro già consolidate, delle piattaforme[98]. Perciò il binomio sfruttamento dei dati - effetti concorrenziali nella "*data-driven-economy"* si fonda su un precario equilibrio che si prospetta sempre più difficile da gestire.

4. Il Caso "*Facebook Germany"*

Dopo anni di confusione nell'inquadramento del rapporto tra *data protection* e diritto *antitrust,* unito ai tentativi delle istituzioni europee e nazionali di rispondere alle sfide prospettate dall'economia digitale e dai suoi *player* difficilmente imbrigliabili e regolabili con gli strumenti giuridici e gli approcci "tradizionali", finalmente vi è stato un primo e forte cambiamento, con un caso che ha interessato *Facebook* in Germania e in cui sono state fatte importanti considerazioni sul tema. Questa circostanza non è casuale, ma si fonda sul vivace substrato culturale e giuridico presente nel paese e sul contributo di importanti studiosi e giuristi, come il prof. Rupprecht Podszun, che stanno cercando di dare risposta ai problemi concorrenziali causati dai mercati digitali e dall'operato delle *big tech*[99]. Nel paese, infatti, il diritto *antitrust* ha sempre occupato un ruolo centrale, anche grazie all'ordoliberalismo, corrente di pensiero socioeconomico originatasi intorno alla Scuola di Friburgo, che negli anni anni Trenta, si oppose

[96] Entrambe le branche del diritto hanno come base giuridica l'art. 114 TFUE, diretto all'avvicinamento delle legislazioni nazionali ed il corretto funzionamento del mercato interno.

[97] AGCM, AGCOM, Garante per la protezione dei dati personali (n.82), 75.

[98] Gustavo Olivieri, *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali,* Orizzonti del Diritto Commerciale, fascicolo speciale ad opera di G. Giappichelli Editore, (giugno 2021), 360-362.

[99] Tra i molti contributi, Rupprecht Podszun, Philip Marsden, *Restoring balance to digital competition - Sensible rules, effective enforcement,* Konrad-Adenauer-Stiftung e. V. , (2020).

fortemente alle derive autoritarie del nazionalsocialismo e pose le basi per la futura costituzione tedesca. Questa corrente di pensiero afferma la necessità della libera concorrenza sul mercato come strumento per garantire il benessere generale dei cittadini, delle imprese e dell'economia, punto condiviso dalle altre dottrine liberiste, ma aggiunge il bisogno di un ruolo attivo dello Stato per assicurare l'effettività della concorrenza e creare l'ecosistema normativo in grado di evitare condotte anticoncorrenziali dei privati, che potrebbero incidere negativamente sugli interessi della società. L'*antitrust* rappresenta dunque l'arma giuridica maestra per generare e mantenere questa "economia sociale di mercato", con un ruolo preponderante delle autorità amministrative. Le caratteristiche distintive del modello *antitrust* tedesco appaiono così, sintetizzando, l'importanza della componente giuridica nell'analisi concorrenziale, in un'ottica di maggiore certezza del diritto, scientificità dell'interpretazione ed applicazione delle regole (con definizione precisa degli istituti giuridici, come avviene, ad esempio, con la nozione di "posizione dominante", generalmente lasciata vaga nelle legislazioni nazionali ma che qui è ben inquadrata) [100], il rapporto di influenza reciproca tra *antitrust* europeo e nazionale, con il secondo mai assorbito dal primo ma anzi sempre pronto ad affermare la propria unicità, e la capacità di saper cogliere le innovazioni e farsi pioniere nella soluzione di problematiche nuove, come è avvenuto proprio nel caso *Facebook* in questione[101].

5. (*Segue:)* Decisione *Bundeskartellamt*

Il 6 febbraio 2019, con decisione B6-22/16, la sesta sezione del *Bundeskartellamt,* l'autorità amministrativa tedesca garante della concorrenza, ha imposto alla società *Facebook Inc.* rilevanti restrizioni alla raccolta e all'utilizzo dei dati degli utenti, per aver sfruttato la sua posizione dominante nel mercato dei *social network* per imporre

[100] Così da assicurare minori spazi di discrezionalità per le autorità amministrative e le istituzioni. A differenza degli altri stati membri, dove l'analisi *antitrust* è spesso più economica che giuridica, in Germania si può osservare il contrario e questo approccio è concretizzato nelle decisioni e nella prassi di autorità e corti.

[101] *Cfr.* Philipp Fabbio, *Il diritto della concorrenza in Germania: osservazioni e valutazioni in prospettiva europea,* Orizzonti del diritto commerciale, fascicolo 3/2019, (2019), 549-585.

condizioni inique. L'importanza di questa decisione sta nell'aver utilizzato le regole ed i criteri propri della *data protection* come parametro, nell'analisi *antitrust,* per la definizione della posizione dominante di *Facebook* (da qui in avanti abbreviato in *"FB")* e delle sue condotte, superando l'interpretazione giuridica precedente, che vedeva i due campi del diritto come due settori separati e paralleli.

Citando le parole del presidente del *Bundeskartellamt,* Andreas Mundt,

> "*today data are a decisive factor in competition. In the case of Facebook they are the essential factor for establishing the company's dominant position. On the one hand there is a service provided to users free of charge. On the other hand, the attractiveness and value of the advertising spaces increase with the amount and detail of user data. It is therefore precisely in the area of data collection and data use where Facebook, as a dominant company, must comply with the rules and laws applicable in Germany and Europe"*[102].

L'autorità comincia la sua analisi partendo da considerazioni sulla struttura sociale di *FB,* con le connesse *Whatsapp, Instagram, Snapchat, Oculus* e *Masquerade,* sul funzionamento della piattaforma, unito ai *business tools* da questa offerti, e *l'advertising*[103]. *Facebook.com* contava in Germania, nell'anno 2018, 23 milioni di utenti giornalieri attivi e 32 milioni mensili. Concentrandosi sui termini e le condizioni che gli utenti devono accettare per usufruire della piattaforma, in particolare da quanto previsto dalla *data policy* e *cookie policy*[104]*,* questi assicurano a *FB* la raccolta di un'estesa quantità di dati discendenti dall'utilizzo che gli utenti fanno dei prodotti forniti dalla società. Vengono inoltre collezionate anche informazioni esterne alla piattaforma, come quelle provenienti da *app* e siti *web* integrati con il *Social Network* (da qui in poi abbreviato in *SN*) (come nel caso *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV)* e da piattaforme delle società *partner,* giungendo perfino

---

[102] Andreas Mundt, *Press Release del Bundeskartellamt per il caso Facebook Germany,* (7 febbraio 2019), consultabile al sito https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2 .

[103] Elementi già analizzati nel primo capitolo di questo elaborato, a cui si rimanda.

[104] https://it-it.facebook.com/policy.php .

ad ottenerle da utenti non iscritti a *Facebook.com*[105]. Tutto questo avviene con scopo principale di fornire agli utenti un'esperienza più personalizzata e su misura, utilizzando come basi giuridiche tutte quelle previste dall'art. 6 del GDPR[106]. Il *Bundeskartellamt,* passando alla parte giuridica del suo accertamento, considera quello dei *social network* privati come mercato merceologico rilevante dal lato della domanda, nonostante *FB* sia una *multi-sided platform* e dunque influisca su altri mercati merceologici, come quello dell'*advertising,* e la Germania come mercato geograficamente rilevante. È interessante notare come la normativa che l'autorità ha deciso di applicare sia il diritto tedesco, segnatamente le sezioni 18 e 19, lettera a), della legge della concorrenza tedesca (GWB)[107], peraltro recentemente emendata proprio per attribuire poteri più incisivi al *Bundeskartellamt* e permettergli così di contrastare condotte abusive di imprese operanti su mercati a più versanti, attuando gli indirizzi della Direttiva 2019/1 e perseguendo i principi fissati dalle recenti legislazioni comunitarie[108]. Così facendo, invece di utilizzare l'art.102 TFUE, in astratto perfettamente applicabile, l'autorità ha conservato la sua competenza sulla questione, evitando l'ingerenza della CGUE e una sua possibile interpretazione differente. Dall'accertamento del *Bundeskartellamt* risulta come, considerando i diversi *SN* operanti in Germania e la differenziazione dei prodotti da questi offerti, *Facebook* non abbia dei reali concorrenti. Dalla scomparsa di *Google+* nel 2019, come *competitor* rimangono solo piattaforme minori e poco utilizzate, mentre

---

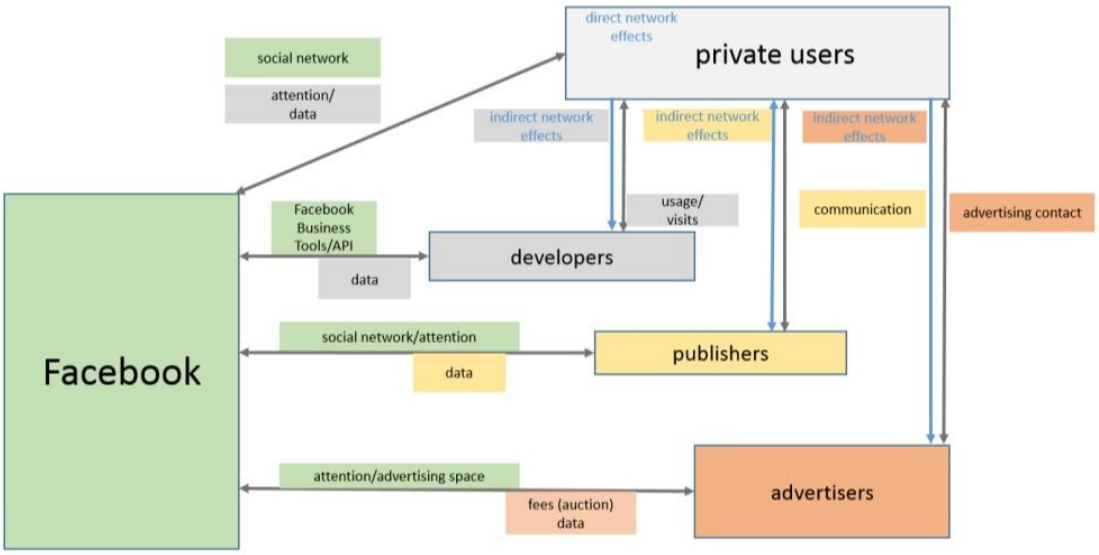
[105] Decisione B6-22/16 del Bundeskartellamt [2019], para 99-108.

[106] Art. 6 GDPR, "*Liceità del trattamento", comma 1* : "*Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è 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"*.

[107] La sez. 18 del GWB riguarda la posizione dominante delle imprese sul mercato, mentre la sez. 19 a) i comportamenti abusivi da parte di imprese dominanti, operanti su più versanti del mercato.

[108] Direttiva (UE) 2019/1 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, [2019], OJ L 11, 14.1.2019, p. 3–33 .

le altre più affermate, come *LinkedIn, Youtube o Snapchat,* ad esempio, offrono solo servizi specifici, che non concorrono a formare il mercato merceologico (senza contare che *Snapchat* è anche una controllata di *FB).* I due versanti principali su cui opera *FB,* quello degli utenti privati che si iscrivono al *social* e gli *advertiser,* vengono uniti proprio dalla piattaforma, sfruttando i già citati effetti di rete diretti ed indiretti, ma non solo gli unici che questa va a intermediare, poiché altri soggetti, come i *publisher* e i *developer,* ne fanno uso.



Fonte: *Bundeskartellamt, Decisione B6-22/16,* 6 febbraio 2019

Da quanto dunque risulta, *FB* è l'impresa dominante del mercato tedesco dei *SN* per utenti privati, con una dominanza quasi assoluta (a livello di utenti giornalieri con quote di mercato maggiori del 95%, o superiori all'80% mensilmente). La quota di mercato è talmente grande che perfino se si considerassero parte di esso altre piattaforme che non lo sono, come *Whatsapp, Youtube, Twitter e Snapchat,* si supererebbe la soglia del 40% stabilita dalla sezione 18, n. 4, del GWB, che sommata agli effetti di rete e alla quantità di dati in possesso di *FB,* genera delle barriere d'entrata difficilmente superabili da nuovi *competitor* che si affacciano al mercato.

La parte più rilevante ed apprezzabile di questa decisione sta nel rilievo che il *Bundeskartellamt* dà ai termini della *data policy* di *Facebook* come criterio rilevante per l'analisi della sua posizione dominante e contemporaneamente, anche all' effetto che da essi discende. Infatti, per l'autorità, questi termini, essendo una manifestazione del

potere di mercato dell'impresa, non ammissibili in una situazione perfettamente concorrenziale, violano le regole del GDPR e sono abusivi *ex* sez. 19, n. 1, del GWB. Basandosi anche sulle precedenti decisioni della Corte Federale Tedesca, come nel caso *Pechstein*[109]*,* dove è stato affermato che bisogna bilanciare tutti gli interessi in gioco per verificare l'illiceità dei termini, compresi i diritti costituzionalmente garantiti, e che la sezione 19 del GWB va applicata ove una parte abbia una forza contrattuale talmente grande da poter dettare i termini e le condizioni del rapporto, il *Bundeskartellamt* afferma che è indispensabile valutare, nell'analisi *antitrust* di una posizione dominante di un'impresa, anche le condotte relative alla *data protection*, soprattutto come nel caso di specie dove si parla di una *big tech,* perché capaci di incidere su diritti costituzionalmente garantiti. Il *Bundeskartellamt,* per giungere alla decisione, ha lavorato a stretto contatto con le altre autorità indipendenti tedesche, concordando che, nonostante non sia sua competenza decidere sulle violazioni del GDPR, le normative *antitrust* e di *data protection* debbano essere utilizzare in sinergia per rispondere alle sfide dei mercati digitali. Alla luce di questo suo ragionamento, il *Bundeskartellamt* ritiene che *Facebook,* attraverso la sua posizione dominante, sia in grado di imporre agli utenti termini della *data policy* che violano il GDPR, in particolare riguardo alle basi giuridiche considerate come giustificazioni al suo trattamento ex art. 6, poiché il consenso prestato dagli utenti, lasciati senza scelta o alternativa, non può considerarsi libero, viste le condizioni "*take-it-or-leave-it"* poco trasparenti.

Quanto premesso, senza contemplare anche il fenomeno del "*privacy paradox"* ed il fatto che gli interessi della società invocati per il trattamento non superano, anzi coinciderebbero, con quelli degli utenti (che sembrano trarre un supposto giovamento dal fornire i propri dati personali). Attraverso i suddetti termini, la piattaforma è in grado di raccogliere un quantitativo sproporzionato di dati, anche da parte di individui non ancora iscritti, potendo così rafforzare la sua posizione sul mercato. L'autorità conclude che *Facebook* ha in questo modo abusato della sua posizione dominante, attraverso cd. *exploitative business terms, ex* art. 19 GWB (giungendo perfino ad un *exclusionary abuse* a danno dei concorrenti). Per questi motivi è stato imposto a *Faceboook.com* il divieto di continuare il trattamento dei dati in forza delle sue condizioni abusive e di implementare soluzioni che mettano fine al problema[110].

---

[109] Caso KZR 6/15 della Corte Federale Tedesca, *Pechstein/International Skating Union,* [2016].

[110] *Cfr.* Bundeskartellamt, *Case summary Decisione B6-22/16,* (15 febbraio 2019).

Citando nuovamente le parole del presidente Andreas Mundt,

> *"With regard to Facebook's future data processing policy, we are carrying out what can be seen as an internal divestiture of Facebook's data. In future, Facebook will no longer be allowed to force its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts. The combination of data sources substantially contributed to the fact that Facebook was able to build a unique database for each individual user and thus to gain market power. In future, consumers can prevent Facebook from unrestrictedly collecting and using their data. The previous practice of combining all data in a Facebook user account, practically without any restriction, will now be subject to the voluntary consent given by the users. Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources"*[111].

6. (*Segue:)* Decisione Corte regionale superiore Düsseldorf

La decisione del *Bundeskartellamt* è stata appellata da *Facebook* dinanzi alla Corte regionale superiore di Düsseldorf chiedendo, come misura interinale, la sospensione dei suoi effetti. La Corte si è mostrata molto critica sull'analisi compiuta dall'autorità.
In *primis,* riconoscendo la corretta individuazione del mercato merceologico e geografico rilevante, sostiene che non si sia verificato un *exploitative abuse ex* sez. 19, n. 1 e 2, GWB da parte di *Facebook* perché il *Bundeskartellamt* non ha fatto adeguate investigazioni, soprattutto su come sarebbero state le ipotetiche condizioni imposte dalla società in un mercato perfettamente concorrenziale. La stessa mancanza di adeguate ricerche e prove viene dichiarata sul punto riguardante l'eccessività dei dati che la piattaforma raccoglierebbe dagli utenti attraverso i suoi strumenti, poiché non è stato

[111] Andreas Mundt (n. 93), 2-3.

trovato un *gap* considerevole tra i suoi *terms* "abusivi" e quelli conformi, e la successiva perdita di controllo ed al danno che gli *users* sperimenterebbero. In tal senso, non ci sono dimostrazioni delle pressioni e delle coercizioni che gli utenti subiscono da *FB* per cedere il loro consenso ed anzi questi, bilanciando i diversi interessi nella scelta di aderire al *social network* cedendo i loro dati, se non sono pienamente informati dei termini e delle condizioni che accettano, non è certo colpa del *SN*, bensì della loro disattenzione. Il semplice fatto di avere condizioni contrattuali sproporzionate non è abbastanza per ritenere un'impresa colpevole di abuso di posizione dominante, ma serve, sia per il diritto UE, *ex* art. 102 TFUE, che tedesco, *ex* sez. 19 GWB, un nesso causale tra l'abuso e la posizione di dominanza del mercato. Questo vale sia nei confronti di condotte abusive a carico dei consumatori, che di quelle dirette ad escludere possibili concorrenti sul mercato, ma nel caso di specie la causalità viene ritenuta insussistente, a differenza di ciò che sostiene il *Bundeskartellamt.* In altre parole, per la Corte mancherebbe un nesso tra il potere di mercato di *Facebook* e l'utilizzo che fa dei dati ed anzi, punto centrale della decisione, "*the necessary causality test should not be based on the provisions of the data protection law, but on the principles of the Cartel Act"*[112]. Così, l'analisi va condotta secondo criteri del diritto *antitrust,* mentre le possibili violazioni della protezione dei dati personali sono irrilevanti, contrariamente a quanto ritenuto dall'autorità. Per verificare se il consenso degli utenti fosse davvero libero, l'onere della prova ricade sul *Bundeskartellamt,* che però non avrebbe presentato risultanze sul punto. La Corte prende in considerazione anche il fenomeno del "*privacy paradox"* citato nella decisione dell'autorità, commentando che le conclusioni di questa sono invalide. Il fatto che la maggior parte degli utenti si dichiari interessato e preoccupato per la tutela della sua *privacy* e dei suoi dati, agendo però poi nella pratica in senso opposto, prestando poca attenzione o non leggendo i termini e le condizioni, non dimostra l'abuso di posizione dominante di *Facebook,* ma solo la disattenzione degli utenti. In più, rispondendo all'affermazione del *Bundeskartellamt* secondo cui il *social* restringe la concorrenza e l'accesso di altre società al mercato, la *High Regional Court* ritiene incomprensibile, richiedendo perciò ulteriori indagini, come la raccolta di data aggiuntivi, e la mera imposizione di termini e condizioni, possa sfociare in tali effetti negativi, soprattutto poiché, nonostante l'elevato numero di utenti mensili (32 milioni), la maggior parte degli utenti del rispettivo mercato geografico non è iscritta

[112] Caso VI-Kart 1/19 (V), Decisione della Corte regionale superiore di Düsseldorf [2019], p 23.

alla piattaforma (circa 50 milioni). I nuovi entrati o i concorrenti sul mercato possono perfettamente vincere il gioco della concorrenza sviluppando servizi più attraenti per gli *users,* nonostante l'effetto *network* di cui beneficia *FB.* Alla luce di tutti questi motivi, la Corte regionale superiore (*Landesgerichthof*) di Düsseldorf ha accordato alla società, con decisione del 26 agosto 2019, come misura interinale, la sospensione degli effetti della decisione del *Bundeskartellamt.*

7. (*Segue:)* Decisione Corte Federale Tedesca *(Bundesgerichtshof)*

Ricapitolando, *Facebook* prevede nei propri termini e condizioni, che gli utenti devono accettare per utilizzare il servizio, la possibilità di raccogliere un'ampia quantità di dati personali, anche provenienti dall'esterno della piattaforma. Il *Bundeskartellamt* con la sua decisione, in cui è stato affermato che i suddetti termini troppo permissivi sono irrispettosi della normativa a tutela dei dati personali ed il risultato dell'abuso di posizione dominante della società informatica, ha ordinato al *social* di non proseguire con il trattamento dei dati abusivo e di implementare misure alternative adeguate, utilizzando per la prima volta una violazione della *data protection* come criterio e spia rilevante per valutare una violazione *antitrust*. Successivamente all'appello della società, la Corte regionale superiore di Düsseldorf, mettendo in discussione con una severa critica la decisione dell'autorità garante della concorrenza, ha sospeso provvisoriamente gli effetti di quest'ultima, utilizzando un approccio maggiormente tradizionale nella sua disamina, probabilmente troppo rigido e formalistico, tenendo separati i due campi del diritto che invece erano stati sfruttati in sinergia. In questo dialogo istituzionale tra corti ed autorità è intervenuta anche la Corte Federale Tedesca (*Bundesgerichtshof)*. Con decisione KVR 69/19, il *Bundesgerichtshof* ha annullato la decisione della Corte di Düsseldorf e l'effetto sospensivo da essa accordato. Per la Corte Federale Tedesca non è possibile dubitare del fatto che *Facebook* abbia una posizione dominante nel mercato dei *social network* tedeschi e di come i suoi *terms & conditions* siano l'effetto dell'abuso di questa, come ha affermato il *Bundeskartellamt.* È interessante osservare come però la Corte non condivida totalmente l'argomentazione dell'autorità, ritenendo non rilevante che il trattamento dei dati ad opera di *FB* sfrutti anche quelli raccolto all'esterno della piattaforma, contrariamente a quanto stabilito dal

GDPR. Il punto considerato decisivo dal *Bundesgerichtshof*, invece, è che i termini privano gli utenti della libertà di scelta. Come già visto, *Facebook* opera in due mercati principali, quello dei *social network* e quello dell'*advertising,* da cui trae la sua fonte di finanziamento, e come impresa dominante ha una **responsabilità speciale** di garantire e mantenere la concorrenza su di essi. Impedendo con i *terms* l'autodeterminazione degli utenti vengono violati anche i diritti riconosciuti dal GDPR e dalla Costituzione tedesca, ma il risultato principale è quello lesivo della concorrenza, perché la mancanza di opzioni in capo agli utenti ingenera un effetto *lock-in,* rafforzato dall'effetto *network* diretto, impedendogli di cambiare piattaforma o scegliere di cedere meno dati, cose che in un mercato concorrenziale sarebbero state perfettamente possibili. Il possesso di quantità maggiori di dati è un fattore altamente rilevante, soprattutto nel mercato dei *social network,* e a tal riguardo è affermato che gli effetti anti concorrenziali su quest'ultimo*,* dominato da *Facebook,* si ripercuotono anche su quello dell'*advertising,* nonostante non sia stato individuato nel caso di specie. Per queste ragioni, la Corte Federale Tedesca ha confermato la decisione del *Bundeskartellamt,* utilizzando però, come si è visto, una diversa argomentazione[113]. Questa decisione rappresenta un enorme passo in avanti verso una più rigorosa disciplina applicabile ai *tech giants,* da anni sostenuta dagli studiosi tedeschi di matrice ordoliberale*,* indicando la strada per i fruttuosi e ben possibili rapporti tra diritto *antitrust* e *data protection*[114]. La vicenda ancora non si è conclusa, poiché la Corte di Düsseldorf, non condividendo la visione del *Bundesgerichtshof,* è tornata sul caso, rinviando pregiudizialmente la questione alla CGUE il 22 aprile 2021. Il rinvio contiene sette questioni su cui la Corte UE deve pronunciarsi.

Focalizzandosi sulla prima richiesta, la più rilevante per il tema in esame*,* viene chiesto

> *"se sia compatibile con gli articoli 51 e seguenti del Regolamento (UE) 2016/679 il fatto che un'autorità garante della concorrenza di uno Stato membro"* [nel caso di specie il *Bundeskartellamt*, dunque non un autorità di controllo *ex.* art . 51 GDPR] *"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*

[113] *Cfr.* Bundesgerichtshof*, Press Release No 080/2020 della decisione KVR 69/19 del Bundesgerichtshof* (23 giugno 2020), tradotta dal *Bundeskartellamt.*

[114] Adam Satariano, *Facebook Loses Antitrust Decision in Germany Over Data Collection,* The New York Times, (23 giugno 2020).

pubblicità, della comunicazione e delle relazioni pubbliche - e la filiale principale di tale impresa è situata in un altro Stato membro e ha la responsabilità esclusiva per il trattamento dei dati personali per l'intero territorio dell'Unione europea –, 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 GDPR, e disponga di porre fine a tale violazione"[115].

La Corte di Düsseldorf, nonostante il dissenso mostrato per la decisione del *Bundesgerichtshof,* fonda l'argomentazione del suo rinvio sul principio di diritto affermato proprio dalla Corte Federale nella sua decisione, la possibilità cioè che una violazione delle regole stabilite a tutela dei consumatori, come quelle previste nel GDPR, possa portare ad un abuso di posizione dominante, principio statuito anche dalla CGUE nel caso *British Airways*[116]. La suddetta impostazione ha però portato la *Regional Court* a concentrare il suo rinvio sulla *data protection* e sul possibile ruolo che le autorità nazionali garanti della concorrenza possano adempiere nel suo *enforcement.* Questo rappresenta una preziosa opportunità per la CGUE, perché potrà pronunciarsi sul rapporto tra diritto *antitrust* e *data protection,* interpretando le regole contenute nel GDPR in un'ottica evolutiva, in modo da rispondere alle sfide dell'economia digitale[117]. Intanto la forte azione propulsiva del *Bundeskartellamt* non si è interrotta, portando nel dicembre 2020 ad un nuovo procedimento per abuso di posizione dominante contro *Facebook.* Questa volta l'oggetto dell'indagine è stato rappresentato dai collegamenti tra la piattaforma del *social network* ed i prodotti di realtà aumentata sviluppati da *Oculus,* controllata di *Facebook.*

---

[115] C-252/21*: Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) — Facebook Inc. and Others v Bundeskartellamt,* [2021], accessibile e consultabile al sito: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0252 .

[116]C-95/04*, British Airways plc v Commission of the European Communities,* [2007], ECLI:EU:C:2007:166. Per un approfondimento: Bacon, Kelyn, *European Court of Justice Upholds Judgment of the European Court of First Instance in the British Airways/Virgin Saga,* Competition Policy International, Vol. 3, No. 2, (Autunno 2007) , (https://ssrn.com/abstract=1077127).

[117] *Cfr.* Reemt Matthiesen, Björn Herbers M.B.L, *ECJ to issue preliminary ruling on German FCO-Facebook case,* CMS Law-Now, (28 aprile 2021), consultabile al sito: https://www.cms-lawnow.com/ealerts/2021/04/ecj-to-issue-preliminary-ruling-on-german-fco-facebook-case .

Il presidente Andreas Mund ha dichiarato, nel comunicato stampa del procedimento, che

> *"in the future, the use of the new Oculus glasses requires the user to also have a Facebook account. Linking virtual reality products and the group's social network in this way could constitute a prohibited abuse of dominance by Facebook. With its social network Facebook holds a dominant position in Germany and is also already an important player in the emerging but growing VR (virtual reality) market. We intend to examine whether and to what extent this tying arrangement will affect competition in both areas of activity"*[118].

Inizialmente la piattaforma di realtà aumentata veniva offerta da *Oculus* separatamente da quella della casa madre, ma di recente la distinzione è venuta meno e *Oculus* è stata trasformata in una funzione aggiuntiva del *social network* di *Facebook.* Non solo. Gli ultimi modelli di *hardware* per l'accesso alla *VR* prodotti dalla società hanno cominciato a chiedere, come condizione di utilizzo, la registrazione con un *Facebook account*. In questo modo gli *account Oculus* non sono più sufficienti e bisogna essere necessariamente utenti della piattaforma principale. Perciò l'autorità ha deciso di intervenire per accertare la concreta esistenza di una condotta di *tying* ad opera della società madre. I visori *VR* costituiscono una grande innovazione, il passaggio dal mondo digitale in due dimensioni a quello in 3D, ma negli anni è stata utilizzata principalmente nel settore dei videogiochi e dell'intrattenimento, con un mercato ancora emergente e in continua crescita. Il *rebranding* di *Facebook* in *Meta* ed i nuovi piani della società hanno cambiato totalmente le carte in tavola, estendendo le possibilità di utilizzo dei sensori per la realtà aumentata potenzialmente a qualunque settore economico, amplificandone l'importanza[119]. Agli inizi di questa nuova rivoluzione digitale al limite della fantascienza, il controllo dei prodotti *hardware* e *software* costituisce un fattore di forte vantaggio competitivo capace di generare rilevanti barriere all'entrata per i nuovi *competitor* e di allentare il progresso tecnologico che solo il gioco

---

[118] *Cfr. Press Release Bundeskartellamt/ Facebook* (10 dicembre 2020).

[119] Per un interessante approfondimento: Cameron Costa, *Inside the metaverse economy, jobs and infrastructure projects are becoming real,* CNBC (15 gennaio 2022), https://www.cnbc.com/2022/01/15/inside-the-metaverse-economy-this-is-what-will-be-for-real-in-2022.html .

della libera concorrenza può assicurare. Anche in questa occasione perciò è apprezzabile la lungimiranza dell'autorità tedesca, che ha anticipato il *trend* dei metaversi e l'ambizione di *Facebook,* ora *Meta,* di conquistare il relativo mercato e diventarne il principale attore. Nei mesi a venire si assisterà al prosieguo dell'*iter* giurisprudenziale della vicenda, dove nuovamente le corti tedesche potrebbero avere la possibilità di farsi portatrici del cambiamento e dell'innovazione.

8. La principale casistica Europea pre-"*Facebook Germany"*

Il caso "*Facebook Germany"* è solo l'attuale epilogo del dibattito in Europa sul rapporto tra *data protection* e diritto *antitrust,* con l'apertura a loro intersezioni e sinergie che di sicuro nel futuro prossimo diverranno più forti e numerose. Negli anni precedenti alla vicenda, i *regulators,* le istituzioni europee e nazionali, incluse le corti, così come la dottrina, si sono interrogati su quale fosse l'assetto migliore da perseguire per la relazione tra questi campi del diritto. Vari studi hanno affermato la positività, quasi l'esigenza, di una maggiore intersezione tra le regole dirette a proteggere i dati personali e quelle per la tutela della concorrenza e dell'interesse dei consumatori, come il già citato *report* congiunto di *Bundeskartellamt* (Autorità della concorrenza tedesca) e *Autorité de la concurrence* (Autorità della concorrenza francese) del 2016[120], ma l'indirizzo dominante è stato quello "separatista". Questa visione traspare, ad esempio, in un articolo del 2017 dei professori Giuseppe Colangelo e Mariateresa Maggiolino, proprio riguardo l'iniziativa del *Bundeskartellamt* contro *Facebook,* in cui viene sostenuta la tesi della separazione, giustificata dalla differenza di obiettivi tra i due corpi normativi, nonostante sia comunque dichiarata la grande importanza dei dati nell'economia digitale[121]. Bisogna, in prima battuta, premettere che l'utilizzo di parametri propri di altri campi del diritto non è un fenomeno inedito nell'analisi *antitrust*. Negli scorsi decenni molteplici sono state le pronunce di abuso di posizione dominante basate sul rispetto di regole diverse da quelle a tutela della concorrenza. Un

[120] *Cfr.* Bundeskartellamt, Autorité de la concurrence (n. 48).

[121] Giuseppe Colangelo, Mariateresa Maggiolino, *Big data, data protection and antitrust in the wake of the Bundeskartellamt case against Facebook,* Rivista italiana di *Antitrust,* n. 1 (2017), 104-112.

esempio per tutti è il caso *AstraZeneca v Commissione europea*[122], dove la CGUE ha dovuto tenere conto del mancato rispetto delle regole sulla proprietà intellettuale.
La Corte, nei paragrafi 105-108 della sentenza, ha affermato che

> "*il Tribunale, nel caso di specie, ha esaminato se, alla luce del contesto in cui è stata messa in atto la prassi considerata fosse tale da indurre le autorità pubbliche a creare indebiti ostacoli normativi alla concorrenza, per esempio attraverso la concessione irregolare di diritti esclusivi a suo vantaggio. Esso ha considerato, a questo riguardo, che il margine di valutazione limitato delle autorità pubbliche o l'assenza di un obbligo ad esse incombente di verificare l'esattezza o la veridicità delle informazioni comunicate potevano costituire elementi rilevanti che dovevano essere presi in considerazione per stabilire se la prassi considerata potesse sfociare nella creazione di ostacoli normativi alla concorrenza. Contrariamente a quanto fanno valere le ricorrenti, detto esame del Tribunale non si basa affatto sul concetto secondo il quale la pratica di cui trattasi costituirebbe un «abuso in sé», indipendentemente dal suo effetto anticoncorrenziale. Al contrario, il Tribunale ha espressamente sottolineato, al punto 377 della sentenza impugnata, che dichiarazioni volte ad ottenere irregolarmente diritti esclusivi costituiscono un abuso solo quando sia dimostrato che, alla luce del contesto oggettivo nel quale vengono rese, tali dichiarazioni sono realmente idonee a spingere le autorità pubbliche ad accordare il diritto esclusivo richiesto*[123]*",* dunque, "***con riferimento in particolare a questi paesi in cui le dichiarazioni ingannevoli dell'AZ gli hanno consentito di ottenere CPC irregolari, le ricorrenti non possono negare l'effetto anticoncorrenziale di dette dichiarazioni***"[124].

La violazione delle norme di *IP law* si è dimostrata sintomo ed elemento centrale dell'abuso di posizione dominante di *AstraZeneca.* Un utilizzo simile delle regole di *data protection* come parametro per le indagini e le decisioni di diritto della concorrenza, in modo non dissimile da quanto fatto dal *Bundeskartellamt,* non è perciò

---

[122] C-457/10*, AstraZeneca v Commissione europea,*[2021], ECLI:EU:C:2012:770.

[123] ibidem, para 105-106.

[124] ibidem*,* para 108.

una possibilità remota ed avulsa dal mondo giuridico[125]. Per meglio comprendere l'evoluzione interpretativa sfociata nel caso *Facebook Germany* gioverà, quindi, analizzare la più importante casistica europea che ha interessato il rapporto tra *data protection* e *antitrust.* Il punto di partenza di questa disamina è sicuramente il caso *Asnef-Equifax*[126] del 2007*,* avente ad oggetto una domanda di pronuncia pregiudiziale sull'interpretazione dell'art. 81 Trattato CE (l'attuale art.101 TFUE), in una vicenda riguardante la compatibilità di un registro tenuto dal gruppo *Asnef-Equifax* relativo ad informazioni creditizie dei clienti, finalizzato a "*fornire servizi di informazione sulla solvibilità e il credito per mezzo del trattamento automatico di dati relativi ai rischi assunti dagli istituti che operano nel settore delle attività di prestito e di credito"*[127], con le regole di diritto della concorrenza stabilite nel trattato.
In quell'occasione la terza sezione della CGUE ha stabilito che

> *"le eventuali questioni relative alla natura riservata dei dati a carattere personale non rientrano, in quanto tali, nel diritto della concorrenza, le stesse possono essere risolte sulla base delle disposizioni rilevanti in materia di tutela di tali dati"*,

come affermato anche dall'avvocato generale nelle sue conclusioni[128]. Non è facile comprendere le ragioni di questa decisione tendente ad escludere il legame tra norme antitrust (sull'abuso di posizione dominante) e l'eventuale raccolta o trattamento illeciti di dati personali ma si può ipotizzare che essa sia figlia del contesto ancora poco maturo, con i fenomeni della *data economy* e del *web 2.0* non ancora "esplosi" e la grande preoccupazione delle istituzioni europee di stabilire un mercato creditizio comune, in vista della promozione delle quattro libertà fondamentali riconosciute dai trattati[129]. Inoltre, negli anni in cui è accaduta la vicenda, le intersezioni tra la protezione dei dati personali ed il diritto *antitrust* erano molto meno ricorrenti, perciò i due campi

---

[125] Francisco Costa-Cabral, Orla Lynskey, *The Internal and External Constraints of Data Protection on Competition Law in the EU,* LSE Law, Society and Economy Working Papers 25/2015*,* 14-24.

[126] C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc),* [2006], ECLI:EU:C:2006:734.

[127] ibidem, para 7.

[128] ibidem, para 63.

[129] Segnatamente, la libera circolazione di merci (art. 28 e ss. TFUE), persone (artt. 45-49 e ss. TFUE), servizi e capitali (artt. 56-63 e ss TFUE).

venivano considerati sufficientemente distinti per risolvere le rispettive controversie[130]. Naturalmente, col passare del tempo, il valore e l'importanza dei dati è andato aumentando ed, ironia della sorte, proprio *Equifax* ha subito, nel 2017, un pesante *data breach* che ha interessato quasi 150 milioni di persone. Un secondo caso da considerare, successivo di solo un anno rispetto alla decisione della CGUE su *Asnef-Equifax,* è l'acquisizione *Google/DoubleClick*[131]*,* in cui la Commissione ha dovuto valutare gli effetti dell'operazione sul regime concorrenziale europeo, vista la sua rilevanza comunitaria. Entrambe le società forniscono diversi servizi informatici e sono attive principalmente nel mercato della pubblicità *online*, settore in rapida ascesa che ha visto negli anni moltiplicare il proprio valore. Dopo aver alacremente individuato le più comuni categorie di *advertising online,* divise tra *search ads* e *non-search ads*[132]*,* i due *genus* principali*,* e le loro diverse configurazioni*,* la Commissione considera i mercati dominanti che verrebbero influenzati[133]. La definizione di questi ad opera delle società interessate, segnatamente la pubblicità attraverso qualunque *medium,* viene ritenuta troppo ampia, anche alla luce delle particolarità insite nella pubblicità in rete, dove il costo dipende dall'effettivo numero di utenti che visualizzano l'annuncio e non dal potenziale bacino ottenuto mediante criteri generali. Segmentando i diversi servizi la Commissione valuta necessario tenere in considerazione solamente il mercato merceologico degli annunci tramite piattaforme digitali, con quello geografico limitato allo spazio economico europeo[134]. In essi *Google* appare l'azienda principale, grazie anche alle società controllate ed ai loro diversi servizi offerti, mentre *DoubleClick* tra le maggiormente rilevanti. Dopo aver analizzato i possibili scenari concorrenziali, le potenziali condotte anticoncorrenziali utilizzabili dalle società, i concorrenti presenti nel

---

[130] Olivia Altmayer, *The Tipping Point – Reevaluating the ASNEF- EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach,* Northwestern Journal of International Law & Business, Volume 39 (2018), 51-53.
https://scholarlycommons.law.northwestern.edu/njilb/vol39/iss1/2 .

[131] *Google/DoubleClick,* Decisione della Commissione COMP/M.4731 [2008], OJ C 184, 22.7.2008, p. 10–12.

[132] Le prime appaiono successivamente ad una ricerca nel *browser,* mentre le secondo in qualunque pagina.

[133] *Google/DoubleClick,* Decisione della Commissione COMP/M.4731 [2008], OJ C 184, 22.7.2008, para 44-56.

[134] ibidem, para 57-84.

mercato e i loro servizi, la Commissione esclude pericoli discendenti dall'operazione[135]. Perfino la fornitura di servizi congiunti (cd. *bundling)* non viene ritenuto dannoso, perché sul mercato sono già presenti concorrenti che ne fanno uso senza che ciò possa ledere i singoli *competitors.* Il punto più importante, nell'economia di questa trattazione, è la valutazione sulla rilevanza, per l'analisi concorrenziale, dell'unione dei vasti *database* in possesso delle due società.
Al riguardo, nel paragrafo 368 della decisione, la Commissione statuisce che

> " *this Decision refers exclusively to the appraisal of this operation with Community rules on competition, namely whether the merger is compatible with the objectives of the Merger Regulation in that it does not impede effective competition in the common market"*[136].

Si conferma così la visione prospettata dalla CGUE nel caso *Asnef-Equifax* dell'anno prima, concludendo asserendo la compatibilità dell'acquisizione[137]. È interessante che nell'indagine portata avanti dalla Commissione europea inizialmente si ritenesse l'operazione non compatibile e potenzialmente pericolosa per il regime concorrenziale tra stati membri, ma che dopo la decisione della *Federal Trade Commission* sulla stessa, precedente di qualche mese rispetto a quella dell'istituzione europea, il risultato finale sia diametralmente opposto. L'autorità americana, dopo aver analizzato gli stessi punti oggetto dell'indagine della Commissione europea, dichiara il via libera all'acquisizione e afferma che

> *"the markets within the online advertising space continue to quickly evolve, and predicting their future course is not a simple task. Accounting for the dynamic nature of an industry requires solid grounding in facts and the careful application of tested antitrust analysis. Because the evidence did not support the theories of potential competitive harm, there was no basis on which to seek to impose conditions on this merger"*[138].

---

[135] ibidem, para 59-340.

[136] ibidem, para 368.

[137] ibidem, para 368.

[138] Federal Trade Commission*, File No. 071-0170 su Google/Doubleclick,* [2007].

La linea interpretativa europea è stata mantenuta anche negli anni a seguire, come in occasione della decisione della Commissione sulla fusione tra *Facebook* e *Whatsapp*[139], in cui l'istituzione europea è stata chiamata, *ex* art. 1-5 del Reg. CE 139/2004[140], a pronunciarsi sull'operazione, dato il superamento delle soglie stabilite dal regolamento. È interessante, in prima battuta, notare che nell'argomentazione della Commissione sull'operazione di acquisto di *Whatsapp* da parte di *Facebook* per ben 19 miliardi di dollari, dopo una sezione dedicata all'individuazione del mercato geografico (lo spazio economico europeo, se non il mondo intero[141]) e merceologico rilevante (servizi di comunicazione, *social network* e *online advertising*)[142], questa si pronunci sulla rilevanza dei dati nel settore dei servizi digitali e di come possano incidere sull'operazione. In particolare è affermato che, a seguito dell'indagine, non risulta che ci siano *switching-costs* rilevanti per gli utenti delle *app* di messaggistica istantanea, anche alla luce dell'effetto *network* diretto, e che, vista la grande velocità del mercato, il possesso di quantità maggiori di dati non è abbastanza per impedire a nuovi *competitors* di entrarvi[143]. Viene, inoltre, statuito che "*in this market any leading market position*

---

https://www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation .

[139] *Facebook/Whatsapp,* Decisione della Commissione Caso COMP/M.7217, [2014].

[140] Regolamento (CE) n. 139/2004 del Consiglio, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni") [2004] OJ L 24, 29.1.2004, p. 1–22 .

L'art 1 del Regolamento, rubricato "*Campo di applicazione",* prevede al comma 1 che "*Il presente regolamento si applica a tutte le concentrazioni di dimensione comunitaria come definite dal presente articolo, fatti salvi l'articolo 4, paragrafo 5, e l'articolo 22."*

L'art. 5 invece, rubricato *"Calcolo del fatturato",* stabilisce al comma 1 che *"Il fatturato totale ai sensi del presente regolamento comprende gli importi ricavati dalla vendita di prodotti e dalla prestazione di servizi realizzati dalle imprese interessate nell'ultimo esercizio e corrispondenti alle loro normali attività, previa detrazione degli sconti concessi sulle vendite nonché dell'imposta sul valore aggiunto e di altre imposte direttamente legate al fatturato. Il fatturato totale di una impresa interessata non tiene conto delle transazioni avvenute tra le imprese di cui al paragrafo 4 del presente articolo. Il fatturato realizzato, nella Comunità o in uno Stato membro, comprende i prodotti venduti ed i servizi forniti ad imprese o a consumatori nella Comunità o nello Stato membro in questione."*

[141] Commissione Europea (n. 115), para 35.

[142] ibidem, para 13-83.

[143] ibidem, para 84-105.

even if assisted by network effects is unlikely to be incontestable. The market of consumer communications apps has a long track record of entry by new players"[144].
I punti sicuramente più importanti di questa decisione sono però quelli dei paragrafi 123 e 164, dove, rispettivamente, viene affermato che l'unione dei *database* di *Facebook* e *Whatsapp* e la loro interoperabilità siano una misura tecnica difficilmente raggiungibile, in base a quanto dichiarato dalle società,[145] e che

> *"for the purposes of this decision, the Commission has analyzed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules"*[146].

La decisione si conclude, così, in un assenso senza condizioni alla concentrazione. Probabilmente anche questa, così come il caso precedente, sconta i tempi non ancora pienamente maturi, in cui fenomeni come le cd. *killer acquisition,* acquisizioni dirette a "fagocitare" possibili nuovi concorrenti sul mercato, e gli effetti di rete non avevano mostrato la loro piena magnitudine, permettendo l'irrobustimento delle posizioni di mercato delle piattaforme digitali più longeve e capaci di vincere il gioco della concorrenza. La Commissione purtroppo si è dovuta presto ricredere, adottando una nuova decisione nel 2017. In essa viene constatata la non veridicità delle informazioni che *Facebook* ha fornito nel 2014 in occasione del *merger.* A differenza di quanto notificato, cioè l'impossibilità o la grande difficoltà nel breve termine di poter associare i profili e gli *ID* degli utenti del *social* a quelli di *Whatsapp,* realizzabile solo con l'intervento volontario e manuale degli *user,* viene scoperto come *FB* già fosse a conoscenza, nel 2014, di come poter realizzare l'associazione, che in seguito verrà concretizzata[147]. Attivare il collegamento *Whatsapp* alla pagina *FB* è molto semplice: da

---

[144] ibidem, para 132.

[145] ibidem, para 123.

[146] ibidem, para 164.

[147] Cfr. Commissione europea, *Sintesi della decisione che infligge ammende a un'impresa, a norma dell'articolo 14, paragrafo 1, del regolamento (CE) 139/2004 del Consiglio, per aver fornito indicazioni inesatte o fuorvianti, 2017/C-286/6,* [2017].

un qualsiasi account nella sezione "impostazioni" della propria pagina *FB* è presente la nuova voce "*WhatsApp"*. Al suo interno si deve inserire il proprio numero ed il codice di verifica che sarà inviato via *chat* da *FB*. Sono poi sufficienti un paio di *click* ed il collegamento è attivo. È quindi possibile aggiungere un pulsante *WhatsApp* alla propria pagina *FB,* che gli utenti potranno usare per inviare messaggi direttamente in *chat.* Inoltre si può mostrare il proprio numero di telefono nelle informazioni della pagina[148]. In questo modo *FB* ottiene un ulteriore vantaggio competitivo perché è in grado di raccogliere e sfruttare i dati e le informazioni degli utenti di *WhatsApp,* ora nella disponibilità della piattaforma madre. Perciò, con decisione C 286/06 del 28 maggio 2017, la Commissione impone due ammende da 55 milioni di euro per violazione dell'art 14, paragrafo 1, lettere a) e b)[149], misure piuttosto blande per il giro d'affari delle società. Questa visione fortunatamente inizia a mutare nel 2016, con la decisione della Commissione sulla concentrazione *Microsoft/LinkedIn*[150]. Considerando i possibili effetti negativi generati dall'unione dei due *database,* la Commissione osserva che le due società sono sottoposte alle regole sulla protezione dei dati personali, e

> "*assuming such data combination is allowed under the applicable data protection legislation, there are two main ways in which a merger may raise horizontal issues as a result of the combination under the ownership of the merged entity of two datasets previously held by two independent firms. First, the combination of two datasets post-merger may increase the merged entity's market power in a hypothetical market for the supply of this data or increase barriers to*

---

[148] Per ulteriori approfondimenti:
https://it-it.facebook.com/business/help/1583303048513172?id=2129163877102343 .

[149] Regolamento (CE) n. 139/2004, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni"), [2004], OJ L 24, 29.1.2004, art. 14*, "Ammende":*
1. La Commissione può, mediante decisione, infliggere alle persone di cui all'articolo 3, paragrafo 1, lettera b), alle imprese o alle associazioni di imprese ammende il cui importo può giungere fino all'1 % del fatturato totale dell'impresa o associazione di imprese interessata ai sensi dell'articolo 5 quando, intenzionalmente o per negligenza: a) forniscano indicazioni inesatte o fuorvianti in una richiesta, dichiarazione, notificazione o integrazione ad una notificazione presentata in conformità dell'articolo 4, dell'articolo 10, paragrafo 5, o dell'articolo 22, paragrafo 3; b) forniscano indicazioni inesatte o fuorvianti in risposta ad una domanda rivolta a norma dell'articolo 11, paragrafo 2.

[150] *Microsoft / LinkedIn,* Decisione della Commissione europea Caso M.8124 [2016], OJ C 388, 21.10.2016, p. 4–4.

entry/expansion in the market for actual or potential competitors, which may need this data to operate on this market. Competitors may indeed be required to collect a larger dataset in order to compete effectively with the merged entity than absent the merger. Second, even if there is no intention or technical possibility to combine the two datasets, it may be that pre-merger the two companies were competing with each other on the basis of the data they controlled and this competition would be eliminated by the merger"[151].

Nel caso di specie non appaiono rischi sotto questo punto di vista e qualsiasi preoccupazione riguardante la *privacy* e la sicurezza dei dati non rientra nel campo d'applicazione e negli obiettivi del diritto *antitrust.* La Commissione riconosce, comunque, la loro rilevanza quale parametro da tenere in considerazione nell'analisi concorrenziale in quanto può influenzare i *competitors* sul mercato e soprattutto i consumatori, lesi da una minore possibilità di scelta[152]. Si nota la maggiore attenzione prestata dall'istituzione alla tematica, molto diversa rispetto a quanto fatto anche solo due anni prima nel caso *Facebook/Whatsapp,* ed il delinearsi dei punti fondamentali che saranno analizzati nel caso "*Facebook Germany"*. Degne di nota sono anche le recenti e molteplici sanzioni inflitte dalla Commissione europea a *Google*, parte dell'intervento più attento e mirato nei confronti dei giganti tecnologici. Il 17 giugno 2017 la Commissione ha applicato alla società statunitense una sanzione di 2.42 miliardi di euro per aver abusato della sua posizione dominante nel mercato dei motori di ricerca, in modo da favorire illegalmente un suo prodotto collegato, *Google Shopping*[153]. Il prodotto principale di *Google* è il suo motore di ricerca, ma nel 2004 è entrato nel mercato dei servizi di *shopping comparison,* dove le imprese dipendono fortemente dal livello di traffico sulle pagine dei loro servizi. Di fronte ai risultati economici relativamente bassi dei concorrenti, *Google* nel 2008 decide di cambiare strategia, facendo sì che gli algoritmi del motore di ricerca mostrino maggiormente i risultati di *Google Shopping*, a dispetto dei prodotti avversari. I consumatori sono soliti cliccare sui primi risultati di ricerca, perciò il traffico per i concorrenti è giunto quasi ad annullarsi.

---

[151] ibidem, para 179.

[152] ibidem, para 180- 250.

[153] Commissione europea, *Comunicato stampa: Multa di 2,42 miliardi di EUR a Google per il vantaggio illegale conferito al proprio servizio di acquisti comparativi",* (27 giugno 2017), https://ec.europa.eu/commission/presscorner/detail/it/IP_17_1784 .

Dopo indagini approfondite, la Commissione ha affermato l'abuso di posizione dominante nel mercato dello *shopping comparison,* naturalmente all'interno dello Spazio Economico Europeo, condannando la società a pagare l'ammenda ed interrompere la condotta abusiva. *Google* ha ricorso alla CGUE, che però nella causa *T-612/17 Google and Alphabet v Commission (Google Shopping)* ha confermato l'analisi della Commissione[154]. Margrethe Vestager, Commissario europeo per la concorrenza, ha osservato come

> *"Google ha lanciato tanti prodotti e servizi innovativi che ci hanno cambiato la vita. Gli effetti sono indubbiamente positivi. Ma nella strategia attuata per il suo servizio di acquisti comparativi, non si è limitata a rendere il suo prodotto migliore di quelli concorrenti per attrarre più clienti. Google ha abusato della sua posizione dominante come motore di ricerca per promuovere il suo servizio tra i risultati della ricerca e per retrocedere quello dei concorrenti. Google ha tenuto un comportamento illegale ai sensi delle norme antitrust dell'UE perché ha impedito ad altre imprese di competere in base ai propri meriti e di innovare. Ma soprattutto, ha negato ai consumatori europei la possibilità di scegliere liberamente i servizi e di sfruttare appieno i vantaggi dell'innovazione"*[155].

Lo stesso approccio, volto a bilanciare l'interesse economico delle società private con il benessere dei consumatori ed il progresso tecnologico, traspare in un secondo procedimento avviato contro la stessa *Google* nel luglio 2018, con una sanzione di 4.34 miliardi di euro e l'obbligo di cessazione della condotte illegali[156]. In questo, la società viene accusata di aver imposto restrizioni illecite agli sviluppatori del sistema operativo *Android* (progettato dalla *Open Handset Alliance,* consorzio di aziende il cui scopo è la

---

[154] Caso T-612/17, *Google and Alphabet v Commission (Google Shopping),* [2021], ECLI:EU:T:2021:763.

[155] Margrethe Vestager, *Comunicato stampa: Multa di 2,42 miliardi di EUR a Google per il vantaggio illegale conferito al proprio servizio di acquisti comparativi",* (27 giugno 2017), https://ec.europa.eu/commission/presscorner/detail/it/IP_17_1784 .

[156] Commissione europea, *Comunicato stampa: la Commissione infligge a Google un'ammenda di 4.34 miliardi di € per pratiche illegali riguardanti i dispositivi mobili Android volte a rafforzare la posizione dominante del motore di ricerca di Google,* (18 giugno 2018), https://ec.europa.eu/commission/presscorner/detail/it/IP_18_4581 .

creazione di *open standard* per dispositivi mobili, con *Google* come capofila e impresa dominante) ai produttori di *device,* per rafforzare la propria posizione dominante sul mercato europeo. In particolare, le condotte contestate consistono nell'aver obbligato le società produttrici e sviluppatrici ad inserire nei propri prodotti *applications* preinstallate di *Google,* senza possibilità di eliminazione (ponendo in essere il cosiddetto *tying*); non aver permesso l'installazione di versioni alternative del sistema operativo (cd. *fork*); aver subordinato i pagamenti nei loro confronti al rispetto delle condizioni dettate. Se un'impresa desidera iniziare a produrre il *software* o l'*hardware* ha bisogno di accettare le condizioni commerciali stabilite da *Google*. Tramite i sopra citati termini però, *Google* abusa della posizione dominante, imponendo condizioni che privilegiano i propri prodotti e servizi a discapito dell'innovazione tecnologica[157]. Nelle conclusioni del Commissario Margrethe Vestager viene ribadita l'importanza dell'intervento:

> *"L'Internet mobile, che costituisce oggi più della metà del traffico Internet globale, ha cambiato la vita di milioni di europei. Il caso in oggetto riguarda tre tipi di restrizioni che Google ha imposto ai produttori di dispositivi mobili che utilizzano Android e agli operatori di rete per fare in modo che il traffico che transita su tali dispositivi venga indirizzato verso il motore di ricerca di Google. Agendo in tal modo, Google ha utilizzato Android come strumento per consolidare la posizione dominante del proprio motore di ricerca. Tali pratiche hanno negato ai concorrenti la possibilità di innovare e di competere in base ai propri meriti ed hanno negato ai consumatori europei i vantaggi di una concorrenza effettiva nell'importante comparto dei dispositivi mobili. Ai sensi delle norme antitrust dell'UE, si tratta di una condotta illegale"*[158].

Una terza decisione della Commissione, datata marzo 2019, impone a *Google* un'ammenda di 1.4 miliardi di euro per aver imposto a siti *web* di terzi condizioni

---

[157] ibidem.

[158] Margrethe Vestager , *Comunicato stampa: la Commissione infligge a Google un'ammenda di 4.34 miliardi di € per pratiche illegali riguardanti i dispositivi mobili Android volte a rafforzare la posizione dominante del motore di ricerca di Google,* (18 giugno 2018), https://ec.europa.eu/commission/presscorner/detail/it/IP_18_4581 .

contrattuali illecite, abusando della sua posizione dominante[159]. Grazie a questi termini attraverso cui i gestori dei siti ottenevano la possibilità di utilizzare *Google AdSense,* prodotto della società per monetizzare attraverso il *display* di annunci pubblicitari, e in cambio si richiedeva di non mostrare gli annunci dei *competitors* nei risultati di ricerca interni alle singole pagine. La restrizione impattava, così, negativamente sulla libera concorrenza del relativo mercato, rafforzando ancora di più la dominanza[160]. Il ricorso di *Google* è ancora pendente dinanzi alla CGUE. L'ultimo caso a cui si farà riferimento è, invece, l'acquisizione di *Fitbit* da parte di *Google* nel 2020[161]. Nella sua approfondita indagine di quasi trecento pagine, la Commissione europea analizza i risvolti concorrenziali dell'operazione, lavorando a stretto contatto con le altre autorità. Riveste un ruolo centrale, in particolare, la dichiarazione dell'EDPB sui possibili effetti della concentrazione sulla privacy e la protezione dei dati degli utenti[162]. Questa potrebbe infatti avere pesanti ripercussioni sugli utenti dei servizi digitali. Nel documento viene fatto notare come

> "*Si teme che l'eventuale ulteriore combinazione e accumulo di dati personali sensibili riguardanti le persone in Europa da parte di una grande azienda tecnologica possa comportare un elevato livello di rischio per i diritti fondamentali alla vita privata e alla protezione dei dati personali. Il comitato ha già dichiarato che ogni qualvolta sia proposta una concentrazione significativa è essenziale valutare le implicazioni a lungo termine per la tutela dei diritti economici, dei diritti dei consumatori e dei diritti in materia di protezione dei dati. Il comitato rammenta pertanto alle parti della prospettata concentrazione, in conformità del principio di responsabilizzazione, gli obblighi loro incombenti ai sensi del regolamento generale sulla protezione dei dati e quindi il dovere di condurre in*

---

[159] Commissione europea, *Comunicato stampa: la Commissione commina a Google un'ammenda pari a 1,49 miliardi di € per pratiche abusive nella pubblicità,* (20 marzo 2019), https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1770 .

[160] ibidem.

[161] *Google/Fitbit* (Caso M.9660), Decisione della Commissione C/2020/9105,[2020], OJ C 194, 21.5.2021, p. 6–6 .

[162] EDPB, *Dichiarazione sulle implicazioni delle concentrazioni per la vita privata,* (19 febbraio 2020), consultabile al *link:* https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-privacy-implications-mergers_en.

modo trasparente una valutazione completa dei requisiti in materia di protezione dei dati e delle implicazioni della concentrazione per la vita privata. Il comitato esorta le parti ad attenuare i possibili rischi della concentrazione per il diritto alla vita privata e alla protezione dei dati prima di notificare la concentrazione alla Commissione europea"[163].

Le preoccupazioni principali della Commissione riguardano l'accesso di *Google* alla tecnologia e al *software* di *Fitbit,* con la possibilità di condotte anticoncorrenziali nel mercato dei *wearable devices* che vedrebbero favoriti i prodotti *Fitbit* grazie a maggiore compatibilità con i *device* aventi *Android* come OS. La questione più importante riguarda tuttavia proprio la protezione dei dati personali, perché il timore delle autorità è che, con l'acquisizione e la successiva unione dei *database* delle due società, *Google* possa avvantaggiarsi di tutti i dati degli utilizzatori di *Fitbit* per pubblicità incredibilmente mirate, dati peraltro particolarmente sensibili, trattandosi di informazioni sulla salute e le condizioni fisiche. La Commissione alla fine ha approvato l'operazione, ma con degli obblighi che Google sarà tenuta a rispettare per i prossimi dieci anni. Tra questi, i più rilevanti appaiono l'obbligo di mantenere tecnicamente separati i due *database,* l'obbligo di non sfruttare i dati raccolti dai dispositivi indossabili per le pubblicità mirate ed infine quello di garantire la possibilità di scelta agli utenti relativamente al trattamento e alla conservazione dei dati personali, ovviamente assicurando l'interoperabilità dei sistemi *Android* per permettere ai concorrenti di entrare nel mercato dei *wearable devices*[164]. Inoltre viene stabilito che un soggetto giuridico creato ad hoc veglierà sul rispetto degli impegni assunti. Nel consueto riassunto conclusivo di Margrethe Vestager viene spiegata la motivazione della decisione:

"We can approve the proposed acquisition of Fitbit by Google because the commitments will ensure that the market for wearables and the nascent digital health space will remain open and competitive. The commitments will determine how Google can use the data collected for ad purposes, how interoperability

[163] ibidem.

[164] Commissione europea, *Press Release: Commission clears acquisition of Fitbit by Google, subject to condition,* (17 dicembre 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 .

between competing wearables and Android will be safeguarded and how users can continue to share health and fitness data, if they choose to"[165].

L'operazione è stata approvata anche negli Stati Uniti, nonostante sia attualmente in corso un'indagine del *Department of Justice* per vagliare i rischi per i dati degli utenti. Diverse sono state tuttavia le critiche da parte della dottrina europea, che ha visto l'approvazione dell'acquisizione come un'opportunità sprecata per la Commissione, lamentando l'applicazione di criteri e metodologie tradizionali, non adeguati ai mercati digitali ed ai *big tech*[166]. Nei prossimi anni sarà possibile valutare appieno gli effetti di questa decisione sul regime concorrenziale e sulla protezione dei dati personali degli utenti.

9. (*Segue:*) Il recente caso dell'AGCM contro *Facebook* e l'approccio italiano alla questione

Dopo l'analisi dei casi europei che hanno segnato le tappe interpretative più importanti del rapporto tra *data protection* e *diritto antitrust* appare necessario considerare l'approccio nazionale italiano, partendo da un recente caso che ha visto protagonisti l'AGCM e *Facebook,* in cui il Consiglio di Stato ha fissato importanti principi sul tema dello sfruttamento dei dati da parte delle società tecnologiche. Nella vicenda, incanalata nell'alveo della *consumer protection law,* l'AGCM contesta a *Facebook* due pratiche commerciali scorrette, per violazione, in astratto, degli artt. 20, 21, 22, 24, 25 del Codice del Consumo (Dlgs. 206/2005): una pratica commerciale ingannevole, *ex* artt. 21 e 22 Cod. Consumo[167], poiché gli utenti, al momento dell'iscrizione al *social*

[165] Margrethe Vestager, *Press Release: Commission clears acquisition of Fitbit by Google, subject to condition,* (17 dicembre 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484

[166] Ad esempio, *Cfr.* Jay Modrall, *Google/Fitbit -The EU Commission misses a step,* Kluwer Competition Law Blog, (17 giugno 2021).

[167] Art. 21 Dlgs. 206/2005 (Codice del Consumo), *"Pratiche commerciali ingannevoli",* commi 1 e 2 *: È considerata ingannevole una pratica commerciale che contiene informazioni non rispondenti al vero o, seppure di fatto corretta, in qualsiasi modo, anche nella sua presentazione complessiva, induce o è idonea ad indurre in errore il consumatore medio riguardo ad uno o più dei seguenti elementi e, in ogni*

network, non sono adeguatamente informati della raccolta, a fini commerciali, dei loro

caso, lo induce o è idonea a indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso:

a) l'esistenza o la natura del prodotto;

b) le caratteristiche principali del prodotto, quali la sua disponibilità, i vantaggi, i rischi, l'esecuzione, la composizione, gli accessori, l'assistenza post-vendita al consumatore e il trattamento dei reclami, il metodo e la data di fabbricazione o della prestazione, la consegna, l'idoneità allo scopo, gli usi, la quantità, la descrizione, l'origine geografica o commerciale o i risultati che si possono attendere dal suo uso, o i risultati e le caratteristiche fondamentali di prove e controlli effettuati sul prodotto;

c) la portata degli impegni del professionista, i motivi della pratica commerciale e la natura del processo di vendita, qualsiasi dichiarazione o simbolo relativi alla sponsorizzazione o all'approvazione dirette o indirette del professionista o del prodotto;

d) il prezzo o il modo in cui questo è calcolato o l'esistenza di uno specifico vantaggio quanto al prezzo;

e) la necessità di una manutenzione, ricambio, sostituzione o riparazione;

f) la natura, le qualifiche e i diritti del professionista o del suo agente, quali l'identità, il patrimonio, le capacità, lo status, il riconoscimento, l'affiliazione o i collegamenti e i diritti di proprietà industriale, commerciale o intellettuale o i premi e i riconoscimenti;

g) i diritti del consumatore, incluso il diritto di sostituzione o di rimborso ai sensi dell'articolo 130 del presente Codice.

2. È altresì considerata ingannevole una pratica commerciale che, nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, induce o è idonea ad indurre il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso e comporti:

a) una qualsivoglia attività di commercializzazione del prodotto che ingenera confusione con i prodotti, i marchi, la denominazione sociale e altri segni distintivi di un concorrente, ivi compresa la pubblicità comparativa illecita;

b) il mancato rispetto da parte del professionista degli impegni contenuti nei codici di condotta che il medesimo si è impegnato a rispettare, ove si tratti di un impegno fermo e verificabile, e il professionista indichi in una pratica commerciale che è vincolato dal codice"

Art. 22 Dlgs. 206/2005 (Codice del Consumo), *"Omissioni ingannevoli",* commi 1 e 2*: " È considerata ingannevole una pratica commerciale che nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, nonché dei limiti del mezzo di comunicazione impiegato, omette informazioni rilevanti di cui il consumatore medio ha bisogno in tale contesto per prendere una decisione consapevole di natura commerciale e induce o è idonea ad indurre in tal modo il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso.*

2. Una pratica commerciale è altresì considerata un'omissione ingannevole quando un professionista occulta o presenta in modo oscuro, incomprensibile, ambiguo o intempestivo le informazioni rilevanti di cui al comma 1, tenendo conto degli aspetti di cui al detto comma, o non indica l'intento commerciale della pratica stessa qualora questi non risultino già evidente dal contesto nonché quando, nell'uno o nell'altro caso, ciò induce o è idoneo a indurre il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".

dati personali, vero prezzo del servizio, mentre viene presentata e rimarcata soltanto la sua gratuità; una pratica commerciale aggressiva, *ex* artt. 24 e 25 dello stesso codice[168], consistente nell'influenza illecita esercitata dalla piattaforma sugli *users,* costretti ad acconsentire alla massima raccolta e condivisione dei loro dati personali, verso i *social network* e i terzi, come opzione di *default* (impostata su un meccanismo di *opt-out)* non illustrata in modo trasparente, difficile da deselezionare e che, una volta fatto, limita notevolmente l'utilizzo della piattaforma[169]. Un punto rimarchevole della decisione dell'AGCM riguarda peraltro il tema della competenza. *Facebook* contestata che non spetti all'autorità conoscere la vicenda, asserendo sia compito dell'Autorità Garante della Privacy. L'AGCM si esprime sulla questione, affermando con lapidaria chiarezza che

> *"la prospettazione suggerita da Facebook al fine di ricondurre la fattispecie sanzionata nell'ambito delle esclusive attribuzioni del Garante Privacy non può però essere condivisa e ciò sulla base della normativa di riferimento che delinea il*

---

[168] Art. 24 Dlgs. 206/2005 (Codice del Consumo), *"Pratiche commerciali aggressive": "È considerata aggressiva una pratica commerciale che, nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, mediante molestie, coercizione, compreso il ricorso alla forza fisica o indebito condizionamento, limita o è idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio in relazione al prodotto e, pertanto, lo induce o è idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso."*

Art. 25 Dlgs. 206/2005 (Codice del Consumo), *"Ricorso a molestie, coercizione o indebito condizionamento": "Nel determinare se una pratica commerciale comporta, ai fini del presente capo, molestie, coercizione, compreso il ricorso alla forza fisica, o indebito condizionamento, sono presi in considerazione i seguenti elementi:*

a) i tempi, il luogo, la natura o la persistenza;

b) il ricorso alla minaccia fisica o verbale;

c) lo sfruttamento da parte del professionista di qualsivoglia evento tragico o circostanza specifica di gravità tale da alterare la capacita' di valutazione del consumatore, al fine di influenzarne la decisione relativa al prodotto;

d) qualsiasi ostacolo non contrattuale, oneroso o sproporzionato, imposto dal professionista qualora un consumatore intenda esercitare diritti contrattuali, compresi il diritto di risolvere un contratto o quello di cambiare prodotto o rivolgersi ad un altro professionista;

e) qualsiasi minaccia di promuovere un'azione legale ove tale azione sia manifestamente temeraria o infondata".

[169] AGCM, Provvedimento n. 27432, procedimento PS11112, (29 novembre 2018), 4-25.

perimetro delle rispettive competenze attribuite alle due Autorità indipendenti e dello specifico interesse che risulta essere violato per effetto della condotta sanzionata. Infatti, la circostanza che alle condotte della società sia applicabile la normativa sulla privacy, non la esonera dal rispettare le norme in materia di pratiche commerciali scorrette. Va, infatti, rilevato che la disciplina della privacy garantisce la protezione dei dati personali, definiti come informazioni relative ad una persona (fisica o giuridica), allo scopo di tutelare dette posizioni giuridiche che si qualificano, quali diritti fondamentali della persona umana, spettando al Garante per la Protezione dei Dati Personali la competenza ad applicare le sanzioni per la violazione degli obblighi ivi previsti. Diversamente, il Codice del Consumo, in materia di pratiche commerciali scorrette, ha l'obiettivo di tutelare il consumatore da scelte economiche indotte da pratiche ingannevoli e aggressive che non trovano regolazione in specifiche discipline. Ne consegue che le due discipline hanno un campo di applicazione materiale differente e perseguono interessi distinti. Di conseguenza non sussiste un conflitto tra le due discipline, integrandosi, piuttosto, le stesse in maniera complementare"[170].

Dunque per quanto le discipline abbiano scopi e oggetti diversi, queste perseguono la tutela di diritti non trascurabili delle persone, in quanto tali o come consumatori, perciò tra di loro non c'è conflitto, ma complementarietà[171]. In base all'art. 27, comma 12, del Cod. Consumo, l'autorità impone a *Facebook* due ammende di 5 milioni di euro e l'onere di rettificare le impostazioni e le informazioni mostrate dalla piattaforma. A seguito della decisione dell'AGCM, *Facebook* ha rettificato il *banner* della pagina d'ingresso ed iscrizione alla piattaforma.

[170] ibidem, para 44-46.

[171] ibidem, para 47.

Fonte: insidemagazine.it

La società ha ricorso al TAR del Lazio. Il Tribunale ha annullato il provvedimento dell'AGCM limitatamente alla seconda condotta, per erronea ricostruzione del meccanismo di funzionamento della piattaforma e mancanza di elementi sufficienti per provare la pratica aggressiva, confermando però la non gratuità del *social,* dove il corrispettivo sono i dati personali degli utenti[172].

Sul punto finale, vera parte rivoluzionaria della sentenza, il TAR avalla le conclusioni dell'autorità, illustrando come

> "la *condotta sanzionata presenta effettivamente tale carattere, in quanto il "claim" utilizzato da Facebook nella pagina di registrazione per invogliare gli utenti a iscriversi ("Iscriviti È gratis e lo sarà per sempre") lasciava intendere l'assenza di una controprestazione richiesta al consumatore in cambio della fruizione del servizio. In proposito, parte ricorrente non può essere seguita laddove sostiene che il richiamo al concetto di gratuità sarebbe giustificato dalla mancata richiesta del pagamento di una somma di denaro e che il consumatore medio attribuirebbe a tale termine, nella sua accezione comune, il significato di mera assenza di un corrispettivo patrimoniale. La pratica, infatti, è stata sanzionata in ragione della incompletezza delle informazioni fornite, che a fronte del "claim" di "gratuità" del*

[172] Cfr. TAR Lazio, sez. I, sentenza n. 260/2020 [2020].

servizio non consentivano al consumatore di comprendere che il professionista avrebbe poi utilizzato i dati dell'utente a fini remunerativi, perseguendo un intento commerciale. In argomento, il provvedimento ha fornito una puntuale motivazione, supportata da un'adeguata istruttoria, sulla carenza di sufficienti informazioni, nel processo di registrazione, circa il valore commerciale dei dati e allo scopo commerciale perseguito"[173].

Il Consiglio di Stato è infine intervenuto per risolvere in via definitiva la vicenda. Il giudice conferma la sentenza del TAR Lazio, respingendo dunque la pratica commerciale aggressiva delineata dall'AGCM nel suo provvedimento, ma confermando quella ingannevole[174]. Viene ulteriormente avallata la lettura data prima dall'autorità amministrativa e poi dal Tribunale, secondo cui non è possibile considerare il servizio offerto da *Facebook* come gratuito, perché i dati raccolti dalla piattaforma vengono sfruttati a fini commerciali, permettendo la profilazione dell'utente ed un *advertising* più mirato. Si legge infatti nella sentenza,

"nel caso di specie, come correttamente rilevato sia dall'Autorità, sia dal giudice di prime cure, il descritto obbligo di chiarezza non risulta rispettato, atteso che le informazioni rese all'utente al primo contatto, lungi dal contenere gli elementi essenziali per comprendere le condizioni e i limiti delle conseguenze che, a fronte della gratuità dei servizi offerti, deriveranno dalla profilazione in termini di indefinibilità dei soggetti che utilizzeranno i dati personali messi a disposizione e del tipo di utilizzo commerciale connesso, lasciano supporre che sia possibile ottenere immediatamente e facilmente, ma soprattutto "gratuitamente" (e per tutto il periodo in cui l'utente manterrà l'iscrizione in piattaforma), il vantaggio collegato dal ricevimento dei servizi tipici di un social network senza oneri economici, omettendo di comunicare che, invece, ciò avverrà (e si manterrà) solo se (e fino a quando) i dati saranno resi disponibili a soggetti commerciali non definibili anticipatamente ed operanti in settori anch'essi non pre-indicati per finalità di uso commerciale e di diffusione pubblicitaria. Tanto basta a integrare gli estremi della pratica ingannevole, in quanto nel contesto del messaggio iniziale

[173] ibidem, para 11.

[174] Cfr. Consiglio di Stato, Sez. VI, sentenza n. 2631, [2021].

non si dà adeguato risalto alle suindicate conseguenze. Tutto quanto sopra si è illustrato, in fatto ed in diritto, milita nel senso di escludere la fondatezza dei motivi di appello dedotti dalla società appellante con riferimento alla sezione del provvedimento sanzionatorio adottato dall'Autorità riferibile alla Pratica a)"[175].

Oltre a questa autorevole conferma del valore dei dati e delle informazioni raccolte dalle piattaforme digitali nella *data economy*, corrispettivo non monetario ma egualmente importante per i modelli di *business* delle società *tech* che offrono servizi digitali, viene, nella sentenza, anche ribadito come l'intersezione normativa tra vari campi del diritto, nel caso di specie la protezione dei dati personali ed il diritto alla tutela della concorrenza e dei consumatori, non possa portare a disapplicazioni o vuoti di tutela di una ai danni dell'altra, perché il legislatore europeo ha, da sempre, ammesso ed incentivato il crearsi di un sistema di protezione "multilivello", in cui le varie discipline si integrano e sostengono a vicenda. Perciò

"*le surriprodotte considerazioni, ad avviso del Collegio, vanno interpretate non nel senso della creazione di "compartimenti stagni di tutela" ma della esigenza di garantire "tutele multilivello" che possano amplificare il livello di garanzia dei diritti delle persone fisiche, anche quando un diritto personalissimo sia "sfruttato" a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore"*[176],

in una visione rinvenibile anche nel caso "*Facebook Germany",* seppur fondata su diverse argomentazioni. Questo caso permette di apprezzare il duplice approccio dell'AGCM, più flessibile rispetto agli altri modelli europei, col contrasto alle pratiche commerciali scorrette, nel campo della *consumer protection,* e agli abusi di posizione dominante, in ambito *antitrust*[177]. Tra le iniziative sul primo fronte rientra il procedimento PS10601 del 2017 nei confronti di *Whatsapp*[178]. Questo si riferisce alla condotta posta in essere da *Whatsapp* in occasione dell'aggiornamento del 25 agosto

[175] ibidem, para 11.

[176] ibidem, para 8.

[177] Cfr. Gustavo Olivieri, *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 365.

[178] AGCM, Provvedimento n. 27432, procedimento PS 10601, [2017].

2016, dove agli utenti veniva richiesto di accettare la modifica dei termini di servizio, tra le cui novità prevedeva il consenso alla raccolta e all'utilizzo dei dati personali da parte di *Facebook* per finalità commerciali[179]. Nella schermata iniziale dell'aggiornamento l'unica alternativa prevista oltre l'accettazione era la rinuncia all'utilizzo dell'applicazione quando in realtà, per gli utenti già iscritti, era possibile negare l'assenso in una successiva schermata, ottenibile solo dopo aver proceduto a leggere le nuove *policy.* Per questo motivo l'AGCM contesta l'aggressività della pratica[180], *ex* artt. 19 e ss., perché idonea ad esercitare un'influenza illecita sui consumatori[181]. Partendo dall'eccezione di incompetenza sollevata dalla società, l'autorità risponde con la stessa lucidità che l'ha caratterizzata nel già considerato procedimento contro *Facebook* del 2018, affermando che

> "*la circostanza che alla condotta della Parte sia applicabile il Codice della privacy, non la esonera dal rispettare le norme in materia di pratiche commerciali scorrette, che rimangono applicabili con riferimento alle specifiche condotte poste in essere dal Professionista, finalizzate all'acquisizione del consenso alla condivisione dei dati personali. In punto di fatto, rileva, inoltre, che il presente procedimento concerne una condotta specificatamente aggressiva consistente nell'aver indebitamente condizionato i consumatori ad accettare integralmente i nuovi Termini di utilizzo di WhatsApp Messenger, in particolare la condivisione dei dati con Facebook, facendo loro credere che sarebbe stato, altrimenti, impossibile proseguire nell'uso dell'applicazione. Tale comportamento non trova divieto e riscontro alcuno nel Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, bensì integra un'ipotesi di pratica commerciale scorretta, il cui accertamento, ai sensi del combinato disposto di cui agli artt. 19,*

---

[179] Tra cui, naturalmente, la profilazione degli utenti e l'utilizzo dei dati per il *marketing* e la pubblicità mirata.

[180] Intendendo "aggressive", a mente dell' art. 24 Dlgs. 206/2005 (Codice del Consumo), le pratiche commerciali che "*nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, mediante molestie, coercizione, compreso il ricorso alla forza fisica o indebito condizionamento, limita o e' idonea a limitare considerevolmente la liberta' di scelta o di comportamento del consumatore medio in relazione al prodotto e, pertanto, lo induce o e' idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".*

[181] Cfr. AGCM, Provvedimento n. 27432, procedimento PS 10601, [2017], 1-5

comma 3 e 27, comma 1-bis, del Codice del Consumo spetta, in via esclusiva, all'Autorità Garante della Concorrenza e del Mercato"[182].

Passando a considerare il merito della vicenda, dalle risultanze dell'indagine dell'AGCM traspare nuovamente il valore economico dei dati personali, confermato anche dalla Commissione europea in occasione della concentrazione *Facebook/Whatsapp.* Al termine dell'analisi, l'autorità conferma l'esistenza della pratica illecita di *Whatsapp,* idonea ad assicurare una raccolta eccessiva dei dati personali degli utenti ed il trasferimento alla società madre, *Facebook,* senza adeguatamente informare i consumatori sulle alternative a loro disposizione[183]. Stessi rimproveri vengono mossi ad altre società tecnologiche, come *Google, Apple* e *Dropbox,* in ulteriori procedimenti[184], per termini poco chiari e trasparenti che permettono alle piattaforme di ottenere il consenso alla raccolta ed allo sfruttamento eccessivo dei dati degli utenti[185]. Passando a considerare il secondo fronte di intervento dell'AGCM, relativo al contrasto delle condotte anticoncorrenziali e agli abusi di posizione dominante che interessano da vicino questioni di *privacy*, di rilievo sono molteplici provvedimenti recenti. Il primo, datato dicembre 2020, ha riguardato la società fornitrice di energia *ENEL s.p.a.,* per le prassi abusive volte all'ottenimento del consenso dei propri clienti al trattamento dei dati personali per finalità di *marketing,* in modo lesivo per i concorrenti[186]. In particolare, la condotte principali consistevano nel richiedere ai propri clienti il consenso per il trattamento dei dati personali per finalità di *marketing* in modo differente, mediante opzioni distinte, tra le imprese parte del proprio gruppo e quelle terze[187]. L'AGCM conclude asserendo la presenza di una fattispecie di abuso di posizione dominante, suscettibile di influenzare negativamente il gioco della concorrenza ed i concorrenti[188]. Anche in questa situazione l'autorità preferisce non entrare nel merito della valutazione delle condotte dal punto di vista di normative differenti, come quella a protezione della *privacy,* statuendo che

---

[182] ibidem, para 50-52.

[183] ibidem, para 57-60.

[184] AGCM, Provvedimenti PS 11147-11149-11150, [2020].

[185] Cfr. Gustavo Olivieri (n. 169), 367.

[186] Cfr. AGCM, Provvedimento 27494, [2018], para 11-13.

[187] ibidem, para 85.

[188] ibidem, para 239.

"*va altresì considerato che il carattere abusivo di un comportamento alla luce dell'articolo 102 TFUE non ha relazione con la sua conformità ad altre normative, giacché gli abusi di posizione dominante consistono, per lo più, proprio in comportamenti leciti alla luce di altri settori dell'ordinamento, diversi dal diritto alla concorrenza. Non si tratta dunque di valutare la legittimità di atti alla luce dei vari settori dell'ordinamento investiti, ma di considerare quelle condotte, pur settorialmente lecite, alla luce della loro portata anticoncorrenziale. Prospettiva in relazione alla quale certi atti, anche se legittimi dal punto di vista settoriale, si colorano come elementi indicatori di uno sproporzionato intento o effetto anticoncorrenziale"*[189].

Alle stesse conclusioni giunge nel provvedimento contro l'ulteriore fornitrice di energia *Acea s.p.a.,* sempre nel dicembre 2018 e per la stessa categorie di condotte[190]. Un caso ancor più recente, dell'ottobre 2020, ha interessato *Google*, per un sospetto abuso di posizione dominante nei vari mercati in cui si articola la filiera del *display advertising*[191]. Dopo aver approfonditamente analizzato le caratteristiche di tutti i segmenti del mercato, valutando l'importanza della maggior quantità di dati in possesso delle aziende per potenziare la profilazione degli utenti e migliorare l'effetto della pubblicità mirata, l'autorità consta la posizione dominante di *Google* in ognuno di essi, grazie alla vasta gamma di servizi offerti dalla società[192]. Seguendo il consueto approccio "rispettoso" ed agnostico nei confronti degli altri campi del diritto, l'AGCM si limita a decidere la vicenda attraverso gli strumenti propri del diritto *antitrust,* notando come

---

189 ibidem, para 246.

190 Cfr. AGCM, Provvedimento 27496, [2018].

191 Cfr. AGCM, Provvedimento 28398, [2020]. Secondo la definizione data dalla stessa autorità al paragrafo 3 del provvedimento, *"per display advertising si intende, in generale, la messa a disposizione degli inserzionisti, da parte dei gestori e/o proprietari di siti web (di seguito, anche editori o publisher), di spazi on-line per il collocamento e l'esposizione di formati e creatività in modalità fissa o mobile, quali ad esempio banner pubblicitari o animazioni che precedono, intervallano o terminano un contenuto video".*

192 ibidem, para 1-71.

"*i predetti servizi, offerti da Google sui mercati nei quali detiene una posizione dominante, consentono di disporre di un insieme di dati di alta qualità circa le caratteristiche dei soggetti che visualizzano spazi pubblicitari (che non si limitano esclusivamente a età, sesso, localizzazione geografica, ma riguardano anche i dispositivi utilizzati, le attività web, le attività con il cellulare, la frequenza di utilizzo dei dispositivi, ecc.) e consentono di ottenere dalla loro combinazione una profilazione puntuale delle attività svolte su Internet dai target dei destinatari, a prescindere dalla circostanza che tale attività riguardi direttamente un servizio Google*"[193].

Grazie allo sfruttamento abusivo di questo vantaggio competitivo,

"*i concorrenti altrettanto efficienti rispetto a Google non sono in grado di fornire servizi di intermediazione della pubblicità online con le medesime capacità di targhettizzazione e di identificazione. Ciò in ragione della combinazione che Google attua tra dati che sono acquisiti in ambiti del tutto estranei alle attività di fornitura di contenuti sul web e di compravendita pubblicitaria, associata alla contestuale condotta discriminatoria che impedisce ai concorrenti di competere sulla base dei loro meriti*"[194].

L'autorità così conclude che

"*pertanto, le condotte in esame consistono nella discriminazione interna ed esterna e, in particolare, nella combinazione di dati acquisiti con servizi in cui Google è in posizione dominante (quali, ad esempio, Android/Google Play, il connesso Google ID, Maps e Chrome) e nel contestuale rifiuto di fornire ai concorrenti attivi nel display advertising l'ID decriptato e di consentire l'utilizzo dei pixel. La combinazione di dati, raccolti per fini diversi rispetto a quelli per cui sono utilizzati da Google nelle predette applicazioni, sembra avere l'effetto di favorire le SSP e DSP di Google. Tali dati, per espresso rifiuto di Google, non possono essere disponibili alle medesime condizioni agli operatori SSP e DSP concorrenti. Anche*

[193] ibidem, para 81.

[194] ibidem, para 85.

alla luce degli orientamenti della Commissione in tema di abuso di posizione dominante di tipo escludente, si rileva che le condotte in esame sono idonee ad ostacolare lo svolgimento di una concorrenza effettiva nel display advertising e negli altri mercati interessati, con preclusione dei concorrenti e con conseguenti effetti negativi per il benessere dei consumatori. In particolare, da un lato, l'assenza di concorrenza tra SSP potrebbe alterare i flussi economici verso i soggetti che offrono spazi pubblicitari, come ad esempio gli editori, con conseguente peggioramento della qualità dei contenuti offerti ai consumatori finali. D'altro lato, le condotte in esame, riducendo la concorrenza in tutta la filiera pubblicitaria del display advertising, potrebbe ridurre gli incentivi allo sviluppo tecnologico dei messaggi pubblicitari (come ad esempio, tecnologie meno invasive per i consumatori) influendo negativamente sull'esperienza di fruizione dei messaggi pubblicitari da parte degli utenti"[195].

Tenendo inoltre conto della rilevanza economica del fenomeno l'AGCM esorta anche l'intervento della Commissione europea, per i possibili effetti anticoncorrenziali che le suesposte condotte possono avere sul commercio tra Stati[196]. Si tratta, dunque, di un approccio basato su basi giuridiche differenti rispetto a quello del *Bundeskartellamt,* molto più vicino invece alla strategia della Commissione nella già vista casistica recente che ha interessato *Google*[197]. A seguito delle modifiche del GWB tedesco, volte ad affrontare con maggior efficacia i *big tech,* anche l'AGCM ha mostrato l'intenzione di muoversi nella medesima direzione. Con la Segnalazione S4143 del 21 marzo 2021 al Presidente del Consiglio dei Ministri italiano[198], contenente le proposte di riforma della legge sulla concorrenza, l'autorità, dopo aver ribadito l'importanza della concorrenza e dell'intervento *antitrust* nei mercati digitali[199], suggerisce l'introduzione di nuove disposizioni ispirate al modello tedesco[200]. Queste permetterebbero un ruolo più centrale dell'autorità nazionale nel contrasto delle condotte distorsive della concorrenza che,

---

[195] ibidem, para 86-87.

[196] ibidem, para 86-87.

[197] Cfr. Gustavo Olivieri (n. 168), 369-370.

[198] Cfr. AGCM, Segnalazione S4143 in merito a Proposte di riforma concorrenziale ai fini della legge annuale per il mercato e la concorrenza inviata al Presidente del Consiglio dei Ministri, [2021].

[199] ibidem, 1-10.

[200] ibidem, 90-104.

come si è visto, ancora sono difficili da inquadrare[201]. La medesima tendenza, nonostante gli approcci leggermente diversi, è dunque ormai chiara sia a livello nazionale che europeo, dove con le nuove proposte del *Digital Service Act* e del *Digital Markets Act* si punta ad innovare l'ecosistema giuridico e normativo.

10. Considerazioni conclusive e di riepilogo del capitolo II: Il *privacy paradox* e l'attuale relazione tra *data protection* e *antitrust*

Il tema considerato nelle varie fasi del caso "*Facebook Germany",* posto anche alla base delle diverse argomentazioni, è stato il cd. *privacy paradox,* il paradosso generato dalla discrepanza tra i propositi degli utenti, interessati alla massima protezione possibile della loro *privacy* e dei loro dati, ed il loro comportamento totalmente contraddittorio alla preoccupazione dichiarata[202]. Come già osservato, il *Bundeskartellamt* ha citato questo paradosso per argomentare l'inadeguatezza del consenso prestato dagli utenti a *Facebook,* al momento dell'iscrizione, come base giuridica per permettere il trattamento dei dati *ex* art. 7 GDPR. Questo per la mancanza delle caratteristiche essenziali che la normativa richiede per considerarlo libero, informato, specifico ed inequivocabile, complice la poca chiarezza dei termini contrattuali e della *data policy* della piattaforma. La Corte regionale superiore di Düsseldorf, al contrario, ha intravisto nelle precedenti affermazioni una fallacia argomentativa, poiché l'unica cosa che l'ipotetico paradosso può mostrare è come, in realtà, siano gli utenti a non interessarsi in concreto al trattamento dei loro dati, di certo non un abuso di posizione dominante da parte di *Facebook.* Il *Bundesgerichtshof* è infine intervenuto per affermare l'illiceità della condotta, attraverso i suoi termini e condizioni che privano gli utenti della loro libertà di autodeterminarsi, violando i diritti fondamentali riconosciutigli dalla costituzione tedesca in quanto persone, utilizzando una diversa linea argomentativa che però non ha schiarito i dubbi sul *privacy paradox.* Anche questa tematica è molto dibattuta dalla dottrina, perché in base alla ricostruzione che se ne da muta lo *standard* di protezione che il diritto deve garantire alle persone, insieme alle condotte pretendibili dalle società

[201] ibidem.

[202] Susanne Barth, Menno D.T. de Jong (n. 84).

che offrono servizi digitali. Molti studi[203] sono stati condotti e tra coloro che si oppongono al *paradox* troviamo il prof. Daniel J. Solove, che nella sua analisi sostiene si tratti di un "*mito originato da una logica fallace"*[204], perché non è possibile misurare correttamente, in via empirica, il valore attribuito dagli utenti alla loro *privacy,* in particolare associandola ad uno monetario, poiché questo è soggettivo e influenzato da diversi fattori non quantificabili. Lo stesso argomenta che fenomeni come questi sono irrimediabilmente affetti da *bias* cognitivi e dunque non attendibili, ad esempio lo "sconto iperbolico" teorizzato da Tversky e Kahneman, che porta le persone a preferire benefici immediati a discapito di quelli di lungo periodo. Il problema principale per lo studioso è l'eccessiva libertà di forme lasciata alle persone nella gestione della loro *privacy,* quando invece la soluzione dovrebbe essere una disciplina più rigorosa[205]. Sul lato opposto, i sostenitori dell'esistenza effettiva del *privacy paradox* concordano sulla necessità di una maggior tutela e sulla presenza di *bias* e fallacie cognitive che affliggono continuamente le persone, tra cui appunto questo paradosso, ma, andando più a fondo, si riconosce che spesso gli utenti vengono influenzati inconsapevolmente dalle piattaforme digitali che utilizzano. Uno strumento che viene ampiamente sfruttato, al limite tra persuasione e manipolazione, sono i cd. "*dark patterns",* interfacce utenti con *layout* strutturati appositamente per sfruttare i *bias* cognitivi delle persone, portandole a compiere azioni non volute realmente, ma desiderate dai titolari dei servizi[206]. Questi meccanismi nascosti, di vario tipo ed intensità, sono facilmente rinvenibili nella maggior parte dei servizi digitali, come ad esempio con impostazioni preimpostate sulla massima raccolta dei dati degli utenti o la scrittura in termini molto piccoli, spesso posta negli angoli estremi dell'interfaccia utente, in modo da evidenziare solo le opzioni vantaggiose per la piattaforma[207]. Essendo metodologie poste su una sottilissima zona

---

[203] Come, ad esempio, Martin, Kirsten, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms* Business Ethics Quarterly, 1-32. (24 novembre 2019); oppure, Alyson Leigh Young, Anabel Quan-Haase, *Privacy protection strategies on facebook*, Information, Communication & Society, 16:4, (2013), 479-500.

[204] Daniel J. Solove, *The Myth of the Privacy Paradox* , 89 George Washington Law Review 1 (2021), GWU Legal Studies Research Paper No. 2020-10, (29 gennaio 2021), 1-5.

[205] ibidem, 49-51.

[206] Jamie Luguri, Lior Strahilevitz, *Shining a Light on Dark Patterns* , 13 Journal of Legal Analysis 43 , University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, (29 marzo 2021), 1-2.

[207] ibidem, 58-61.

grigia tra il lecito e l'abuso, non è affatto facile per le autorità farvi fronte. Inoltre è sempre più diffusa la ricostruzione interpretativa che vede la *privacy* e i dati personali come un prezzo non monetario pagato dagli utenti per utilizzare i servizi digitali, come affermato anche dal Consiglio di Stato nel caso precedentemente trattato. Sicuramente la questione, ancora irrisolta, negli anni a seguire verrà affrontata dalle autorità e dalle corti, con l'aumentare della consapevolezza sul funzionamento dei mercati digitali e degli effetti di questi sulla *privacy* degli utenti. Tirando, dunque, le somme sull'attuale rapporto tra *data protection* e diritto *antitrust,* si è partiti dall'approccio agnostico e separatista di corti ed istituzioni dei primi anni Duemila, con il caso *Asnef-Equifax.* Le due branche del diritto venivano viste come comparti a tenuta stagna, ognuno con le proprie regole ed il proprio campo di applicazione, perciò possibili intersezioni dovevano essere risolte disapplicando l'altra normativa. Naturalmente questa visione, confermata anche in *Google/DoubleClick,* scontava la ancora poca comprensione degli emergenti mercati digitali e dei loro limitati effetti sulle persone e i loro diritti. Col passare degli anni ed il *boom* di *social network* e servizi digitali del *web 2.0*, il fenomeno comincia ad assumere una magnitudine totalmente diversa, ma l'approccio adottato rimane ancorato ancora agli stessi criteri tradizionali. Nella decisione della Commissione Europea sulla fusione *Facebook/Whatsapp* si perviene così ad una riconferma dei principi affermati nel caso *Asnef-Equifax.* Ben presto, però, diventa chiaro che ci sono fenomeni che l'interpretazione tradizionale non è in grado di risolvere, e questa inversione di tendenza la si osserva chiaramente nella decisione sulla concentrazione *Microsoft/LinkedIn.* Il caso *Facebook Germany* si inserisce in questo filone, utilizzando per la prima volta la *data protection* come criterio rilevante dell'analisi *antitrust.* La comprensione dell'importanza dei dati personali degli utenti per le piattaforme e le società operanti sul mercato *digitale,* insieme alla consapevolezza di cosa può accadere in caso di abusi, come ha mostrato *Cambridge Analytica* ed anche la *Brexit,* sta permettendo di superare l'approccio separatista originario, in direzione di una più forte sinergia tra la normativa a tutela dei dati personali e quella concorrenziale. Attualmente si è soltanto all'inizio del cambiamento, che diverrà sempre più necessario con l'evolversi della *data economy,* lo *switch* verso il *web 3.0*, la comparsa dei metaversi e la digitalizzazione di interi settori produttivi, fenomeni in cui la *data protection* ed il diritto *antitrust* si intrecciano sempre di più e giocano un ruolo fondamentale. Soltanto in questo modo sarà possibile realizzare il sistema di tutela multilivello auspicato a livello europeo, con al centro i diritti della persona, e

certamente col passare del tempo, ed il suo concretizzarsi, i principi che adesso, quasi timidamente, iniziano ad affermarsi sul panorama giuridico, diverranno fondamentali.

CAPITOLO III

NORMATIVA VIGENTE, NUOVI STRUMENTI REGOLATORI E PREVISIONI SUL FUTURO

"If it is true that the economics of platform markets may encourage anti- competitive market structures, there are at least two approaches we can take. Key is deciding whether we want to govern online platform markets through competition, or want to accept that they are inherently monopolistic or oligop- olistic and regulate them instead "- Lina M. Khan, Presidente Federal Trade Commission[208].

1. Intersezioni tra i due campi del diritto

Lo sviluppo dell'economia digitale, con i rapidi mutamenti e le particolarità che la caratterizzano, ha portato le autorità a confrontarsi continuamente con fenomeni inediti. Nuove fattispecie di difficile inquadramento, in astratto di interesse per diversi settori del diritto, hanno aumentato l'incertezza e la necessità di rinnovare gli strumenti giuridici tradizionali, difficilmente applicabili in questo contesto. Si è considerato il dibattito e l'evoluzione interpretativa, ancora in corso, sulle relazioni tra *data protection* e diritto *antitrust.* Molte sono le situazioni *borderline* e non sempre si è certi della rispettiva competenza nel caso concreto, dove ci sono fattori rilevanti per entrambe le normative[209]. I principali elementi di questa intersezione, evidenziati dalla recente casistica europea sul tema, ruotano intorno alla centralità dei dati personali, soprattutto in grandi quantità, per i *business model* delle società digitali. Questi, definiti dal Commissario europeo per la concorrenza Margrethe Vestager come "*la nuova valuta di Internet"*[210]*,* possono influenzare fortemente la concorrenza tra imprese, interessate ad ottenerne quantità sempre maggiori per migliorare il *decision making* ed il vantaggio sui

[208] Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L. J. (2017), 769.

[209] *Cfr.* Ariel Ezrachi, *BEUC Discussion Paper on "The Goals of EU Competition Law and the Digital Economy",* (Agosto 2018), 6-19.

[210] James Kanter, *Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies*, New York Times, (3 ottobre 2014).

concorrenti. La *privacy* è sempre più riconosciuta come un fattore non monetario importante nell'analisi concorrenziale, in particolare nel settore delle piattaforme digitali che operano in mercati a più versanti, dove l'apparente gratuità su di un versante rende complessa l'applicazione di metodologie ampiamente utilizzate, come il cd. *test del monopolista ipotetico* (misurato attraverso l'impiego del cosiddetto *SSNIP test,* da *Small but Significant and Non-transitory Increase of Price),* adoperato per individuare e misurare, all'interno del mercato rilevante, il potere di mercato di un'azienda[211]. Il possesso di importanti moli di dati può generare barriere all'ingresso del mercato e rafforzare la posizione dell'impresa in esso, sfociando in una situazione in cui "*the winner takes all*", molto comune nei mercati digitali e che premia il cosiddetto *first mover*. In queste condizioni sono molto più probabili condotte abusive ai danni dei consumatori che forniscono i dati, considerando che per il momento servizi alternativi con un livello di tutela della *privacy* maggiore sono ancora una nicchia poco diffusa[212]. La necessità è dunque quella di una maggiore collaborazione tra autorità garanti, in modo da individuare gli effetti a cui le sopra citate condotte possono portare, a danno dei consumatori finali, e sviluppare metodi congiunti per una risposta più soddisfacente[213]. Nonostante queste sinergie, i campi della *data protection* e del diritto *antitrust* conservano le proprie insostituibili caratteristiche e peculiarità, perciò in quest'ottica è necessario analizzare le rispettive normative europee per comprendere appieno similitudini, differenze e punti d'incontro messi in risalto dall'economia digitale.

---

[211] Allen P. Grunes, Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big data*, University of Tennessee Legal Studies Research Paper No. 269, (28 aprile 2015), 1-7.

[212] ibidem, 8-10. Ma ancora, UK Competition & Market Authority, *The commercial use of consumer data,* (giugno 2015), 85-90. Alternative come il *browser Brave* o il motore di ricerca *duckduckgo* sono in continua crescita, ma molto distanti dai numeri delle concorrenti più affermate come Google (per approfondire il caso di *duckduckgo* https://duckduckgo.com/traffic).

[213]ibidem, 14-15.

2. Disciplina europea a tutela dei dati personali

L'evoluzione sociale e normativa che ha portato all'adozione del GDPR e delle attuali regole sulla *data protection* è stata lunga e complessa. Tornando indietro fino al 1890, in America, con il celeberrimo articolo "*The right to privacy"* dei giuristi Samuel D. Warren e Louis D. Brandeis, pubblicato sull' *Harvard Law Review*, viene per la prima volta delineato il diritto alla *privacy,* riflesso del diritto alla vita costituzionalmente garantito. Viene notato

> "*that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection"*[214].

In particolare, il diritto a vedere tutelate la propria vita personale e la proprietà privata in principio proteggeva quasi unicamente da violazioni fisiche. Col tempo è nata così l'esigenza di una maggiore protezione contro la lesione delle opere immateriali. Dopo un'analisi dello stato dell'arte degli strumenti giuridici dell'epoca per soddisfare le richieste di tutela ed i casi in cui venivano a soccombere di fronte a diritti con più peso nel caso concreto, è interessante osservare, nell'affermazione della necessità di un continuo aggiornamento delle metodologie giuridiche per stare al passo coi tempi, come le conclusioni a cui giungono i due studiosi siano una rilettura in chiave moderna dei principi stabiliti già nella *Magna Carta Libertatum* (1225) e nell' *Habeas Corpus Act* (1679). Il diritto che emerge da questa disamina è quello di "essere lasciati soli", giustificato dalla grande diffusione della stampa dell'epoca e dalla conseguente maggior facilità con cui le notizie potevano circolare. Questi fenomeni generavano una maggiore probabilità di episodi in cui la riservatezza dei cittadini poteva essere lesa[215]. L'importanza di questo diritto è esplosa negli anni Trenta del XX secolo, dove i regimi totalitari hanno tentato di controllare totalmente la vita dei cittadini, annichilendo la loro sfera personale di fronte alla supremazia dello stato. Il caso emblematico è quello della Germania nazista, in cui la polizia e gli ufficiali del regime schedarono ogni singolo

[214] Samuel D. Warren, Louis D. Brandeis, *The Right of Privacy*, Harvard Law Review, Vol. 4, No. 5. (15 dicembre 1890), 193-220, accessibile al *link:* https://www.cs.cornell.edu/~shmat/courses/cs5436/warrenbrandeis.pdf .

[215] ibidem.

cittadino, casa per casa, giustificandosi di agire per l'interesse superiore della sicurezza nazionale[216]. Fu così che riuscirono a portare a compimento, in un termine relativamente breve, la loro opera di emarginazione nei confronti degli ebrei residenti in Germania. Allo stesso modo, dopo la seconda guerra mondiale, la polizia segreta Stasi nella Germania dell'Est teneva monitorato il comportamento di ogni persona alla ricerca di possibili sovversivi. Non è un caso perciò che nello stato di Hesse, Germania ovest, fu approvata nel 1970 la prima legge di *data protection* al mondo, delineando per la prima volta i principi fondamentali ripresi anche nelle normative successive, come la necessità di una base giuridica per il trattamento[217]. La legge aveva però un campo di applicazione limitato, non esteso all'intera nazione. L'importanza della protezione dei dati personali era ormai diventata un punto fondamentale per gli stati europei, sempre in relazione a ciò che accadde nei regimi dittatoriali dei decenni prima, perciò a partire dal 1973, con la legge svedese sulla *data protection* valida su tutto il territorio nazionale, i vari paesi europei hanno approvato le rispettive leggi a tutela dei dati. Mancava ancora una comune linea d'azione nell'attività legislativa dei diversi stati, un enorme limite per la reale tutela dei diritti dei cittadini. Così, per armonizzare le differenti discipline nazionali, nel 1990 fu approvata la già citata Direttiva 95/46/CE. La motivazione fu anche economica, poiché le diverse regole nazionali limitavano la libera circolazione dei dati personali nel mercato unico europeo. *Internet* era ancora agli albori e nel giro di pochi anni si è reso necessario un aggiornamento della normativa per far fronte ai rischi posti dall'evoluzione dei servizi digitali. Nella società dell'informazione l'originario "*right to privacy"*, il diritto di essere lasciati soli teorizzato a fine Ottocento da Warren e Brandeis, non è più abbastanza, data la notevole quantità di informazioni raccolta dai sistemi informatici. Il diritto alla *privacy* ottiene così una nuova declinazione, il diritto alla protezione dei dati personali, proiezione digitale delle persone in rete. Nella

---

[216] Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History,* Time (24 maggio 2018), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ .

[217] Olga Stepanova and Patricia Jechel,*The Privacy, Data Protection and Cybersecurity Law Review: Germany,* The Law Reviews (5 novembre 2021), https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany.

direzione di questo cambiamento si è mossa anche la Direttiva *e-privacy* 2002/58/CE[218], volta a proteggere i dati personali e la riservatezza delle persone nell'ambito delle comunicazioni elettroniche, dettando le regole per i cd. *cookies*. Come infatti risulta dal considerando n. 5,

> "*nelle reti pubbliche di comunicazione della Comunità è in atto l'introduzione di nuove tecnologie digitali avanzate che pongono esigenze specifiche con riguardo alla tutela dei dati personali e della vita privata degli utenti. Lo sviluppo della società dell'informazione è caratterizzato dall'introduzione di nuovi servizi di comunicazione elettronica. L'accesso alle reti digitali mobili è ormai a disposizione e alla portata di un vasto pubblico. Queste reti digitali hanno grandi capacità e possibilità di trattare i dati personali. Il positivo sviluppo transfrontaliero di questi servizi dipende in parte dalla fiducia che essi riscuoteranno presso gli utenti in relazione alla loro capacità di tutelare la loro vita privata"*[219].

Dopo l'attentato dell'11 settembre 2001 è diventato centrale bilanciare i bisogni di sicurezza nazionale con la riservatezza dei dati personali. La necessità di una riforma organica per rendere la normativa aggiornata, uniforme e capace di far fronte allo sviluppo di *Internet,* ha portato all'adozione del Regolamento generale sulla protezione dati personali 679/2016, punto di svolta per il settore della *data protection*[220]. Prima di analizzarne le previsioni, bisogna far cenno agli strumenti di diritto internazionale che costituiscono lo sfondo del panorama giuridico in cui si muovono le regole nazionali ed europee. Nel 1948 fu adottata, in seno all'ONU, la Dichiarazione universale dei diritti umani (UDHR)[221], che all'art. 12 sancisce il diritto alla vita privata, confermato anche

---

[218] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), [2002], OJ L 201, 31.7.2002, p. 37–47.

[219] ibidem.

[220] Cfr. Thomas Streinz, Paul Craig, Gráinne de Búrca, *The Evolution of EU Law* , OUP (3rd edn 2021), 902-936.

[221] Assemblea Generale delle Nazioni Unite, *Dichiarazione Universale dei Diritti Umani*, Risoluzione 219077A, (dicembre 1948). L'art. 12 stabilisce: "*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a*

dalla Convenzione internazionale sui diritti civili e politici (ICCPR) all'art. 17[222]. Il diritto alla vita privata ha una portata leggermente differente rispetto al diritto alla protezione dei dati personali. Entrambi mirano a tutelare valori fondamentali, quali la libertà e la dignità umana, fondamentali per lo sviluppo della personalità e della vita privata delle persone, ma mentre il primo rappresenta un divieto generale di interferenza da parte dello stato, sacrificabile in casi di interessi predominanti, il secondo costituisce un diritto "nuovo", moderno, che instaura un sistema di regole e misure per tutelare i dati ogni volta che vengono trattati[223]. Guardando al vecchio continente, nel quadro del Consiglio d'Europa, la Convenzione europea dei diritti dell'uomo (CEDU), adottata nel 1950, stabilisce all'art. 8 il diritto al rispetto della vita privata e familiare, nel cui ambito l'interpretazione della Corte Europea dei Diritti dell'Uomo, organo chiamato a valutare l'adempimento delle previsioni della convenzione da parte degli stati aderenti, ha incluso anche il diritto alla protezione dei dati personali[224]. Un importante caso sulla *data protection* dinanzi alla Corte, è sicuramente *Barbulescu v Romania* (2017), dove si è potuta apprezzare l'applicazione dell'art. 8 e la sua interpretazione[225]. Sempre nell'ambito del Consiglio d'Europa è rinvenibile la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108 del 1981, attualmente unico strumento giuridico di diritto

---

lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni."

[222] Assemblea Generale delle Nazioni Unite, *Convenzione internazionale sui diritti civili e politici,* Risoluzione 2200A (XXI), (dicembre 1966). L'art. 17 stabilisce "*Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese".*

[223] Per un approfondimento: Giorgio Pino, *Il costituzionalismo dei diritti*, Il Mulino, (2017).

[224] Consiglio d'Europa, *Convenzione europea dei diritti dell'uomo,* STCE n. 5, 1950. L'art. 8 prevede: "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".*

[225] *Bărbulescu v. Romania*, n. 61496/08, (2017).

internazionale vincolante in materia di *data protection* [226]. Questo trattato copre il trattamento di dati personali compiuti sia da privati che da organismi pubblici, regolando anche i trasferimenti transfrontalieri, libera tra gli aderenti alla convenzioni ma con restrizione verso paesi terzi, ed il divieto di trattamento di dati sensibili senza opportune garanzie. Sono fissati molti dei principi, come quelli di liceità, correttezza e proporzionalità, e dei diritti contenuti anche nel GDPR. La Corte Europea dei Diritti dell'Uomo non ha competenza per le questioni riguardanti il rispetto della convenzione, anche se in diverse pronunce ha utilizzato questa nelle sue argomentazioni. La Convenzione è stata completata da raccomandazioni del Comitato dei Ministri del Consiglio d'Europa, che si sono susseguite negli anni, e nel 2011 la stessa è stata "modernizzata" e rivista, con l'obiettivo di rafforzarne la tutela e l'effettività[227].

3. (*Segue:)* Il Regolamento generale sulla protezione dati personali 679/2016 (GDPR).

In principio i trattati fondanti delle Comunità europee non prevedevano regole sulla protezione dei dati personali e dei diritti umani in generale, data la natura principalmente economica delle istituzioni. L'obiettivo principale era la creazione di un mercato unico senza frontiere doganali, in cui le merci, le persone, i servizi ed i capitali potessero circolare liberamente, creando benessere e ricchezza. Essendo l'Unione europea un'istituzione sovranazionale originata dalla volontaria e parziale cessione di sovranità da parte degli Stati membri, che hanno acconsentito alla propria autolimitazione per rendere effettivo e autonomo il suo ruolo, fondamentale è il cd. principio di attribuzione previsto all'art. 3 del Trattato sull'Unione europea (TUE)[228]. In

[226] Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STCE n. 108, [1981].

[227] Varie istituzioni europee (n.3) , 20-30.

[228] Trattato sull'Unione europea, versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 15–368. All'art. 3 prevede: "*L'Unione si prefigge di promuovere la pace, i suoi valori e il benessere dei suoi popoli. L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima. L'Unione instaura un mercato interno. Si adopera per lo sviluppo sostenibile dell'Europa,*

forza di questo principio "*l'Unione persegue i suoi obiettivi con i mezzi appropriati, in ragione delle competenze che le sono attribuite nei trattati"*[229], non potendo prescindere da queste poiché ciò prevaricherebbe il potere attribuitogli dagli stati[230]. I trattati istitutivi non contemplavano espressamente la presenza di diritti fondamentali riconosciuti agli individui ma la CGUE, negli anni, con la sua interpretazione ha permesso la loro tutela grazie al riconoscimento di questi come parte dei principi

---

basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico. L'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociali, la parità tra donne e uomini, la solidarietà tra le generazioni e la tutela dei diritti del minore. Essa promuove la coesione economica, sociale e territoriale, e la solidarietà tra gli Stati membri. Essa rispetta la ricchezza della sua diversità culturale e linguistica e vigila sulla salvaguardia e sullo sviluppo del patrimonio culturale europeo. L'Unione istituisce un'unione economica e monetaria la cui moneta è l'euro. Nelle relazioni con il resto del mondo l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione dei suoi cittadini. Contribuisce alla pace, alla sicurezza, allo sviluppo sostenibile della Terra, alla solidarietà e al rispetto reciproco tra i popoli, al commercio libero ed equo, all'eliminazione della povertà e alla tutela dei diritti umani, in particolare dei diritti del minore, e alla rigorosa osservanza e allo sviluppo del diritto internazionale, in particolare al rispetto dei principi della Carta delle Nazioni Unite. L'Unione persegue i suoi obiettivi con i mezzi appropriati, in ragione delle competenze che le sono attribuite nei trattati".

[229] Trattato sull'Unione europea, versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 15–368. art. 3, comma 6.

[230] Le competenze dell'UE si dividono in esclusive (art. 3 TFUE) , concorrenti (art. 4 TFUE) e di sostegno (art. 6 TFUE) . Nelle prime solamente l'Unione può legiferare, mentre gli stati devono limitarsi a dare esecuzioni agli atti ("*unione doganale; definizione delle regole di concorrenza necessarie al funzionamento del mercato interno; politica monetaria per gli Stati membri la cui moneta è l'euro; conservazione delle risorse biologiche del mare nel quadro della politica comune della pesca; politica commerciale comune*"). Nelle concorrenti sia l'UE che gli stati possono adottare atti vincolanti, ma quest'ultimi solo se l'UE non ha ancora agito o ha rinunciato a farlo ("*mercato interno; politica sociale,coesione economica; sociale e territoriale; agricoltura e pesca, tranne la conservazione delle risorse biologiche del mare; ambiente; protezione dei consumatori; trasporti; reti transeuropee; energia; spazio di libertà, sicurezza e giustizia; problemi comuni di sicurezza in materia di sanità pubblica, per quanto riguarda gli aspetti definiti nel presente trattato").* Nelle competenze di sostegno l'UE può solo sostenere e coordinare le misure adottate dagli stati membri (*"tutela e miglioramento della salute umana; industria; cultura; turismo; istruzione, formazione professionale, gioventù e sport;) protezione civile; cooperazione amministrativa"*). Trattato sull'Unione europea, versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 15–368.

generali di diritto europeo. Nel 2000 l'UE ha dato concretezza a questi diritti, estrapolati dalle costituzioni degli stati membri e dai rispettivi obblighi internazionali, nella Carta dei diritti fondamentali dell'Unione Europea (CDFUE)[231], documento in principio solo politico ma che ha assunto valore vincolante, di diritto primario, col trattato di Lisbona del 2007 (entrato in vigore nel dicembre 2009). Nella Carta non soltanto viene garantito il diritto al rispetto della vita privata all'art. 7, ma è previsto espressamente il diritto alla protezione dei dati personali nell'art. 8[232]. Oltre ad essere un enorme passo in avanti, testimonianza dell'evoluzione sociale e tecnologica e della rilevanza che i dati personali hanno assunto negli ultimi decenni, dopo aver enunciato il diritto alla protezione dei dati personali riconosciuto ad ogni persona, l'art. 8 stabilisce i principi che devono caratterizzare il trattamento: lealtà, liceità e limitazione delle finalità. Vengono inoltre previsti il diritto di accesso ai dati e di rettifica, insieme alla previsione della necessaria presenza di un'autorità indipendente che vigili sul rispetto delle regole. Gli organi e le istituzioni europee, così come gli stati membri nell'attuazione del diritto europeo, sono obbligati a rispettare questo diritto e a garantirlo. Oltre che nella CDFUE, il diritto alla protezione dei dati personali viene previsto anche nel TFUE, all'art. 16, nel titolo riguardante i principi generali dell'Unione europea[233]. Questo passaggio è fondamentale, perché l'art. 16 diviene la nuova base giuridica per la competenza dell'UE in tema di *data protection,* fino ad allora rappresentata dal mercato interno e dall'armonizzazione

---

[231] Carta dei diritti fondamentali dell'Unione europea, [2012] GU C 326 del 26.10.2012, pagg. 391–407.

[232] Carta dei diritti fondamentali dell'Unione europea, [2012] GU C 326 del 26.10.2012, pagg. 391–407. L'art. 8, rubricato *"Protezione dei dati di carattere personale",* prevede che*"Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".*

[233] Trattato sul funzionamento dell'Unione europea*,* versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 47–390. Art. 16:*" Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea".*

delle legislazioni nazionali. Proprio questo articolo è stato il fondamento giuridico per l'adozione del GDPR, nel 2016. Fino a quel momento lo strumento giuridico principale in tema di protezione dei dati personali è stata la Direttiva 95/46/CE, contenente i principi e i diritti già affermati dalla Convenzione n. 108 e dalle normative nazionali, ma che non essendo direttamente vincolante permetteva agli stati membri un margine di manovra nel suo recepimento. Con l'intento di creare un sistema armonizzato e aggiornato agli sviluppi tecnologici, nel 2016 è stato adottato il celeberrimo regolamento, entrato in vigore due anni dopo. Come accennato in precedenza, questa normativa ha come ampio campo di applicazione, *ex* artt. 2 e 3, il trattamento dei dati personali, informazioni riguardanti persone fisiche identificate o identificabili nel territorio dell'Unione, i cd. interessati. I soggetti che intervengono nell'ambito del trattamento sono individuati e definiti all'art. 4. In particolare, il titolare del trattamento, persona fisica o giuridica che stabilisce le finalità del trattamento, ed il responsabile, colui che realizza il trattamento per conto del titolare[234]. Ove il titolare non sia stabilito nel territorio dell'Unione, come ad esempio nel caso di imprese multinazionali, è necessaria la designazione per iscritto di un rappresentante che ne faccia le veci. Bisogna notare che le persone giuridiche non sono coperte dal GDPR, ma ricevono una protezione, seppur minore, dall'art. 8 della CEDU[235]. I principi fondamentali che caratterizzano il trattamento dei dati personali sono previsti nell'art. 5 del Regolamento. Questi sono, rispettivamente, i principi di liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza dei dati; limitazione della conservazione; integrità e riservatezza[236]. Passandoli in rassegna uno per uno, il principio di liceità richiede la presenza del consenso dell'interessato, che *ex* art. 7 deve essere libero, informato, specifico e inequivocabile, o di altra base giuridica, quali l'esecuzione di un contratto, l'adempimento di un obbligo legale, la necessità di

[234] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88, art. 4.

[235] Come è stato stabilito dalla Corte Europea dei Diritti Umani nel caso *Bernh Larsen Holding AS e a. c. Norvegia,* n. 24117/08, [2013].

[236] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88, (art. 5).

salvaguardare gli interessi vitali di un terzo o dell'interessato, la necessità per l'esecuzione di un compito di interesse pubblico o il perseguimento di un interesse legittimo del titolare, se superiore a quelli dell'interessato[237]. La correttezza e la trasparenza del trattamento impongono un comportamento corretto del titolare e la fornitura di adeguate informazioni agli interessati. Il principio di limitazione delle finalità stabilisce la necessaria specificità dello scopo del trattamento e la possibilità di un'ulteriore solo se compatibile con il primo. I principi di minimizzazione ed esattezza richiedono che il trattamento sia ristretto soltanto a quanto necessario e che i dati debbano essere sempre aggiornati o rettificati. Per rispettare l'integrità e la riservatezza, invece, sono necessarie misure e protocolli adeguati per garantire la sicurezza degli stessi. Enunciati i principi generali, il GDPR riconosce una serie di diritti agli interessati, così da fornire una protezione maggiore nel mondo digitale sempre più complesso e pieno di minacce. Questi sono il diritto ad essere informati, il diritto alla rettifica, il diritto alla cancellazione dei dati, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati e il diritto di opposizione[238]. La giurisprudenza ha negli anni chiarito il campo di applicazione e le sfaccettature di ognuno. Analizzando le pronunce più rilevanti, partendo dal diritto ad essere informati, nel caso *Smaranda Bara e a. d. Preşedintele Casei Naţionale de Asigurări de Sănătate e a.* la CGUE è intervenuta su una vicenda avente ad oggetto il trasferimento tra due amministrazioni pubbliche senza che gli interessati venissero informati[239]. Nel caso di specie, la signora Smaranda Bara ed altri lavoratori autonomi rumeni non sono stati informati dall'amministrazione tributaria rumena della trasmissione delle loro dichiarazioni dei redditi alla Cassa nazionale malattia, per un successivo trattamento ad opera di quest'ultima. La Corte stabilisce che il diritto ad essere informati obbliga il titolare del trattamento a fornire tutte le informazioni necessarie agli interessati, dove

> "*tali informazioni attengono all'identità del responsabile del trattamento dei dati, alle finalità del trattamento e a ogni altra informazione necessaria per effettuare un trattamento leale dei dati"*[240]. Quest'obbligo "*di informare le persone*

[237] ibidem, art. 6.

[238] ibidem, artt. 12-22.

[239] C-201/14, *Smaranda Bara e a. / Preşedintele Casei Naţionale de Asigurări de Sănătate e a.,* [2015], ECLI: ECLI:EU:C:2015:638.

[240] ibidem, para 32.

interessate dal trattamento dei loro dati personali è ancora più rilevante poiché condiziona necessariamente l'esercizio da parte loro dei diritti, da un lato, di accesso ai dati trattati e della rispettiva rettifica, sancito all'articolo 12 della direttiva 95/46, e, dall'altro, di opposizione al trattamento dei medesimi, sancito all'articolo 14 della stessa direttiva. Ne consegue che la condizione del trattamento leale dei dati personali prevista all'articolo 6 della direttiva 95/46 obbliga un'amministrazione pubblica a informare le persone interessate della trasmissione di tali dati a un'altra amministrazione pubblica che li tratterà in qualità di destinataria di detti dati"[241].

All'eccezione sollevata dalle amministrazioni rumene, secondo cui gli Stati membri possono limitare il campo di applicazione del diritto per motivi di necessità nazionale, la Corte replica che le restrizioni devono essere introdotte *ex lege,* condizione nel caso di specie non riscontrabile[242]. Viene così data ragione agli interessati, vista la natura propedeutica del diritto di essere informati rispetto a tutti gli altri[243]. Il secondo diritto, quello alla rettifica dei dati personali, viene considerato dalla Corte europea dei diritti dell'uomo nel caso *Ciubotaru c. Moldova*[244]. Il signor Ciubotaru, cittadino moldavo, ha richiesto la modifica dell'indicazione della propria origine etnica da moldava a rumena. La questione era sorta quando il ricorrente ha cercato di sostituire la propria carta d'identità sovietica con quella moldava, indicando nel campo relativo all'origine etnica la propria provenienza rumena. Dal rifiuto di rilascio dell'autorità per mancanza di prove effettive che dimostrassero la sua pretesa è discesa l'iniziativa contro lo stato moldavo. La Corte stabilisce, in prima battuta, che il caso ricade nell'ambito dell'art. 8 CEDU perché tratta di un elemento, quale l'origine etnica, estremamente determinante per la sfera privata di una persona, in particolare in Moldavia dove l'etnia è un tema molto sentito e dibattuto. La decisione finale a cui si giunge è perciò la seguente:

"*The Court would further observe that Mr Ciubotaru's claim is based on more than his subjective perception of his own ethnicity. It is clear that he is able to provide objectively verifiable links with the Romanian ethnic group such as language,*

[241] ibidem, para 33-34.

[242] ibidem, para 39.

[243] ibidem, para 46.

[244] *Ciubotaru c Moldova,* n. 27138/04, [2010].

name, empathy and others. However, no such objective evidence can be relied on under the Moldovan law in force. Having regard to the circumstances of the case as a whole, it cannot be said that the procedure in place to enable the applicant to have his recorded ethnicity changed complied with Moldova's positive obligations to safeguard his right to respect for his private life. For the Court, the State's failure consists in the inability for the applicant to have examined his claim to belong to a certain ethnic group in the light of the objectively verifiable evidence adduced in support of that claim. The Court therefore concludes that the authorities failed to comply with their positive obligation to secure to the applicant the effective respect for his private life. There has, accordingly, been a breach of Article 8 of the Convention"[245].

Riassumendo, dunque, la Moldavia viene considerata responsabile della violazione dell'art. 8 CEDU per non aver permesso la rettifica delle informazioni personali di un suo cittadino, garantendogli il rispetto della propria vita privata. Un altro caso importantissimo, forse uno dei più celebri e rilevanti, è sicuramente *Google Spain*[246]*,* relativo al diritto alla cancellazione (cd. diritto all'oblio). Il caso aveva ad oggetto la segnalazione all'*Agencia Española de Protección de Datos* di un cittadino nei confronti di *Google* e di un famoso quotidiano locale, *La Vanguardia,* diretta alla cancellazione dai risultati di ricerca di un articolo obsoleto in cui si trattava delle sue condizioni economiche problematiche, ormai superate. La prima questione che viene in rilievo è la risposta all'argomentazione di *Google,* in cui la società sostiene che l'unico soggetto a cui rivolgersi sia il titolare della pagina *web* poiché l'algoritmo del motore di ricerca si limita a fornire i *link* dei siti. La Corte, differentemente, ritiene che *Google,* nella sua attività di raccolta, organizzazione, indicizzazione e fornitura di dati e risultati, rivesta la qualità di titolare del trattamento *ex* art. 2 direttiva 95/46 in quanto le operazioni sicuramente rappresentano un trattamento di dati personali[247] ed è il motore di ricerca a

[245] ibidem, para 58-59.

[246] C-131/12, *Google Spain SL e Google Inc. c Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* [2014]. ECLI:EU:C:2014:317.

[247] Come affermato nel caso C-101/01, *Bodil Lindqvist*, [2003], para 25, EU:C:2003:596, dove si è stabilito che il mero caricamento dei dati personali su una pagina *web* configuri un trattamento.

determinarne finalità e modalità di svolgimento[248]. Si riconosce che il trattamento dei dati ad opera dei motori di ricerca è in grado di influire pesantemente sul diritto alla *privacy* e alla protezione dei dati personali, poiché partendo da informazioni limitate o parziali come un nome ed un cognome si è in grado, attraverso i risultati mostrati, di ricostruire il profilo dettagliato di una persona[249]. Questo è uno dei grandi benefici apportati da *Internet,* la possibilità di accesso in tempo reale ad informazioni pressoché infinite. Per la CGUE è dunque necessario operare un bilanciamento tra i vari interessi in gioco, perché

> "*vista la gravità potenziale di tale ingerenza, è giocoforza constatare che quest'ultima non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati. Tuttavia, poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica"*[250].

Nonostante l'importanza di avere informazioni sempre aggiornate nella società odierna, fortemente digitalizzata, non è possibile sacrificare la protezione dei dati personali delle persone. I motori di ricerca come *Google*, titolari del trattamento dei dati nonostante il loro compito sia fornire e presentare le informazioni in rete, devono intervenire ove ci sia bisogno di rimuovere informazioni obsolete che possano danneggiare gli interessati, come nel caso di specie. Viene affermato così l'esistenza di un diritto alla cancellazione

---

[248] C-131/12, *Google Spain SL e Google Inc. c Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* [2014]. ECLI:EU:C:2014:317. , para 26-40.

[249] ibidem, para 80.

[250] ibidem, para 81.

dei dati personali, un diritto non assoluto, che necessita di essere valutato con un approccio *case by case* alla luce di tutti gli interessi in gioco e alla loro rilevanza[251]. La Corte conclude stabilendo che

> *"relativamente ad una situazione come quella in esame nel procedimento principale, che riguarda la visualizzazione – nell'elenco di risultati che l'utente di Internet ottiene effettuando una ricerca a partire dal nome della persona interessata con l'aiuto di Google Search – di link verso pagine degli archivi online di un quotidiano, contenenti annunci che menzionano il nome di tale persona e si riferiscono ad un'asta immobiliare legata ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali, occorre affermare che, tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubblicazione iniziale era stata effettuata 16 anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Pertanto, dal momento che nella fattispecie non sembrano sussistere ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso, nel contesto di una ricerca siffatta, a dette informazioni – aspetto questo che spetta però al giudice del rinvio verificare –, la persona interessata può esigere, a norma degli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, la soppressione dei link suddetti da tale elenco di risultati.Dalle suesposte considerazioni discende che occorre rispondere alla terza questione dichiarando che gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a*

[251] ibidem, para 82-90.

disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi"[252].

Essendo il diritto all'oblio non assoluto, l'esito di una vicenda può variare in base alla diversa importanza degli interessi confliggenti presenti nel singolo caso. Nella causa *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c Salvatore Manni*[253], ad esempio, il diritto alla cancellazione dei dati personali ha dovuto soccombere rispetto al pubblico interesse. Il sig. Manni, amministratore di una società vincitrice di un bando volto alla realizzazione di un villaggio turistico, ha richiesto alla Camera di commercio di Lecce la cancellazione dei suoi dati personali dal registro delle imprese in quanto preoccupato che le informazioni in esso contenute, in particolare relative al suo ruolo di amministratore di una società precedentemente fallita, potessero allontanare i potenziali clienti degli immobili costruiti[254]. La Corte pondera il diritto affermato dal ricorrente con la *ratio* del registro delle imprese, registro pubblico istituito per dare attuazione alla direttiva 68/151 CEE, diretto a

"*facilitare e accelerare l'accesso delle parti interessate alle informazioni sulle società, semplificando in modo significativo le formalità relative alla pubblicità cui le stesse sono tenute"*[255].

---

[252] ibidem, para 98-99. Si veda inoltre, Varie istituzioni europee, *Manuale sul diritto europeo in materia di protezione dei dati,* (ed. 2018, Ufficio pubblicazioni UE, 2018), 247-249.

[253] C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c Salvatore Manni*, [2017], ECLI:EU:C:2017:197.

[254] ibidem.

[255] Direttiva 68/151 CEE [1968], OJ L 65, 14.3.1968, p. 8–12, considerando n. 3.

Queste informazioni sono fondamentali all'interno del mercato unico europeo, soprattutto in caso di società a responsabilità limitata, come nella vicenda in analisi, dove l'unica garanzia è il patrimonio societario. Non è possibile stabilire *ex ante* un termine fisso oltre il quale si può chiedere la cancellazione delle informazioni, poiché ci sono rapporti giuridici ed economici che persistono anche per molti anni dopo lo scioglimento di una società, e

> "*a tale proposito, si deve rilevare che il solo presumere che gli immobili di un complesso turistico costruito dalla Italiana Costruzioni, di cui il sig. Manni è attualmente amministratore unico, non si vendano perché i potenziali acquirenti di tali immobili hanno accesso ai dati in questione nel registro delle imprese, non può essere sufficiente a costituire una simile ragione, tenuto conto, in particolare, del legittimo interesse di questi ultimi a disporre di tali informazioni. Alla luce dell'insieme delle considerazioni che precedono, si deve rispondere alle questioni sollevate dichiarando che l'articolo 6, paragrafo 1, lettera e), l'articolo 12, lettera b), e l'articolo 14, primo comma, lettera a), della direttiva 95/46, in combinato disposto con l'articolo 3 della direttiva 68/151, devono essere interpretati nel senso che, allo stato attuale del diritto dell'Unione, spetta agli Stati membri determinare se le persone fisiche di cui all'articolo 2, paragrafo 1, lettere d) e j), della direttiva da ultimo citata possano chiedere all'autorità incaricata della tenuta del registro di verificare, in base ad una valutazione da compiersi caso per caso, se sia eccezionalmente giustificato, per ragioni preminenti e legittime connesse alla loro situazione particolare, decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società interessata, limitare l'accesso ai dati personali che le riguardano, iscritti in detto registro, ai terzi che dimostrino un interesse specifico alla loro consultazione"*[256].

La Corte conclude così la non azionabilità del diritto alla cancellazione dei dati nella situazione del Manni, data la maggiore rilevanza degli interessi perseguiti dal registro delle imprese[257]. Dopo la rapida analisi giurisprudenziale, bisogna notare che questi

[256] CGUE, *Comunicato stampa n. 27/17 sulla causa Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c Salvatore Manni*, (9 marzo 2017), para 63-64.

[257] Cfr. Varie istituzioni europee, *Manuale sul diritto europeo in materia di protezione dei dati,* (ed. 2018, Ufficio pubblicazioni UE, 2018), 249-250.

diritti possono essere limitati, in base all'art. 23, soltanto in casi previsti dalla legge, naturalmente proporzionati all'interesse perseguito[258]. A chiusura del sistema vengono previste autorità nazionali ed europee di vigilanza, per rendere effettivo quanto stabilito nella normativa e attribuire agli interessati strumenti, e regole per il trasferimento transfrontaliero dei dati[259]. Il GDPR ha rappresentato una rivoluzione per la *data protection* europea, istituendo un *framework* unico e rigoroso, capace di dare risposta, grazie al suo ampio campo di applicazione, alle problematiche della *data economy* e alle innovazioni tecnologiche che possono incidere sui diritti degli interessati. L'utilizzo di complessi algoritmi, di cui non è rivelato il funzionamento, per l'analisi dei *Big data* e la profilazione degli utenti, insieme all'introduzione di sistemi di *Artificial Intelligence* (AI) per il *decision making,* pongono seri problemi per l'applicazione del dettato normativo, oltre che di responsabilità. In particolare, i principi del GDPR maggiormente interessati dall'utilizzo di queste misure tecnologiche sono la minimizzazione dei dati, dove il modello dei *Big data* si pone totalmente all'antitesi per la sua continua necessità di nuovi dati, il principio di limitazione delle finalità, poiché non sempre sono definite le finalità del trattamento, spesso ulteriori e incompatibili a quelle iniziali, ed il principio di esattezza dei dati, con i dati aggregati da più fonti e che non è possibile verificare o aggiornare[260]. Naturalmente il GDPR fornisce diversi strumenti per tutelare gli interessati contro queste condotte. In *primis,* gli interessati hanno il diritto di essere informati, *ex* art. 12 del Regolamento, e ricevere dal titolare tutte le informazioni riguardanti il trattamento dei loro dati personali, anche da possibili processi decisionali automatizzati, in ossequio del principio di trasparenza sancito nell'art. 5. Queste informazioni possono non essere fornite dal titolare solo se richiederebbero uno sforzo sproporzionato, non rinvenibile però nella mera complessità dei mezzi utilizzati per il trattamento. Gli interessati hanno poi il diritto di accedere, rettificare, cancellare i dati che li riguardano e limitare il loro trattamento, oltre che il diritto di opporsi, *ex* art. 21,

---

[258] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88, art. 23.

[259] Già osservate nell'analisi dei casi *Schrems.*

[260] Cfr. Garante europeo della protezione dei dati, *Parere sull'applicazione coerente dei diritti fondamentali nell'era dei Big data,* parere 8/2016, (23 settembre 2016).

ad esso[261]. Sono possibili deroghe a questi ultimi solo per finalità di ricerca scientifica, storica o statistica nel pubblico interesse[262]. Contro la importante problematica della profilazione attraverso processi automatizzati, l'art. 22 prevede l'importante diritto per l'interessato di

> "*non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona"*[263].

I titolari possono essere esentati dal rispetto del diritto quando la decisione basata su trattamento automatizzato

> "*sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; si basi sul consenso esplicito dell'interessato"*[264].

La problematica maggiore riguardo la profilazione e il *micro-targeting advertising* è la poca consapevolezza degli interessati sui processi che subiscono i loro dati, forse uno dei più grandi ostacoli che incontra l'esercizio dei loro diritti. I dati che compongono i *Big data* possono essere anonimizzati, quindi ricadere fuori dal campo di applicazione del GDPR, o pseudonimizzati, sottostanti invece alle regole del Regolamento, ma nella maggior parte dei casi tutto avviene a scatola chiusa, quindi la sensibilizzazione degli utenti è fondamentale per renderli più consapevoli[265]. Comunque il Regolamento ha

---

[261] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88,, artt. 19-21. I titolari del trattamento possono essere esentati da soddisfare le richieste basate sul diritto di opporsi se dimostrano legittimi interessi predominanti rispetto quelli degli interessati, ma mai in caso di trattamento ai fini di marketing diretto.

[262]ibidem, art. 89.

[263] ibidem, art. 22, comma 1.

[264] ibidem, art. 22, comma 2.

[265] Varie istituzioni europee (n.3) , 398-404.

permesso un'evoluzione importante per la *data protection* europea, tanto da essere il punto di riferimento anche per gli altri stati paesi extra-UE, e rappresenta una fase del progresso normativo europeo sulla protezione dei dati personali che nei prossimi anni si farà sempre più rapido.

4. Strumenti giuridici del diritto *antitrust*

Si è soliti far coincidere la nascita del diritto *antitrust* moderno con l'approvazione, negli Stati Uniti, dello Sherman Act nel 1890, volto a proteggere la concorrenza e migliorare il benessere dei consumatori attraverso prezzi più equi e qualità dei servizi più elevata. Nella *Section 1* (articolo 1) questo prevedeva l'illegalità di ogni contratto o accordo tra imprese che potesse limitare la concorrenza (cartello), mentre nella *Section* 2 è enunciata la criminosità dei tentativi di monopolizzare parte del commercio tra stati[266]. Assumere una posizione dominante sul mercato non era dunque proibito di per sé, ma solo i tentativi di abuso della propria posizione per restringere la concorrenza ed eliminare i *competitors.* Lo Sherman Act fu lo strumento che permise alla Corte Suprema di Stati Uniti, nel 1911, di smantellare il monopolio petrolifero della *Standard Oil* di John D. Rockefeller, dividendola in trentaquattro società separate e creando un importante precedente per i successivi casi giurisprudenziali e lo sviluppo della legislazione *antitrust*[267]. Stessa sorte capitò anche alle società *Alcoa* (1945)[268] e *AT&T* (1983)[269]. Un passo in avanti nell'analisi *antitrust* fu realizzato grazie alla Scuola di Chicago, scuola di pensiero economico fondata negli anni Trenta da economisti dell'Università di Chicago, tra cui spicca Milton Friedman, il cui approccio divenne

---

[266] Sherman Antitrust Act, Enrolled Acts and Resolutions of Congress, 1789-1992, General Records of the United States Government; Record Group 11, National Archives, [1890].

[267] *Standard Oil Co. of New Jersey v. United States,* 221 U.S. 1 [1911]. Per un approfondimento: https://www.hg.org/legal-articles/infamous-antitrust-cases-6025 .

[268] *Alcoa,* U.S. Court of Appeals for the Second Circuit - 148 F.2d 416 [1945]
. Nella decisione, il giudice L. Hand mise in rilievo l'importante punto secondo cui un monopolio può originarsi *in re ipsa,* senza che ci sia bisogno della volontà di qualcuno.

[269] *United States v. AT&T Inc.* - 310 F. Supp. 3d 161 D.D.C. [1984].

dominante negli *USA e* in Europa negli anni Settanta fino a tutti gli anni Novanta[270]. Il fulcro dell'analisi della Scuola risiede nell'importanza attribuita al libero mercato, privo di interventi statali, dove gli individui razionali, inseguendo la ricerca del massimo profitto, col loro agire realizzano la massima efficienza allocativa[271]. In quest'ottica, solo col *laissez-faire* è possibile conseguire i due obiettivi del diritto *antitrust,* cioè la concorrenza tra imprese, il più possibile vicina alla perfetta, e il benessere dei consumatori, come affermato da Robert Bork nel suo *"The Antitrust Paradox"*[272]. Un ruolo molto importante per calcolare quest'ultimo elemento è dato dalla *price theory,* che ha nel prezzo il principale riferimento per i consumatori. Diverse sono state le critiche a questo approccio, in particolare per la troppa attenzione posta sul *consumer welfare* piuttosto che sulla struttura del mercato, portando all'aumento dei prezzi e il ridursi della concorrenza[273]. Il modello diviene ancora più di difficile applicazione nei confronti dei *tech giants,* con la loro espansione in diversi mercati e la strategia di perseguire la crescita più che il profitto nel breve termine, vendendo i prodotti a prezzi predatori che sembrano apportare soltanto benefici ai consumatori, seppur diminuendo la qualità degli stessi, generalmente sul lato privacy[274]. Il caso emblematico è Amazon. In Europa, invece, a caratterizzare il modello *antitrust,* influenzato dai dettami della Scuola di Chicago, è la cosiddetta "terza via" di matrice ordoliberale, teorizzata dalla Scuola di Friburgo. Lungi dal ritenere sufficiente il *laissez-faire,* per la visione europea lo Stato ha il compito centrale di promuovere la concorrenza, eliminando gli ostacoli al libero mercato, regolando il comportamento delle imprese che acquistano un potere troppo grande e tutelando gli interessi dei consumatori. La struttura del mercato discendente da questa corrente di pensiero risulta essere quella della "concorrenza completa"[275]. L'inizio del diritto della concorrenza europeo si può far coincidere con la stipula del Trattato di Roma nel 1957, istitutivo delle Comunità economica europea[276]. Il

[270] Olivia Altmayer (n. 114), 40.

[271] Editori dell'Encyclopedia Britannica, *Chicago School of economics,* Encyclopedia Britannica. Una visione molto simile alla "Mano invisibile" teorizzata da Adam Smith.

[272] Cfr. Robert Bork, *The Antitrust Paradox: a policy at war with itself,* (1978).

[273] Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L. J. (2017), 737- 746.

[274] Cfr. Roberto Pardolesi, *Tutto (o quasi) quel che avreste voluto sapere sul principio del consumer welfare in diritto antitrust,* Orizzonti del Diritto Commerciale, fascicolo speciale ad opera di G. Giappichelli Editore, (Giugno 2021), 320- 330.

[275] ibidem, 320-322.

[276] Trattato che istituisce la Comunità economica europea, [1957].

diritto *antitrust* ha rivestito sin dal principio un ruolo fondamentale nel processo d'integrazione europea, perché potente strumento in grado di incentivare e garantire il commercio tra stati e le quattro libertà pilastro dell'Unione. Inizialmente ha adempiuto lo scopo di eliminare gli ostacoli al commercio tra Stati membri, per poi puntare al controllo delle concentrazioni e lo smantellamento dei monopoli statali, liberalizzando interi settori[277]. Una grande innovazione si è avuta con l'adozione del Regolamento 1/2003/CE, che ha portato ad un maggiore decentramento dei poteri di *enforcement,* modernizzando l'approccio alla luce dell'evoluzione del mercato interno ed il numero crescente di stati membri. Guardando alle fonti della normativa UE di diritto concorrenziale, esse sono contenute nel Titolo VII del TFUE ("*Norme comuni sulla concorrenza, sulla fiscalità e sul ravvicinamento delle legislazioni")*, agli artt. 101-107, dopo aver previsto all'art. 3 dello stesso trattato la competenza esclusiva dell'Unione in materia di "*definizione delle regole di concorrenza necessarie al funzionamento del mercato interno*"[278]. Per l'applicazione delle regole è necessario prima comprendere la loro portata. Le singole fattispecie fanno riferimento al concetto di "impresa", non definito *ex lege,* che per la CGUE bisogna intendere come "*qualsiasi entità esplicante un'attività economica, indipendentemente dallo stato giuridico di questa entità e dal suo modo di finanziamento"*[279]*,* avente dunque nel suo carattere economico, nella sua attività di scambio, il *discrimen*[280]. Chiarito questo primo punto, bisogna individuare i mercati merceologici e geografici rilevanti, interessati dalla condotta concorrenziale. Per la definizione del primo si considerano i prodotti e le merci interscambiabili tra loro, mentre per il secondo si definisce l'ambito geografico in cui le imprese sono soggette a

---

[277] EDPS, *Preliminary Opinion on "Privacy and competitiveness in the age of Big data: The interplay between data protection, competition law and consumer protection in the Digital Economy",* (26 marzo 2014), 12- 14. Accessibile al link:

https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en .

[278] Trattato sul funzionamento dell'Unione europea*,* versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 47–390, art. 3.

[279] C-41/90, *Klaus Hofner e Fritz Elser c. Macroton GmbH*, [1991], ECLI:EU:C:1991:161.

[280] Nozione perciò molto ampia e pragmatica che trascende le singole definizioni nazionali di "attività economica" o "impresa".

condizioni concorrenziali analoghe[281]. Individuati questi fondamentali concetti, è possibile proseguire con l'analisi concorrenziale delle tre fattispecie rilevanti previste dal TFUE: le intese restrittive della concorrenza, lo sfruttamento abusivo di posizione dominante e le concentrazioni. L'art 101 TFUE, sulla falsariga della *Section* 1 dello Sherman Act succitato, statuisce, al comma 1, il divieto delle intese, comportamenti concordati (come gli accordi tra imprese, le decisioni di associazioni di imprese e le pratiche concordate) che abbiano come oggetto o effetto la limitazione della concorrenza nel mercato interno, pregiudicando il commercio tra stati membri. Dopo aver listato un elenco esemplificativo di cinque tipi d'intese, al comma 2 viene chiarito che la conseguenza della violazione del divieto è la loro nullità di pieno diritto, con la possibilità per chiunque di agire in giudizio per accertarla. Non sono, tuttavia, vietate tutti i comportamenti concordati tra imprese, ma soltanto quelli suscettibili di restringere in modo consistente il processo concorrenziale, non rilevando le cd. "intese minori". Inoltre, al comma 3, sono previste delle esenzioni dal divieto automatico del comma 1, per le diverse tipologie di intese che perseguono fini utilitaristici o sociali, come il progresso tecnologico o il miglioramento della produzione[282]. La seconda fattispecie di interesse per il diritto *antitrust* consiste nell'abuso di posizione dominante. L'art. 102 del TFUE (omologo della norma contenuta nella *Section 2* dello Sherman Act) afferma l'incompatibilità col mercato interno dello sfruttamento abusivo di posizione dominante, da parte di una o più imprese, che possa pregiudicare in maniera rilevante il commercio tra stati membri, con un elenco tipizzato delle pratiche abusive. In questo caso non è proibito il possesso di una posizione dominante sul mercato, ma solo il suo sfruttamento abusivo, suscettibile di ledere la concorrenza nel mercato interno, senza alcuna esenzione (a differenza dell'art. 101). Per valutare la posizione dominante è necessario, come visto, delineare il mercato merceologico e geografico di riferimento, in modo da verificare la quota di mercato dell'impresa e la sua influenza sul gioco della concorrenza[283]. Due sono le forme principali di abuso: le *exclusionary conducts,* attraverso le quali l'impresa dominante esclude dal mercato le concorrenti,

---

[281] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Al26073#:~:text=il%20mercato%20geografico%20rilevante%20comprende,di%20concorrenza%20sono%20sufficientemente%20omogenee

.

[282] Trattato sul funzionamento dell'Unione europea, versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 47–390, art. 101.

[283] ibidem, art. 102.

come le strategie di *bundling,* vendita riunita di due prodotti distinti, *tying ,* l'acquisto di un prodotto subordinato all'acquisto di un secondo, e l'abuso di dipendenza economica; l'*exploitation*, dove i consumatori sono direttamente lesi, come nell'applicazione di prezzi eccessivamente alti[284]. La Commissione europea ha un ruolo centrale nel contrasto delle condotte lesive della concorrenza ed è interessante notare come, col già citato Regolamento 1/2003/CE, siano stati aumentati i suoi poteri, semplificando il sistema. A differenza del regime precedente al 2003, dove erano applicabili simultaneamente le normative nazionali e comunitarie, ora è stabilito che la normativa prevalente in caso di fenomeni che possono ledere la concorrenza sul mercato interno è quella europea, con gli artt. 101 e ss. del TFUE, rendendo le discipline nazionali residuali, applicabili alle pratiche con portata solo locale. Nell'ottica di creare un sistema razionale e decentrato, vengono analiticamente regolate le relative competenze, con il ruolo predominante della Commissione come organo di vigilanza e controllo. Da queste previsioni prende vita una rete unica tra autorità nazionali garanti della concorrenza e Commissione europea, con stretta collaborazione e un fitto scambio di informazioni per assicurare un mercato libero e concorrenziale[285].

5. Proposte regolatorie e nuovi orizzonti

Sono state considerate le principali previsioni dell'arsenale giuridico europeo diretto a far fronte alle violazioni delle regole a tutela dei dati personali e della concorrenza, sempre più collegate. Questi strumenti sono però abbastanza? Sul versante *antitrust,* in particolare, autorità, istituzioni e studiosi si sono interrogati sull'adeguatezza dell'attuale disciplina nei confronti delle condotte abusive dei *big tech* e nella regolazione dei mercati digitali. Nonostante l'opinione di parte della dottrina, che ritiene

[284] EDPS, *Preliminary Opinion on "Privacy and competitiveness in the age of Big data: The interplay between data protection, competition law and consumer protection in the Digital Economy",* (26 marzo 2014), 19- 22.

[285] Antonio Marcello Calamia, Viviana Vigiak, *Diritto dell'unione europea,* Giuffrè editore, (2018), 257-272.

perfettamente al passo coi tempi le previsioni attuali[286], la visione maggioritaria considera necessario un cambiamento per rispondere agli stravolgimenti sociali ed economici causati dallo sviluppo tecnologico. Interessante è in tal senso l'*Investigazione sulla concorrenza nei mercati digitali* della Sottocommissione del Congresso statunitense per l'*antitrust*, il diritto commerciale e amministrativo della commissione per la magistratura, datata ottobre 2020[287]. Nel *report* di circa quattrocento pagine, l'autorità statunitense analizza le principali caratteristiche dei mercati digitali e dei *player* che ne fanno parte, mettendone in luce la struttura fortemente centralizzata, le barriere all'entrata che possono ostacolare o rallentare l'innovazione ed i possibili effetti negativi che lo sfruttamento abusivo dei *Big data* può avere sui consumatori e la società[288]. Particolarmente rilevante è anche il riflesso della struttura del mercato sulle libertà economiche e politiche dei partecipanti, poiché dall'indagine traspare come

> "*the Subcommittee encountered a prevalence of fear among market participants who depend on the dominant platforms. Repeatedly, market participants expressed deep concern that speaking about the dominant platforms' business practices—even confidentially without attribution— would lead a platform to retaliate against them, with severe financial repercussions. The source of this fear was twofold. Some firms were so dependent on the platform that even potentially risking retaliation caused alarm. Others had previously seen a platform retaliate against someone for raising public concerns about their business practices and wanted to avoid the same fate. "*[289].

---

[286] Vedi John A. Fortin, *Algorithms and Conscious Parallelism: Why Current Antitrust Doctrine is Prepared for the Twenty-First Century Challenges Posed by Dynamic Pricing*, Tulne Journal of Technology & Intellectual Property (18 agosto 2020), Vol. 23, forthcoming.

[287] Congresso degli Stati Uniti, Sottocommissione per l'*antitrust*, il diritto commerciale e amministrativo della commissione per la magistratura del Congresso statunitense, *Investigazione sulla concorrenza nei mercati digitali,*(2 ottobre 2020).

[288] Cfr. Mario Libertini, *Digital markets and competition policy. Some remarks on the suitability of the antitrust toolkit ,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 338-341.

[289] Congresso degli Stati Uniti, Sottocommissione per l'*antitrust*, il diritto commerciale e amministrativo della commissione per la magistratura del Congresso statunitense, *Investigazione sulla concorrenza nei mercati digitali,* (2 ottobre 2020), 73-74.

Dopo un'analisi delle GAFAM e delle caratteristiche economiche delle loro piattaforme e servizi, la Sottocommissione propone possibili soluzioni e raccomandazioni per migliorare lo stato concorrenziale del mercato: *in primis,* ridurre le situazioni di conflitto d'interesse, garantire la maggiore interoperabilità tra i servizi e le piattaforme e introdurre una presunzione di anticompetitività per le acquisizioni delle grandi piattaforme; rafforzare la legislazione *antitrust* tornando allo spirito originale della disciplina, strumento per proteggere non solo il *consumer welfare,* ma ulteriori e molteplici interessi; rafforzare l'*enforcement,* con un ruolo di vigilanza più attivo delle istituzioni (nel caso americano soprattutto la *FTC)* e l'introduzione di una forma di *private enforcement*[290]. Lo sfruttamento dei *Big data* da parte delle imprese che hanno nella raccolta massiva dei dati un elemento centrale del modello di *business,* può sfociare in operazioni di difficile *enforcement* e lesive della concorrenza. Nonostante i molti benefici per consumatori e aziende, diversi possono essere gli effetti negativi sul regime concorrenziale, come già mostrato nel corso dell'elaborato. In mercati dove il controllo di maggiori quantità di dati personali permette di superare i *competitors* e conquistare un *market share* rilevante, difficilmente attaccabile grazie alle esternalità di rete e alle economie di scala e scopo che premiano il *first mover*, pochi sono gli incentivi per le imprese dominanti ad innovare e migliorare la qualità dei prodotti. Questa perdita di qualità e innovazione viene accentuata dalla prassi delle cd. *killer acquisition,* l'acquisizione da parte delle *big tech* di società con prodotti altamente innovativi che potrebbero, nel lungo periodo, minare la loro dominanza, come nel caso di *Whatsapp* e *Facebook*[291]. Nella *data economy* il solo fattore del prezzo, fondamentale per l'analisi del *consumer welfare,* può portare a visioni distorte dello stato concorrenziale del mercato. La quasi totalità delle piattaforme digitali offre i propri servizi gratuitamente ai consumatori, perciò assumono una maggiore rilevanza ulteriori elementi per la valutazione del loro benessere, come la tutela della *privacy*[292]. Per questo

---

[290] ibidem, *377-403.* Per ulteriore approfondimento, Cfr. Mario Libertini, *Digital markets and competition policy. Some remarks on the suitability of the antitrust toolkit ,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 343-346.

[291] Vedi: Thibault Schrepel, *The "Enhanced No Economic Sense Test": Experimenting With Predatory Innovation*, 7 N.Y.U. J. INTELL. PROP. & ENT. L. 30, 53 (2018).

[292] Daniel D. Sokol, Roisin E Comerford, *Antitrust and Regulating Big data*, 23 George Mason Law Review 119 (2016) , University of Florida Levin College of Law Research Paper No. 16-40 (4 settembre 2016), 1140-1151.

motivo la *data protection* viene considerata sempre di più nelle analisi *antitrust,* come è avvenuto nel caso "*Facebook Germany",* e si sta puntando ad una più forte sinergia tra le due discipline[293]. Un fenomeno inedito è quello della cosiddetta "*collusione algoritmica tacita*", dove i prezzi dei prodotti delle imprese viene determinato dagli algoritmi che continuamente analizzano il mercato e reagiscono automaticamente alle variazione dei prezzi dei concorrenti, generando situazioni di collusione che sicuramente possono impattare sul benessere dei consumatori e sulla concorrenza tra imprese, ma che in concreto sono complesse da scovare e regolare perché alle forme di collusione tacita sono generalmente considerate non applicabili le previsioni dell'art. 101 TFUE[294]. Mediante l'utilizzo di algoritmi sicuramente si ottiene la razionalizzazione della filiera produttiva, con riduzione dei costi e miglior utilizzo delle risorse, portando beneficio ai consumatori sia dal punto di vista monetario che per l'aumento della qualità dei servizi offerti. L'utilizzo scorretto di questi sistemi rappresenta un fenomeno altamente dannoso per il gioco della concorrenza, considerando la velocità e l'automatismo della risposta a determinati eventi o fattori. Sono tre i modi principali in cui è possibile abusare in maniera anticoncorrenziale dei modelli algoritmici: lo sfruttamento degli algoritmi per il realizzarsi di un'intesa precedentemente stabilita; l'utilizzo degli stessi per facilitarne la nascita; la collusione algoritmica tacita, creazione cioè automatica ed *ex novo* di un intesa[295]. Il primo è sicuramente il più diffuso ed affrontato dalle autorità *antitrust*, dove ad esempio gli algoritmi sono intervenuti per controllare automaticamente il concretizzarsi delle condizioni collusive prestabilite o per aggravare politiche di prezzo lesive per i concorrenti[296]. Nella seconda ipotesi, i sistemi possono creare le condizioni necessarie per una futura intesa anticoncorrenziale. Nell'ultimo scenario, invece, si assiste a strutture algoritmiche che, monitorando il mercato ed i concorrenti, si ritrovano ad assumere tacitamente politiche e

---

293 Cfr. Ariel Ezrachi (n. 142), 5-8.

294 Vedi: Ariel Ezrachi, Maurice E. Stucke, *Sustainable and unchallenged algorithmic tacit collusion*, 17 NW. J. TECH. & INTELL. PROP. 217 (2020), ma anche Ariel Ezrachi, Maurice E. Stucke*, Artificial Intelligence & Collusion: When Computers Inhibit Competition,* University of Illinois Law Review, Vol. 2017, (2017), Oxford Legal Studies Research Paper No. 18/2015, University of Tennessee Legal Studies Research Paper No. 267, (8 Aprile, 2015).

295 Cfr. Marilena Filippelli, *La collusione algoritmica,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 375-377.

296 ibidem, 378-379.

comportamenti allineati a quelli altrui[297]. L'intervento normativo regolatorio è molto complesso e ancora inadeguato, nonostante la sempre più forte affermazione di queste fattispecie, come dimostra il *report* della Commissione europea sull'*e-commerce* datato 2017[298]. Da quanto emerge dal documento, oltre alle vere e proprie forme di collusione algoritmica, la maggior parte delle imprese attive nel settore dell'*e-commerce* utilizza sistemi decisionali o di monitoraggio basati su algoritmi, quindi in potenza il rischio è molto alto e latente[299]. Il principale strumento di regolazione è l'imposizione di sistemi algoritmici programmati in modo da evitare condotte collusive, ma naturalmente la linea di confine è molto labile e i risvolti rimangono spesso imprevedibili. L'approccio più recente sul problema sembra essere, in Europa così come negli *USA,* la considerazione, nelle tre diverse forme in cui la fattispecie può realizzarsi, degli algoritmi come proiezione dell'impresa, cercando di adattare le regole tradizionali ai nuovi fenomeni[300]. Tornando a considerare invece le questioni antitrust ed il loro rapporto con la *data protection,* in un'ottica più generale, il più grande limite della disciplina attuale è rappresentato dalla possibilità d'intervento delle autorità *antitrust* solamente *ex post,* quando i danni già si sono realizzati. Di fronte a queste criticità, l'Unione europea negli ultimi anni ha intrapreso un percorso di riforma ed ammodernamento dell'apparato legislativo. Oltre al Regolamento generale sulla protezione dati personali 679/2016 nel settore della *data protection,* sono da citare il Regolamento 881/2019 (cd. "Cybersecurity Act")[301], il Regolamento 1807/2018, relativo alla libera circolazione dei

---

297 ibidem, 384-385.

298 Commissione europea, *Report from the Commission to the Council and the European Parliament – Final Report on the E-Commerce sector inquiry*, (10 maggio 2017).

299 ibidem. Inoltre, Cfr. Marilena Filippelli, *La collusione algoritmica,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 387.

300 Cfr. Marilena Filippelli, *La collusione algoritmica,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) 388-402. È stata anche avanzata l'idea di considerare la collusione algoritmica come una sorta di "abuso di posizione dominante collettiva". Per un approfondimento in tal senso si rimanda a, Monopolkommission, *Algorithms and Collusion,* (3 luglio 2018).

301 Regolamento (UE) 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»), [2019], OJ L 151, 7.6.2019, p. 15–69.

dati non personali all'interno dell'UE[302], la Direttiva *Copyright* 2019/790[303], la proposta di Regolamento *ePrivacy*[304] ed il *whitepaper* della Commissione sull'approccio europeo etico all'Intelligenza Artificiale[305]. Nel febbraio 2020 la Commissione ha annunciato la strategia di transizione digitale europea diretta a plasmare il futuro dell'Unione basato sull'economia dei dati, per renderla pronta alla nuova era digitale[306]. I tre pilastri su cui si fonda questo approccio sono: la tecnologia al servizio delle persone; un'economia digitale equa e competitiva; una società aperta, democratica e sostenibile[307]. Grazie all'iniziativa

> "*l'UE può divenire un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico. Per concretizzare tale ambizione, l'UE può fare affidamento sia su un quadro giuridico solido, in termini di protezione dei dati, diritti fondamentali, sicurezza e cybersicurezza, sia sul suo mercato interno, caratterizzato da imprese competitive di tutte le dimensioni e da una base industriale diversificata. Se vuole conquistarsi un ruolo guida nell'economia dei dati, l'UE deve agire subito e affrontare in maniera concertata questioni che vanno dalla connettività all'elaborazione e alla conservazione dei dati, dalla potenza di calcolo alla cybersicurezza. Dovrà inoltre migliorare le proprie strutture di governance per la*

---

[302] Regolamento (UE) 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, [2018], OJ L 303, 28.11.2018, p. 59–68.

[303] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE , [2019], OJ L 130, 17.5.2019, p. 92–125.

[304] Proposta di Regolamento della Commissione, relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final [2017].

[305] Commissione europea, *White paper on artificial intelligence - a European approach to excellence and trust,* [2020].

[306] Commissione europea, *Strategy for a Europe Fit for the Digital Age,* [2020].

[307] Per approfondimenti visitare il sito: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_it .

gestione dei dati e ampliare i propri pool di dati di qualità disponibili per l'utilizzo e il riutilizzo"[308].

Fondamentale in questa svolta digitale epocale è la strategia europea per i dati, aggiornata e pubblicata sempre nel febbraio 2020, dove si riconosce la loro importanza e le difficoltà tuttora presenti nell'assicurarne la tutela ed evitare gli abusi delle *big tech*[309]. Gli strumenti più rivoluzionari di questo pacchetto di riforme sono sicuramente la proposta di regolamento relativo a mercati equi e contendibili nel settore digitale (*Digital Markets Act, DMA)*[310] e la proposta di regolamento relativo a un mercato unico dei servizi digitali (*Digital Service Act*, *DSA*)[311]. Partendo dal *DMA,* riconoscendo l'importanza dell'economia digitale, le sue peculiarità e quelle delle piattaforme che la caratterizzano, questa proposta mira ad introdurre una normativa apposita per il settore digitale ed i suoi *player.* Analizzando le sue principali previsioni, all'art. 1 il DMA stabilisce i tre obiettivi perseguiti dalla riforma: garantire la contestabilità dei mercati digitali, cioè fare in modo che nei mercati sia sempre possibile entrare per le nuove imprese, così da mantenere alta l'innovazione e la concorrenza; assicurare l'equità dei rapporti *business to business,* per non permettere alle imprese più forti di abusare del proprio potere contrattuale; rafforzare il mercato interno, fornendo una disciplina uniforme e certa[312]. Lo stesso articolo precisa l'ambito di applicazione del Regolamento, limitato ai "*Core Platforms Services"* (*CPS)* offerti da *gatekeepers,* ovunque stabiliti, ad utenti *business* o finali presenti nell'Unione europea[313]. L'art. 2 definisce poi cosa debbano intendersi per *CPS* o *gatekeepers:* i primi sono indicati in un elenco chiuso di servizi, quali i servizi di intermediazione *B2C,* come i *marketplace online* o gli *app store*, i motori di ricerca, *i social network*, le piattaforme di *video-sharing*, i servizi di comunicazione interpersonale, sistemi operativi, servizi di *cloud computing* e servizi

[308] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, una strategia europea per i dati, COM/2020/66 final [2020], 1-2.

[309] ibidem.

[310] Proposta di regolamento relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), COM/2020/842 final, [2020].

[311] Proposta di regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali), COM/2020/825, [2020].

[312] ibidem, art. 1, comma 1.

[313] ibidem, art. 1, comma 2.

pubblicitari; i *gatekeepers,* invece, sono i fornitori di *CPS* designati in base all'art. 3[314]. Le regole del DMA non si applicano a tutti i *CPS,* ma solo ai *gatekeeper* fornitori di uno o più servizi digitali compresi nell'elenco, perciò è fondamentale la loro corretta identificazione. L'art. 3 prevede tre criteri per qualificare un fornitore come *gatekeeper:* il suo impatto rilevante sul mercato, la gestione di un *CPS* che rappresenti un punto di accesso importante affinché gli utenti *business* raggiungano i consumatori, ed infine la consolidazione della propria posizione di mercato, prevedibilmente duratura assicurata anche nel breve/medio termine[315]. Lo stesso articolo, per facilitare l'individuazione di queste figure, stabilisce delle soglie di dimensione e fatturato che una volta superate fanno scattare una presunzione relativa. Le soglie sono: 6,5 miliardi di fatturato negli ultimi tre anni o il valore di capitalizzazione di mercato maggiore o uguale a 65 miliardi, unito alla presenza in almeno tre stati membri; un *CPS* che conta più di 45 milioni di utenti attivi mensilmente o 10 mila annuali, sempre stabiliti nell'Unione[316]. Se il fornitore supera una di queste soglie, ha l'obbligo di notificarlo alla Commissione entro tre mesi, insieme a tutte le informazioni necessarie, cosicché questa possa pronunciarsi nel termine di due mesi, salvo che si dimostri il non realizzarsi della presunzione. La Commissione valuta la struttura concorrenziale del mercato e le caratteristiche del *gatekeeper,* potendo in ogni momento revocare la sua decisione e comunque dovendo operare un riesame, almeno ogni due anni, sul mantenimento dei criteri[317]. I soggetti identificati come *gatekeeper* devono sottostare a due liste di obbligazioni, che si applicano in automatico. La prima, cosiddetta *black list,* è costituita da sette obbligazioni dettagliate direttamente applicabili e che principalmente consistono in divieti, come quello di non combinare dati provenienti da diverse fonti. La seconda, denominata *grey list,* contiene undici obblighi più ampi, che necessitano l'ulteriore specifica in concreto della Commissione, alla luce dell'effettività e necessarietà della misura, in un dialogo col soggetto. Peraltro la Commissione può aggiornare la lista di obbligazioni mediante una clausola di flessibilità[318]. Le sanzioni che l'istituzione può imporre ai *gatekeeper* non *compliant* sono molto rilevanti, giungendo fino al 10% del fatturato totale dell'anno precedente, naturalmente con il

[314] ibidem, art. 2.

[315] ibidem, art. 3, comma 1.

[316] ibidem, art. 3, comma 2.

[317] ibidem, art. 4.

[318] ibidem, art. 10.

rispetto delle obbligazioni violate, con un ulteriore 5% di fatturato medio giornaliero come penalità di mora per ogni giorno di ritardo[319]. Come si è potuto notare, questo Regolamento opera un forte accentramento dei poteri in capo alla Commissione europea, vero fulcro del sistema che diventa così molto simile alla *Federal Trade Commission (FTC)* americana, riducendo di molto le attribuzioni delle autorità garanti della concorrenza nazionali, riunite in un comitato consultivo per i mercati digitali, organo appunto consultivo e di indirizzo, e in concreto lasciate ad occuparsi dei fenomeni locali[320]. La grande novità di questa disciplina è rappresentata dal passaggio da una regolamentazione *ex post* ad una *ex ante*, che permette così di razionalizzare l'*enforcement,* controllare meglio le condotte delle imprese dominanti e i loro effetti sulla concorrenza ed i consumatori, senza bisogno di accertare l'abusività della condotta o il danno a quest'ultimi. Si interviene così per risolvere le criticità incontrate nell'applicazione delle regole tradizionali alle peculiarità dei mercati digitali. L'obiettivo è quello di creare un modello europeo uniforme volto a regolare i giganti del *web* e le loro piattaforme, come avvenuto col GDPR nel settore della *data protection*[321]. Questa proposta è sicuramente un progresso importante della normativa *antitrust,* permettendo di rispondere in modo più adeguato ai mercati digitali, ma sono stati evidenziati dagli interpreti alcuni punti su cui agire per migliorare nella legislazione futura. Ad esempio il prof. Podszun propone di aumentare i poteri in capo alle autorità nazionali, stabilire più modalità attraverso cui i privati possono partecipare al processo di individuazione e controllo dei *gatekeepers,* restringere i termini in cui la Commissione deve agire e creare un meccanismo di emendamento rapido delle regole per mantenere costantemente aggiornate le regole, avulso da influenze politiche[322]. Questo è fondamentale affinché i consumatori siano davvero liberi nelle loro scelte, senza essere influenzati illecitamente dalle piattaforme che utilizzano, come anche

---

[319] ibidem, artt. 25-26.

[320] ibidem, artt. 32.

[321] Cfr. Gustavo Olivieri (n. 169), 374.

[322] Rupprecht Podszun, Philipp Bongartz, Sarah Langenstein, *Proposals on How to Improve the Digital Markets Act* (18 febbraio 2021), accessibile al sito https://ssrn.com/abstract=3788571. Inoltre la preoccupazione è che la qualità dei servizi digitali possa, nel breve periodo, diminuire in modo apprezzabile per le stringenti obbligazioni che il *DMA* pone alle piattaforme digitali qualificate come *gatekeepers*. Si veda ad esempio, Zach Meyers, *No pain, no gain? The Digital Markets Act,* Centre For European Reform, (Gennaio 2022).

affermato dal *Bundesgerichtshof* nel caso "*Facebook Germany"*[323]. Peraltro è interessante notare come in Germania, nel gennaio 2021, sia stato adottato il decimo emendamento al *GWB,* con previsioni dirette ad affrontare meglio le dinamiche dei mercati digitali in modo equivalente al DMA. Oltre alla sinergia tra legislatore e autorità tedesche che questa vicenda mette in luce, la riforma è diretta anche a mettere pressione al legislatore europeo nel contrasto ai *big tech.* Anche l'autorità garante della concorrenza italiana nel marzo 2021 ha proposto al governo una riforma del diritto *antitrust* sul modello tedesco. Passando invece a considerare il *Digital Service Act* (DSA)[324], essa consiste in una proposta di regolamento volta ad innovare il regime della Direttiva 2000/31/CE (cd. "direttiva *ecommerce")*, normativa che stabilisce la responsabilità dei fornitori di servizi della società dell'informazione, secondo la tripartizione tra *mere conduit, caching* e *hosting*[325]. La disciplina prevedeva l'esenzione da responsabilità ove le diverse tipologie di *provider* avessero avuto un comportamento non attivo in caso di attività o contenuti illeciti degli utenti, sancendo comunque la mancanza di un obbligo generale di controllo e perseguimento di questi[326]. Le regole sono state strutturate in questo modo, all'inizio degli anni duemila, per permettere la libera circolazione dei servizi digitali e il loro progresso, ma lo scenario ora è totalmente diverso. Per questo motivo il DSA, lasciando comunque in piedi la tripartizione della Direttiva *ecommerce,* prevede delle regole più stringenti per le piattaforme online, soprattutto per quelle di maggiori dimensioni, per il controllo dei contenuti pubblicati e la tutela degli utenti. All'art. 1 della proposta di regolamento, nello stabilire l'oggetto e l'ambito di applicazione della normativa, dopo aver affermato che lo scopo della riforma consiste nel

> "*contribuire al corretto funzionamento del mercato interno dei servizi intermediari e stabilire norme uniformi per un ambiente online sicuro, prevedibile e affidabile,*

[323] Rupprecht Podszun, *Digital Ecosystems, Decision-Making, Competition and Consumers – On the Value of Autonomy for Competition* (19 marzo 2019), consultabile presso https://ssrn.com/abstract=3420692 .

[324] Proposta di Regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali), COM/2020/825, [2020].

[325] Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), [2000], OJ L 178, 17.7.2000, p. 1–16 .

[326] ibidem, art. 15.

in cui i diritti fondamentali sanciti dalla Carta siano tutelati in modo effettivo"[327], si enuncia che il regolamento "*stabilisce in particolare: a) un quadro per l'esenzione condizionata dalla responsabilità dei prestatori di servizi intermediari; b) norme relative a specifici obblighi in materia di dovere di diligenza adattati a determinate categorie di prestatori di servizi intermediari; c) norme sull'attuazione e sull'esecuzione del presente regolamento, anche per quanto riguarda la cooperazione e il coordinamento tra le autorità competenti*"[328].

Lasciando, come già detto, in vigore la tripartizione della direttiva *ecommerce,* vengono introdotte delle obbligazioni progressive e proporzionate applicabili in base alle loro dimensioni ed al loro *status.* A seguito di previsioni destinate a tutti gli intermediari che forniscono servizi della società dell'informazione, principalmente consistenti in obblighi di trasparenza (artt. 10-13), la normativa contiene regole per i servizi di *hosting* (artt. 14-15), per le piattaforme *online* (artt. 16-24) ed infine per piattaforme online di grandi dimensioni (artt. 25-33), cioè quelle con più del 10% dei 450 milioni di consumatori europei[329]. Tra gli obblighi delle piattaforme di grandi dimensioni più interessanti troviamo quello di valutare ogni anno i rischi sistemici dall'uso dei loro servizi, contenuto dell'art. 26[330], l'adozione di misure volte ad attenuare i rischi individuati, *ex* art. 27[331], e la necessità di *audit* annuali indipendenti per il controllo del

---

[327] Proposta di Regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali), COM/2020/825, [2020], art. 1, comma 2.

[328] ibidem, art. 1.

[329] ibidem. Si veda inoltre, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_it .

[330] ibidem, art. 26. Tra i rischi l'articolo 26 cita espressamente "*la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi per l'esercizio dei diritti fondamentali al rispetto della vita privata e familiare e alla libertà di espressione e di informazione, del diritto alla non discriminazione e dei diritti del minore, sanciti rispettivamente dagli articoli 7, 11, 21 e 24 della Carta; c) la manipolazione intenzionale del servizio, anche mediante un uso non autentico o uno sfruttamento automatizzato del servizio, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori, del dibattito civico, o con effetti reali o prevedibili sui processi elettorali e sulla sicurezza pubblica*".

[331] ibidem, art. 27. Esempi di misure, nominate dall'art. 27, sono "*a) l'adeguamento dei sistemi di moderazione dei contenuti o di raccomandazione, dei loro processi decisionali, delle caratteristiche o del funzionamento dei loro servizi, o delle loro condizioni generali; b) misure mirate volte a limitare la visualizzazione della pubblicità associata al servizio de esse prestato; c) il rafforzamento dei processi*

rispetto delle previsioni, stabilita dall'28[332]. Anche questa normativa attribuisce maggiori poteri di vigilanza ed *enforcement* in capo alla Commissione europea, vera garante del sistema e protagonista della risposta europea ai mercati digitali e ai *big tech.* La proposta, nonostante le molte novità, richiede ulteriore modifiche e perfezionamenti, ed attualmente è in atto il processo legislativo a livello europeo per migliorarne le previsioni, nell'ottica di una maggiore efficacia e di tutela delle piccole-micro imprese europee[333]. In ogni caso anche questa riforma rappresenta una risposta risoluta ai problemi sorti negli ultimi anni con le piattaforme digitali. Degna di nota è anche la recentissima proposta di regolamento della Commissione per l'armonizzazione delle regole europee sull'accesso e lo sfruttamento dei dati (cosiddetto "*Data Act")*[334]. Questa proposta, datata 23 febbraio 2022, punta a rafforzare ulteriormente il *framework* europeo in tema di dati, prevedendo norme volte ad aumentare la certezza giuridica e regolare le relazioni tra i soggetti pubblici e privati ed i consumatori, migliorando la protezione di questi ultimi, spesso privi di forza contrattuale[335]. Vengono anche introdotte nuove previsioni per consentire alle autorità pubbliche di accedere ai dati in possesso dei privati per motivi di interesse pubblico, permettendo ai consumatori di poter cambiare *provider* di servizi digitali con più facilità. È inoltre innovato il regime della direttiva 96/9/CE in materia di protezione dei *database*[336]. Viene aggiunto così un nuovo, importante, tassello alla strategia europea sui dati e all'evoluzione digitale dell'Unione[337].

---

interni o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici; IT 65 IT d) l'avvio o l'adeguamento della cooperazione con i segnalatori attendibili in conformità all'articolo 19; e) l'avvio o l'adeguamento della cooperazione con altre piattaforme online attraverso i codici di condotta e i protocolli di crisi di cui rispettivamente agli articoli 35 e 37".

[332] ibidem, art. 28.

[333] Cfr. Enzo Mazza, *Digital Service Act (DSA): i nodi che restano dopo l'Ok del Parlamento Ue,* Agenda digitale, 21 gennaio 2022. Per un *overview* sulle proposte di modifica della dottrina: Mikolaj Barczentewicz Mikolaj, *The Digital Services Act: Assessment and Recommendations*, (27 giugno 2021).

[334] Proposta di Regolamento relativo a regole armonizzate sull'accesso e l'uso dei dati (*Data Act)*, COM/2022/68 final, [2022].

[335] ibidem.

[336] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, [1996], OJ L 77, 27.3.1996, p. 20–28.

[337] Per ulteriori approfondimenti:

https://digital-strategy.ec.europa.eu/en/policies/data-act .

8. (*Segue:)* Centralità dei diritti costituzionali come fondamento delle riforme europee

Cercando di individuare *fil rouge* dietro le recenti iniziative legislative europee, ciò che traspare è una precisa strategia normativa e politica dell'Unione. Questo indirizzo programmatico è rinvenibile nella recentissima proposta della Commissione europea per una "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale", adottata il 26 gennaio 2022[338]. Al punto 1 del preambolo si legge che

> *"la trasformazione digitale interessa ogni aspetto della vita delle persone. Offre notevoli opportunità in termini di miglioramento della qualità della vita, innovazione, crescita economica e sostenibilità, ma presenta anche nuove sfide per il tessuto, la sicurezza e la stabilità delle nostre società ed economie. Con l'accelerazione della trasformazione digitale è giunto il momento che l'Unione europea (UE) specifichi come si dovrebbero applicare i suoi valori e diritti fondamentali nel mondo online"[339], specificando poi ai punti 5 e 6 che "la dichiarazione mira a illustrare le intenzioni politiche comuni. Non solo ricorda i diritti più pertinenti nel contesto della trasformazione digitale, ma dovrebbe anche fungere da punto di riferimento per le imprese e altri soggetti interessati nello sviluppo e nella diffusione di nuove tecnologie. La dichiarazione dovrebbe inoltre guidare i responsabili politici nella riflessione sulla loro visione della trasformazione digitale: una trasformazione digitale che mette al centro le persone; che si basa sulla solidarietà e sull'inclusione; che ribadisce l'importanza della libertà di scelta; che promuove la partecipazione allo spazio pubblico digitale; che garantisce la sicurezza, la protezione e il conferimento di maggiore autonomia e responsabilità, e la sostenibilità. È opportuno rafforzare ulteriormente il controllo democratico della società e dell'economia digitali, nel pieno rispetto dei principi dello Stato di diritto, di una giustizia efficace e dell'applicazione della legge"[340].*

---

[338] Dichiarazione della Commissione sui diritti e i principi digitali per il decennio digitale, COM(2022) 28 final [2022].

[339] ibidem, punto 1 del preambolo.

[340] ibidem, punti 5-6 del preambolo. Illuminanti sono anche le dichiarazioni di Margrethe Vestager in occasione della proposta: "*Vogliamo tecnologie sicure che servano alle persone e che rispettino i nostri*

È rilevante che in questa proposta che mira a fissare i punti fermi dell'azione europea dei prossimi anni, nell'ambito della propria trasformazione digitale, si parli dell'"*l'importanza della libertà di scelta"*[341] e di "*rafforzare ulteriormente il controllo democratico della società e dell'economia digitale"*[342]. Questa scelta è giustificata dall'ormai matura consapevolezza degli interrogativi e dei pericoli posti dall'ecosistema digitale. Dopo anni di liberismo e *laissez-faire* nel settore digitale, volti ad incentivare lo sviluppo degli emergenti mercati tecnologici ed il loro progresso innovativo, si è giunti all'inedita situazione di soggetti privati con un potere di natura sempre più pubblicistica. La sottile linea tra il potere economico di questi giganti tecnologici ed il concetto di "sovranità", proprio del diritto pubblico, sta lentamente svanendo ed a riprova di questa nuova veste ibrida sono stati istituiti organi interni alle piattaforme diretti alla risoluzione delle controversie che possono sorgere, come una sorta di giurisdizione privata (autodefinita autonoma e indipendente), però in grado di incidere fortemente sui diritti costituzionalmente garantiti[343]. Ciò ha stravolto profondamente l'approccio interpretativo di diritto costituzionale, orientato alla regolazione del rapporto tra potere statale ed individuo, per la prima volta portato ad affrontare l'influenza del potere privato sui diritti fondamentali[344]. La vicenda di *Cambridge Analytica* ha mostrato la fragilità dei diritti delle persone in rete e la magnitudine dei danni causati alle democrazie mondiali dall'abuso delle piattaforme digitali. La preoccupazione sempre più forte delle istituzioni ad ogni livello è che i dati degli individui vengano utilizzati per esercitare un'influenza illecita su di essi, sfruttando la profilazione e la raccolta massiva di informazioni ad opera degli algoritmi per spingere gli utenti a compiere azioni non autonome, violando la loro capacità di autodeterminazione e incidendo su

---

diritti e valori. Anche quando siamo online. E vogliamo che tutti abbiano la possibilità di svolgere un ruolo attivo nelle nostre società sempre più digitalizzate. Questa dichiarazione ci fornisce un chiaro punto di riferimento sui diritti e i principi del mondo online".

[341] ibidem.

[342] ibidem.

[343] Cfr. Federica Resta, *I poteri privati e gli arbitri dei diritti,* Medialaws, (1 dicembre 2020). L'esempio più eclatante è l'*Oversight Board* istituito da *Facebook* per le controversie riguardanti i contenuti della piattaforma (https://oversightboard.com/) . Per un interessante approfondimento si veda l'intervento sul tema di Ginevra Cerrina Feroni, accessibile al sito: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9542545 .

[344] ibidem.

fasi fondamentali della vita sociale e democratica, come le elezioni politiche[345]. Proprio il *focus* sulla tutela della dignità umana è stato il punto centrale della decisione del *Bundesgerichtshof* sul caso "*Facebook Germany",* in cui la Corte ha dato voce al cambio di paradigma in atto sull'interpretazione dei diritti costituzionalmente garantiti nell'economia digitale. In essa è infatti stabilito che

> "*the right to informational self-determination does not entail a general, or indeed comprehensive, right to determine the use of one's data. It does, however, guarantee individuals the possibility of influencing, in a differentiated manner, the context and the way in which their personal data are made available to and used by others. In other words, individuals are guaranteed the right to be substantially involved in the decision as to which characteristics can be ascribed to them. This constitutional guarantee also has an impact on legal relationships under private law and must be taken into account in the interpretation of general clauses under civil law to which Section 19 GWB also belongs. The fact that fundamental rights have an impact in civil law as constitutional value decisions that have to be upheld does not mean that their requirements under civil law are always less far-reaching or less demanding than their protective effects directly directed at the state.* ***Depending on the circumstances, especially when a private company – as in this case – gains a dominant position and provides the very framework in which public communication takes place, private companies can be bound by fundamental rights to a similar or equal extent as the state.*** *In such a case, strict structural requirements regarding the processing of data and limitations in relation to the purpose for which they may be used – in particular in connection with a requirement to obtain consent – can be an adequate or possibly even constitutionally required means to protect the right to informational selfdetermination"*[346].

---

[345] Cfr. Daniel Susser, Beate Roessler, Helen Nissenbaum, *Technology, autonomy, and manipulation,* Internet Policy Review, 8(2), (2019), 2-4. Per un approfondimento sul tema della manipolazione si veda: Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs,(2019).

[346] Bundesgerichtshof, decisione KVR 69/19, [2020], para 104- 105. Traduzione di cortesia fornita dal *Bundeskartellamt.* Per approfondimento, Rupprecht Podszun, *Facebook case: the reasoning,* D'Kart, Antitrust Blog (28 agosto 2020).

I diritti fondamentali cristallizzati nelle carte costituzionali hanno, in base all'interpretazione tradizionale, solamente efficacia verticale, nei confronti dello stato[347]. Nella decisione rivoluzionaria del *Bundesgerichtshof,* invece, è affermata senza veli la possibilità che un soggetto privato accentri così tanto potere economico, diventando talmente dominante, da essere trattato al pari di uno stato, con il discendente obbligo di rispettare i diritti fondamentali, tra cui primeggia quello alla *privacy.* Per la Corte Federale Tedesca, in pratica, non è in gioco soltanto la protezione dei dati degli utenti, la loro tutela in quanto consumatori e la concorrenza del mercato, ma la stessa democrazia, la dignità inviolabile della persona e le basi su cui si fonda la nostra società democratica, profili che traspaiono anche nell'iniziale denuncia del *Bundeskartellamt.* In quest'ottica, con un approccio di matrice ordoliberale, le regole poste a tutela della *privacy* e della concorrenza divengono il *medium* per la protezione di diritti e valori fondamentali, trascendendo i singoli obiettivi delle discipline e concorrendo alla garanzia della *big picture.* Di fronte a questo nuovo "leviatano" è in corso una rivisitazione delle categorie giuridiche e filosofiche tradizionali, portando gli studiosi costituzionalisti ad interrogarsi sull'applicazione orizzontale dei diritti fondamentali. Come afferma Robert Alexy[348], per ogni diritto diritto fondamentale può riconoscersi una duplice dimensione: una verticale, nei confronti dello stato e della sua autorità, ed una orizzontale, tra privati[349]. Se in origine la seconda veniva esclusa, l'evoluzione economica e sociale ha richiesto un cambio di paradigma, spingendo per la rilevanza dei diritti costituzionalmente garantiti anche nei confronti di soggetti privati. Data la dimensione globale delle piattaforme digitali e della loro influenza, purtroppo l'interpretazione non è sempre uniforme. Se in Europa Corti, autorità di settore ed istituzioni si stanno muovendo in questa direzione, negli Stati Uniti si è restii a riconoscere la suddetta efficacia orizzontale. La ragione di questa differente visione risiede nella differente matrice storica da cui è scaturito il costituzionalismo americano, in cui l'accento sull'autonomia privata e la libertà individuale nei confronti dello stato[350]

---

[347] Cfr. Giorgio Pino, *Il costituzionalismo dei diritti*, Il Maulino, (2017).

[348] Cfr. Robert Alexy, *Teoria dei diritti fondamentali*, Bologna, (2012).

[349] Cfr. Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018), 1-2.

[350] Originario nemico dei primi padri pellegrini americani.

è talmente marcato da impedire l'applicazione tra privati dei diritti costituzionali. Ciò può essere sintetizzato nelle parole del costituzionalista di Harvard Mark Tushnet, che afferma: *"judicialisation of relations between private persons is as an intolerable intrusion of the State into the sphere of private autonomy"*[351]. L'eclatante testimonianza è come l'applicazione della libertà d'espressione, garantita dal I Emendamento alla Costituzione americana, venga negata dalla cd. *state action doctrine*[352] nelle relazioni *inter privatos,* poiché i diritti e le libertà garantiti dalla *Bill of Rights* hanno come unica controparte lo stato, data l'intangibilità della sfera di autonomia degli individui[353]. Alla luce di questa differenza e della primaria importanza, negli *US,* del *freedom of speech*[354]*,* deve leggersi il triste episodio dell'assalto al Campidoglio americano del gennaio 2021. In Europa, differentemente, nonostante la grande considerazione della suddetta libertà, il diritto alla *privacy* e alla tutela della dignità umana, reazione ai soprusi dei regimi nazifascisti del secolo scorso, rappresenta il valore fondante delle Costituzioni e delle carte dei diritti internazionali, non sacrificabile nel bilanciamento con altri diritti[355]. La CGUE si è rivelata molto ricettiva ed attenta sul tema, mostrando propensione all'affermazione dell'efficacia orizzontale dei diritti stabiliti nella CDFUE, primo tra tutti il diritto alla *privacy ex* artt. 7-8 della Carta, appunto. Questo approccio traspare dal già citato caso *Google Spain,* in cui la decisione di applicare il diritto all'oblio

---

[351] Mark Tushnet, *The Issue of State Action/Horizontal Effect in Comparative Constitutional Law*, *International Journal of Constitutional Law*, 1, (2003); Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018), 3-4.

[352] Si veda, Wilson R. Huhn, *The State Action Doctrine and The Principle of Democratic Choice,* in *Hofstra Law Review*, 84, 2006; Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018), 2.

[353] *Bill of Rights*, *General Records of the United States Government,* record Group 11, [1789]. Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018), 2.

[354] Di cui giova ricordare la grande importanza storica per i cittadini americani, date le persecuzioni religiose e politiche che hanno spinto i primi coloni a lasciare il vecchio continente.

[355] Cfr. Oreste pollicino, *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali le sfide per il giurista (teorico e pratico)?,* Giustizia insieme, (15 aprile 2021), accessibile al link: https://www.giustiziainsieme.it/it/attualita-2/1671-l-algoritmo-e-la-nuova-stagione-del-costituzionalismo-digitale-quali-le-sfide-per-il-giurista-teorico-e-pratico .

contenuto nella direttiva 95/46, riflesso del più generale *right to privacy,* nei confronti di *Google*, soggetto di natura privata, implicitamente manifesta la necessità di intervenire per contrastare il potere non più solamente economico delle piattaforme e dei *big tech*[356]. L'indirizzo ora illustrato sta venendo perseguito, oltre che dalle istituzioni europee, dai legislatori e dalle corti nazionali[357]. Sulla scia di questo nuovo "costituzionalismo digitale", il pacchetto di riforme dell'UE diretto ad adeguare il sistema europeo all'economia digitale, soprattutto mediante il *DMA* ed il *DSA,* mira a superare le due principali debolezze che hanno reso meno efficace la strategia dell'Unione negli anni passati: il *laissez-faire* nei confronti dei *big tech* e la frammentarietà delle normative parte della strategia sul mercato unico digitale[358]. L'arma principale per combattere i giganti tecnologici in questa nuova fase è rappresentata dalle regole procedurali. Il Costituzionalismo digitale ha infatti nella procedura lo strumento per la tutela dei diritti fondamentali degli individui in rete, ad esempio con i più stringenti obblighi di trasparenza imposti dal *DSA* e dal *DMA*[359]. In realtà questa idea non è affatto nuova, poiché già negli anni Ottanta il grande giurista e filosofo Norberto Bobbio affermava la necessità di eliminare, attraverso la maggiore trasparenza, i "poteri occulti" che tentano di minare la sovranità dello stato[360]. Mediante questa ricostruzione e con il supporto dei recentissimi strumenti normativi adottati a livello europeo, sarà finalmente possibile affrontare con maggiore efficacia le sfide del digitale e gli abusi dei *big tech.* Per quanto il problema sia di rilevanza mondiale, già

---

356 Cfr. Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018), 24-25.

357 Come nel caso delle recenti riforme tedesche e francesi contro le *hate speech* sui *social network* (per approfondimenti si veda, Federica Resta, *I poteri privati e gli arbitri dei diritti,* Medialaws, (1 dicembre 2020).

Perfino nei paesi ex comunisti dell'Est Europa è in atto questo processo, Cass R. Sunstein, *Against Positive Rights Feature*, 2 East European Constitutional Review 35 (1993); Si veda, GCR, *Europe, Middle East And Africa Antitrust Review 2021,* (2021) accessibile al sito: https://globalcompetitionreview.com/review/the-european-middle-eastern-and-african-antitrust-review/2021.

358 Cfr. Oreste pollicino (n. 329).

359 ibidem.

360 ibidem. Si veda anche Editori de "La Stampa", *Norberto Bobbio, il segreto della democrazia: non avere segreti,* La Stampa (16 ottobre 2011).

con il GDPR l'Unione ha confermato l'obiettivo di estendere la tutela dei dati personali dei cittadini europei all'esterno del suo territorio, con efficacia globale, come risulta anche dai due casi *Schrems*. Con l'utilizzo delle regole a protezione della concorrenza, invece, verranno affrontate le distorsioni interne al mercato europeo, dannose per le imprese ed i consumatori, in modo da mantenere l'ecosistema economico e giuridico sano e sostenibile. Grazie a questo approccio sinergico tra *data protection* e diritto *antitrust,* con al centro una nuova visione dei diritto costituzionale adattato al mondo digitale e la non sacrificabilità della dignità umana nel confronto con l'iniziativa ed il potere economico delle grandi piattaforme, di natura ormai semi-pubblicistica, l'Unione Europea sta entrando in una nuova fase rivoluzionaria in cui verranno poste le basi per la creazione di una società digitale veramente inclusiva e rispettosa dei valori fondanti europei[361].

9. *Data protection* e diritto *antitrust* nell'approccio ai *big tech* di Stati Uniti, Cina e Russia. Previsioni sul futuro.

I dati personali, le piattaforme digitali e l'affermarsi dei *big tech* rappresentano, per le loro caratteristiche peculiari, un fenomeno che va ben oltre i confini dei singoli paesi. Ogni nazione, in base alla propria visione politica e al proprio sistema giuridico, ha adottato un approccio diverso, ma vista la globalità della questione le singole misure hanno un'efficacia limitata. La necessità che si fa sempre più forte è quella di un approccio internazionale concordato, capace di regolare i singoli aspetti giuridici, economici e sociali emersi. Per questo motivo non è possibile prescindere da un'analisi comparatistica delle soluzioni normative trovate dai maggiori *player* internazionali, osservandone i punti di forza e le falle, nell'attesa di un tale *framework* comune. In particolare, analizzate le previsioni principali dell'Unione europea, è interessante considerare gli strumenti giuridici adottati da Stati Uniti, Cina e Russia. Incominciando dagli *USA,* la tematica li tocca da vicino poiché le GAFAM e gli altri principali *big tech,* con i loro servizi e le loro piattaforme, sono tutti americani. Questo elemento ha

[361] Cfr. Giovanni De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, International Journal of Constitutional Law, 2020, 41-70. Ma ancora, Giovanni De Gregorio, Oreste Pollicino, *The European Constitutional Road to Address Platform Power, VerfBlog,* (31 agosto 2021), accessibile al sito: https://verfassungsblog.de/power-dsa-dma-03/ .

caratterizzato la risposta normativa nei loro confronti, con il diritto inesorabilmente legato all'amministrazione politica. Sul fronte della *data protection* è stata accennata la frammentarietà della disciplina, priva di una normativa unica a livello federale. L'approccio minimalista americano alla protezione dei dati personali è profondamente diverso da quello europeo, più garantista, così come sono diverse le radici filosofiche e ideologiche poste alla sua base. In Europa la protezione dei dati personali è un diritto costituzionalmente riconosciuto, contenuto nei trattati e poi affermato nei singoli dettagli dai vari atti legislativi, mentre negli *USA* essa è tutelata parzialmente dalle regole poste a protezione dei consumatori. A livello costituzionale, il Quarto Emendamento protegge cittadini e residenti americani da interferenze statali nella loro vita personale, senza però affermare un vero e proprio diritto alla *privacy*[362]. La mancanza di uno specifico diritto costituzionalmente garantito ha fatto sì che la protezione fosse suddivisa in tanti atti legislativi settoriali, come il *Privacy Act* del 1974 relativo alla raccolta di informazioni da parte delle autorità governative[363], generando un sistema complesso, di difficile applicazione e spesso inadeguato, come riconosciuto anche dal Gruppo di lavoro Articolo 29 (ora sostituito dall'EDPS)[364]. Tutto ciò rende difficile affrontare la raccolta massiva di dati da parte di enti pubblici e privati, il loro sfruttamento ed i possibili abusi[365]. Nonostante le poche iniziative legislative a livello federale, i singoli stati americani negli ultimi anni hanno iniziato a dotarsi di un proprio apparato di norme sulla *data protection,* tra cui spicca sicuramente il *California Consumer Privacy Act* (CCPA), adottato nel 2018 e entrato in vigore nel 2020[366]. Ispirata al GDPR europeo, con l'affermazione dei suoi principi fondamentali e dei diritti riconosciuti agli interessati, seppure in modo più vago, molteplici sono le peculiarità che lo caratterizzano. *In primis* si tratta di una legge a tutela dei consumatori stabiliti nello stato della California, perciò il campo di applicazione è molto più limitato rispetto

[362] Si nota perciò anche un campo di applicazione più ristretto, limitato solamente a cittadini e residenti americani, a differenza della previsione ampia del GDPR che protegge qualsiasi persona fisica identificata o identificabile.

[363] Privacy Act , 5 U.S.C., [1974], § 552a.

[364] Gruppo di lavoro Articolo 29, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government,* (dicembre 1999).

[365] Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?*,Colorado Technology Law Journal, Vol. 18, No. (1, 2020), 107-116.

[366] California Consumer Privacy Act (CCPA), [2018]. https://oag.ca.gov/privacy/ccpa .

al GDPR. Non si fa riferimento ai dati come definiti dalla normativa europea, bensì alle "*personal information"* che permettono di individuare i consumatori o le loro famiglie. Non è richiesta la presenza di una base giuridica per il trattamento e la regola generale è la liceità di tutti i trattamenti, salvo quelli che possono ledere i diritti dei consumatori. Le previsioni si applicano alle imprese stabilite in California che superano determinate soglie di fatturato e dimensioni, senza applicazione extraterritoriale. Nonostante le differenze rispetto alla normativa Ue, il CCPA costituisce un grande passo in avanti per la tutela della *privacy* della California ed anche un catalizzatore per l'adozione di normative simili negli altri stati americani, introducendo regole più chiare, unitarie e stringenti, soprattutto relativamente agli obblighi di informazione delle imprese e delle misure da adottare in caso di *data breach*[367]. Recentemente anche a livello federale sta maturando l'idea di adottare una normativa uniforme per la tutela dei dati personali, perciò l'auspicio è di vedere nei prossimi anni approvata una disciplina centrale capace di dare maggiore certezza e aumentare l'attuale livello di protezione[368]. Sul versante *antitrust,* invece, la situazione è ancor di più legata alla politica. Negli ultimi anni, sotto l'amministrazione Trump, l'approccio è stato molto blando e accomodante, in un'ottica nazionalistica. Diversamente, la nuova amministrazione Biden sembra aver adottato un cambio di passo, schierandosi apertamente contro l'eccessivo potere dei *big tech,* per i rischi da questi posti alla democrazia e ai diritti costituzionalmente garantiti. Iconica è la nomina nel giugno 2021 di Lina M. Khan, giurista famosa per le sue forti posizioni critiche contro i giganti del *web* e autrice del celeberrimo articolo "*Amazon's Antitrust Paradox"*[369]*,* a presidente della *FTC,* l'autorità statunitense posta a garanzia della concorrenza e dei consumatori. Proprio questa autorità si sta schierando con fermezza contro i *big tech*, muovendo investigazioni e procedimenti nei loro confronti. Un esempio è la denuncia contro *Facebook* nell'agosto 2021 per la sua strategia di *killer acquisitions* volta ad eliminare i concorrenti dal mercato, portatori di innovazione,

[367] Emmanuel Pernot-Leplay (n. 229), 118-124.

[368] Riccardo Berti, *Privacy, la strada degli USA verso la prima norma federale,* Agenda Digitale, (25 marzo 2021), consultabile al sito https://www.agendadigitale.eu/sicurezza/privacy/privacy-la-strada-degli-usa-verso-la-prima-norma-federale/.

[369] Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L. J. (2017).

fagocitandoli[370]. La causa è ancora solo agli inizi, ma è importante il netto cambio di strategia della *FTC* e delle istituzioni americane, riconoscendo la necessità di agire repentinamente per fronteggiare i pericoli che i giganti digitali pongono alla democrazia. Passando a considerare il panorama normativo in Cina sulla *data protection* e i rapporti con i *big tech,* è interessante notare come l'approccio cinesi rappresenti una "terza via" rispetto il modello garantista europeo e quello minimalista statunitense. Lo sviluppo del concetto di *privacy,* insieme al diritto ad esso associato e alle relative regole, è molto recente. A differenza di Stati Uniti e Unione europea, che già negli anni settanta-ottanta iniziarono a sviluppare un primo *framework* sulla tutela della *privacy,* partendo dalle linee guida in materia pubblicate dall'OECD[371], in Cina il contesto culturale e ideologico, unito alla struttura principalmente rurale del paese, ha rappresentato un ostacolo per l'evoluzione del settore. I Principi Generali del Diritto Civile cinese (GPCL)[372] del 1986 proteggevano soltanto il diritto alla reputazione e solo nel 2017 sono stati aggiornati, prevedendo all'art. 111 regole a tutela delle informazioni personali[373]. In campo penale, la Legge penale cinese protegge, all'art. 252, il diritto alla segretezza della corrispondenza, mentre all'art. 2 della Legge sulla Responsabilità Extracontrattuale cinese (2010) è specificamente previsto il diritto alla *privacy*[374]. Il

---

370 https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush .

371 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (1980).

372 Principi Generali del Diritto Civile della Repubblica Popolare Cinese, [1986].

373 ibidem, art. 111: *"The personal information of natural persons is protected by law. Where any organization or individual needs to obtain someone else's personal information, they shall obtain it in accordance with law and ensure information security; they must not unlawfully collect, use, process, or transfer the personal information of others, and must not unlawfully buy, sell, provide or disclose others' personal information".*

374 Legge Penale della Repubblica democratica cinese [1979]. Art. 252, come modificato dal VII emendamento [2009]*: "Whoever conceals, destroys or unlawfully opens another person's letter, thereby infringing upon the citizen's right to freedom of correspondence, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of no more than one year or criminal detention".*

Legge sulla Responsabilità Extracontrattuale cinese [2010], art. 2: "*Civil rights' as mentioned in this Law refer to personal and property rights and interests, including, inter alia, the right to live, right to health, right of name, right of reputation, right of honor, right to portrait, right to privacy, right of self-determination in marriage, guardianship, ownership usufructuary right, real right for*

paese negli anni ha potuto ispirarsi agli strumenti giuridici già utilizzati in Europa e negli *USA*, ma a partire dal 2010 ha cominciato a delineare il proprio peculiare approccio alla protezione dei dati personali[375]. Questo si basa su tre normative, risultato di questo graduale processo legislativo: la Legge sulla cybersicurezza (CLS) del 2016, la Legge sulla protezione delle informazioni personali (PIPL) e la Legge sulla sicurezza del dati (DSL), entrambe del 2021. La prima ha l'obiettivo di rafforzare lo spazio digitale cinese, renderlo più sicuro e razionalizzare le regole già esistenti in materia, in modo da essere al passo con i paesi stranieri. La PIPL rappresenta un'evoluzione della CLS, potenziando gli strumenti giuridici e ampliandone il campo di applicazione. Gli obiettivi perseguiti da quella normativa sono principalmente tre, cioè la protezione dei cittadini cinesi dalle condotte abusive che possono interessare le loro informazioni personali, lo stimolo al miglioramento della legislazione sulla *data economy* e infine la tutela degli interessi pubblici definiti dallo stato. Essa si applica a tutti i soggetti che processano informazioni personali, compresi gli organi governativi ove ciò non sia possibile per questioni di segretezza, introducendo la necessaria presenza del consenso degli interessati o di un'altra base giuridica giustificata, come in caso di interessi pubblici insuperabili. Le previsioni sono di chiara ispirazione europea, così come la rilevanza extraterritoriale delle norme, distinguendosi però per la più vaga affermazione dei principi e dei diritti riconosciuti dal GDPR, che nella normativa in analisi sono ristretti al diritto alla cancellazione dei dati e di rettifica, mentre gli altri solo raccomandati. Rilevanti sono anche le regole volte a contrastare le decisioni algoritmiche automatizzare e lo sfruttamento delle informazioni da parte dei giganti tecnologici. Mentre questa disciplina si concentra sul rapporto tra interessati e coloro che processano i dati, la DSL mira a perseguire la sicurezza nazionale. Loquace è in tal senso è il ruolo del Consiglio per la Sicurezza Nazionale cinese come principale promotore e garante del suo sviluppo legislativo. La normativa prevede la protezione di diverse categorie di informazioni personali suddivise per importanza, con all'apice i "*core national data",* le informazioni di interesse nazionale il cui uso illecito è pesantemente punito. Le definizioni contenute nelle norme sono molto ampie, così come ampio è il concetto di "informazioni personali", perciò alle articolazioni territoriali dello stato è affidato il compito di armonizzare e applicare le regole. Tutto

security, copyright, patent right, exclusive right to use trademark, right of discovery, stock rights, and right of inheritance".

[375] Emmanuel Pernot-Leplay (n. 229), 70-91.

questo si inscrive nel più ampio disegno del paese di affermare la propria sovranità nazionale, anche nella *data economy,* inasprendo le misure contro i giganti *tech* cinesi, prima molto blande[376]. Considerando, infine, la situazione normativa in Russia, la situazione è ovviamente molto simile all'Unione Europea. Il paese è infatti parte del Consiglio d'Europa e firmataria della Convenzione n. 108, che come si è osservato trattando dell'evoluzione normativa europea, ha posto le basi per la prima affermazione dei principi e dei diritti propri della *data protection.* Grazie a questo trattato è perciò presente un substrato di previsioni che costituiscono il panorama in cui devono muoversi i trattamenti dei dati personali. Anche qui sono contenute regole sul rispetto della *privacy* in norme dei diversi settori del diritto, come l'art. 150 del codice civile russo o l'art. 137 del codice penale[377], mentre la disciplina centrale è rappresentata dalla Legge della Federazione Russa No. 152 FZ sui dati personali del 2006 (DPA), dove viene confermato quanto stabilito nella Convenzione 108[378]. Nonostante questo apparato normativo e le misure tecniche adottate per lo *storage* e la sicurezza dei dati, diverse sono le problematiche create dallo sfruttamento dei *Big data.* Per quanto i dati vengono anonimizzati o conservati in modo che non sia possibile risalire alle persone interessate, la combinazione di diversi *database* e l'utilizzo di avanzati algoritmi di *data mining* possono vanificare gli sforzi delle autorità, senza considerare come i lunghi tempi di conservazione aumentino il rischio di *data breach*[379]. Anche per questo motivo la Russia sta puntando, come tutti gli altri grandi *player* internazionali, a regole più severe contro

---

[376] Cfr. Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?,* Penn State Journal of Law & International Affairs, Vol. 8, No. 1, (2020). Per un approfondimento: Franco Pizzetti, *Il nuovo approccio cinese e l'importanza di un mercato unico digitale globale,* Agenda Digitale (27 agosto 2021), consultabile al sito, https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-sicurezza-dei-dati-pizzetti-limportanza-del-sistema-cinese-nello-scenario-globale/ .

[377] Codice civile della Federazione Russa [1994], art. 150. Codice penale della Federazione Russa [1996], art. 137.

[378] Legge della Federazione Russa No. 152 FZ [2006]. Interessante notare che nel 2014 la legge sia stata emendata, stabilendo la necessità di conservare i dati personali unicamente nei server russi. Per approfondimento: https://www.dlapiperdataprotection.com/index.html?t=law&c=RU#:~:text=The%20amendments%20require%20all%20personal,handling%20of%20Russian%20personal%20data. .

[379] Cfr. Anna Konstantinovna Zharova, Vladimir Mikhailovich Elin, *'The use of Big data: a Russian perspective of personal data security',* 33 Computer Law & Security Review, (2017), 482- 501.

i giganti del *web*[380]. Ora, giunti a questo punto della trattazione, è possibile trarre delle conclusioni e tentare di anticipare i *trend* e gli scenari che possono realizzarsi nel prossimo futuro. Nel corso dell'elaborato si è fatto cenno agli elementi principali della *data economy,* alle piattaforme digitali che la caratterizzano e ai modelli di *business* delle imprese che le gestiscono. Più volte si è evidenziata la centralità del dato nell'economia odierna e le potenzialità dirompenti dei *Big data* per cittadini, imprese ed intere nazioni. Non è possibile dubitare della sempre maggiore importanza che rivestiranno i dati ed il digitale, diventando il centro propulsivo delle economie mondiali. Se negli scorsi decenni l'approccio adottato dalla maggioranza dei *player* internazionali è stato un *laissez-faire* giustificato dalla novità del fenomeno e dalla poca comprensione dei suoi meccanismi, così come dei relativi effetti sulla società e i mercati, recentemente l'approccio è totalmente cambiato. Lo strapotere dei *tech giants* non è più tollerato, neppure dagli Stati Uniti che lo hanno sempre favorito, ed il tempo delle legislazioni accomodanti è terminato, perché si sono compresi i rischi che questa stortura del sistema può generare. La strada maestra è indicata con chiarezza nella proposta della Commissione per il "Decennio digitale europeo", un dichiarazione contenente la *vision* che ispirerà l'azione dell'UE negli anni a venire[381]. Gli obiettivi perseguiti sono la digitalizzazione di imprese e servizi pubblici, la creazione di infrastrutture digitali e di competenze in materia che possano portare l'Unione ad essere all'avanguardia nel panorama internazionale, sempre con al centro i diritti delle persone[382].

In quest'ottica, le regole sulla protezione dei dati personali ed il diritto *antitrust* rappresentano e rappresenteranno sempre di più i principali argini di contenimento degli abusi della *data economy*. Per le differenze tra le due normative, c'è sempre stata una separazione piuttosto netta tra i loro campi d'applicazione e le loro norme, ma con i

---

[380] Fonte: https://www.competitionpolicyinternational.com/russia-regulators-to-crack-down-on-us-big-tech-in-2020/ .

[381] Proposta di decisione del Parlamento europeo e del Consiglio, che istituisce il programma strategico per il 2030 "Percorso per il decennio digitale", COM/2021/574 final, [2021].

[382] Per un approfondimento: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it .

mercati digitali la linea di confine si è fatta estremamente sottile. Alla luce di tutto ciò, qual è allora la versione più corretta d'intendere il rapporto tra queste due discipline?

CONCLUSIONI

Nella trattazione di questo elaborato si è tentato di analizzare lo stato dell'arte sul rapporto, spesso conflittuale, tra i campi della *data protection* e del diritto *antitrust,* con l'obiettivo di fare chiarezza e cercare soluzioni che potessero rispondere alle problematiche della *data economy.* Dopo aver accennato alle tappe principali dell'evoluzione digitale fino ai giorni nostri, si sono considerate le caratteristiche fondamentali dei *big tech*, a partire da *Facebook,* in modo da comprendere appieno i motivi del loro successo e poter trattare consapevolmente i casi della recente giurisprudenza sul tema. Il fulcro della tesi è costituito sicuramente dal caso "*Facebook Germany",* in cui, nelle diverse fasi del procedimento, è venuta per la prima volta affermata chiaramente la stretta relazione esistente tra il campo della protezione dei dati personali ed il diritto *antitrust* nei mercati digitali. Dopo anni di giurisprudenza europea contenente la visione separatista e a tenuta stagna tra le diverse discipline, la denuncia del *Bundeskartellamt* contro il *social network* ha sollevato il velo di Maya sul tema, riconoscendo la rilevanza delle condotte illecite, relative al campo della *data protection,* anche nell'analisi *antitrust,* quali sintomo di abusi di posizione dominante e criteri per valutare la qualità dei servizi offerti. La Corte Federale Tedesca ha confermato la lettura dell'autorità, basandosi però su un differente ragionamento giuridico fondato principalmente sui diritti costituzionalmente garantiti degli utenti in quanto persone, ma il caso è sicuramente una pietra miliare ed un enorme balzo in avanti nel modo di approcciarsi alla tematica. Questa spinta innovativa è stata individuata anche negli strumenti giuridici europei già presenti e in quelli che nei prossimi anni entreranno in vigore. Rimarchevoli sono state le proposte del *DMA* e del *DSA*, che con la loro disciplina *ad hoc* per i giganti digitali e la nuova serie di obblighi stringenti a questi imposti, rappresentano l'*upgrade* di cui l'armamento giuridico dell'UE aveva da tempo bisogno. In particolare è apprezzabile la creazione di un sistema di sorveglianza e controllo *ex ante,* di semplice applicazione e più snello. La rinnovata attenzione verso la tutela in rete dei diritti costituzionalmente garantiti, come risulta anche dalla decisione del *Bundesgerichtshof,* dopo il liberismo digitale ed il *laissez-faire* dei decenni passati, costituisce il substrato giuridico e filosofico posto alla base delle recenti riforme e dell'azione europea. Ormai è divenuto chiaro il bisogno di maggior tutela degli

individui *online* e l'impatto che le piattaforme digitali possono avere su di essi e le democrazie mondiali. Questa nuova consapevolezza è riscontrabile anche a livello internazionale, ed infatti guardando fuori dai confini europei si è constatato un cambio di passo sulle sfide poste dall'economia digitale, quali l'eccessivo potere dei *big tech* e lo sfruttamento dei grandi *database* in loro possesso. Così, anche negli Stati Uniti, in Cina ed in Russia, il processo di aggiornamento legislativo, nonostante i diversi obiettivi politici, sta procedendo in modo spedito. A livello globale è lecito aspettarsi un intensificarsi del processo di digitalizzazione, con maggiore attenzione posta dai diversi paesi su fenomeni emergenti quali le criptovalute, i metaversi e la Defi. In questo mondo sempre più incentrato sui dati è necessario agire in modo repentino per evitare di subire il cambiamento, invece che avvantaggiarsene. In questo senso è fondamentale che i campi della *data protection* e del diritto *antitrust,* sempre più connessi ma rispettando le proprie peculiarità, cooperino sinergicamente per dare una risposta adeguata alla casistica avente ad oggetto la *data economy* e i suoi protagonisti. Probabilmente la soluzione migliore è un giusto mezzo tra la visione separatista classica e quella più progressista che vorrebbe una disciplina unica. Questa "terza via" è difatti quella affermata dal *Bundeskartellamt* nel caso *Facebook Germany* e dalle principali autorità garanti nazionali ed europee, riconoscendo e rispettando le differenze tra i due campi del diritto ma, allo stesso tempo, focalizzandosi sui punti in comune e sulle intersezioni che possono risolvere le zone grigie che in molti casi recenti si sono presentate. In quest'ottica, le diverse istituzioni hanno da anni avviato una stretta collaborazione per fissare principi e regole comuni, svolgere indagini conoscitive e supportarsi a vicenda. Potrebbe così perfino valutarsi l'ipotesi della riunione delle diverse autorità in un unico apparato, per rendere coerente, rapida ed efficiente l'azione contro gli abusi dei giganti tecnologici, eliminando i dilemmi regolatori nelle fattispecie *borderline.* Gli *standard* e le regole della *data protection* possono essere un valido criterio di valutazione nell'analisi *antitrust* delle condotte anticoncorrenziali dei *big tech*, poiché spesso termini e condizioni abusivi sul piano dello sfruttamento dei dati possono essere sintomo di sfruttamenti illeciti della posizione di mercato. Viceversa, ricordando che nella concorrenza tra prodotti digitali senza un corrispettivo monetario la qualità del prodotto è data anche dal livello di protezione della *privacy* degli utenti, anche i mezzi e le risultanze sul piano *antitrust* possono costituire un valido supporto per le autorità garanti della protezione dei dati. Il caso che ha interessato *Facebook* è stato soltanto uno dei primi in cui si è cercato di affermare questa visione, ma non è

logicamente dubitabile che nella casistica futura essa possa ulteriormente attecchire e maturare. È in atto un cambiamento epocale la cui portata non è ancora compresa appieno e i cui effetti non si sono totalmente realizzati. Gli ultimi *trend,* come lo sviluppo dei metaversi e della "Defi", la finanza decentralizzata senza bisogno di intermediari basata su *Blockchain* e *smart contracts*[383]*,* si fondano unicamente sui dati e sul digitale e rappresenteranno la vera sfida nei prossimi anni per istituzioni ed autorità. Un salto di qualità è stato fatto in Europa con il DMA, prevedendo per la prima volta un'azione di controllo *ex ante* nei confronti dei *big tech,* ma nel corso della sua concreta applicazione sarà possibile valutarne l'effettività e i punti deboli. Siamo agli albori di quello che gli studiosi definiscono "*antitrust* 3.0*"* o "*computational antitrust",* con strumenti predittivi per il controllo dei *player* del mercato e l'ausilio di metodologie proprie della *data science* per colmare il *gap* informativo tra autorità e imprese[384]. La professoressa Fabiana di Porto[385] propone di applicare i metodi computazionali e di *natural language processing (NLP)* anche per velocizzare l'analisi della mole di documenti e informazioni nelle indagini *antitrust* e perfino migliorare la qualità della legislazione, controllandone l'evoluzione normativa[386]. In una visione più generale, per essere davvero all'altezza di questi cambiamenti repentini, diverse sono le soluzioni che possono essere implementate. Il punto di partenza imprescindibile è sicuramente la maggiore sensibilizzazione di utenti e cittadini sul funzionamento dei mercati digitali, sullo sfruttamento dei loro dati ed i pericoli che possono celarsi nella *data economy.* Si è visto come la poca consapevolezza dei consumatori sia l'ostacolo più grande all'effettività delle previsioni normative e all'operato delle autorità, perché la conoscenza e la formazione sono i primi argini fondamentali alle condotte abusive a cui sono sottoposti. Inoltre cambiando il modo di intendere i dati nell'azione normativa e di *enforcement,* concentrandosi non solo sulla loro rilevanza economica ma considerandoli maggiormente come la proiezione digitale delle persone in rete, gli utenti potranno

[383] Per approfondimenti sulla Defi: https://www.cnbc.com/2021/06/18/whats-defi-crypto-based-decentralized-finance-explained.html .

[384] Cfr. Thibault Schrepel, *Computational Antitrust: An Introduction and Research Agenda,* Stanford Computational Antitrust (Vol. 1) 2021, (15 gennaio 2021).

[385] Professoressa titolare della cattedra di *Law & Technology* presso l'università del Salento.

[386] Tra i diversi contributi, Fabiana Di Porto, Tatjana Grote, Gabriele Volpi, Riccardo Invernizzi, *'I See Something You Don't See'. A Computational Analysis of the Digital Services Act and the Digital Markets Act,* vol 6, Stanford Computational Antitrust, 2021, (21 maggio 2021).

veramente beneficiarne. La sfida più grande per le istituzioni è quella di affrontare i *big tech* e l'impero che hanno costruito negli anni, bilanciando innovazione e interventi per ristabilire la concorrenza. L'approccio più semplice sarebbe imporre a queste imprese maggiori obblighi di trasparenza e magari richiedere la separazione concreta dei *database* delle loro piattaforme controllate. Questa strategia più blanda non sembra però accontentare tutta la dottrina. La soluzione più effettiva, sostenuta anche dal Prof. Pierluigi Congedo[387], consisterebbe nello smembramento dei giganti del *web*, come è avvenuto con la società *Standard Oils* nel secolo scorso, per restaurare lo stato concorrenziale del mercato ormai afflitto da veri e propri monopoli. Sicuramente questa misura, per quanto severa, è la più effettiva nel medio/lungo periodo, e il dibattito su questo "ritorno al passato" si sta facendo sempre più acceso e centrale. Ad accompagnare questo approccio, sul versante opposto bisogna creare incentivi ed aperture normative, ad esempio sfruttando delle *regulatory sandbox,* per favorire la crescita delle imprese che tentano di crescere puntando su innovazione e sviluppo sostenibile. Stiamo entrando in una nuova era digitale, dai confini ancora non ben delineati, che rivoluzionerà ancor di più l'economia e la società mondiale e da cui dipenderà il futuro delle democrazie. Soltanto con questa linea d'azione forte e sinergica sarà possibile contrastare gli abusi a cui stiamo assistendo oggi e aspirare al concretizzarsi del sistema multilivello di tutela, con al centro la persona, immaginato dall'Unione europea.

[387] Si vedano, di Pierluigi Congedo, *Separazione funzionale o strutturale nelle industrie regolate? I vincitori non puniscono; possibilmente cooperano (e innovano*), Concorrenza e Mercato 16/2008, (2009), 375-410. Sulla medesima linea, *The "regulatory authority dixit" defence in European Competition Law enforcement,* vol. 7 no. 10 Yearbook of Antitrust and Regulatory Studies, Centre for Antitrust and Regulatory Studies, University of Warsaw, (2014), 35-58.

BIBLIOGRAFIA

Trattati e convenzioni internazionali

1. Assemblea Generale delle Nazioni Unite, *Dichiarazione Universale dei Diritti Umani*, Risoluzione 219077A, (dicembre 1948).
2. Consiglio d'Europa, *Convenzione europea dei diritti dell'uomo,* STCE n. 5, (1950).
3. Trattato che istituisce la Comunità economica europea, [1957].
4. Assemblea Generale delle Nazioni Unite, *Convenzione internazionale sui diritti civili e politici,* Risoluzione 2200A (XXI), (dicembre 1966).
5. Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STCE n. 108, [1981].
6. Trattato sull'Unione europea*,* versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 15–368.
7. Carta dei diritti fondamentali dell'Unione europea, [2012] GU C 326 del 26.10.2012.
8. Trattato sul funzionamento dell'Unione europea*,* versione consolidata, [2012]. OJ C 326, 26.10.2012, p. 47–390.

Articoli giuridici ed economici

1. Milton Friedman, *A Friedman doctrine-- The social responsibility of business is to increase its profits,* New York Times (13 settembre 1970).
2. Cass R. Sunstein, *Against Positive Rights Feature*, 2 East European Constitutional Review 35 (1993).
3. John A. Fortin, *Algorithms and Conscious Parallelism: Why Current Antitrust Doctrine is Prepared for the Twenty-First Century Challenges Posed by Dynamic Pricing*, Tulne Journal of Technology & Intellectual Property (18 agosto 2020), Vol. 23, forthcoming.
4. Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L. J. (2017).

5. Daniel D. Sokol, Roisin E Comerford, *Antitrust and Regulating Big data*, 23 George Mason Law Review 119 (2016) , University of Florida Levin College of Law Research Paper No. 16-40 (4 settembre 2016).

6. Michael Goodyear, *A Rising Tide Lifts All Consumers: Penumbras of Foreign Data Protection Laws in the United States*, Richmond Journal of Law and Technology (7 luglio 2020).

7. David Evans, *Attention Platforms, the Value of Content, and Public Policy*, Review of Industrial Organization (2019).

8. William J. Magnuson, *A Unified Theory of Data*, Harvard Journal on Legislation (8 settembre 2020), Vol. 58, Iss. 1, (2021), Texas A&M University School of Law Legal Studies Research Paper No. 20-38.

9. Ariel Ezrachi, *BEUC Discussion Paper on "The Goals of EU Competition Law and the Digital Economy",* (Agosto 2018).

10. Giuseppe Colangelo, Mariateresa Maggiolino, *Big data, data protection and antitrust in the wake of the Bundeskartellamt case against Facebook,* Rivista italiana di *Antitrust,* n. 1 (2017).

11. Martin, Kirsten, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms* Business Ethics Quarterly, 1-32. (24 novembre 2019).

12. Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?,* Penn State Journal of Law & International Affairs, Vol. 8, No. 1, (2020).

13. Thibault Schrepel, *Computational Antitrust: An Introduction and Research Agenda,* Stanford Computational Antitrust (Vol. 1) 2021, (15 gennaio 2021).

14. Wu Youyou, Michal Kosinski, David Stillwell, *Computer-based personality judgments are more accurate than those made by human,* PNAS, 112 (4), (27 gennaio 2015).

15. Reinsel, John Gantz, John Rydning, "*Data Age 2025: The Evolution of Data to Life-Critical. Don't Focus on Big data; Foc*

16. Mario Libertini, *Digital markets and competition policy. Some remarks on the suitability of the antitrust toolkit ,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021) .

17. Rupprecht Podszun, *Digital Ecosystems, Decision-Making, Competition and Consumers – On the Value of Autonomy for Competition* (19 marzo 2019).

18. Enzo Mazza, *Digital Service Act (DSA): i nodi che restano dopo l'Ok del Parlamento Ue,* Agenda digitale, 21 gennaio 2022.

19. Reemt Matthiesen, Björn Herbers M.B.L, *ECJ to issue preliminary ruling on German FCO-Facebook case,* CMS Law-Now, (28 aprile 2021).

20. Vikram Bhargava, Manuel Velasquez, *Ethics of the Attention Economy: The Problem of Social Media Addiction*. Business Ethics Quarterly*, 31*(3), (2021).

21. Bacon, Kelyn, *European Court of Justice Upholds Judgment of the European Court of First Instance in the British Airways/Virgin Saga,* Competition Policy International, Vol. 3, No. 2, (Autunno 2007).

22. GCR, *Europe, Middle East And Africa Antitrust Review 2021,* (2021).

23. Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?*, Colorado Technology Law Journal, Vol. 18, No. (1, 2020).

24. Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!* (November 30, 2010), Tilburg Law School Legal Studies Research Paper Series No. 03/2011.

25. Philipp Fabbio, *Il diritto della concorrenza in Germania: osservazioni e valutazioni in prospettiva europea,* Orizzonti del diritto commerciale, fascicolo 3/2019, (2019).

26. Fabiana Di Porto, Tatjana Grote, Gabriele Volpi, Riccardo Invernizzi, *'I See Something You Don't See'. A Computational Analysis of the Digital Services Act and the Digital Markets Act,* vol 6, Stanford Computational Antitrust, 2021, (21 maggio 2021).

27. Özlem Bedre-Defolie, Rainer Nitsche, *When Do Markets Tip? An Overview and Some Insights for Policy*, Journal of European Competition Law & Practice, Volume 11, Issue 10, (dicembre 2020).

28. Marilena Filippelli, *La collusione algoritmica,* Orizzonti del Diritto Commerciale, fascicolo speciale, G. Giappichelli Editore, (Giugno 2021).

29. Oreste Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws – Rivista dir. media*, 3, (2018).

30. Lapo Filistrucchi, Damien Geradin, Eric van Damme, Eric Affeldt, *Market Definition in Two-Sided Markets: Theory and Practice*, Journal of Competition Law and Economics, vol. 10 (2), 2014.

31. Kyeonggook Park, Robert Seamans, Feng Zhu, *Multi-Homing and Platform Strategies: Historical Evidence from the US Newspaper Industry*, Harvard Business School Technology & Operations Mgt. Unit Working Paper No. 18-032, (1 dicembre 2018).

32. Andrei Hagiu, Julian Wright, *Multi-Sided Platforms*, International Journal of Industrial Organization, Vol. 43, 2015, (19 marzo 2015).

33. Nicholas Economides, *Network Externalities, Complementarities, and Invitations to Enter*, (1997).

34. Thabani Nyoni, Wellington Garikai Bonga, *Neuromarketing: No Brain, No Gain!* (28 febbraio 2017), Dynamic Research Journals' Journal of Economics and Finance (DRJ-JEF), Volume 2, Issue 2.

35. Allen P. Grunes, Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big data*, University of Tennessee Legal Studies Research Paper No. 269, (28 aprile 2015).

36. Zach Meyers, *No pain, no gain? The Digital Markets Act,* Centre For European Reform, (Gennaio 2022).

37. John M. Yun, *Overview of Network Effects & Platforms in Digital Markets* (11 novembre 2020), 1-10. The Global Antitrust Institute Report on the Digital Economy.

38. Alyson Leigh Young, Anabel Quan-Haase, *Privacy protection strategies on facebook*, Information, Communication & Society, 16:4, (2013), 479-500.

39. Rupprecht Podszun, Philipp Bongartz, Sarah Langenstein, *Proposals on How to Improve the Digital Markets Act* (18 febbraio 2021).

40. Rupprecht Podszun, Philip Marsden, *Restoring balance to digital competition - Sensible rules, effective enforcement,* Konrad-Adenauer-Stiftung e. V. , (2020).

41. Pierluigi Congedo, *Separazione funzionale o strutturale nelle industrie regolate? I vincitori non puniscono; possibilmente cooperano (e innovano*), Concorrenza e Mercato 16/2008, (2009)

42. Jamie Luguri, Lior Strahilevitz, *Shining a Light on Dark Patterns* , 13 Journal of Legal Analysis 43 , University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, (29 marzo 2021).

43. Gustavo Olivieri, *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali,* Orizzonti del Diritto Commerciale, fascicolo speciale ad opera di G. Giappichelli Editore, (giugno 2021).

44. Ariel Ezrachi, Maurice E. Stucke, *Sustainable and unchallenged algorithmic tacit collusion*, 17 NW. J. TECH. & INTELL. PROP. 217 (2020).

45. Daniel Susser, Beate Roessler, Helen Nissenbaum, *Technology, autonomy, and manipulation,* Internet Policy Review, 8(2), (2019).

46. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs,(2019).

47. Asuncion Esteve, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA,* International Data Privacy Law (2017, Vol. 7, No. 1).

48. Mikolaj Barczentewicz Mikolaj, *The Digital Services Act: Assessment and Recommendations*, (27 giugno 2021).

49. Wei Cui, *The Digital Services Tax: A Conceptual Defense* (22 aprile 2019). 73(1) Tax Law Review 69-111 (2019).

50. Thibault Schrepel, *The "Enhanced No Economic Sense Test": Experimenting With Predatory Innovation*, 7 N.Y.U. J. INTELL. PROP. & ENT. L. 30, 53 (2018).

51. Thomas Streinz, Paul Craig, Gráinne de Búrca, *The Evolution of EU Law* , OUP (3rd edn 2021).

52. Hiranya K. Nath, *The Information Society* , The Information Society. Space and Culture, India, [S.l.], v. 4, n. 3, p. 19-28, mar. 2017, (31 marzo 2017).

53. Marco Botta, Wiedemann, Klaus, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, Antitrust Bulletin (2 ottobre 2019).

54. Francisco Costa-Cabral, Orla Lynskey, *The Internal and External Constraints of Data Protection on Competition Law in the EU,* LSE Law, Society and Economy Working Papers 25/2015.

55. Mark Tushnet, *The Issue of State Action/Horizontal Effect in Comparative Constitutional Law,* International Journal of Constitutional Law, 1, (2003).

56. Daniel J. Solove, *The Myth of the Privacy Paradox* , 89 George Washington Law Review 1 (2021), GWU Legal Studies Research Paper No. 2020-10, (29 gennaio 2021).

57. Olga Stepanova and Patricia Jechel, *The Privacy, Data Protection and Cybersecurity Law Review: Germany,* The Law Reviews, (5 novembre 2021).

58. Susanne Barth, Menno D.T. de Jong, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,* Telematics and Informatics, Volume 34, Issue 7, (2017).

59. Samuel D. Warren, Louis D. Brandeis, *The Right of Privacy*, Harvard Law Review, Vol. 4, No. 5. (15 dicembre 1890).

60. Pierluigi Congedo, *The "regulatory authority dixit" defence in European Competition Law enforcement,* vol. 7 no. 10 Yearbook of Antitrust and Regulatory Studies, Centre for Antitrust and Regulatory Studies, University of Warsaw, (2014).

61. Giovanni De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, International Journal of Constitutional Law, 2020, 41-70.

62. Wilson R. Huhn, *The State Action Doctrine and The Principle of Democratic Choice,* in *Hofstra Law Review*, 84, (2006).

63. Olivia Altmayer, *The Tipping Point – Reevaluating the ASNEF- EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach,* Northwestern Journal of International Law & Business, Volume 39 (2018).

64. Anna Konstantinovna Zharova, Vladimir Mikhailovich Elin, *The use of Big data: a Russian perspective of personal data security,* 33 Computer Law & Security Review, (2017).

65. Orie T. Shafer, *The 42 V's of Big data and Data Science*", Elder Research – Data Science & Predictive Analytics, (2017).

66. Roberto Pardolesi, *Tutto (o quasi) quel che avreste voluto sapere sul principio del consumer welfare in diritto antitrust,* Orizzonti del Diritto Commerciale, fascicolo speciale ad opera di G. Giappichelli Editore, (Giugno 2021).

Libri e manuali

1. M. Delmastro, A. Nicita, *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna (2019).

2. Gian Franco Campobasso, *Diritto commerciale 1, Diritto dell'impresa,* 7° edizione a cura di M. Campobasso, Utet Giuridica, (2017).

3. Antonio Marcello Calamia, Viviana Vigiak, *Diritto dell'unione europea,* Giuffrè editore, (2018).

4. Paul D. MacLean, *Evoluzione del cervello e comportamento umano. Studi sul cervello trino*, Einaudi (1984).

5. Giorgio Pino, *Il costituzionalismo dei diritti*, Il Mulino, (2017).

6. Varie istituzioni europee, *Manuale sul diritto europeo in materia di protezione dei dati,* (ed. 2018, Ufficio pubblicazioni UE, 2018).
7. John Sloman, Dean Garratt, *Microeconomia,* Il Mulino (2014).
8. Intesa Sanpaolo Innovation Center, IMT School for Advanced Studies Lucca, *Neuroscience Impact.*
9. Robert Alexy, *Teoria dei diritti fondamentali*, Bologna, (2012).
10. Robert Bork, *The Antitrust Paradox: a policy at war with itself,* (1978).
11. David Bollier, *The Promise and Peril of Big data*, Washington, 2010.

Articoli scientifici

1. Marcus Stephenson-Jones, , Kai Yu, Sandra Ahrens, Jason M. Tucciarone, Aile N. van Huijstee, Luis A. Mejia, Mario A. Penzo, Lung-Hao Tai, Linda Wilbrecht, Bo Li, *A basal ganglia circuit for evaluating action outcomes.* Nature 539, 289–293 (2016).
2. Oscar Arias-Carrión, Maria Stamelou, Eric Murillo-Rodríguez, Manuel Menéndez-González, Ernst Pöppel, *Dopaminergic reward system: a short integrative review,* Int Arch Med. 2010; 3: 24, (6 ottobre 2010).
3. Melissa G. Hunt, Rachel Marx, Courtney Lipson e Jordyn Young, *No More FOMO: Limiting Social Media Decreases Loneliness and Depression Read More,* Journal of Social and Clinical Psychology, (2018).
4. Cecilie Schou Andreassen, *Online social network site addiction: A comprehensive review,* Current Addiction Reports*, 2*, (2015).
5. Judita Habermann, *Self-Control and Social Media Addiction (Facebook): A Quantitative Analysis* (26 giugno 2021).
6. Yubo Hou, Dan Xiong, Tonglin Jiang, Lily Song, Qui Wang, *Social media addiction: Its impact, mediation, and intervention*. Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13*(1), (2019).

Casi Corte di Giustizia Europea (CGUE)

1. C-41/90, *Klaus Hofner e Fritz Elser c. Macroton GmbH*, [1991], ECLI:EU:C:1991:161.
2. C-101/01, *Bodil Lindqvist*, [2003], para 25, EU:C:2003:596.
3. C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc),* [2006], ECLI:EU:C:2006:734.
4. C-95/04*, British Airways plc v Commission of the European Communities,* [2007], ECLI:EU:C:2007:166.
5. C‑131/12, *Google Spain SL e Google Inc. c Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* [2014]. ECLI:EU:C:2014:317.
6. C-362/14, *Maximilian Schrems c. Data Protection Commissioner,* [2015], ECLI:EU:C:2015:650.
7. C-201/14, *Smaranda Bara e a. / Președintele Casei Naționale de Asigurări de Sănătate e a.,* [2015], ECLI: ECLI:EU:C:2015:638.
8. C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c Salvatore Manni*, [2017], ECLI:EU:C:2017:197.
9. C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, 29 febbraio [2019], ECLI:EU:C:2019:629.
10. C-311/18, *Maximilian Schrems c. Data Protection Commissioner,* [2020], ECLI:EU:C:2020:559**.**
11. C-252/21*: Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) — Facebook Inc. and Others v Bundeskartellamt,* [2021].
12. C-457/10*, AstraZeneca v Commissione europea,* [2021], ECLI:EU:C:2012:770.
13. Caso T-612/17, *Google and Alphabet v Commission (Google Shopping),* [2021], ECLI:EU:T:2021:763.

Atti e decisioni della Commissione europea

1. Decisione della Commissione 2000/520/CE [2000], OJ L 215, 25.8.2000.
2. *Google/DoubleClick,* Decisione della Commissione COMP/M.4731 [2008], OJ C 184, 22.7.2008.

3. *Facebook/Whatsapp,* Decisione della Commissione Caso COMP/M.7217, [2014].

4. Commissione europea, *Advancing the Internet of Things in Europe,* SWD/2016/0110 final, [2016].

5. C/2016/4176*,* Decisione di esecuzione della Commissione 2016/1250 [2016], OJ L 207, 1.8.2016, p. 1–112.

6. *Microsoft / LinkedIn,* Decisione della Commissione europea Caso M.8124 [2016], OJ C 388, 21.10.2016, p. 4–4.

7. Commissione europea, *Sintesi della decisione che infligge ammende a un'impresa, a norma dell'articolo 14, paragrafo 1, del regolamento (CE) 139/2004 del Consiglio, per aver fornito indicazioni inesatte o fuorvianti, 2017/C-286/6,* [2017].

8. Commissione europea, *Report from the Commission to the Council and the European Parliament – Final Report on the E-Commerce sector inquiry*, (10 maggio 2017).

9. Commissione europea, *Comunicato stampa: Multa di 2,42 miliardi di EUR a Google per il vantaggio illegale conferito al proprio servizio di acquisti comparativi",* (27 giugno 2017).

10. Margrethe Vestager, *Comunicato stampa: Multa di 2,42 miliardi di EUR a Google per il vantaggio illegale conferito al proprio servizio di acquisti comparativi",* (27 giugno 2017).

11. Proposta di Regolamento della Commissione, relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final [2017].

12. Commissione europea, *Comunicato stampa: la Commissione infligge a Google un'ammenda di 4.34 miliardi di € per pratiche illegali riguardanti i dispositivi mobili Android volte a rafforzare la posizione dominante del motore di ricerca di Google,* (18 giugno 2018).

13. Margrethe Vestager, *Comunicato stampa: la Commissione infligge a Google un'ammenda di 4.34 miliardi di € per pratiche illegali riguardanti i dispositivi mobili Android volte a rafforzare la posizione dominante del motore di ricerca di Google,* (18 giugno 2018).

14. Commissione europea, *Comunicato stampa: la Commissione commina a Google un'ammenda pari a 1,49 miliardi di € per pratiche abusive nella pubblicità,* (20 marzo 2019).
15. *Google/Fitbit* (Caso M.9660), Decisione della Commissione C/2020/9105, [2020], OJ C 194, 21.5.2021, p. 6–6 .
16. Commissione europea, *Press Release: Commission clears acquisition of Fitbit by Google, subject to condition,* (17 dicembre 2020).
17. Margrethe Vestager, *Press Release: Commission clears acquisition of Fitbit by Google, subject to condition,* (17 dicembre 2020).
18. Commissione europea, *White paper on artificial intelligence - a european approach to excellence and trust,* [2020].
19. Commissione europea, *Strategy for a Europe Fit for the Digital Age,* [2020].
20. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, una strategia europea per i dati, COM/2020/66 final [2020].
21. Proposta di regolamento relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), COM/2020/842 final, [2020].
22. Proposta di regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali), COM/2020/825, [2020].
23. Margrethe Vestager, *Press Release: New Commission report shows the importance of digital resilience in times of crisis,* (11 giugno 2020).
24. Proposta di decisione del Parlamento europeo e del Consiglio, che istituisce il programma strategico per il 2030 "Percorso per il decennio digitale", COM/2021/574 final, [2021].
25. Dichiarazione della Commissione sui diritti e i principi digitali per il decennio digitale, COM(2022) 28 final [2022].
26. Proposta di Regolamento relativo a regole armonizzate sull'accesso e l'uso dei dati (*Data Act)*, COM/2022/68 final, [2022].

Legislazione Unione Europea

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei

dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), [2016], OJ L 119, 4.5.2016, p. 1–88.

2. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, [1995], OJ L 281, 23.11.1995, p. 31–50.

3. Direttiva 68/151 CEE [1968], OJ L 65, 14.3.1968.

4. Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, [1996], OJ L 77, 27.3.1996, p. 20–28.

5. Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), [2000], OJ L 178, 17.7.2000, p. 1–16 .

6. Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), [2002], OJ L 201, 31.7.2002.

7. Regolamento (CE) n. 139/2004 del Consiglio, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni"), [2004], OJ L 24, 29.1.2004.

8. Regolamento (UE) 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, [2018], OJ L 303, 28.11.2018, p. 59–68.

9. Direttiva (UE) 2019/1 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, [2019], OJ L 11, 14.1.2019.

10. Direttiva (UE) 2019/1 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, [2019], OJ L 11, 14.1.2019.

11. Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE , [2019], OJ L 130, 17.5.2019, p. 92–125.

12. Regolamento (UE) 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»), [2019], OJ L 151, 7.6.2019, p. 15–69.

Atti delle istituzioni europee ed internazionali

1. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (1980).

2. Gruppo di lavoro Articolo 29, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government,* (dicembre 1999).

3. Gruppo di lavoro articolo 29 , *Parere 5/2009 sui social network on-line*, WP 163, (12 giugno 2009).

4. Parlamento Europeo, *Risoluzione del Parlamento europeo dell'11 dicembre 2012 Una strategia di libertà digitale nella politica estera dell'UE (2012/2094 (INI)),* (11 dicembre 2012).

5. EDPS, *Preliminary Opinion on "Privacy and competitiveness in the age of Big data: The interplay between data protection, competition law and consumer protection in the Digital Economy",* (26 marzo 2014).

6. Gruppo di lavoro articolo 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision* (13 aprile 2016).

7. CGUE, *Comunicato stampa n. 27/17 sulla causa Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c Salvatore Manni*, (9 marzo 2017).

8. Wojciech Wiewiórowski, *Data Protection Day 2020: Facing New Challenges,* discorso in occasione della conferenza della presidenza croata al Consiglio Europeo di Zagabria, (16 gennaio 2020).

9. ENISA, *Analisi delle minacce settoriali / tematiche*, (Da gennaio 2019 ad aprile 2020); ENISA, *L'anno in Rassegna*, (da gennaio 2019 ad aprile 2020).

10. EDPB, *recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2,* (18 giugno 2020).
11. EDPB, *Dichiarazione sulle implicazioni delle concentrazioni per la vita privata,* (19 febbraio 2020).

Casi Corte Europea dei Diritti dell'Uomo

1. *Ciubotaru c Moldova,* n. 27138/04, [2010].
2. *Bernh Larsen Holding AS e a. c. Norvegia,* n. 24117/08, [2013].
3. *Bărbulescu v. Romania*, n. 61496/08, (2017).

Atti e decisioni delle autorità nazionali italiane

1. Atti del Convegno presso il Garante per la protezione dei dati personali,, "*Big data e Privacy. La nuova geografia dei poteri*", (30 gennaio 2017).
2. AGCM, Provvedimento n. 27432, procedimento PS 10601, [2017].
3. AGCM, Provvedimento 27494, [2018].
4. AGCOM, *Big data- Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/ CONS,* (giugno 2018).
5. AGCM, Provvedimento n. 27432, procedimento PS11112, (29 novembre 2018).
6. AGCM, AGCOM, Garante per la protezione dei dati personali*, Indagine conoscitiva sui Big data,* (10 febbraio 2020)
7. AGCM, Provvedimento 28398, [2020].
8. AGCM, Provvedimenti PS 11147-11149-11150, [2020].

Atti e decisioni delle autorità nazionali tedesche

1. Bundeskartellamt (Autorità della concorrenza tedesca), Autorité de la concurrence (Autorità della concorrenza francese), *Competition Law and Data, joint report,* (10 maggio 2016).

2. Monopolkommission, *Algorithms and Collusion,* (3 luglio 2018).
3. Andreas Mundt, *Press Release del Bundeskartellamt per il caso Facebook Germany,* (7 febbraio 2019).
4. Bundeskartellamt, *Case summary Decisione B6-22/16,* (15 febbraio 2019).
5. Decisione B6-22/16 del Bundeskartellamt [2019].

Atti e decisioni delle autorità nazionali americane

1. Federal Trade Commission*, File No. 071-0170 su Google/Doubleclick,* [2007].
2. Congresso degli Stati Uniti, Sottocommissione per l'*antitrust*, il diritto commerciale e amministrativo della commissione per la magistratura del Congresso statunitense, *Investigazione sulla concorrenza nei mercati digitali,* (2 ottobre 2020).

Atti e decisioni delle autorità nazionali inglesi

1. UK Competition & Market Authority, *The commercial use of consumer data,* (giugno 2015).

Casi Corti Tedesche

1. Caso KZR 6/15 della Corte Federale Tedesca, *Pechstein/International Skating Union,* [2016].
2. Caso VI-Kart 1/19 (V), Decisione della Corte regionale superiore di Düsseldorf [2019].
3. Bundesgerichtshof*, Press Release No 080/2020 della decisione KVR 69/19 del Bundesgerichtshof* (23 giugno 2020), tradotta dal *Bundeskartellamt.*
4. Bundesgerichtshof, decisione KVR 69/19, [2020].

Casi Corti Italiane

1. TAR Lazio, sez. I, sentenza n. 260/2020 [2020].
2. Consiglio di Stato, Sez. VI, sentenza n. 2631, [2021].

Casi Corti Stati Uniti d'America

1. *Standard Oil Co. of New Jersey v. United States,* 221 U.S. 1 [1911].
2. *Alcoa,* U.S. Court of Appeals for the Second Circuit - 148 F.2d 416 [1945]
3. *United States v. AT&T Inc.* - 310 F. Supp. 3d 161 D.D.C. [1984].

Legislazione Stati Uniti d'America

1. Bill of Rights, General Records of the United States Government, record Group 11, [1789].
2. Sherman Antitrust Act, Enrolled Acts and Resolutions of Congress, 1789-1992, General Records of the United States Government; Record Group 11, National Archives, [1890].
3. Privacy Act , 5 U.S.C., [1974].
4. California Consumer Privacy Act (CCPA), [2018].

Legislazione Federazione Russa

1. Codice civile della Federazione Russa [1994].
2. Codice penale della Federazione Russa [1996].
3. Legge della Federazione Russa No. 152 FZ [2006].

Legislazione Repubblica Popolare Cinese

1. Legge Penale della Repubblica democratica cinese [1979].
2. Principi Generali del Diritto Civile della Repubblica Popolare Cinese, [1986].
3. Legge sulla Responsabilità Extracontrattuale cinese [2010].

Blog, siti web e articoli di testate *online*
(ultimo accesso il 28 febbraio 2022)

1. James Kanter, *Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies*, New York Times, (3 ottobre 2014).
2. Editori dell'Encyclopedia Britannica, *Chicago School of economics,* Encyclopedia Britannica.
3. Filippo Mastroianni, *Come è cambiata la geografia del Web (dal 1995 al 2015),* IlSole24Ore (9 luglio 2017).
4. Flavia Cerquozzi, *"Diritto di accesso ad Internet" e Costituzione,* Iusinitinere (24 ottobre 2020).
5. Sam Fleming, *EU must prepare for 'Era of pandemics', Von der Leyen says,* Financial Times (28 febbraio 2021).
6. Rupprecht Podszun, *Facebook case: the reasoning,* D'Kart, Antitrust Blog, (28 agosto 2020).
7. Michela Rovelli, *Facebook e Instagram lasciano l'Europa? Cosa c'è dietro le parole di Meta in un documento ufficiale,* Corriere della Sera (7 febbraio 2022).
8. Adam Satariano, *Facebook Loses Antitrust Decision in Germany Over Data Collection,* The New York Times, (23 giugno 2020).
9. Mike Isaac, Sheera Frenkel, *Facebook Says Trump's Ban Will Last at Least 2 Years,* NewYorkTimes (7 giugno 2021).
10. Amy B. Wang, *Former Facebook VP says social media is destroying society with 'dopamine-driven feedback loops',* The Washington Post, (12 dicembre 2017).
11. Editori dell'Encyclopedia Britannica, *Foundation of the Internet,* Encyclopedia Britannica.
12. Jay Modrall, *Google/Fitbit -The EU Commission misses a step,* Kluwer Competition Law Blog, (17 giugno 2021).
13. Mike Wheatley, *Google Flu Trend: A case of Big data gone bad?,* Silicon Angle (24 marzo 2014).

14. Franco Pizzetti, *Il nuovo approccio cinese e l'importanza di un mercato unico digitale globale,* Agenda Digitale (27 agosto 2021).
15. Cameron Costa, *Inside the metaverse economy, jobs and infrastructure projects are becoming real,* CNBC (15 gennaio 2022).
16. Federica Resta, *I poteri privati e gli arbitri dei diritti,* Medialaws, (1 dicembre 2020).
17. Jena Hilliard, Theresa Parisi, *What is social media addiction?,* Addiction Center, (8 ottobre 2020).
18. Hannah Towey, *Mark Zuckerberg said he wanted to transform Facebook from a social-media company into 'a metaverse company',* Businessinsider (22 luglio 2021).
19. Dave Smith, *Weapons of Micro Destruction: How our 'Likes' hijacked democracy,* Towardsdatascience.com (17 ottobre 2018).
20. Oreste pollicino, *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali le sfide per il giurista (teorico e pratico)?,* Giustizia insieme, (15 aprile 2021).
21. Editori de "La Stampa", *Norberto Bobbio, il segreto della democrazia: non avere segreti,* La Stampa (16 ottobre 2011).
22. Glenn Greenwald, Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others,* The Guardian, (7 giugno 2013).
23. Riccardo Berti, *Privacy, la strada degli USA verso la prima norma federale,* Agenda Digitale, (25 marzo 2021).
24. *Quanto dobbiamo prendere sul serio il metaverso?,* IlPost (12 novembre 2021).
25. Giovanni De Gregorio, Oreste Pollicino, *The European Constitutional Road to Address Platform Power, VerfBlog,* (31 agosto 2021).
26. Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History,* Time (24 maggio 2018).
27. "*The world's most valuable resource is no longer oil, but data*", The Economist, (6 Maggio 2017).
28. John Mac Ghlionn, *The metaverse: Mark Zuckerberg's Brave New World,* Cointelegraph (11 agosto 2021).
29. Julie Hani, (Fit4D), *The Neuroscience of behavior change,* StartupHealth, 8 agosto 2017.