SAPIENZA
UNIVERSITÀ DI ROMA

FACOLTÀ DI GIURISPRUDENZA

UNIVERSITÀ DI ROMA – LA SAPIENZA

DOTTORATO DI RICERCA IN "*AUTONOMIA PRIVATA, IMPRESA, LAVORO E TUTELA DEI DIRITTI NELLA PROSPETTIVA EUROPEA ED INTERNAZIONALE*"

CURRICULUM DI "*DIRITTO COMMERCIALE E DELL'ECONOMIA*"

XXXIII CICLO

I BIG DATA NELL'ECONOMIA DIGITALE: DISCIPLINA ANTITRUST, CONSUMERISTICA E DEI SERVIZI DI PAGAMENTO

PIETRO GRIECO

A tutte le persone che, ciascuna per la propria parte, mi hanno sostenuto ed accompagnato in questo mio lungo percorso.

Un ringraziamento speciale va al Professor Mario Libertini che, dispensando preziosi insegnamenti, mi ha seguito sin dall'inizio con grande cura e dedizione nella redazione dell'intero elaborato.

Un ricordo affettuoso non può che andare al Professor Cesare Massimo Bianca che fino all'ultimo ha creduto in me.

Indice

Introduzione

"Scientia potestas est" è un aforisma comunemente attribuito a Francesco Bacone e, sin dal 1597, ha attraversato indenne i vari secoli sottolineando il ruolo centrale della conoscenza, intesa in senso lato come "informazione".

È infatti indubbio che l'informazione, oggi più che mai, sia assurta al ruolo di risorsa strategica, tanto da influenzare l'efficienza dei sistemi e così divenire fattore di sviluppo sociale ed economico.

L'importanza dell'uso dei dati nei processi decisionali di imprese, istituzioni e singoli cittadini si è manifestata nella diffusione dei processi di "datizzazione".

Il termine "datizzazione" è un neologismo che indica le tecniche che consentono la conversione in formato digitale – cioè in dati – di qualsiasi informazione. La raccolta delle informazioni e la loro gestione in forma strutturata sono dunque strumenti indispensabili per qualsiasi operatore di mercato, e sono destinati ad assumere un'importanza sempre crescente, anche e soprattutto nel settore bancario e finanziario, come quello dei pagamenti.

L'utilizzo intensivo dei *Big Data* costituisce un fenomeno che interessa sempre più l'intera economia e società. Agli indubbi vantaggi in termini di riduzione dei costi di transazione per imprese e consumatori, si affiancano nuovi rischi sotto il profilo concorrenziale, della protezione dei dati personali e del pluralismo informativo.

Le sfide poste dallo sviluppo dell'economia digitale e dai Big Data richiedono, comunque, uno sfruttamento pieno delle sinergie esistenti tra regolazione *ex-ante* e regolazione *ex-post*; e ciò, a tutela della *privacy*, della concorrenza, del consumatore e del pluralismo.

In particolare, la disponibilità in capo alle grandi piattaforme digitali (c.d. *Big Tech*), attive su scala globale, di enormi volumi e varietà di dati (personali e non personali, strutturati e non strutturati) e della capacità di analizzarli ed elaborarli, ha dato luogo ad inedite forme di sfruttamento economico del dato e, a sua volta, ad una sua valorizzazione.

Tutto ciò ha generato nuove concentrazioni di potere, inteso non solo come "potere di mercato", ma più in generale come potere economico e perfino politico, interessando i diritti fondamentali, i profili concorrenziali, il pluralismo e la stessa tenuta dei sistemi democratici.

Il rapporto tra la politica della concorrenza e l'economia digitale è talmente centrale da essere stato incluso anche tra gli argomenti affrontati nella riunione del G7 di luglio 2019.

Si tratta, pertanto, di un fenomeno che merita attenzione da parte di tutte le istituzioni che contribuiscono a definire la *governance* dei mercati.

Le piattaforme digitali possiedono oggi enormi patrimoni informativi e utilizzano algoritmi e tecniche automatizzate di raccolta, selezione ed analisi dei dati fondati sull'autoapprendimento (c.d. *machine*

learning).

Si tratta di una vera e propria rivoluzione dell'informazione, che sta trasformando il mondo, ponendo sfide sempre più complesse per gli operatori del diritto.

L'uso della tecnologia digitale e la consapevolezza della sua importanza sono aumentati anche alla luce della recente pandemia di COVID – 19, che ha costretto tutti ad un ripensamento delle abitudini di vita e di lavoro.

I *Big Data* sono uno strumento tecnologico emergente, che si sviluppa a grande velocità (ogni millisecondo), e sono guidati dai *social network* o dalla rete internet.

In particolare, i *social network* sono diventati lo strumento di informazione principale e le piattaforme *online* sono diventate così i nuovi *leader* mondiali nel settore della pubblicità, sottraendo il mercato ai *media* tradizionali. Le *BigTech,* infatti, fondano il loro *business* sull'acquisizione, il trattamento e l'elaborazione di informazioni e di dati da profili *social* degli utenti, la cui disponibilità è direttamente proporzionale all'intensità d'uso della rete da parte di cittadini, imprese, consumatori ed istituzioni.

Nel maggio del 2017 una celebre copertina dell'Economist affermava non a caso che: "*la risorsa più preziosa al mondo non è più il petrolio, sono i dati*".

In origine il dibattito era legato al solo aspetto della riservatezza dei dati personali, mentre oggi alla tutela della *privacy* si affiancano anche altri profili; tali profili nascono e si accentuano con il riconoscimento del dato come valore economico, ovvero come valore di cambio in un'ottica negoziale.

Negli ultimi anni il tema dei *Big Data* e il modo in cui questi sono combinati tramite gli algoritmi, è sempre più al centro del dibattito delle istituzioni di tutto il mondo, nonché delle diverse Autorità di settore coinvolte.

Queste ultime, infatti, hanno notato come siano nati modelli di *business* fondati sulla raccolta ed elaborazione di dati di vario genere.

Ciò premesso, le questioni giuridiche che ne derivano, riguardano in particolare i temi della *privacy*, della concorrenza e della regolazione dei mercati.

Per queste ragioni nel presente elaborato si adotta un approccio olistico del dato, superando divisioni legate a singole discipline.

A tal proposito, una compiuta disamina del fenomeno dei *Big data* e del ruolo da essi svolto sulle dinamiche competitive, sull'innovazione e sulla posizione degli utenti finali, tanto in relazione all'accesso a beni e servizi di consumo, a informazioni e notizie rilevanti, quanto in riferimento alla rilevanza della selettività degli algoritmi nella determinazione delle scelte, appare fondamentale, anche al fine di individuare i più efficaci strumenti di tutela nei mercati e nei settori di competenza, in particolare quello bancario e finanziario.

Il fenomeno dei Big data sta assumendo dunque, anche dal punto di vista prettamente giuridico, un rilievo sempre più evidente, sotto molteplici profili: dal diritto privato alla protezione dei dati personali, dalla disciplina antitrust alla tutela dei consumatori, con riguardo alla quale sta peraltro sorgendo un profilo collettivo mai emerso in precedenza.

Infatti, il valore delle informazioni raccolte *online* non risiede più solo nel suo scopo primario, ossia nell'uso per finalità commerciali dei dati personali, ma altresì nell'utilizzo secondario, per la cui realizzazione la prestazione del consenso esplicito ("liberamente" espresso dagli utenti) potrebbe non essere più sufficiente a garantire il rispetto della privacy e la tutela dei consumatori.

Pertanto, la necessità di conciliare il *trade-off* tra il valore commerciale dell'informazione e il rispetto di diritti individuali e collettivi fondamentali, quali la *privacy*, la tutela della concorrenza e le garanzie del pluralismo informativo, rende indispensabile un'analisi trasversale e multidisciplinare del fenomeno dei *Big Data*, che tenga conto dell'impatto dello stesso sulla concorrenza (con particolare riguardo al vantaggio competitivo generato dalla disponibilità di dati in via esclusiva), sulla tutela dei consumatori e sulla protezione dei dati personali.

CAPITOLO I

L'evoluzione del diritto alla protezione dei dati personali e l'avvento dei Big Data: la regolazione dei singoli rapporti tra impresa e consumatore nella società dell'informazione all'interno di un mercato unico digitale

Sommario: *Premessa* **1.1** *Un po' di storia: il diritto che insegue la società* **1.2** *Lo storico modello nordamericano.* **1.3** *L'Unione europea:* **1.3.1** *Il GDPR, il bilanciamento tra i diversi diritti fondamentali* **1.3.2** *Il nuovo ruolo del consenso dell'interessato* **1.3.3** *Segue. GDPR: una breve trattazione dei principali diritti dell'interessato al trattamento dei dati personali* **1.3.4** *Il GDPR e il rapporto con i Big Data* **1.3.5** *Un lento processo di patrimonializzazione dei dati e la tutela del consumatore europeo verso un mercato unico digitale: la natura non solo contrattuale del rapporto tra l'interessato e il titolare dei dati personali* **1.3.6** *Un breve cenno al Digital Services Act e alla proposta di nuovi obblighi di trasparenza per le Big Tech* **1.3.7** *Il GDPR come benchmark internazionale: il caso californiano e quello cinese* **1.4** *Il fenomeno dei Big Data come modello commerciale nella società digitale* **1.4.1** *I Big Data Analytics, il cloud computing e l'Intelligenza Artificiale* **1.4.2** *Alcuni esempi dell'utilizzo dei Big Data nei vari mercati* **1.5** *Rilievi conclusivi preliminari: la regolazione del mercato grazie alla regolazione dei singoli rapporti individuali*

1 - Premessa

La disamina dei Big Data e del loro valore economico non può prescindere dallo studio dell'evoluzione storico-giuridica del diritto alla protezione dei dati personali, che ha riflettuto le diverse società che nel tempo si sono succedute, fino ad arrivare all'odierna società dell'informazione digitale.

Il lettore più appassionato al mercato dei *Big Data*, dunque, scuserà se la prima metà del capitolo sarà dedicata all'evoluzione del diritto alla protezione dei dati personali.

Tra le principali caratteristiche della rivoluzione dei *Big Data* rientrano l'aumento del livello di trasparenza dei mercati e del parallelo sviluppo di nuove forme di tecnologie capaci di analizzare, estraendone valore, la mole di dati disponibile.

I *Big Data* consistono, infatti, in un'enorme mole di dati eterogenei, non classificati in maniera rigorosa[1]; tra questi troviamo i dati personali, che vanno analizzati alla luce del Regolamento (UE) 2016/679 del 27 aprile 2016 meglio conosciuto come GDPR (*General Data Protection Regulation*)[2].

[1] I Big Data Analytics permettono infatti di ricostruire i dati personali rendendo del tutto superata la tradizionale classificazione tra dati personali e dati non personali. Così DELMASTRO E NICITA, *Big data: come stanno cambiando il nostro mondo*, il Mulino, 2019, 36.

[2] Per un approfondimento sul Regolamento (UE) 2016/679 v. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa*, 2018, 3, 1098 ss.; L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli,

Il GDPR (di seguito anche "il Regolamento") è entrato in vigore il 25 maggio 2018 e costituisce una delle misure fondamentali della strategia del Mercato Unico Digitale (*Digital Single Market*)[3] in quanto riconosce, seppur non in via assoluta[4], un elevato livello di tutela dei dati personali.

Infatti, nell'ambito della rivoluzione digitale (c.d. rivoluzione 4.0), tecnologica ed economica alla quale si sta assistendo negli ultimi anni, l'Unione Europea intende dar vita ad un Mercato Unico Digitale – favorendo uno sviluppo virtuoso dell'economia dei *Big Data*, *dell'Internet of Things* e dei servizi di *cloud computing* – i cui pilastri sono rappresentati da un elevato livello di protezione dei consumatori e dei loro dati personali. Il GDPR rappresenta dunque uno *step* importante nel raggiungimento di tale scopo, in quanto il consumatore "iperconnesso" utilizza assiduamente servizi di comunicazione elettronica e servizi di applicazioni *smart*, rendendo fondamentale la creazione di un sistema che assicuri un elevato grado di tutela dei dati personali.

Nel GDPR, in linea anche con la vecchia disciplina, i dati personali dell'interessato vengono tutelati indipendentemente dell'esistenza di un rapporto negoziale, in quanto tali dati costituiscono un diritto fondamentale e indisponibile dell'individuo; quest'ultimo, tuttavia, come si vedrà meglio in seguito, agisce anche in veste di consumatore. Pertanto, si verifica una sovrapposizione dei due apparati di tutela (Codice del consumo e GDPR), entrambi in grado di aumentare la protezione delle transazioni.

L'utilizzo intensivo dei *Big Data*, gli algoritmi e l'intelligenza artificiale assumono inevitabile centralità nella nuova strategia europea digitale[5]: da un lato, occorre creare ecosistemi europei per l'intelligenza artificiale e il *cloud computing*, nonché innovativi "*European Data Spaces*" in settori economici strategici e in aree di pubblico interesse; dall'altro lato, occorre rafforzare le tutele per gli individui, le loro competenze digitali e la loro capacità di esercitare pienamente i propri diritti, quali ad esempio quelli relativi al trattamento dei dati (personali)[6].

2017; E. CALZOLAIO, *Il Regolamento europeo sulla protezione dei dati personali: spunti introduttivi e profili problematici*, in *Diritto Mercato Tecnologia*, num. Spec. 2017, 19 ss.; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 21 novembre 2018; G. COMANDÉ, G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, Roma, 2018; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e Impresa*, 2018, 106 ss.; F. DI RESTA, *La nuova privacy europea*, Torino, 2018, G.M. RICCIO, G. SCORZA, E. BELLISARIO (a cura di), *GDPR e normativa privacy*. Commentario, Milano, 2018; G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016.

[3] Sul punto v. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final; Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Verso uno spazio comune europeo dei dati*, COM(2018) 232 final.

[4] Esso infatti, ai sensi del considerando n. 4, "*va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità".* Più in generale, per comprendere come i diritti fondamentali influenzano l'autonomia privata v. M. LIBERTINI *Sull'efficacia orizzontale in diritto privato delle norme sui diritti fondamentali dei trattati europei*, in *Persona e mercato* [rivista telematica], 2018, 212-219.

[5] Cfr. Commissione europea, *A European Strategy for Data*, COM (2020) 66 final; e Commissione europea, *White Paper on Artificial Intelligence – a European Approach to Excellence and Trust*.

[6] Cfr. AGCM, Relazione annuale sull'attività svolta 31 marzo 2020, 21 ottobre 2020.

Oggi, come nel 2010, un elemento cardine della strategia digitale europea e nazionale è lo sviluppo delle reti che garantiscono connessioni ultraveloci a internet[7].

Inoltre, ad aprile 2021, la Commissione europea ha posto in pubblica consultazione una proposta di Regolamento in materia di Intelligenza artificiale[8].

L'intelligenza artificiale, evidenzia la Commissione, è una tecnologia strategica, in rapida evoluzione e con enormi potenzialità, sebbene l'utilizzo di tale tecnologia possa comportare rischi specifici significativi per l'applicazione di diverse norme dell'UE volte a tutelare i diritti fondamentali, garantire la sicurezza e attribuire responsabilità.

Questa strategia, il 15 dicembre 2020, ha ottenuto una svolta in quanto è stato pubblicato il doppio pacchetto di proposte regolamentari in ambito europeo (*Digital Services Act - DSA* e *Digital Markets Act – DMA*).

In particolare, il *DSA*[9] è diretto a migliorare la sicurezza degli utenti *online* in tutta l'Unione e a migliorare la protezione dei loro diritti fondamentali. In altre parole, non guarda soltanto al mercato unico e alla circolazione dei servizi digitali, ma anche alle nuove sfide per la tutela dei diritti fondamentali e della democrazia nella società dell'informazione.

Inoltre, il GDPR non fornisce regole specifiche in materia di *Big Data* e, pertanto, l'analisi delle sue previsioni deve sempre partire dal bilanciamento dei diversi diritti fondamentali, tra le libertà economiche e i diritti della personalità[10].

I dati personali, sui quali ci si concentrerà maggiormente nel prosieguo, non sono l'unica tipologia di dati presenti nel fenomeno dei *Big Data* ma sono quelli che sollevano le maggiori problematiche giuridiche, in quanto riguardano la persona e costituiscono un costo non indifferente per l'attività economica del titolare del trattamento, oltre che un rischio per l'attività d'impresa.

Per tale motivo, in materia di *Big Data*, sia le norme nazionali che quelle internazionali richiamano frequentemente i principi previsti per il trattamento dei dati personali (es. minimizzazione dei dati[11], correttezza e trasparenza, finalità, consenso libero, specifico e informato), rivelando però come tali

---

[7] Cfr. Commissione europea, *Shaping Europe's Digital Future*, Febbraio 2020.

[8] Cfr. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. L'obiettivo del Regolamento è di garantire che l'IA sia sicura, adeguatamente disciplinata e in linea con i diritti fondamentali dell'UE. La consultazione avrà termine il 24 giugno 2021.

[9] Cfr. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:825:FIN&from=en.

[10] DE GREGORIO e TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy Digitale*, TOSI (a cura di), *Giuffrè Francis Lefebvre*, 2019, p 459.

[11] Tale principio è stato altresì menzionato da COMMISSIONE EUROPEA, *Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, in https://ec.europa.eu/commission/presscorner/detail/it/ip_20_626. Si è infatti di recente parlato di questo principio per il c.d. *contact tracing* della nuova App Immuni per il tracciamento dei contatti da coronavirus. Infatti, proprio applicando questo principio, secondo il quale il titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, si è scelto di utilizzare un approccio decentralizzato che a differenza di quello centralizzato non consentirebbe la potenziale identificabilità della persona.

principi siano messi a dura prova nello scenario del trattamento di grandi quantità di dati.

La dimensione strutturale dei trattamenti automatizzati fa emergere altri due concetti o principi, previsti entrambi all'art. 25 del GDPR: *i)* il principio della *privacy by design* che mediante tecniche organizzative adeguate, come la pseudonomizzazione[12], mira a trasformare la tutela dei diritti e delle libertà delle persone in modo tale da considerare la *privacy* non un costo ma un valore[13] ; *ii)* il principio della *privacy by default*, il quale consente che vengano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento[14].

Ecco che quindi le problematiche legate alla *privacy* vengono gestite e risolte anche a livello di organizzazione dell'impresa titolare del trattamento[15].

Dunque, lo studio dei *Big Data* non può prescindere dai valori affermati dai trattati internazionali e dai diritti fondamentali, nei quali rientrano anche il diritto alla *privacy* e il più ampio diritto alla protezione dei dati personali (che comprende oltre al principio di riservatezza e della privacy, anche quello alla disponibilità e all'integrità dei dati personali)[16].

Infatti, la complessa disciplina che ha trovato uniforme regolamentazione nel GDPR, nelle varie Direttive collegate e nelle leggi nazionali mira a tutelare non solo la *privacy*, ma anche la dignità della persona nel corretto esercizio dei suoi diritti fondamentali[17]. A tal proposito, è necessario attuare un

---

[12] Il dato viene 'pseudonomizzato' e cioè sottoposto ad un processo di cancellazione di tutti gli elementi astrattamente "personali" e identificativi non è infatti generalmente protetto dalle norme sulla privacy e fornisce valore aggiunto. Questo dato però, combinato con altri dati anonimi può anche condurre all'identificazione di un soggetto. In altri termini, un *data-set* anonimo, qualora venga sottoposto ad un determinato trattamento, può dar vita a dati nuovi (anche di carattere personale), a loro volta riutilizzabili fino a che non si riterranno più utili, ovvero una volta esaurite le tecniche (e le idee) per una loro combinazione. V. MAYER-SCHÖNBERGER V. – CUKIER K., *Big data*, Milano, 2013, pp. 237 ss.

[13] Sui nuovi approcci v. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contr. e impr./Europa*, 2015, 1, p. 200.

[14] *Id.*

[15] F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 262.

[16] In altre parole, il diritto alla protezione dei dati personali, diventato per la prima volta diritto fondamentale proprio qui in Europa, ha un perimetro molto più ampio della semplice tutela della riservatezza e della privacy, diritto tra l'altro a cui molti in questo periodo sono astrattamente disposti a rinunciare in cambio di sicurezza sulla propria salute.

[17] Sul concetto ambiguo di dignità G. RESTA, *La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei Diritti)*, in *Riv. dir. civ.*, 2002, 825-829, 833 il quale sottolinea che la "[d]ignità è nozione che può avere una forte carica emancipatoria, anche e soprattutto nel senso del rafforzamento dei diritti sociali degli individui, ma che nello stesso tempo può essere impiegata, con argomentazioni apodittiche, per determinare una pesante restrizione dei diritti di libertà altrui". Difatti, "[s]e la dignità viene ricostruita come uno degli attributi della libertà [...], la persona potrà invocare il rispetto della propria dignità nei confronti di tutte le violazioni apportate dai terzi, mentre il principio di dignità non potrà a sua volta esserle opposto al fine di circoscrivere la sua sfera di libertà. [...] Viceversa, se è la libertà ad essere concepita come uno degli attributi della dignità [...], l'invocazione del rispetto della dignità umana sarà di per sé idonea a giustificare la limitazione della libertà medesima". V. anche G. ALPA, *Dignità. Usi giurisprudenziali e confini concettuali*, in *Nuova giur. civ. comm.*, 1997, II, 415 ss.; P. MOROZZO DELLA ROCCA, *Il principio di dignità della persona umana nella società globalizzata*, in *Dem. dir.*, 2004, 2, 195 ss. Il concetto di dignità come principio di orine pubblico inoltre non può essere derogato dall'autonomia privata. Così v. G. PIEPOLI, *Dignità e autonomia privata*, in *Pol. dir.*, 2003, 1, 59. Invece relativamente al concetto di di dignità come limite all'autonomia contrattuale parla anche l'Autorità garante per la protezione dei dati personali: si veda il comunicato stampa del 27 luglio 2006, reperibile sul sito www.garanteprivacy.it, relativo al progetto di un *reality show* da realizzarsi tramite riprese televisive all'interno delle carceri, in cui il Garante afferma che "consenso degli interessati è importante, ma non è di per sé sufficiente"

approccio olistico del dato, così come testimoniato da decenni in Europa[18] e proposto di recente anche negli Stati Uniti, dove l'approccio tradizionale per settori è stato abbandonato a beneficio di proposte che si concentrano su una regolamentazione della protezione dei dati a livello federale[19].

I sistemi di sorveglianza e di profilazione di massa, resi possibili dalle tecnologie digitali, generano facilmente diseguaglianze e discriminazioni; se non vi sono adeguate garanzie, essi possono minare l'esercizio di tutti i diritti della persona, nessuno escluso.

Quindi, da un lato, le moderne tecniche di trattamento dei dati rivestono un ruolo chiave per lo sviluppo della società dell'informazione[20], dall'altro, pongono nuove sfide per la tutela della *privacy* e la più ampia protezione dei dati personali[21]. Ed è in quest'ambito che si inserisce il fenomeno dei *Big Data*, delle decisioni automatizzate e del trattamento in massa dei dati personali[22].

Non è un caso, infatti, che il Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali (c.d. Convenzione 108[23]), abbia introdotto delle linee guida recanti una regolamentazione quadro sui *Big Data* e l'intelligenza artificiale, con lo scopo di prevenire il loro impatto potenzialmente negativo sulla dignità umana[24]. Tali linee guida tengono conto anche delle nuove tutele previste dalla Convenzione 108 modernizzata (c.d.

---

[18] Vedi da ultimo la Convenzione 108+ e il *General Data Protection Regulation* (GDPR) che rappresentano lo sviluppo rispettivamente della Convenzione 108 e della Direttiva 95/46/EC.

[19] Senate Bill ('SB') S.3300 introdotta il 13 febbraio 2020 per istituire una Federal data protection agency ('DPA') e per alter proposte ('the Bill') <https://www.congress.gov/bill/ 116th- congress/senate- bill/3300>, e le proposte più recenti by Sen. John Thune (R- S.D.) di settembre 2020 <https://www.commerce.senate.gov/ services/files/BD190421- F67C-4E37- A25E- 5D522B1053C7>

[20] L'informazione, così intesa, viene considerata già da tempo come un bene giuridico. Così PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. dir. civ*., 1990.

[21] Cfr. DE GREGORIO e TORINO, *op.cit*., p 447.

[22] A. MANTELERO, G. VACIAGO, *The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, in *Computer Law Rev Int'l*, 2013, 161 ss; R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. inf.*, 2013, III, 604; ZENO-V. ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the "big data revolution"*, in *Conc. merc.*, 2016, vol. 23, 29 ss.

Sull'evoluzione della disciplina in materia di protezione di dati personali, v. la ricostruzione svolta da A. MANTELERO, *The future of consumer protection in the E.U. Re-thinking the "notice and consent" para- digm in the new era of predictive analytics*, in *Computer Law & Sec. Rev.*, 2014, 30, 647 ss.

[23] Nel 2011 il Comitato dei ministri e del Consiglio d'Europa ha terminato il processo di modernizzazione della Convenzione di Strasburgo del 1981 ora denominata Convenzione 108 del Consiglio d'Europa. Essa rappresenta ad oggi l'unico strumento giuridicamente vincolante a livello internazionale in materia di trattamento automatico dei dati potendo ad essa aderire anche Stati non membri del Consiglio d'Europa. Si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che pubblico, e quindi anche ai trattamenti effettuati da polizia e autorità giudiziaria. La normativa mira a proteggere gli individui da abusi e a regolamentare i flussi transnazionali dei dati, e trae diretta ispirazione dall'art. 8 della Convenzione europea dei diritti dell'uomo".

In questa Convenzione sono ribadite le regole da rispettare per la raccolta e il trattamento di dati come il principio di correttezza, di liceità delle finalità del trattamento e della qualità dei dati

[24] Council of Europe, '*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*', T-PD(2017)1 (2017) https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0; Council of Europe, '*Guidelines on Artificial Intelligence and Data Protection*' T-PD(2019)01 (2019) https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificialintelligence-and-personal-data-protection.

Convenzione 108+ adottata nel 2018[25]) il cui processo di modernizzazione si è concluso il 5 marzo 2019 con la firma del Protocollo emendativo della Convenzione.

Lo stesso Parlamento Europeo, nella propria Risoluzione del 14 marzo 2017, ha espressamente rilevato che "*dall'impiego dell'analisi dei Big Data si osserva una confusione tra i dati personali e quelli non personali, il che può portare alla creazione di nuovi dati personali*".

Inoltre, il Considerando n. 26 del GDPR dà una definizione ampia di dato personale, prevedendo che: "*è auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile"* precisando, al contempo, che *"per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente*" ed escludendo, infine, dall'applicazione del GDPR le sole informazioni anonime, e cioè le "*informazioni che non si riferiscono ad una persona fisica identificata o identificabile"*.

Pertanto, col supporto del GDPR, la Convenzione 108 – nell'imperversare delle strategie di monetizzazione diretta e soprattutto indiretta in cui rientrano le tecnologie di *Big Data Analytics* – si propone "*di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano*".

Da ciò emerge come nella definizione di dato personale rientrano anche informazioni di per sé neutre, poiché ad esempio riferite ad oggetti, sempre che queste siano collegabili a persone fisiche e quindi suscettibili di essere qualificate come dati personali[26].

Il concetto di dato personale va quindi inteso in chiave evolutiva e dunque insieme a quelle informazioni che, se associate ad altri dati dell'individuo, possono produrre altri dati che lo riguardano.

Le ragioni dell'estensione dell'applicabilità del GDPR e della protezione dei dati personali anche ai *Big Data* risiedono dunque nelle peculiari e pericolose potenzialità delle nuove tecnologie e delle nuove tecniche di analisi (c.d. *Data Analytics),* che comprendono altresì possibili re-identificazioni di un interessato (c.d. *single out*) anche attraverso informazioni apparentemente anonime[27].

---

[25] Protocollo emendativo CETS n°223 della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

[26] Tale approccio trova conferma anche nelle affermazioni di Soro A., Presidente del Garante per la protezione dei dati personali, nel suo recente intervento in tema di "*Big Data e Libertà nella dimensione digitale*", in cui l'analisi delle dinamiche di gestione dei Big Data conduce a riconoscere come la nozione di dato anonimo stia subendo una "*contrazione speculare all'estensione del concetto di dato personale, in funzione ampliativa della tutela".*

[27] Così il GARANTE DELLA PROTEZIONE DEI DATI PERSONALI, *Relazione 2018*, 7 maggio 2019, 91.

La protezione dei dati personali risulta dunque essere funzionale alla correttezza del processo analitico fondato sui dati stessi[28].

I *Big Data* coinvolgono quindi l'utilizzo dei dati personali raccolti attraverso diverse fonti informative, con specifici rischi per la riservatezza e la protezione dei dati personali degli interessati. Come vedremo infatti, per molto tempo e in particolare in Europa, gli studiosi della materia hanno concentrato l'attenzione sul dato personale quale espressione della dignità umana, piuttosto che come bene ed oggetto di un negozio giuridico.

Ripercorrere i passaggi salienti dello sviluppo evolutivo è fondamentale anche per comprendere le ragioni che hanno condotto il legislatore europeo, i giudici nazionali, le corti europee e le Autorità di settore a parlare di valore economico dei dati.

1.1 - Un po' di storia: il diritto che insegue la società

L'analisi del diritto in senso soggettivo inizia con l'età moderna mediante un percorso che, dalle teorie giusnaturalistiche a cavallo tra il Seicento e il Settecento, arriva al positivismo giuridico dell'Ottocento, con la sua concezione statalista che considera i diritti soggettivi come derivanti dalla volontà dello Stato[29].

Bobbio sosteneva che i diritti umani fossero diritti storici, nati dunque in determinate circostanze storiche per tutelare certi bisogni in linea con il cambiamento della società[30].

È possibile così distinguere diverse generazioni di diritti: dai diritti di libertà (di ispirazione liberale e individualista) a quelli sociali, fino ad arrivare ai diritti dell'era tecnologica, tra i quali rientra il diritto alla *privacy* qui esaminato.

Nel corso del tempo, il termine *privacy* è passato da un'accezione di riservatezza a quella di controllo sui propri dati personali, fino ad arrivare ad includere anche l'identità personale[31].

---

[28] Così A. SORO, *L'universo dei dati e la libertà della persona*, in *Il discorso del presidente Antonello Soro*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (a cura di), 7 maggio 2019, p. 17.

[29] C. FARALLI , *Il diritto alla privacy. Profili storico-filosofici*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p.2 ss.

[30] N. BOBBIO, *L'età dei diritti*, Torino, 1990.

[31] Sul tema v. C.M. BIANCA, F.D. BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007; C.M. BIANCA *Istituzioni di diritto privato*, Giuffrè, Milano 2018, II ed. p.100 ss; RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012; S. PATTI, *Comm. sub. Art. 23*, in *Protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196*, C.M. BIANCA e BUSNELLI, Padova, 2007, I, p.553s; RESTA e ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. e proc. civ.*, 2018, p. 411 ss.; ZENO-V.ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, con Francesco Cardarelli e Salvatore Sica, *collana Diritto dell'informatica*, Giuffrè, 2004; S. RODOTÀ, *Intervista su privacy e libertà*, *Laterza*, 2005; P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972, p. 82 ss.; P. RESCIGNO, *Il diritto all'intimità della vita privata*, in *Studi in onore di F. Santoro Passarelli*, IV, Napoli, 1993, p. 119; RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, p. 299 ss.; MAZZAMUTO, *Il principio del consenso ed il problema della revoca, in Libera circolazione e protezione dei dati*

All'inizio il concetto di *privacy* nasce come diritto alla riservatezza[32], ovvero come "diritto ad essere lasciati soli" (c.d. *the right to be let alone*) con un'evidente accezione passiva, mentre in seguito acquista un significato di senso attivo, inteso come potere della persona di disporre dei propri dati personali e di controllarli (c.d. *privacy* elettronica).

Inoltre, i dati sono resi disponibili per la fruizione di beni e servizi (bancomat, servizi di pagamento, cellulare, servizi sanitari ecc).

La legislazione americana, come vedremo nel paragrafo successivo, ha fatto da apripista con il *Freedom of Information Act* del 1965 che aveva lo scopo di assicurare al cittadino il controllo di tutte le informazioni che lo riguardavano.

In Europa, invece, il primo provvedimento volto a introdurre una normativa precisa sul trattamento dei dati personali è la Direttiva UE del 24 ottobre 1995 (95/46/CE)[33], che segue la direzione già presa con la già citata Convenzione di Strasburgo n. 108 del 28 gennaio 1981 (c.d. Convenzione 108 del Consiglio d'Europa), ratificata dalla l. 21 febbraio 1989, n. 98 sulla protezione della persona rispetto al trattamento automatizzato di dati.

Successivamente, interviene la Carta dei diritti fondamentali dell'Unione Europea (c.d. Carta di Nizza) del 7 dicembre 2000, "costituzionalizzata" solo nel 2009, divenendo parte integrante del Trattato di Lisbona[34].

Il diritto alla *privacy* affonda dunque le sue radici nell'*humus* del costituzionalismo europeo e nel DNA del nostro ordinamento europeo[35].

In Italia, già negli anni Settanta, alcune sentenze della Corte Costituzionale[36] avevano ricondotto il diritto alla riservatezza agli artt. 2, 3 e 13 della Costituzione, dando vista alla c.d. tesi personalistica

---

personali, a cura di PANETTA, Milano, 1996, p. 994 ss.; MASSINETTI e DI CIOMMO, *Diritti della personalità*, in *Diritto Civile*, a cura di MARTUCCELLI e PESCATORE, Milano, 2011, p. 599 ss.; A. ORESTANO *La circolazione dei dati personali*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, II, Milano, 2003. 119; GALGANO, *Diritto privato*, 18° ed., Padova-Milano, 2019, p. 261.

[32] Sul diritto alla riservatezza v. C.M. BIANCA, *Il diritto alla riservatezza*, in *Scritti in onore di A. De Cupis*, Milano, 2005; AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978; BALLARANI, *Soggettività del minore e potestà genitoriale nella problematica del diritto alla riservatezza*, Torino, 2004; BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997; CATAUDELLA, *La tutela civile della vita privata*, Milano, 1972; G. GIACOBBE, *Il "diritto alla riservatezza" in Italia*, Firenze, 1974; SAVORANI, *La notorietà della persona da interesse protetto giuridico a bene giuridico*, Padova, 2000.

[33] Tale direttiva, in vista del recepimento da parte degli Stati e al fine della formazione di un mercato unico, si proponeva da una parte un intento di armonizzazione e dall'altra quello di indirizzare i paesi ancora sprovvisti di tale disciplina.

[34] All'art. 8.1 della suddetta Carta è previsto il diritto di ogni individuo "*alla protezione dei dati di carattere personale che lo riguardano*" così da essere costituzionalizzato e diventando uno dei diritti fondamentali dell'Unione europea. All'art. 52 della stessa Carta è poi stabilito che tali diritti, in cui rientra il diritto alla privacy, non sono assoluti, ma possono essere limitati per finalità di interesse generale a patto che si tratti di misure proporzionate e purché non si leda il contenuto essenziale di tali diritti.

[35] Così O. POLLICINO, *Covid19/ Perché si possono restringere le libertà fondamentali*, in https://www.viasarfatti25.unibocconi.it/notizia.php?idArt=21654, 26 marzo 2020 (ultima visita: 5 aprile 2020).

[36] Tali sentenze avevano infatti consentito di rubricare un diritto alla privacy tra i diritti fondamentali.

esaminata nel seguito della trattazione[37].

A partire dagli anni Novanta, la Corte Costituzionale[38] effettua il passaggio interpretativo che inserisce nella nozione di *privacy* sia la tutela della riservatezza sia la protezione dei dati personali[39], affermando un diritto generale della personalità (quello di identità personale) in quanto espressione unitaria del rilievo riconosciuto all'individuo nell'ordinamento[40].

Sul piano legislativo, la Direttiva 1995/46/CE riceve attuazione con la Legge 31 dicembre 1996 n. 675, abrogata e sostituita dal d.lgs. 196/2003[41] (cd. Codice della privacy), tuttora in vigore anche se in più parti modificato; questo codice rappresenta la prima legge italiana sui diritti fondamentali della persona, tutelando appunto la dignità umana[42].

In altre parole, già prima del 1996 la giurisprudenza enucleava un diritto generale della personalità[43] (quello alla identità personale) come unico valore presente nell'ordinamento, rispetto al quale gli altri profili costituiscono solo delle sfaccettature[44]. Tuttavia, l'emersione di una complessa normativa sui dati personali ha costretto gli interpreti a misurarsi di volta in volta con il legislatore europeo, arrivando ad elencare una tassonomia dei vari diritti appartenenti alle persone in relazione ai loro dati personali.

Pertanto, il diritto alla *privacy*, già con l'emanazione della Legge 31 dicembre 1996, n. 675, perde pian piano il suo inquadramento nel diritto generale della personalità, costruito grazie alla giurisprudenza, dividendosi in una moltitudine di diritti volti alla tutela dei dati personali[45].

---

[37] L'apicale problema della natura del diritto alla riservatezza informatica, se sia patrimoniale o riconducibile ai diritti della personalità, verrà trattato nel proseguo della trattazione, rinviandosi per adesso agli studi di L.C. UBERTAZZI L, *Riservatezza informatica ed industria culturale*, in *I diritti d'autore e connessi. Scritti*, Milano, Giuffré, 2003, 136 ss. spec. 137; OTTOLIA, *Privacy e social networks: profili evolutivi della tutela dei dati personali*, in AIDA, 2011, 360 ss.

[38] Cfr. *Corte cost*. 139/1990 e 81/1993.

[39] CALIFANO, *Privacy: Affermazione e pratica di un diritto fondamentale*, Napoli, 2016.

[40] GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1958, p. 458.

[41] Il testo è stato recentemente aggiornato con il Decreto Legislativo n°101 del 10 agosto 2018 che rende la norma "*compliant*" rispetto alle disposizioni introdotte dal nuovo Regolamento europeo sulla privacy (GDPR).

[42] Sul punto v. F.D. BUSNELLI, *Spunti per un inquadramento sistematico*, in *Tutela della privacy, Commentario, Nuove leggi civ. comm.*, a cura di BIANCA, BUSNELLI et al., 1999, p.329 e C.M. BIANCA *Istituzioni di diritto privato*, cit. p. 102 che evidenzia come la legge di attuazione della direttiva del 1995 amplia il contenuto normativo del diritto alla riservatezza, andando a formalizzare l'esigenza del soggetto di disporre, gestire e controllare le informazioni che lo riguardano nei diversi ambiti e contesti di vita, esigenza che viene intesa anche come diritto della persona alla protezione dei dati personali. Tale legge è stata frutto di un'imposizione da parte dell'Europa, in quanto condizione per usufruire dei benefici della Convenzione di Schengen sulla libera circolazione delle merci e delle persone; infatti, l'art. 4, primo comma, della stessa prevede che il trattamento non riguarda solamente la diffusione dei dati personali, ma più estensivamente qualsiasi operazione di loro raccolta, conservazione, elaborazione, utilizzazione o cancellazione.

[43] Cass., 20 aprile 1963, n. 1963, n. 990 in *Foro It.*, 1963, I, 879 e in *Giur. It*. 1964, I, 469; Cass., 22 maggio 1975, n. 2129 in *Foro It.*, 1976, I, p. 2895.

[44] Per una sintesi MESSINETTI e DI CIOMMO, *Diritti della personalità*, in *Diritto Civile*, a cura di MARTUCCELLI e PESCATORE, Milano, 2011, p. 599 ss

[45] Sulla legge in questione v. G. ALPA, *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996, n. 675 e successive modifiche*, Formello, 1998; E. PELLECCHIA, *Tutela della privacy (l. 31 dicembre 1996, n. 675)*, in *Nuove leggi civ. comm.*, 1999, 2-3, 459-478.

Si pongono dunque le basi per una società dell'informazione, ed è infatti solo con la legge del 1996 che viene fatto esplicito riferimento alla riservatezza e all'identità personale, ai quali si aggiunge, con il d.lgs. 30 giugno 2003, n. 196, il più ampio diritto alla protezione dei dati personali.

Quindi la diffusione di una disciplina, europea prima e nazionale poi, sulla tutela dei dati personali ha modificato la prospettiva rispetto alla quale gli studiosi si sono approcciati ai diritti della personalità.

Da una parte, un aspetto positivo è che prima l'esperienza giurisprudenziale era volta di solito a riconoscere i diritti della personalità (*e.g.* il diritto alla riservatezza) solo alle persone rinomate, mentre oggi il trattamento dei dati personali è disciplinato in una prospettiva universale, con la protezione dei dati personali che opera per chiunque.

Dall'altra parte, un aspetto negativo o potenzialmente pericoloso è che ora spetterà prima al legislatore e, in mancanza, al singolo giudice effettuare di volta in volta un bilanciamento tra il diritto del soggetto alla tutela dei propri dati e il diritto alla libera iniziativa economica degli operatori del mercato, i quali acquisiscono, usano e cedono i dati degli utenti[46]. Dunque, il diritto alla *privacy*, così come siamo stati abituati a concepirlo ed a studiarlo, muta e si trasforma, uscendo sempre più dal diritto generale della personalità per entrare nell'ambito del diritto delle obbligazioni e del diritto dell'economia.

La distinzione tra *privacy* e protezione dei dati personali emerge anche nella Carta di Nizza del 2000, dove all'art. 7 è previsto il diritto di ogni individuo al rispetto della propria vita privata e familiare, mentre all'art. 8, con separata disposizione, è previsto il diritto della persona alla protezione dei propri dati personali[47].

I due diritti rimangono però pur sempre connessi, in quanto l'abusivo trattamento dei dati personali minaccia il diritto al rispetto della vita privata e, di conseguenza, il diritto alla protezione dei dati ingloba in sé anche il diritto alla *privacy*. Una conferma ci arriva anche dal d.lgs. 196/2003, il quale all'art. 2, primo comma, prevede che il trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali, con particolare riferimento alla riservatezza.

C'è poi il diritto all'oblio, collegato sia al diritto alla *privacy* sia al trattamento dei dati personali, che tutela l'interesse del soggetto a cancellare le informazioni relative alla propria immagine o ai propri

[46] G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 104 ss., dove commenta il pensiero di Kohler, il quale "contrappone ai diritti che hanno ad oggetto i beni della personalità, fisici e incorporali, quelli che insistono sui beni immateriali esterni alla persona e suscettibili di oggettivizzazione".

[47] In effetti, gli articoli 7 e 8 della Carta, insieme all'articolo 16 TFEU, costituiscono la base del rispetto della vita privata e familiare e della protezione dei dati personali nel contesto dell'Unione .

dati personali del passato[48].

Per anni, il diritto all'oblio ha fatto da contrappeso alla libera circolazione dei dati, consentendo di tutelare la riservatezza della persona; tale diritto è stato fondamentale durante la prima metà degli anni Novanta, reagendo al primo emergere della tecnologia del *World Wide Web.*

Con l'avvento di Internet, infatti, alla dialettica tra diritto alla riservatezza dell'individuo e diritto di cronaca dei *mass-media,* si sostituisce la più pericolosa dialettica tra individuo e Internet; quest'ultima nel 1998, con la nascita di *Google,* viene ulteriormente sostituita, diventando dialettica tra individuo e motore di ricerca o piattaforma[49]. Dunque, il diritto alla riservatezza affronta una nuova sfida, sebbene in questo nuovo contesto il diritto all'oblio perda il suo smalto; se fino ad allora l'individuo poteva ottenere la cancellazione "*ex tunc*" delle informazioni che lo riguardavano, nella nuova società dell'informazione egli ottiene una mera cancellazione "*ex nunc*", con l'unico risultato di non rendere più conoscibili le informazioni che lo riguardano[50].

Infine, anche il diritto all'oblio – di pari passo con l'evoluzione del più ampio diritto alla protezione dei dati personali – viene considerato inizialmente come particolare espressione del diritto alla riservatezza[51], mentre successivamente viene considerato quale diritto al controllo della propria immagine sociale nella rete internet; ed è così che, in epoca digitale, si inizia a parlare di identità personale sui *social network* [52].

1.2 – Lo storico modello nordamericano

Prima di esaminare il nuovo Regolamento europeo (c.d. GDPR), la disciplina attualmente vigente nel nostro ordinamento, vale la pena soffermarsi preliminarmente sull'esperienza nordamericana che, come accennato nel primo paragrafo, è stata sin dall'inizio un importante modello per la nascita e lo sviluppo del diritto alla *privacy*.

Le origini moderne del diritto alla *privacy* risalgono al XIX secolo, quando l'industrializzazione

---

[48] Sul diritto all'oblio v. anche G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ*. 1990, p. 801 ss; V. CUFFARO, *Cancellare i dati personali. Dalla damnatio memoriae al diritto all'oblio*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 219 ss.; AULETTA, *Diritto alla riservatezza e "droit a l'oubli"*, in *L'informazione e i diritti della persona*, a cura di ALPA, BESSONE et al., Napoli, 1983, p.127; G. GIACOBBE, *Diritto all'oblio* in *Atti del convegno di Urbino 17 maggio 1997*, a cura di GABRIELLI, Napoli, 1999, p.30 ss.; PIZZETTI, *Il caso del diritto all'oblio*, Torino, 2013; MEZZANOTTE, *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009.

[49] V. CUFFARO, *Cancellare i dati personali. Dalla damnatio memoriae al diritto all'oblio, cit.*, 2019, p. 224.

[50] Il diritto all'oblio trova tuttora una specifica fonte nell'art. 7 d.lgs. n. 196 del 2003 sul trattamento dei dati personali e in particolare nell'ambito del diritto alla cancellazione, trasformazione, blocco, rettificazione, aggiornamento e integrazione dei propri dati personali. Inoltre, una specifica sua regolamentazione è contenuta all'art. 12 del progetto di regolamento del Parlamento Europeo e del Consiglio del 25 gennaio 2012 concernente la tutela delle persone fisiche con riferimento al trattamento dei dati personali e la loro libera circolazione.

[51] *Cass. civ. 7 dicembre 2005, n.26999.*

[52] *Cass. civ. 5 aprile 2012, n.5525; Cass.civ. 26 giugno 2013, n. 16111; C.M.* BIANCA *Istituzioni di diritto privato, cit., p. 103.*

prende piede in concomitanza all'introduzione delle macchine da stampa rotativa e delle macchine fotografiche, che permettevano di decorare gli articoli anche con le foto dei loro protagonisti.

In realtà, fino al 1914, la giurisprudenza della Corte Suprema Federale degli U.S.A. aveva seguito in gran parte i precetti della *common law* inglese. Tuttavia, già con il caso *Boyd v. United States* del 1886 la Corte aveva ritenuto di dover applicare il Quarto e il Quinto emendamento per affermare che *"the essence of the offence"* fosse costituita dall'invasione del diritto inalienabile alla sicurezza personale, alla libertà personale e alla proprietà privata[53].

Fu così che due giuristi statunitensi, Samuel Warren e Louis Brandeis, nel 1890 trassero spunto da ciò per pubblicare, sulla già allora prestigiosa *Harvard Law Review,* un saggio intitolato *The right of Privacy,* nel quale esponevano una loro articolata e complessa teoria giuridica sull'esistenza del diritto *de quo* che nel 1888, già un paio di anni prima, il giudice Thomas Cooley aveva definito "*the right to be let alone*".

I due giuristi americani furono dunque i primi a porsi il problema relativo a quali informazioni della vita privata di un soggetto potessero essere pubblicate, e quali invece meritassero una tutela nell'ambito della riservatezza delle persone[54].

Negli Stati Uniti, si possono attualmente distinguere almeno tre approcci: (i) uno "liberista" che considera i dati come dei beni in sé, negoziabili liberamente sul mercato[55]; (ii) un altro "industrialista" che trasforma i dati in diritti assimilabili al *copyright*[56], paragonandoli così ad oggetto di scambio e, infine, (iii) un terzo "personalista" che classifica il diritto alla *privacy* come diritto della persona[57].

La tendenza liberista è ad esempio molto forte in Posner che, con il metodo dell'analisi economica del diritto, esprime una sua concezione "mercatista" dei diritti.[58]

Va detto però che Posner non si occupava della *privacy* così come la intendevano Warren e Brandeis

---

[53] A.G. PARISI, *Privacy e mercato digitale,* Pacini, Pisa, 2020,15.

[54] Inoltre, mentre all'inizio il rimedio offerto dall'ordinamento era diretto solo a contrastare l'intrusione materiale e violenta nella vita o nei beni, successivamente viene esteso anche alla dimensione spirituale dell'uomo e alla tutela della sua reputazione o di beni materiali come i prodotti dell'intelletto.

[55] Tale approccio si trova già in COHEN, *Examined Lives: Information Privacy and the Subject as Object*, in *Stanford Law Rev*., 2000, 52, p. 1373 ss; e poi anche in SCHWARTZ, *Property, Privacy, and Personal Data*, in *Harvard Law Rev*., 2004, 111, p. 2056 ss; e più di recente in HEMNES, *The Ownership and Exploitation of Personal Identity in the New Media Age*, in *J. Marshall Rev. Intell. Prop. L*., 2012, 12, p. 1 ss.

[56] Termine con il quale s'intende il diritto d'autore nei paesi di *common law* come gli Stati Uniti. L'analogia tra titolarità dei dati e titolarità dei diritti d'autore è in effetti una costante della letteratura statunitense ZIMMERMAN, *Living Without Copyright in a Digital World*, in Albany Law Rev., 2007, 70, p. 1375 ss; P. SAMUELSON, *Privacy As Intellectual Property?*, *Standford Law Review*, 52, 5, pp. 1125-1173.

[57] J. ROTHMAN, *The Inalienable Right of Publicity,* in *Georgetown Law J*., 2012, 101, p. 185. Senza voler qui ripercorrere l'evoluzione del *right of publicity* si rimanda per tutti a G. PONZANELLI, *La povertà dei «sosia» e la ricchezza delle «celebrità»: il «right of publicity» nell'esperienza italiana,* in *Dir. inf.*, 1988, 129 ss.; A.M. TONI, Il Right of publicity nell'esperienza nordamericana, in *Contr. impr*., 1996, 82 ss.

[58] R. POSNER, *The right of Privacy*, in *Georgia Law Rev*., 1978. E sul suo pensiero cfr. CALABRESI, *Il futuro del law and economics. Saggi per una rimeditazione ed un ricordo*, Milano, 2018. Non è un caso infatti che proprio gli Stati Uniti sono stati tra i primi a dotare gli utenti di un ampio diritto alla portabilità dei dati, che consente al titolare di farne l'utilizzo che meglio ritiene, compreso il loro trasferimento a terzi o la possibilità di riappropriarsene

a fine Ottocento, nelle forme di curiosità del pubblico sulla vita privata altrui e nel conflitto tra questi ultimi e la stampa, bensì nella forma della c.d. *informational privacy* collegata all'economia dell'informazione[59]. È dunque da questa idea di *privacy* che emerge la concezione di "*property rights*" riguardanti le informazioni private acquisite, come ad esempio il segreto commerciale.

La commercializzazione dei dati consente di ridurre i costi transattivi, sostiene lo sviluppo tecnologico e permette agli utenti di ottenere maggiori servizi.

Infatti, gli studiosi che sostengono la tesi liberista della libera negoziazione dei dati partono dalla convinzione che la commercializzazione delle informazioni non possa solo portare benefici alle imprese, che tramite la profilazione prestano servizi più efficienti e prodotti innovativi ai consumatori, ma anche a questi ultimi che hanno così una scelta di prodotti e servizi più variegata e adeguata alle loro specifiche esigenze[60].

Un'evidente contraddizione dell'approccio liberista è che la persona possiede la sua identità digitale con la quale si identifica, mentre i terzi possono persino appropriarsene[61].

Il secondo approccio invece, come abbiamo accennato, fa un'assimilazione con il *copyright*, tutelando il titolare dei dati da eventuali illeciti dell'impresa.

Occorre però ricordare che, essendo in un paese di *common law*, il *copyright* non ha una sua configurazione codicistica, come invece avviene per il nostro diritto all'immagine; per superare tale problematica gli studiosi hanno qualificato la *privacy* come un *copyright* particolare.

Ebbene, nonostante la maggior parte degli studiosi americani aderisca al primo approccio, di tipo negoziale, una buona parte di studiosi sposa invece il secondo approccio, limitando così la circolazione dei dati sull'onda dei valori della persona e dell'interesse morale sotteso al singolo dato[62].

---

[59] Sul punto v. A. ACQUISTI, C.R. TAYLOR e L. WAGMAN, *The Economics of Privacy*, in *J. Ec. Lit., Vol 52, No. 2, 2016*; STIGLER, *An Introduction to Privacy in Economics and Politics, The Journal of Legal Studies, The Law of Privacy*, 1980, 9, 4, p. 623-644;

[60] Cfr. G. ALPA, *La "proprietà" dei dati personali*, N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 31 dove sostiene che Un problema però nell'approccio liberista sta nelle modalità con cui le informazioni vengono acquisite. Da qui nasce infatti l'esigenza di prevedere delle regole di controllo su tali modalità, così da poter monitorare preventivamente un potenziale illecito dell'impresa visto che il rimedio della "*compensation*" (il nostro risarcimento del danno) sembra poco efficace poiché tardivo.

[61] HEMNES, op. cit. Tale contraddizione però non è poi così netta, e viene spiegata dai liberisti considerando che l'attività dell'impresa di selezionare migliaia di dati riferibili alla singola persona, per poi collezionarli e gestirli.

[62] RITTER e MAYER, *Regulating Data as Property: A New Costruct For Moving Forward*, in *Duke L. & Techn. Rev*., 16, 1, p. 221 ss. Per una sintesi del dibattito negli Stati Uniti e delle varie posizioni v. N. PURTOVA, *Property rights in personal data: Learning from the American discourse*, in *Computer & Law Sec. Rev*., 2009, vol. 25, 507 ss.; A. ACQUISTI, C. TAYLOR, L. WAGMAN, *The Economics of Privacy, cit.* 450 ss. La questione dei dati come *commodity* e in quanto tale oggetto di scambio ha recentemente ricevuto in Europa una rinnovata attenzione, come si vedrà meglio più avanti nel paragrafo successivo anche alla luce delle iniziative legislative dell'Unione per la regolamentazione del mercato unico digitale, su cui v. la *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final. In proposito cfr. A. DE FRANCESCHI, M. LEHMANN, *Data as Tradeable Commodity and New Measures*

La critica mossa a questo secondo approccio è quella basata sul fatto che i dati della persona non hanno quella originalità propria dei dati oggetto del diritto d'autore, in quanto non sono creati dal titolare e normalmente non sono sfruttati a scopo di profitto[63].

Infine, il terzo approccio, sostenuto da un numero più ristretto di studiosi nordamericani, classifica il diritto alla *privacy* come diritto della persona, invocando anche la tutela della dignità.

Va detto che allo stato attuale la normativa nordamericana sulla *privacy* poggia su due pilastri: gli *statutes* della legge ordinaria e l'impianto costituzionale.

In America infatti non esiste ad oggi una legge federale, bensì una serie di strumenti legali a livello statale che tutelano la protezione dei dati, tra i quali: i) il *Federal Trade Commission Act*: legge approvata nel 1914 di creazione della *Federal Trade Commission – FTC*, che si occupa di tutelare i consumatori da pratiche commerciali scorrette; ii) il *Financial Services Modernization Act*, che tutela i consumatori nel settore dei servizi finanziari; iii) il *Health Insurance Portability and Accountability Act* (HIPAA), che regolamenta le informazioni sanitarie utilizzate da ospedali, compagnie assicurative sanitarie, farmacie e relativi responsabili del trattamento; e iv) il *CAN-SPAM Act*, che regolamenta la raccolta e l'uso dei numeri telefonici e indirizzi mail per finalità di *marketing*.

In altri termini, l'Europa segue un approccio generalista – dove la *privacy* è tutelata indipendentemente dal settore di applicazione – e centralizzato, mentre gli Stati Uniti seguono un approccio specialista e settorializzato.

Da una parte, l'approccio americano è sicuramente più efficace ed adattabile alle mutazioni tecnologiche, dall'altra parte, tale approccio fa diventare la *privacy* un bene economico da poter scambiare all'interno di un ampio mercato dei dati personali, svalorizzandone così l'aspetto individuale.

L'approccio settoriale determina una moltiplicazione delle norme, rendendo estremamente difficile per il cittadino conoscere effettivamente i suoi diritti; manca inoltre un'autorità federale che si occupa della protezione dei dati, ma esistono diverse autorità a seconda del tipo di dati e dell'utilizzo. In particolare, in relazione alla tutela della *privacy*, la FTC stabilisce che le persone giuridiche devono fornire i propri servizi conformandosi a determinati principi: i) *privacy by design*, secondo cui i servizi devono essere progettati per garantire la tutela della *privacy*; ii) *privacy choices for consumers*, che permettere al consumatore di esprimere e ritirare il consenso al trattamento dei dati; e iii) *greater transparency*, che consiste nel fornire indicazioni chiare sulle modalità di trattamento dei dati, sulla

for their Protection, in *The Italian Law Journal*, 2015, 1, 51 ss.; H. ZECH, *Data as a Tradeable Commodity*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, 2016, 51 ss. e in particolare, per quanto riguarda i dati personali, 66-69.

[63] G. ALPA, *La "proprietà" dei dati personali*, cit., 28. Così anche DELMASTRO, NICITA, op.cit., 32, dove si afferma che mentre l'informazione può essere consumata fino all'infinito da una molteplicità di soggetti e può essere limitata, il diritto d'autore attribuisce una titolarità temporanea e un pieno diritto di proprietà (*property rule*).

tipologia dei trattamenti e sui soggetti ai quali possono essere comunicati.

Il rapporto della FTC esclude esplicitamente le persone giuridiche che raccolgono dati direttamente dai consumatori; inoltre, la FTC si occupa di regolamentare i trattamenti in assenza di relazione contrattuale tra consumatore e impresa.

La medesima situazione si ha con riferimento ai diritti degli interessati (*data subject*); non c'è infatti una legge federale che preveda il diritto di accesso, ma alcune delle norme (e.g. HIPAA) prevedono il diritto di accesso ai dati per singoli settori (*e.g.* i dati sanitari per l'HIPAA).

Tuttavia, il diritto alla portabilità e il diritto di cancellazione non sono previsti negli Stati Uniti; infatti, al fine di garantire lecito il trasferimento dei dati negli Stati Uniti è sempre stato richiesto, prima dal c.d. *Safe Harbor,* poi dal c.d. *Privacy Shield,* un controllo di adeguatezza della protezione dei dati personali offerta negli Stati Uniti. In altre parole, tali due trattati internazionali "fornivano" uno "scudo" che forniva copertura per il trasferimento dei dati negli Stati Uniti.

L'uso dell'imperfetto non è casuale; in primo luogo, con la sentenza "*Schrems I*"[64] del 2015 la Corte di Giustizia dell'UE (anche CGUE) ha invalidato il *Safe Harbor*, constatando che le autorità americane potessero accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile con le finalità del loro trasferimento e oltre a quanto strettamente necessario e proporzionato per la protezione della sicurezza nazionale.

Di recente, con la sentenza *"Schrems II"*[65] la CGUE, il 16 luglio 2020, ha invalidato anche il trattato successivo, il *Privacy Shield,* ritenendo che gli Stati Uniti non proteggessero adeguatamente, e comunque in modo non equivalente all'Unione europea, i dati trasferiti dagli Stati membri[66].

Pertanto, visto quanto accaduto al *Safe Harbor* prima ed al *Privacy Shield* dopo, è evidente come la ratifica di un nuovo trattato sia di per sé del tutto insufficiente.

L'unica soluzione possibile potrebbe essere che gli USA scendano a patti con la propria sovranità ed intervengano in maniera concreta sulla legislazione interna, in modo da renderla più coerente i principi su cui si basa una società democratica nel trattamento dei dati personali.

Il discorso è invece diverso con riferimento al *California Consumer Privacy Act* – CCPA che, come vedremo di seguito, ha preso spunto proprio dal GDPR e dai principi e diritti in esso riconosciuti.

[64] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, causa C-362/14.

[65] Sentenza della Corte (Grande Sezione) del 16 luglio 2020, causa C-311/18

[66] Per un approfondimento cfr. I. ROTUNNO, La gestione del flusso trasfrontaliero dei dati dopo la sentenza Schrems II disponibile su https://www.orrick.com/it-IT/Insights/2020/11/La-gestione-gel-flusso-trasfrontaliero-dei-dati-dopo-la-sentenza-Schrems-II, 13 novembre 2020; G. FAGGIOLI e A. CATALETA, *Sentenza Schrems è una vittoria per la sovranità digitale degli europei: ecco perché,* disponibile su https://www.agendadigitale.eu/sicurezza/sentenza-schrems-e-una-vittoria-per-la-sovranita-digitale-degli-europei-ecco-perche/, 21 luglio 2020.

1.3 – L'Unione europea:

1.3.1 Il GDPR e il bilanciamento dei diritti fondamentali

Una volta compresi dal modello statunitense i diversi approcci che si possono dare al diritto alla protezione dei dati personali, è più agevole comprendere le ragioni e gli indirizzi che hanno portato all'emanazione del GDPR[67].

Il Regolamento si preoccupa non solo dei diritti della persona, ma anche delle finalità di carattere economico delle imprese, dal momento che l'acquisizione e la commercializzazione dei dati richiede di profilare gli utenti interessati al trattamento.

Per la prima volta, con il GDPR, il tema della libertà di circolazione dei dati si inserisce dal punto di vista normativo, senza però lasciarlo prevalere sul diritto della persona[68].

Il GDPR quindi è intervenuto per elevare la libera circolazione dei dati alla stessa stregua della protezione della persona e per evitare di lasciare spazio interpretativo ai legislatori nazionali[69].

Il Regolamento attua così un maggiore e rafforzato equilibrio tra due anime contrapposte: da un lato, quella del diritto alla protezione dei dati personali[70], dall'altro, quella del diritto al trattamento e alla libera circolazione dei dati personali.[71]

La prima anima è espressamente prevista dall'art. 16, primo paragrafo, del TFUE e dall'art. 8, primo paragrafo, della Carta di Nizza.

Lo stesso *considerando* n.1 del GDPR stabilisce che: "*La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale*". Di seguito, al *considerando* n.

---

[67] In termini generici FINOCCHIARO (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, cit., p. 113 ss.; N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 35 ss.

[68] Questa però non è una novità assoluta, perché già con la Direttiva del 1995 si guardava al tema dei dati personali come valore e fenomeno economico tanto che al *considerando* n. 3 si equiparava la circolazione dei dati alla circolazione delle merci, dei servizi e delle persone nel mercato interno, mentre al *considerando* n. 8 si rendeva esplicito l'obiettivo fondamentale del mercato interno di eliminare gli ostacoli alla libera circolazione dei dati personali.

[69] Infatti al Considerando n. 9 si legge che: "*Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE*."

[70] Il diritto alla protezione dei dati personali viene qualificato come diritto della personalità secondo la classificazione più tradizionale di diritto privato. Così C.M. BIANCA *Istituzioni di diritto privato, cit*, 89.

[71] Ciò diversamente dalla tutela della precedente direttiva che, in quanto direttiva di armonizzazione minima, aveva comunque lasciato ai legislatori nazionali un certo margine di manovra; proprio per questo in Italia si era adottato una preferenza per il diritto alla protezione dei dati personali piuttosto che a quello inerente al loro trattamento e circolazione, preferenza confermata anche nel Codice della *privacy* nel 2003.

4 si prevede che: "*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della funzione sociale*"[72].

Ciò da una parte è in linea con l'art. 52 della Carta di Nizza esaminato all'inizio della trattazione, dall'altra, la negazione di cui al *considerando* n. 4 non sembrerebbe avere un precedente normativo; infatti, il riferimento all'assolutezza parrebbe essere meramente funzionale alla negazione di una prerogativa appunto assoluta di alcuni diritti fondamentali a scapito di altri diritti parimenti fondamentali, così da lasciare che un eventuale conflitto non venga risolto a priori, ma attraverso un bilanciamento in concreto di diversi interessi e diritti[73].

Il GDPR non si esprime quindi sul bilanciamento dei vari diritti personali e patrimoniali coinvolti e lascia aperta la strada dell'interpretazione, rimettendo al giudice la decisione del caso concreto secondo il principio di proporzionalità e a patto che non si leda il contenuto essenziale dei diritti in questione.

Relativamente alla seconda anima, e cioè a quella del diritto al trattamento e alla libera circolazione dei dati personali, un'interpretazione estesa dell'art. 16 della Carta di Nizza include questi diritti nella formula generale della libertà d'impresa[74].

Sorge spontaneo quindi un richiamo all'art. 41 della nostra Costituzione, relativo alla libertà di iniziativa economica privata[75], che al secondo comma ne consente una limitazione (c.d. limitazione funzionale) a favore della tutela della dignità umana ovvero dei diritti della persona, sia nella sua prospettiva individuale sia in quella collettiva[76].

La differenza però tra il quadro nazionale e quello europeo è che: nel primo, la limitazione consiste più genericamente nella dignità umana ed è espressamente prevista nello stesso articolo che riconosce la libertà di iniziativa economica; nel secondo, la limitazione della libertà economica proviene da un articolo diverso, l'art. 8 della Carta di Nizza, e riguarda il diritto alla *privacy*. Da tale differenza si

---

[72] Sul punto, non manca in dottrina chi sostiene che tale affermazione sia frutto di una "svista" dato che la funzione sociale andrebbe riferita al trattamento dei dati personali e non diritto alla protezione dei dati personali. Cfr. N. ZORZI GALGANO, *op. cit.*, p. 35 ss. Inoltre, in Italia la questione sulla funzione sociale è stata a lungo oggetto di discussione con riferimento alla proprietà e il tenore dell'art. 42, terzo comma, Cost. Nello specifico, la funzione sociale si è intesa nell'ottica di porre delle limitazioni al diritto della proprietà al fine di renderla "accessibile a tutti" S. RODOTÀ, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013; GALGANO, *Trattato di diritto civile*, Padova, 2009, I, p. 334; M. LIBERTINI, *I fini sociali come limite eccezionale alla tutela della concorrenza: il caso Alitalia (nota a Corte Cost. 22 luglio 2010, n. 270)*, in *Giuri. Cost*, 2010, 4, p.3296 ss; RICCI, *La "funzione sociale" del diritto al trattamento dei dati personali*, in *Contr. e impr*., 2017, 2, p. 584 ss. che tuttavia sostiene che la funzione sociale sia da riferire direttamente ai dati anziché al trattamento degli stessi.

[73] Così anche la giurisprudenza europea (Corte UE, sent. 13 maggio 2014, *Google Spain*, causa C-131/12 e Corte UE, 9 marzo 2017, Manni, Causa C-398/15) e nazionale (Cass., 20 marzo 2018, n. 6919, nonché Cass., 24 giugno 2016, n. 13161.

[74] N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy, cit., 46.*

[75] Sul tema v. BALDASSARRE, alla voce *Iniziativa economica privata*, in *Enc. Dir.*, Milano, 1971, XXI, P. 582 ss.; MORBIDELLI, alla voce *Iniziativa economica privata*, in *Enc. Giur.*, XVII, Roma, 1989.

[76] Sull'estensione dei diritti della personalità anche alla persona intesa in una prospettiva collettiva v. A. ZOPPINI, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, in *Riv. dir. civ.*, 2002, p. 851 ss.

comprende come la libertà d'impresa del quadro europeo abbia una maggiore forza rispetto alla libertà di iniziativa economica privata del quadro nazionale [77].

In questa nuova prospettiva appare significativo il Considerando n. 5, il quale prevede che: "*L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto ad un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione tra attori pubblici e privati, comprese persone fisiche associazioni e imprese[…]".*

Altrettanto significativo è il *considerando* n. 6, che recita: *"La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente alle imprese quanto alle Autorità pubbliche di utilizzare dati personali come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali e il loro trasferimento verso Paesi terzi e organizzazioni internazionali, garantendo un elevato livello dei dati personali".*

Emerge così uno sviluppo esponenziale della circolazione dei dati, sebbene venga assicurato anche un più elevato livello di tutela dei dati personali nel rispetto del consumatore.

In sintesi, il GDPR parte dall'assunto che tutti gli interessi protetti siano fondamentali, e ciò in quanto i servizi relativi al trattamento e alla libera circolazione dei dati sono esplicazioni della libertà economica e della libertà del mercato quale diritto fondamentale. In altri termini, il diritto della persona sui dati non è più l'unico diritto fondamentale da tutelare e, di conseguenza, va contemperato e bilanciato con gli altri diritti altrettanto fondamentali[78], i quali sono riflessi nella tutela garantita dallo stesso GDPR.

Alla luce di quanto appena esposto, potrebbe emergere a prima vista una certa antinomia tra le disposizioni della Carta, che tutelerebbero maggiormente il diritto alla *privacy,* e alcune delle disposizioni del GDPR, che invece tutelerebbero maggiormente quello alla libera circolazione dei dati.

È necessario piuttosto che tali diversi diritti fondamentali vengano bilanciati secondo il principio di

---

[77] A confermare questa differenza interviene anche il GDPR grazie al quale assume grande rilievo il profilo relativo alla libera circolazione dei dati e quindi alla loro commercializzazione. Sulla commercializzazione dei diritti della persona in dottrina cfr. F. FERRARA, *Teoria del negozio illecito nel diritto civile italiano,* Milano, 1914, 36, il quale già all'epoca sosteneva che *"[u]n'azione può essere immorale in sé, in modo assoluto, e può diventare immorale, cioè originariamente lecita, assumere carattere riprovato, per speciali circostanze che vengono a modificarne la natura. Abbiamo allora un'azione immorale in senso relativo, in quanto essa non è intrinsecamente tale, ma fa svolgere una immoralità di relazione. La prestazione diventa immorale: o quando è soggetta ad una coazione giuridica incompatibile con la sua natura, o quando è posta in un rapporto causale con un compenso economicamente vantaggioso, che viene secondo i casi a deturpare o rendere sospetta e sfruttatoria la prestazione"* .

[78] G. RESTA, *La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei Diritti),* in *Riv. dir. civ.*, 2002, 801-848.

proporzionalità, sacrificando il meno possibile l'altro diritto fondamentale coinvolto nel bilanciamento[79].

1.3.2 Segue – Il nuovo ruolo del consenso dell'interessato

Il consenso dell'interessato a fondamento del trattamento è al contempo sia condizione di liceità del trattamento stesso ai sensi dell'art. 6 GDPR, sia presupposto di legittimazione per il terzo (impresa) titolare del trattamento medesimo. [80]

Prima che entrasse in vigore il GDPR il consenso veniva previsto come presupposto fondamentale, dato che i casi in cui il consenso veniva escluso erano previsti solo come eccezioni; oggi invece con il GDPR il consenso non è più un presupposto fondamentale e prioritario, a causa anche della complessità dei diritti, profili e interessi in esso previsti[81].

In altre parole, la direttiva del 1995 rendeva le cose senz'altro più semplici poiché stabiliva che i dati che riguardavano la salute non solo non potessero essere ceduti ma neanche comunicati.

Invece i dati relativi alla salute possono ora essere negoziati e, di conseguenza, il trattamento dei dati di ognuno non impedisce il proliferare standardizzato ed esponenziale del trattamento di altri sui medesimi dati nella società dell'algoritmo.

Il suddetto diritto alla cancellazione (o diritto all'oblio) rientra infatti in questa funzione della tutela identitaria.

Il Considerando n. 54 del GDPR prevede che: "*Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato*."

È infatti lo stesso art. 6.1 del GDPR a stabilire che la base giuridica del trattamento non è più il solo consenso dell'interessato ma può essere ad esempio anche un contratto di cui l'interessato è parte (qualora il trattamento sia necessario per la sua esecuzione), così come la tutela degli interessi vitali dell'interessato stesso o di un'altra persona fisica, nonchè il caso in cui il trattamento sia necessario per adempiere un obbligo legale[82]. In base all'art. 6 del Regolamento, dunque, consenso e contratto

---

[79] Sui contrapposti interessi dell'interessato e del titolare Art. 21, par. 1 regolamento 2016/679. Su tale giudizio di bilanciamento PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ*., 2017, p. 400.

[80] Per un approfondimento v. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio del dir. civ. e comm*., 2018, 1, p. 67 ss.

[81] BRAVO, *Il consenso e le altre condizioni di liceità, in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati*, diretto da FINOCCHIARO, Bologna, 2017, p. 101 ss; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, 2, 540 ss.

[82] Così l'art. 6.1 GDPR che stabilisce che: *"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*

sono due dei fondamenti di liceità del trattamento. Tuttavia, questi sono anche istituti centrali per il diritto civile in generale, e per la tutela dei consumatori[83]; ciò conferma la tendenza dell'ordinamento a considerare il contratto sempre più come uno strumento di razionalità del mercato diretto ad assicurare non solo i rapporti commerciali, ma anche altri valori e diritti della persona.

Diversamente, il caso in cui il trattamento sia necessario per adempiere un obbligo legale è riscontrabile, ad esempio, nell'ambito delle informazioni raccolte dalla Centrale dei Rischi in ambito bancario[84]; si tratterebbe di un trattamento effettuato in adempimento di obblighi di legge; dunque, gli intermediari sono esonerati dall'obbligo di acquisire il consenso per trasmetterli non solo alla Banca d'Italia ma anche ad altri intermediari, stranieri inclusi, appartenenti allo stesso gruppo bancario, nel rispetto del principio di strumentalità e del principio di riservatezza[85].

Il consenso è inoltre "libero" e, in quanto tale, sempre revocabile[86], risultando inconcepibile una esecuzione forzata del consenso prestato.

Inoltre, il consenso deve essere "specifico" e quindi la sua richiesta non può essere generica, ma deve risultare diretta ad esporre in modo chiaro le finalità e le caratteristiche del trattamento.

In quest'ambito, assumono quindi rilevanza gli obblighi informativi del titolare del trattamento, al fine di far prestare all'interessato un consenso informato e consapevole; in caso contrario, il consenso sarà invalido, impedendo così la liceità del trattamento[87].

---

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. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti."

[83] D'IPPOLITO, *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali personali* in *A.A. Vv, Consumerism 2019. Dodicesimo rapporto annuale. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?* Consumer's Forum e Università degli studi Roma Tre, 2020, 70 ss., spec. 74, disponibile in https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf.

[84] Nel caso in cui si tratti di un soggetto pubblico esso ha di per sé il diritto di trattare i dati personali, nel perseguimento delle proprie funzioni istituzionali, a prescindere dal consenso dell'interessato. Così F. VELLA e G. BOSI, *Diritto ed economia di banche e mercati finanziari*, il Mulino, Bologna, 2019, pp. 423.

[85] Inoltre la Banca d'Italia è formalmente un ente pubblico non economico e quindi essa stessa potrà gestire tali dati a prescindere del consenso dell'interessato anche perché le è espressamente affidato il potere di gestire tali dati per le finalità di istituzionali di vigilanza ex artt. 51 e 53 del TUB (Testo Unico Bancario). Per un approfondimento FRIGENI, *Segnalazione presso le centrali rischi creditizie e tutela dell'interessato*, in *Banca borsa e Titoli di Credito*, 2013; MUCCIARONE, *Centrale dei rischi e esclusione degli enti collettivi dalle tutele del codice della privacy*, in *Banca borsa Titoli di Credito*, 2015;

[86] I diritti della personalità sono infatti indisponibili perché sono diritti che il loro titolare non può alienare e ai quali non può rinunciare. Così GALGANO, *Diritto privato*, cit., p. 96. L'art. 7.3 del GDPR prevede a tal proposito che: *"L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*"

[87] Così S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, in *Memorie del Dipartimento di Giurisprudenza dell'Università di Torino*, Ledizioni LediPublishing,

Il consenso deve inoltre essere inequivoco, non dovendo essere confondibile per l'interessato - consumatore. A tal proposito, il 19 giugno 2020 si è pronunciato anche il *Conseil d'Etat* francese, che ha confermato la sanzione di 50 milioni di euro emanata dal CNIL (l'Autorità garante francese) nei confronti di *Google.* Infatti, il supremo organo di giustizia amministrativa francese oltre a confermare la giurisdizione dell'autorità garante, ha affermato che la *privacy policy* di Google non fosse facilmente accessibile e, di conseguenza, il consenso prestato dagli interessati al trattamento non fosse valido; ciò in quanto il consenso richiesto dall'impresa titolare non era specifico e inequivocabile, dato che era richiesto per tutte le operazioni. Diversamente, il GDPR prevede espressamente che il consenso è specifico solo se prestato distintamente per ogni singolo scopo[88].

La forma di questo consenso è libera per gli atti di diritto privato europeo e comprende sia una dichiarazione espressa, sia un comportamento positivo che possa manifestare univocamente la volontà dell'interessato[89]. Dunque, la condotta omissiva o il silenzio non sono considerabili alla stregua di un consenso[90].

Relativamente invece alla configurazione del consenso e alla sua natura, si può rilevare l'esistenza di diverse teorie che per chiarezza espositiva si possono ricondurre a tre.

La prima è la tesi personalista[91], che vede il consenso come atto giuridico meramente autorizzativo o come un atto unilaterale (una mera "delega") con caratteristiche incompatibili con quelle proprie della

Milano, 9/2018 p. 200 secondo cui: "La diversità di conseguenze rispetto al caso di revoca del consenso si giustifica sulla base della considerazione che, se il consenso è invalido, si ha un vizio genetico del contratto nel cui oggetto rientra il trattamento dei dati, che non può che determinarne l'invalidità; nel caso di revoca il difetto è invece funzionale".

[88] Cfr. https://noyb.eu/en/eu50-million-fine-google-confirmed-conseil-detat.

[89] Per un approfondimento v. D. BALDINI, *Il difficile equilibrio tra consenso della persona interessata e legittimo interesse del titolare del trattamento: problemi e prospettive nei rapporti tra fonti interne e dell'Unione europea in tema di tutela dei dati personali*, in *Osservatorio sulle fonti*, 3/2017.

[90] Infatti, a tal proposito il considerando n. 32 prevede che: "*Il consenso dovrebbe essere espresso mediante un atto positivo, inequivocabile, con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento di dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso, il silenzio, l'inattività, o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il consenso abbia più finalità, il consenso dovrebbe applicarsi prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferente immotivatamente con il servizio per il quale il consenso è espresso*".

[91] Si veda *ex multis* D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv*., 1998, 350 ss; e RODOTÀ, *Tecnologie e diritti*, Bologna, 1995 che insistono sulla natura autorizzatoria del consenso in connessione ad un carattere di indisponibilità del diritto fondamentale alla protezione dei dati personali. Una sfaccettatura di questa teoria è quella parte della dottrina che riconduce il consenso autorizzativo alla categoria del consenso dell'avente diritto, come scriminante di un fatto altrimenti illecito v. S. PATTI *Comm. sub. Art. 23, op. cit.* Altra sfaccettatura invece è quella che afferma che il consenso in materia di protezione dei dati personali, per le sue caratteristiche particolari, è difficilmente riconducibile alle categorie tradizionali da cui sembra distinguersi per diversi aspetti cfr. G. ALPA, *La "proprietà" dei dati personali, cit.*

volontà, escludendo dunque categoricamente la sua natura contrattuale.[92] Gli studiosi che sostengono questa tesi si basano anche sull'art. 7.3 del GDPR, che ammette sempre la revoca del consenso da parte dell'interessato, differentemente da quanto accade invece nell'ambito del rapporto contrattuale in caso di recesso *ad nutum*[93]; inoltre, tale revoca opererebbe *ex nunc*[94], facendo venir meno, una volta espressa, gli effetti del consenso ed eliminando così le condizioni di liceità.

Una seconda tesi, quella patrimoniale[95], vede invece il consenso come atto di natura negoziale, insistendo sulla sua natura dispositiva al trattamento e tenendo conto dell'esistenza di un mercato generato dalla circolazione dei dati economicamente valutabili.

Infine, una terza tesi, che è più recente ed è meglio conosciuta come una sfaccettatura della seconda, vede il consenso come manifestazione della volontà riconducibile a quella necessaria per l'istaurazione di un contratto, la cui tipologia potrebbe cambiare a seconda dei soggetti coinvolti e delle singole situazioni concrete[96].

Quest'ultima tesi sembra essere quella più condivisibile, in quanto maggiormente in linea con i più recenti interventi del legislatore europeo nell'ambito del pacchetto di direttive meglio conosciuto come "New Deal per i consumatori", completato di recente dalla direttiva UE 2161/2019 (di seguito anche, direttiva *Omnibus*).

Inoltre, il primo comma dell'art 7 del GDPR prevede che: "*Qualora il trattamento sia basato sul*

---

[92] Secondo i sostenitori di tale tesi il consenso è una mera delega funzionale unicamente a identificare la persona per permettere l'erogazione del servizio che, quindi, non sarebbe ceduto in cambio del dato ma offerto gratuitamente. Tale tesi si fonda anche su alcuni disposizioni del GDPR come il Considerando n. 68 che pone alternativamente il consenso e il contratto come ad intendere che siano due fattispecie giuridiche differenti stabilendo che:"[..] *Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto*.[..]" Lo stesso farebbe intendere anche l'art. 20.1 del GDPR in materia di diritto alla portabilità dei dati ponendo come primo presupposto per esercitare tale diritto che il trattamento sia fondato alternativamente o sul consenso o su un contratto.

[93] Tuttavia la dottrina che sposa la tesi patrimoniale o negoziale giustifica questa "revoca *ad nutum*" così ampia per il particolare contesto a tutela dell'interessato e diversamente da quanto accade in altri contesti più tradizionali di sfruttamento del diritto di personalità come quello della proprietà industriale dove tale revoca non è ammessa. Così S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, 149.

[94] Così anche l'art. 7.3 del GDPR che stabilisce che:"[..] *La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.[..]"*

[95] ZENO ZENCOVICH, *Sull'informazione come "bene" (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv*., 1999, 485 ss; CUFFARO, *A proposito del ruolo del consenso*, in *Trattamento dei dati personali e tutela della persona* a cura di CUFFARO, RICCIUTO e ZENO ZENCOVICH, Milano, 1999, 117 ss. Una sfaccettatura di questa tesi è quella proprietaria secondo la quale la previsione della condizione di un consenso per l'accesso ne rivelerebbe la natura proprietaria *de facto* e quindi, entro alcuni limiti, la sua alienabilità. Tra i sostenitori di questa tesi: DELMASTRO e NICITA, op. cit., 30 ss che riprendono un ragionamento di G. CALABRESI, A.D. MELAMED, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85(6) Harvard Law Review*, 1972 che affermava che l'obbligo di ottenere il consenso per l'accesso a determinati beni caratterizza, all'interno della *property rule,* la tutela inibitoria e cioè la regola di protezione forte del diritto di proprietà rispetto alla più debole tutela risarcitoria della liability rule che assicura solo un risarcimento in caso di accesso di terzi in assenza di consenso.

[96] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato* in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019 pp. 95 ss

consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali". In altre parole, il legislatore europeo fa ricadere sull'impresa titolare del trattamento l'onere di dimostrare la prestazione del consenso da parte dell'interessato.

Tale accezione del consenso non è però una novità nel diritto europeo e in materia di diritto dei consumatori, dato che anche qui troviamo un'asimmetria economica tra l'utente-interessato e il terzo titolare del trattamento che è un'impresa.

Altra disposizione rilevante, che vale la pena di commentare ai nostri fini, è quella del quarto comma dello stesso articolo in esame, che prevede: "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*."

Tale paragrafo è applicabile anche a molte piattaforme di *social network,* le quali di prassi chiedono, contestualmente al consenso, anche l'adesione dell'utente al contratto standardizzato predisposto dalla stessa impresa, ed avente ad oggetto i suoi servizi. La controprestazione in questo caso consisterebbe nei dati personali dell'utente/interessato oggetto di trattamento, che sono utilizzati spesso per finalità promozionali.

Tali finalità, seppur estranee al contratto in questione, ne diventano strettamente collegate per atto di autonomia privata, fino a dar vita ad una fattispecie di collegamento negoziale. È questo il caso avvenuto tra *Facebook* e *Cambridge Analityca*[97] avente ad oggetto i *Big Data* e cioè una cessione massiva dei dati dei propri utenti[98].

Molti dei presupposti richiesti dal GDPR per ritenere valido il consenso prestato dall'interessato vengono descritti nelle Linee guida n. 5, adottate il 4 maggio 2020 *dall'European Data Protection Board* – EDPB.

A tal proposito, appare interessante ai nostri fini il messaggio di accettazione della nuova *privacy policy* che WhatsApp ha inviato ai propri utenti nei primi giorni del 2021; in particolare, WhatsApp ha annunciato l'aggiornamento delle impostazioni sulla *privacy*, obbligando gli utenti a dare il proprio consenso entro e non oltre l'8 febbraio 2021, al fine di poter continuare ad utilizzare il servizio. La nuova *policy* prevede la condivisione dei dati raccolti sulla sua piattaforma di messaggistica con altre piattaforme, anch'esse di proprietà di Mark Zuckerberg (Facebook, Messenger e Instagram), al fine di avere profili utenti sempre più completi a cui poter inviare annunci pubblicitari personalizzati. Tale condotta dell'impresa ha portato milioni di utenti ad accettare distrattamente le nuove condizioni, con

[97] PARISI, *op. cit*, 113 ss.

[98] Cfr. Garante per la protezione dei dati personali, provv. 10 gennaio 2019 n. 5, in *garanteprivacy.it*.

il conseguente malcontento degli stessi. Tra queste c'è anche quella di Elon Musk, fondatore di Tesla e SpaceX, che con un breve *tweet* (che in breve tempo ha raggiunto migliaia di *like* e condivisioni) ha incoraggiato gli utenti a migrare su un'altra piattaforma di messaggistica istantanea (Signal) [99]. Questa reazione degli utenti aiuta a comprendere come la *privacy* sia sempre più considerata dall'utente/consumatore come qualità del servizio offerto, con importanti ripercussioni anche in materia di diritto della concorrenza, come vedremo nei capitoli seguenti.

Ebbene, si deve *in primis* considerare che la condotta in questione di WhatsApp investe diversi settori (oltre a quello concorrenziale[100]), in quanto il consenso richiesto non riguarda solo la tutela dei dati personali, ma anche la materia civilistica della cessione dei dati e quella consumeristica dell'informazione da fornire all'interessato in quanto appunto consumatore[101].

Sovrapponendo le indicazioni contenute nelle citate Linee guida si percepisce come il messaggio di WhatsApp, oltre a non contenere la facoltà di rifiutare il consenso, ha potenzialmente ingenerato un equivoco: da un lato, la piattaforma specifica che tale consenso non è richiesto nello spazio europeo (applicando il GDPR), dall'altro lato, propone tale consenso citando proprio l'art. 3 del GDPR sull'ambito di applicazione territoriale. Infatti, anche se il cittadino europeo dovesse prestare il proprio consenso, esso dovrebbe considerarsi come illegittimo[102].

Inoltre, l'informativa non è né chiara né precisa, ed il messaggio di accettazione non contiene la facoltà di rifiutare il consenso, in chiaro contrasto con la prassi delineata nelle Linee guida dell'EDPB sopra citate.

Infine, il consenso, sia nei sistemi di *common law* che in quelli di *civil law*, dovrebbe essere libero, attuale, informato, revocabile, ed inequivocabile; tuttavia, manca tuttora un'unità sul significato da attribuire al consenso.

Infatti, da una parte non si possono assimilare diversi concetti ad un medesimo termine giuridico, dall'altra parte l'interessato/consumatore agisce spesso in modo irrazionale e, dunque, dovrebbe essergli garantita una maggiore protezione[103]. In altre parole, nella recente prassi applicativa, non sembra che il consenso sia realmente libero e pertanto sarebbero necessari ulteriori interventi.

---

[99] Signal è un *software* gratuito e *open source* che fa della sicurezza il suo punto di forza. A differenza sia di Whatsapp che di Instagram, Signal memorizza pochissimi metadati, salvando sui propri server solo il giorno in cui l'utente si connette al servizio. Tale piattaforma utilizza un protocollo che protegge le informazioni scambiate al punto che le conversazioni e i *file* restano memorizzati esclusivamente sul dispositivo. Inoltre, attraverso codici di sicurezza si può verificare autonomamente l'identità dei propri corrispondenti in *chat*.

[100] Vedi § 3.8

[101] V. VESCIO DI MARTIRANO, *WhatsApp, la nuova privacy policy è fonte di equivoci*, 2021 in https://www.key4biz.it/whatsapp-la-nuova-privacy-policy-e-fonte-di-equivoci/338701/.

[102] Cfr. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[103] Sul punto v. RICHARDS, M. NEIL, HARTZOG, WOODROW, *The Pathologies of Digital Consent* (April 11, 2019). 96 *Washington University Law Review 1461* (2019), disponibile su SSRN: https://ssrn.com/abstract=3370433.

1.3.3 – *Segue.* GDPR: una breve trattazione dei principali diritti dell'interessato al trattamento dei dati personali

Il GDPR riconosce diversi diritti alla persona fisica: il diritto di accesso, il diritto di rettifica, quello di opposizione, quello di cancellazione, di limitazione di trattamento e infine il diritto alla portabilità dei dati[104].

Il diritto di accesso è previsto all'art. 15 del GDPR[105] (oltre che all'art. 8, secondo comma della Carta di Nizza) ed è il diritto di controllo dell'interessato, preordinato a rendere lo stesso consapevole del trattamento e a verificarne la liceità controllando i dati personali che ne sono oggetto.

Tramite il diritto di accesso l'interessato ha la possibilità di avere conferma dal titolare che sia in atto un trattamento di dati che lo riguardi, e può essere esercitato dall'interessato a prescindere dalla prova di una valida giustificazione a fondamento della relativa istanza.[106].

Alla luce del nuovo GDPR, al diritto di accesso si accompagna anche quello di ottenere almeno una copia dei dati personali oggetto di trattamento[107].

Il controllo è finalizzato a conoscere quale aspetto della vita privata è noto a terzi; a tal proposito, si parla anche di diritto di accesso all'informazione "propria"[108].

Tale diritto, così come anche altri, va esercitato nel rispetto del principio di proporzionalità, nell'ambito del bilanciamento tra norme giuridiche che tutelano diverse libertà fondamentali e diversi soggetti coinvolti nel trattamento[109].

---

[104] Per un approfondimento v. RICCI, *I diritti dell'interessato, in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da Finocchiaro, Bologna, 2017, p. 220; PELINO, *I diritti dell'interessato, in Il nuovo regolamento europeo: commentario alla nuova disciplina sulla protezione dei dati personali* a cura di BOLOGNINI, PELINO e BISTOLFI, Milano, 2016, p. 249.

[105] L'art. 15 GDPR prevede che: "*L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a)le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.[..]*"

[106] Così RODOTÀ, *Tecnologie e diritti*, *cit*.; RICCI, *I diritti dell'interessato*, cit. p. 219 ss.

[107] Così l'art. 15.3 GDPR che prevede che: *Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune*

[108] G. DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato*", N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 246.

[109] Così NAVARRETTA, *Libertà fondamentali dell'U.E. e rapporti fra privati: il bilanciamento di interessi e i rimedi civilistici*, in *Riv. dir. civ.*, 2015, I, p.878.

Il diritto di rettifica invece è trattato all'art. 16 del GDPR[110] all'interno della Sezione 3, nel quale è previsto anche il diritto alla cancellazione (o diritto all'oblio); entrambi, infatti, rispondono ad una funzione identitaria.

Nell'esercitare il diritto di rettifica, l'interessato al trattamento chiede al titolare la variazione dei dati personali inesatti o l'integrazione degli stessi ove incompleti.

Invece, il diritto alla cancellazione, previsto all'art. 17, implica la distruzione e la rimozione definitiva di ogni copia o riproduzione dei dati personali. Ad essa il GDPR equipara l'anonimizzazione dei dati con la quale non è più possibile l'identificazione della persona interessata. C'è poi il diritto di limitazione[111], previsto all'art. 18 del GDPR, consistente nel diritto dell'interessato ad ottenere dal titolare alcune limitazioni, al ricorrere di ipotesi tassative previste al primo comma dell'articolo in esame[112].

Il suo esercizio implica una specifica richiesta da parte dell'interessato in quanto è consentito in caso di contestazione dell'esattezza dei dati personali, oppure quando il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati. Tale diritto rievoca l'istituto del blocco dei dati trattati in violazione di legge dell'ormai abrogato art. 7, terzo comma, del Codice della *privacy*, con la differenza che il diritto di limitazione è consentito anche in altri casi, come ad esempio quando l'interessato si oppone ad un trattamento lecito per motivi connessi alla sua situazione particolare o in caso di prevalenza dei motivi legittimi del titolare del trattamento[113].

Inoltre, la limitazione dei dati ha durata necessariamente temporanea, deve essere revocata dopo aver realizzato i fini specifici del trattamento, e sempre che l'utente/interessato venga informato dal titolare di tale revoca[114].

---

[110] L'art.16 GDPR stabilisce che:*"L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa*."

[111] Sul diritto di limitazione v. N. FORGÓ, S. HÄNOLD, B. SCHÜTZE, *The Principle of Purpose Limitation and Big Data,* in M. Corrales et al. (eds), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation,* Singapore, 2017, 17.

[112] L'art. 18.1 prevede che: "*L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato." L'art. 18, secondo paragrafo, prevede invece che: "Se il trattamento è limitato (...), tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro."*

[113] G. DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato*", cit., p. 249.

[114] Relativamente alle modalità della limitazione del trattamento, il *considerando* n. 67 prevede che: "*Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel*

Diverso è poi il diritto di opposizione, previsto all'art 21 del GDPR, che consiste nel potere dell'interessato, in casi tassativi, di opporsi in qualsiasi momento al trattamento dei dati che lo riguardano.

I casi tassativi sono diversi; un esempio è quello in cui 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[115].

In altre parole, anche quando la legge legittima autonomamente il titolare a procedere con il trattamento a prescindere del consenso dell'interessato, quest'ultimo ha pur sempre la possibilità di opporsi al trattamento adducendo la sua "situazione particolare"; spetterà in questo caso al titolare dimostrare che i suoi interessi legittimi prevalgono sulla posizione soggettiva manifestata dall'interessato con l'opposizione[116].

Il diritto di opposizione si differenzia inoltre dal diritto di revoca del consenso, vista nel precedente paragrafo: mentre il primo ha effetti *ex tunc,* pregiudicando sin dall'inizio la circolazione dei dati, il secondo lascia impregiudicata la liceità del trattamento avvenuto prima della revoca e quindi opera *ex nunc*[117].

Diverso è il caso in cui le finalità del trattamento siano quelle di *marketing* diretto; in questo caso, infatti, l'interessato ha sempre il diritto di opposizione ai sensi dell'art. 21.3 del GDPR[118].

Inoltre, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati, mediante il c.d. *opt in* ai sensi della Direttiva 2002/58/CE.

Secondo il GDPR, tale diritto è esercitabile anche riguardi dati personali tratti ai fini di ricerca storica o scientifica o a fini statistici, purché l'interessato sia in una "situazione particolare" e salvo che il titolare dimostri un motivo legittimo di interesse pubblico che non consenta un'interruzione del

---

rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato."

115 Sul punto il considerando n. 69 stabilisce che: "*Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato*".

116 Gli effetti dell'esercizio del diritto in questione, in altri termini, comportano l'interruzione definitiva del trattamento salvo che il titolare dimostri motivi legittimi di carattere imperativo che giustifichino la non interruzione del trattamento. Così N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, cit., p. 58.

117 G. DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato*", cit, p. 255.

118 Così anche il *considerando* n. 70 che stabilisce che: "*Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione."*

trattamento in questione[119].

In altri termini, la nuova disciplina europea conserva una residua sfera di autonomia delle esistenze individuali rispetto alla c.d. dittatura dell'algoritmo e al fenomeno dei *Big Data*[120].

Infine, l'ultimo diritto rilevante – che ha un ruolo centrale nel fenomeno dei Big Data – è il diritto alla portabilità dei dati, introdotto all'art. 20 del GDPR[121]; tale diritto non è nuovo nel panorama europeo, in quanto era già conosciuto in altri ambiti come quello bancario e delle telecomunicazioni [122] e, come si vedrà nel quarto capitolo, è ancora attuale nel nuovo quadro regolamentare dei servizi di pagamento, con riferimento alla portabilità dei dati di un conto di pagamento ad un altro operatore[123].

Più in generale, il diritto alla portabilità dei dati consiste nel diritto di ricevere, su un formato strutturato di uso comune e leggibile da dispositivo automatico, i dati personali già forniti ad un titolare del trattamento e di trasmetterli in libertà senza alcun impedimento ad un altro titolare.

I due presupposti del diritto alla portabilità, previsti all'art. 20.1 del GDPR, sono: *i)* che il trattamento sia fondato sul consenso dell'interessato, anche per i dati sensibili o su un contratto da eseguire; e *ii*) che il trattamento sia effettuato con mezzi automatizzati.

In altre parole, il diritto alla portabilità non può applicarsi se il trattamento non ha una fonte contrattuale o non c'è stato il consenso dell'interessato, salvo che il trattamento sia effettuato con mezzi automatizzati, come l'algoritmo all'interno del fenomeno dei *Big Data Analytics*.

Inoltre, tale diritto non può essere esercitato nei confronti dei titolari che abbiano trattato i dati

---

[119] Per un approfondimento sul trattamento per scopi storici scientifici e statistici prima del GDPR si veda P. SIRENA, *Trattamento per scopi storici, statistici o scientifici, Profili generali e trattamento per scopi storici*, Capo I e II, Titolo VII, a cura di C.M. BIANCA, BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007, p.1413-1424; M. BIANCA, *Il trattamento per scopi statistici o scientifici*, Titolo VII, Capo III, a cura di C.M. BIANCA, BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007, p.1426-1441.

[120] G. FIORIGLIO, *Freedom, Authority and Knowledge online: The Dictatorship of the Algorithm*, in *Revista Internacional de Pensamiento Politico*, 2015, 10, 395 ss.

[121] S. TROIANO *Il diritto alla portabilità dei dati*, N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, pp. 198, 2019.

[122] Sulla portabilità del mutuo FARACE, *portabilità del mutuo e atto di surrogazione*, in *Rivista di diritto civile*, 2012, 6, pt. 2, p. 615 ss; P. SIRENA, *La "portabilità del mutuo" bancario o finanziario*, in *Riv. dir. civ*., 2008, 4, pt.1, p. 449 ss.; FUSARO, *La portabilità dei mutui nel Testo Unico Bancario*, in *Contratto e impresa*, 2011, 6, p. 1422 s.; BOSCO, *Portabilità e rinegoziazione dei mutui*, in *Giur. merito*, 2010, 1, p. 265 ss; DOLMETTA, *Questioni sulla surrogazione per volontà del debitore ex art. 8 Legge n. 40/2007 (c.d. "portabilità del mutuo")*, in *Banca, borsa, tit. cred*., 2008, 4, pt. 1, p. 395 ss; GIAMPIERI, *Il decreto sulle liberalizzazioni. La portabilità del mutuo, le intenzioni del legislatore e gli effetti (forse indesiderati) della norma*, in *Nuova giur. civ*., 2007, p. 467 ss.; CEOLIN, *La c.d. portabilità dei mutui e la cancellazione semplificata delle ipoteche nel decreto Bersani bis (d.l. 31 gennaio 2007, n.7)*, in *Nuove leggi civ*., 2008, 2-3, p. 259 ss.; MUCCIARONE, *La portabilità dei conti: prime note*, in *Banca, borsa, tit. cred*., 2016, p. 581 ss. Invece sulla portabilità del numero telefonico v. PINTO, *Mobile Number Portabilità (MNP): tempi di attivazione, perdita del credito residuo e costo del servizio*, in *Il nuovo diritto*, 2007, 5-7, pt. 4, p. 412 ss; MASPES, *Trasferimento ad altro operatore di telefonia mobile*, in *Corriere trib*., 2009, 39, p. 3163 ss. La portabilità del numero è stata introdotta in Italia attraverso due provvedimenti dell'AGCOM: le delibere n. 12/01/CIR e 19/01/CIR. Infine, con riferimento alla portabilità transfrontaliera di servizi a contenuto online nel mercato interno ai sensi del Reg. UE 2017/1128 v. PEIFER, *Territorialità e portabilità dei servizi di contenuti "online",* in Aida, 2016, p. 230.

[123] A tal proposito, si rinvia la discussione al quarto capitolo e, in particolare, al § 4.1.2.

nell'esercizio delle loro funzioni pubbliche – quando il trattamento è stato necessario per l'adempimento di un obbligo legale cui è soggetto il titolare – per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri cui è investito il titolare del trattamento[124].

Con riferimento al rapporto con altri diritti, la portabilità non pregiudica l'esercizio del diritto all'oblio e quello alla limitazione[125]; per certi versi, esso viene visto come un'evoluzione del diritto di accesso, in quanto consente di acquisire conoscenza dei dati personali conservati o trattati dal titolare. Tuttavia, il diritto alla portabilità, a differenza del diritto di accesso, consente di ottenere una copia personale dei dati su un supporto personale di uso comune, leggibile anche da dispositivo automatico, consentendo così il riutilizzo dei dati per finalità decise dall'interessato[126].

Infatti, il diritto alla portabilità comporta che il trasferimento dei dati avvenga sia dall'interessato ad un titolare diverso, sia direttamente da un titolare all'altro[127]; a tal proposito, si parla di dimensione dinamica del controllo dell'interessato che diviene il *dominus* dei suoi dati, potendo anche trasferirli a terzi.

Da una parte, la polifunzionalità del diritto alla portabilità esalta al massimo livello il controllo dell'interessato sui propri dati[128], evidenziando la sua natura di diritto fondamentale al pari degli altri diritti (*e.g.* il diritto di accesso) di cui costituisce un'evoluzione[129]. Dall'altra parte, il diritto alla

---

[124] Così l'art. 20.3 del GDPR e il considerando n. 68 che prevede che: *"[..]Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento[..].*

[125] Così il *considerando* n. 68 che stabilisce: "[..]*Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto[..]".*

[126] Così il considerando n. 68: "*Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. [..]"*

[127] Così l'art. 20.2 del GDPR e il considerando n. 68 che prevede che:*" [..]Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.* [..]"

[128] Cfr. MONTELEONE, *Il diritto alla portabilità dei dati. Tra diritti della persona e diritti del mercato*, in *LUISS Law Review*, 2017, p. 205.

[129] Si tratta quindi dell'espressione più elevata dell'autodeterminazione informativa sancita dall'art. 8 della Carta di Nizza che però non menziona espressamente il diritto alla portabilità diversamente dal diritto di accesso che invece è previsto

portabilità rafforza una visione patrimonialistica, che vede i dati personali come *commodities*[130].

Il diritto alla portabilità è previsto anche all'art. 6 del Reg. UE 2018/1807, in materia di libera circolazione dei dati non personali nell'Unione europea, con l'obiettivo di creare un'economia di dati competitiva fondata sui principi della trasparenza e interoperabilità (nell'ambito della quale si considerino *standard* aperti), incoraggiando e facilitando anche l'elaborazione di codici di condotta di autoregolamentazione a livello europeo[131]. Ciò a conferma del ruolo importante che tale diritto riveste nel fenomeno dei Big Data, in cui rientrano anche dati non personali.

Da un lato, il diritto alla portabilità consente all'interessato di non rimanere vincolato al titolare originario, ma di poter liberamente sceglierne un altro. Dall'altro lato, esso incentiva comportamenti rischiosi per l'interessato e per la sua identità digitale, trasferendo in massa i propri dati.

Pertanto, tale diritto potrebbe minacciare la *privacy* dell'interessato, dato che il trasferimento in massa consente il facile e rapido reimpiego dei dati, e dunque in contrasto con il principio di minimizzazione dei dati menzionato al *Considerando* n. 156 e dall'art. 5, par. 1, lett. c) del GDPR; e ciò, diversamente da quanto accade per tutti gli altri diritti dell'interessato sopra menzionati, che rispondono coerentemente con l'esigenza di minimizzazione dei dati.

Il diritto alla portabilità accentua dunque il c.d. *free flow* dei dati, cioè la sua circolazione e mercificazione, facendo divenire sempre più labile il confine tra dati personali previsti dal GDPR e dati non personali disciplinati dal Reg. UE 2018/1807, in un'ottica di abbandono del principio personalistico e a vantaggio di quello liberistico[132]. In altre parole, meno persona e più mercato.

Ebbene, il diritto alla portabilità sembra essere in linea con lo sviluppo di un mercato concorrenziale dei servizi della società dell'informazione. Tuttavia, il suo impiego per la promozione della concorrenza[133] non è esente da profili problematici di diritto antitrust.

Infatti, da una parte, tale diritto è un punto di raccordo tra la disciplina di tutela dei dati personali e

---

espressamente. Così SOMAINI, *The right to data portability and user control: ambition and limitation*, in *Riv. dir. media*, 2018, p. 8.

130 Cfr. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit. p. 399.

131 U. PAGALLO et al., *What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT*, in R. LEENES ET AL. (cur.), *Data Protection and Privacy: (In)visibilities and Infra-structures*, Springer, 2017, 74-76.

132 M. LILLÀ MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza e regole*, 2/2019, pp. 293-314.

133 Il diritto alla portabilità, infatti, dovrebbe contribuire a scongiurare il lock-in tecnologico e ad aumentare la concorrenza tra le imprese che forniscono servizi digitali. Da questo punto di vista l'art. 16, par. 4, secondo periodo, della Direttiva (UE) n. 2019/770 del 22 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, si distingue dall'art. 20 RGPD. Nell'ambito della Direttiva, il diritto alla portabilità sorge solo in relazione a contenuti diversi dai dati personali, che sono stati forniti o creati dal consumatore utilizzando il contenuto digitale o il servizio digitale, e solo dopo che il consumatore ha risolto il contratto. La Direttiva, dunque, tutela piuttosto il diritto di recesso del consumatore al fine di evitare effetti di blocco. In particolare, le norme servono ad evitare che il timore dell'utente che il contenuto possa essere perso con il recesso dal contratto abbia un ruolo nella decisione di esercitare tale diritto. Parimenti, anche il Regolamento UE 2017/1128 sulla portabilità cross border dei contenuti online ha un altro focus, in quanto le norme sulla portabilità transfrontaliera mirano a garantire che i contenuti digitali acquisiti da un consumatore in uno Stato membro siano accessibili gratuitamente da qualsiasi altro Stato membro.

quella in materia di concorrenza, trattandosi di una situazione giuridica soggettiva – il cui esercizio rimane saldamente nelle mani dell'interessato e la cui violazione può formare oggetto di sindacato avanti all'autorità di protezione dei dati[134] – idonea a produrre anche significativi effetti pro-concorrenziali, in termini sia di circolazione dei dati che di mobilità degli utenti. Dall'altra parte, sussistono diversi ostacoli all'effettivo sviluppo della portabilità, i quali sono connessi anche alla scarsa consapevolezza degli utenti circa l'esistenza di tale diritto, ai vincoli alla loro mobilità (dovuti anche alla presenza di esternalità di rete) e ai confini ancora incerti della portabilità, che include soltanto una parte dei dati a disposizione del titolare del trattamento.

Dunque, come vedremo meglio in seguito, la disciplina a tutela dei dati personali, per certi versi, confligge con quella a tutela della concorrenza; e ciò nella misura in cui, per poter consentire l'accesso ai propri dati, il titolare del trattamento deve acquisire il consenso dei soggetti interessati.

1.3.4 – Il GDPR e il rapporto con i *Big Data*

Attraverso uno sguardo prospettico è possibile vedere come la rilevanza dei Big Data, in relazione alla commercializzazione dei dati, diventi un fenomeno sempre meno arginabile dalle disposizioni del GDPR[135].

Dalle considerazioni sopra esposte, si può ritenere che nella materia dei Big Data il riferimento alla seconda anima del GDPR – quella relativa al trattamento e alla circolazione dei dati – abbia un significato più pregnante rispetto alla prima anima, relativa alla protezione dei dati delle persone fisiche.

In materia di Big Data, le norme nazionali ed internazionali, nonché i trattati internazionali, richiamano sempre i principi previsti per il trattamento dei dati personali (*i.e.* minimizzazione dei dati, correttezza e trasparenza, finalità, consenso libero, specifico e informato), rilevando come tali principi siano messi a dura prova in uno scenario di trattamento di grandi quantità di dati.

Il GDPR, pur non facendo alcun espresso riferimento ai Big Data, prevede particolari diritti per garantire la trasparenza, anche al tempo dell'intelligenza artificiale. Tra questi diritti troviamo ad esempio il diritto ad essere informato, di cui agli artt. 13 e 14, e il già esaminato diritto di accesso dell'art. 15, dove in particolari ipotesi di profilazione e di processi decisionali automatizzati, è previsto che l'individuo venga informato in modo chiaro e semplice sulle modalità di funzionamento. Inoltre, l'art. 22 del GDPR, che prevede il caso specifico di processo decisionale totalmente automatizzato, stabilisce che lo scambio di comunicazioni tra l'interessato e il titolare del trattamento

[134] In tale prospettiva, cfr. le Linee Guida sul diritto alla portabilità dei dati – WP242 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016 e poi emendate, a seguito di consultazione pubblica, e adottate il 5 aprile 2017.
[135] DE GREGORIO e TORINO, *Privacy, tutela dei dati personali e Big Data,* p. 484.

includa anche informazioni significative sulla logica utilizzata nel trattamento, nonché sull'importanza e sulle conseguenze previste per la persona.

Sebbene, quindi, una parte della dottrina ritenga che il GDPR sia idoneo anche per le decisioni automatizzate sottese ai Big Data[136], la dottrina maggioritaria è concorde nel sostenere che i principi del GDPR, ad iniziare dal principio di trasparenza[137], non siano adeguati alla nuova realtà della società dell'algoritmo.

Infatti, c'è chi sostiene che in questa nuova realtà, il principio di trasparenza e il diritto di conoscere le ragioni della decisione automatizzata non abbia sufficienti basi di diritto positivo, e che anzi l'affidabilità del calcolo predittivo dell'algoritmo compensi l'inapplicabilità del principio di trasparenza.

L'identità diventa quindi il risultato di una profilazione, un'operazione computazionale che riconduce la persona ad una categoria tipologica e quindi standardizzata sulla base di regole statistiche[138].

Ecco che quindi all'autodeterminazione dell'individuo si sostituisce l'efficienza dell'eterodeterminazione informatizzata[139]; tale osservazione può essere meglio compresa se la si inquadra in una società, come quella odierna, in cui gli algoritmi contribuiscono a definire nuove modalità per elaborare una enorme quantità di dati.

I profili più problematici con i principi del GDPR sono il riutilizzo di dati personali attraverso l'utilizzo di algoritmi complessi, i quali hanno processi decisionali spesso opachi; infatti, non è un caso che la trasparenza sia al centro del dibattito sugli algoritmi[140].

Le tecniche utilizzate nel campo dei Big Data sono complesse e difficili da spiegare all'interessato, per garantirne la consapevolezza delle modalità e le conseguenze relative al trattamento dei dati personali. Ciò in quanto l'analisi dei Big Data implica il riutilizzo di dati e spesso non è possibile prevedere sin dall'inizio gli usi che possono farsi (c.d. "*transparency paradox*"[141]).

Però, come si è già detto, il principio di trasparenza non è l'unico aspetto del GDPR di difficile applicazione alla realtà dei Big Data, perché c'è anche il principio di finalità del trattamento, secondo il quale al momento della raccolta e dell'analisi dei dati, il titolare deve informare l'interessato sulle

---

136 GOODMAN e FLAXMAN, *EU Regulations on Algorithmic Decision making and Right to Explanation*, in www.ora.ox.ac.uk.

137 Così WATCHER, MITTELSTADT e FLORIDI, *Why a Right to Explanation of Automated Decision- Making Does Not Exist in the General Data Protection Regulation*, in *Int'l Data Privacy Law*, 2017, p. 76ss.

138 DURANTE, *Rethinking human identity in the age of automatic computing. The philosophical idea of trace*, in *Law, Human Agency and Automatic Computing*, a cura di Aa Vv. p. 85

139 HARCOURT, *Against Prediction. Profiling, Polishing and punishing in an Actuarial Age*, Chicago-London, 2007.

140 B. CUSTERS, T. CALDERS, B. SCHERMER et al., *Discrimination and Privacy in the Information Society*, Heidelberg, 2013; T. ZARSKY, *Transparent predictions*, in *University of Illinois Law Review*, 2013, 4, 1507 ss.; S.M. BENJAMIN, *Algorithms and Speech*, in *University of Pennsylvania Law Review*, 2013, 161, 1445 ss.; M. TURILLI, L. FLORIDI, *The ethics of information transparency*, in *Ethics and Information Technology*, 2009, 11, 2, 105.

141 N. M. RICHARDS, J.H. KING, *Three Paradoxes of Big Data*, in *Stanford Law Review Online*, 2013, 66, 41 ss.

finalità che divergono da quelle iniziali.

In particolare, con riferimento alle limitazioni delle finalità, il gruppo di lavoro denominato "Articolo 29" ha previsto che il titolare dovesse garantire la riservatezza e sicurezza dei dati, prevedendo il consenso tramite il meccanismo dell'"*opt-in*" ai fini della profilazione dell'interessato[142].

La raccolta così massiccia dei dati nel fenomeno dei Big Data influisce anche sul principio di minimizzazione dei dati, inteso nel senso di svolgere il trattamento dei dati con proporzionalità, necessità e non eccedendo rispetto alla quantità di dati che si intende elaborare[143].

Tale principio può esser facilmente rispettato nel fenomeno degli *Small Data* che utilizzano le tecniche tradizionali di analisi dei dati, mentre incontra grandi problematiche in materia di Big Data, dal momento che le tecniche di analisi automatizzate mediante algoritmi hanno una grande facilità di immagazzinare una miriade di informazioni. Inoltre, nei Big Data, anche i dati apparentemente non necessari possono rilevarsi di grande utilità e valore in un fenomeno di aggregazione[144].

Altro aspetto particolare è quello della conservazione dei dati, in quanto il principio di limitazione della stessa si trova in conflitto con la capacità di memorizzare grandi masse di dati e con il basso costo di archiviazione degli stessi.

Invece, con riferimento al principio di accuratezza, le tecniche di *data mining* non riescono a garantirne il suo rispetto in quanto questa modalità di raccolta utilizza varie fonti, come ad esempio *social media* e altre fonti terze. In altri termini, l'incremento delle fonti di provenienza dei dati è direttamente proporzionale al rischio di un conflitto con il principio di accuratezza[145].

Inoltre, l'art. 9 del GDPR sul trattamento di particolari categorie di dati personali risulta di difficile applicazione in quanto è complesso selezionarli e distinguerli dagli altri per due ragioni: in primo luogo, il volume elevato dei Big Data consente di procedere ad un'analisi distinguendo solo tra dati strutturati e non strutturati e; in secondo luogo, i dati personali "particolari" (relativi a salute, razza, opinioni politiche, orientamento sessuale ecc) possono esser ricavati anche da dati non particolari grazie alle decisioni automatizzate dell'algoritmo[146].

---

[142] Gruppo di lavoro "Articolo 29", *Opinion 03/2013 on purpose limitation*, aprile 2013. Secondo il gruppo di lavoro, ai fini di valutare la compatibilità con il principio di limitazione delle finalità, occorre tenere in considerazione i seguenti fattori: a) il rapporto tra le finalità per le quali i dati sono stati raccolti e gli scopi dell'ulteriore trattamento; b) il contesto in cui sono stati raccolti i dati e le ragionevoli aspettative degli interessati riguardo al loro ulteriore utilizzo; la natura dei dati e l'impatto dell'ulteriore trattamento sugli interessati; le salvaguardie applicate dal titolare del trattamento per garantire un trattamento equo e per prevenire qualsiasi impatto indebito sugli interessati; ARTICLE 29 *WorkIng Party, Guidelines on Consent under Regulation* 2016/679, WP259, 28 November 2017 ARTICLE 29 *WorkIng Party, Parere 15/2011 sulla definizione di consenso*, WP187, 13 luglio 2011.

[143] L.A. BYGRAVE, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, 2002.

[144] Così O. TENE, J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytic's*, in *Northwestern Journal of Technology and Intellectual Property*, 2013, 11, 5, 239 ss.

[145] Cfr. D. BOYD, K. CRAWFORD, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, in *Information Communication and Society*, 2015, 15, 662 ss.

[146] T. ZARSKY, *Incompatible: the GDPR in the age of big data*, in *Seton Hall Law Review*, 2017, 47, 1014 ss.

Invece, sotto il profilo dell'*accountability*, nonostante ci siano difficoltà concrete nell'applicazione dei principi sopra richiamati, ai sensi dell'art. 24.1 del GDPR[147], spetta comunque al titolare del trattamento assicurare il rispetto dei principi generali, oltre che dimostrare di aver adottato tutte le misure tecniche e organizzative adeguate a poter eseguire il trattamento in conformità al Regolamento. In altri termini, sono stati trasferiti in capo al titolare e al responsabile del trattamento i rischi derivanti dal trattamento dei dati personali, ed i costi relativi al loro contenimento, in funzione preventiva del danno, potenzialmente recato a diritti e libertà fondamentali della persona.

Inoltre, rientrano a pieno titolo nel principio di *accountability* due concetti richiamati in premessa e previsti all'art. 25 del GDPR: quello del *privacy by design*[148] e del *privacy by default*[149], che consentono al titolare-impresa di gestire e risolvere le problematiche legate alla *privacy* a livello organizzativo.

In primo luogo, il concetto di *privacy by design* ha come scopo quello di prevenire i rischi, e non di risolverli, secondo la *ratio* del c.d. *risk based approach*[150], ad esempio mediante tecniche organizzative quali la pseudonimizzazione del dato, così da renderlo anonimo –in questo modo,

---

[147] Infatti l'art. 24.1 GDPR stabilisce che: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario."*

[148] L'art. 25.1 GDPR prevede che: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati."*

[149] L'art. 25.2 GDPR prevede che: *"Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica."*

[150] Il concetto di rischio viene previsto al Considerando 75 del GDPR: *"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*" e al Considerando 76 stabilendo che: *"La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.*"

l'interessato non è più identificabile (c.d. *deidentification*) – e arginando le regole della *privacy*.
In secondo luogo, il concetto di *privacy by default* consente all'impresa di applicare il principio di minimizzazione, prevedendo che la stessa, per impostazione predefinita, possa trattare i dati personali nella misura necessaria e sufficiente alle finalità previste.
In altri termini, in base a quanto dispone l'art. 25 del Regolamento, il titolare è tenuto ad adottare tutte le misure tecniche ed organizzative adeguate al rischio, a cui vengono esposti i dati trattati sin dal momento preparatorio e progettuale dell'attività di trattamento (*privacy by design*), così come ha il compito di limitare il trattamento ai soli dati necessari, limitando al contempo gli accessi da parte di terzi a tali dati e la durata della loro conservazione (*privacy by default*).
Sotto altro profilo invece, più propriamente civilistico, nella nuova società dell'informazione digitale, i *database*[151] di grandi dimensioni sono considerati come "beni immateriali commerciabili"[152]; tali nuovi beni sono però ancora privi di protezione giuridica espressamente riconosciuta dal legislatore.
Nella pratica, per accedere ai servizi (*e.g.* di un *social network)* l'utente deve registrarsi accettando le condizioni generali di utilizzo – comprensive anche delle clausole di esonero della responsabilità del prestatore e delle licenze d'uso dei contenuti immessi – e deve prestare, consciamente o inconsciamente, il proprio consenso al trattamento dei dati personali.
Questi dati personali trattati in blocchi combinati e combinabili, innumerevoli volte, possono produrre 'nuovo valore', cioè correlazioni e risultati utili.
I trattamenti 'secondari' dei dati risultano quindi potenzialmente più importanti in termini economici di quelli primari, con il rischio evidente di elusione ed inefficacia delle normative di settore[153].
Infine, va ricordato che l'esame dei Big Data non si esaurisce nei dati personali, ma riguarda anche dati non personali (*e.g.* i dati climatici e metereologici), riutilizzabili senza incontrare limiti di liceità, tempo e finalità e, come abbiamo visto, sono regolati dal Reg. UE 2018/1807.[154]

---

[151] PALAZZOLO, *La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (UE) n. 2016/679*, in *Contr. e impr.*, 2017, p. 613 ss.
[152] T. FIA, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo notiziario giuridico*, 2019, fasc. 1, pp. 60-133, p. 65. Più in generale invece per una disamina dei beni immateriali si veda GRECO P., *I diritti sui beni immateriali*, Utet Giuridica, 1948; G. OLIVIERI, *Dal mercato delle cose al mercato delle idee Relazione al Convegno "Le parole del diritto commerciale"*, Macerata, 7 aprile 2017 in *Rivista delle società*, 2017, fasc. 4, pp. 815-824.
[153] G. GIANNONE CODIGLIONE, *Libertà di impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali ([Free enterprise, competition and net neutrality in the transnational market of personal data])*, in *Il Diritto dell'informazione e dell'informatica*, 2015, fasc. 4-5, pp. 271-304, p. 285.
[154] Sui dati non personali v. G.M. RUOTOLO, *I dati non personali: l'emersione dei "big data" nel diritto dell'Unione europea (Non-personal Data: The Surfacing of Big Data in European Union Law)*, in *Studi sull'integrazione europea*, 2018, fasc. 1, pp. 97-116; T. FIA, *La tutela dei dati non personali: accesso, proprietà e regolamentazione, cit.*

1.3.5 *Segue* – Un lento processo di patrimonializzazione dei dati e la tutela del consumatore europeo verso un mercato unico digitale: la natura non solo contrattuale del rapporto tra l'interessato e il titolare

I diritti sopra menzionati e previsti dal GDPR, con particolare riferimento al diritto alla portabilità dei dati, rientrano nell'ottica di una patrimonializzazione dei dati.

Dunque, tali dati sono di particolare rilevanza non tanto dal punto di vista della persona come valore fondante dell'ordinamento, ma dal punto di vista patrimoniale e quindi per il loro valore economico[155].

Nella dottrina italiana si sono potute distinguere due distinte teorie. In primo luogo, la teoria personalista[156], di derivazione francese e tedesca, che vede la protezione dei dati come espressione e immagine della persona[157]. Tale teoria, infatti, si fonda sulla incommerciabilità dei diritti della personalità, usando come fondamento di diritto positivo l'art. 5 del codice civile italiano, che pone significativi limiti alla possibilità di disporre del proprio corpo sulla scia della gratuità degli atti di disposizione dello stesso[158].

La seconda teoria invece è quella patrimoniale, di derivazione statunitense, che fa più attenzione all'ottica negoziale[159], facendosi forte del tradizionale sfruttamento industriale del diritto della personalità in tema di diritto d'autore e di proprietà industriale[160].

Tale teoria si basa sul fatto che i *Big Data* possono costituire un bene giuridicamente rilevante da tutelare in ragione degli investimenti fatti per la loro acquisizione, gestione, analisi ed utilizzo[161]. Si applica così l'art. 102 bis, n.1 lett. a) della Legge sul diritto d'autore (L. 22 aprile 1941, n. 633, così come modificata, per quanto qui di interesse, dal Dlgs. 6 maggio 1999, n. 169, attuativo della Direttiva 96/9/CE concernente la tutela giuridica delle banche dati) secondo cui per costitutore di una banca dati si intende "*chi effettua investimenti rilevanti per la costituzione di una banca dati o per la sua*

---

155 ARPETTI, *Economia della privacy: una rassegna della letteratura*, in *Riv. dir. media*, 2018, p. 2.

156 RESTA, *I diritti della personalità*, in *Le persone fisiche e i diritti della personalità*, a cura di ALPA e RESTA, in *Trattato di diritto civile*, diretto da SACCO, Milano, 2006, p. 361 ss. Agli stessi esiti della concezione personalista arriva anche la concezione paternalistica che proteggendo la persona da se stessa gli impedisce appunto di "vendersi". In tema cfr. F. COSENTINO, *Il paternalismo del legislatore nelle norme di limitazione dell'autonomia dei privati*, in *Quadrimestre*, 1993, 1, 119 ss.; R. CATERINA, *Paternalismo e antipaternalismo*, in *Riv. dir. civ.*, 2005, 6, 771 ss. e, in particolare, 777 s.

157 G. ALPA, *La "proprietà" dei dati personali*, *cit.* p.11.

158 S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, *cit.*, *81*.

159 S. RODOTÀ, *Conclusioni*, in *Trattamento dei dati e tutela della persona*, a cura di CUFFARO, RICCIUTO e ZENO ZENCOVICH, Milano, 1998, p. 308.

160 Per un approfondimento generale v. M. LIBERTINI *Lezioni di diritto industriale*, Torre, Catania, II ed., 1990; M. LIBERTINI, *Tutela e promozione delle creazioni intellettuali e limiti funzionali della proprietà intellettuale*, in A.I.D.A. (Annali Italiani del Diritto d'Autore), 2014, 299-336; V. MANGINI– A.M. TONI, *Manuale breve di diritto industriale*, Giappichelli, Torino, 2015; A. VANZETTI– M. DI CATALDO, *Manuale di diritto industriale*, Giuffrè, Milano, 2012.

161 A.G. PARISI, op.cit., 133.

verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro".

Quindi, l'impresa (che gestisce il sito o il motore di ricerca) è il costitutore di una banca dati al quale è riconosciuto il diritto *sui generis*[162] di vietare le operazioni di estrazione o il reimpiego della stessa. Ebbene, grazie a questa teoria, si evita la negoziazione con ciascun titolare, riconoscendo a quest'ultimo un diritto di proprietà sui propri dati e, allo stesso tempo, si favorisce la circolazione di questi da parte delle imprese che costituiscono le banche dati.

Tale impostazione industrialistica ha infatti influenzato la riflessione dottrinale sui diritti della personalità, dal momento che lo stesso legislatore distingue i diritti di tipo economico, che sorgono dalla creazione di un'opera o d'invenzione, da quelli c.d. morali[163]. Infatti, mentre i primi sono liberamente disponibili, i secondi non lo sono. Tale evoluzione, intervenuta in ambito industriale, è la testimonianza di come lo sfruttamento commerciale degli attributi immateriali sia un fenomeno già noto e risalente. In quest'ottica, il contratto avente ad oggetto il contenuto economico del diritto sarebbe lecito, mentre quello avente ad oggetto il contenuto morale sarebbe illecito[164].

Tale teoria riconoscerebbe così un contenuto economico e commerciale anche ai diritti immateriali della personalità riconducendo i limiti dell'autonomia privata, in sede di contrattualizzazione di tali diritti, ai casi di illiceità del contratto[165]. Peraltro, tale teoria sembra prevalere anche in virtù delle ultime pronunce dei giudici[166] e delle Autorità nazionali[167] ed europee, nonché del recente evolversi del diritto dell'Unione europea.

---

[162] Tale diritto è sui generis in quanto inquadrato nella categoria dei diritti connessi al diritto d'autore e ha un contenuto del tutto eterogeneo. Così BOGNI, *Big Data: diritti IP e problemi della privacy*, in *Dir. Industriale*, volume n. 2/2015.

[163] In questo senso, con particolare riferimento al contenuto patrimoniale del diritto all'immagine nell'ordinamento italiano, cfr. G. RESTA, *Autonomia privata e diritti della personalità*, 41 ss.; V. METAFORA, *Il mito di Narciso e la giurisprudenza: a pro- posito del diritto sul proprio ritratto*, in *Riv. crit. dir. priv.*, 1990, 867 ss; M. PROTO, *Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale*, 2012.

[164] S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, *cit.* 84.

[165] D. MESSINETTI, voce *Personalità (diritti della)*, in *Enc. dir.*, XXIII, Milano, 1983, 355-406, 382-384 dove afferma che "il valore costituito dalla persona rivela la sua capacità a divenire criterio ordinante di una normativa di ordine pubblico (o di buon costume)" e che, quindi, "il valore normativo della persona può essere chiamato ad integrare i criteri secondo cui si giudica della liceità di comportamenti posti in funzione nel conseguimento di un determinato risultato. Ne consegue che la qualificazione di liceità, in tale prospettiva, più che al valore rappresentato dalla persona, attiene direttamente alla considerazione e valutazione dell'attività concretamente posta in essere" .

[166] V. *ex multis* Cass., 11 ottobre 1997, n. 9880, in *Resp. civ. prev.*, 1998, II, 1063-1067, con nota di A. DASSI, *La natura atipica del contratto di sponsorizzazione*, 1067-1070;, Cass., 16 aprile 1991, n. 4031, in *Nuova giur. civ comm.*, 1992, I, 54 ss. con nota di M. RICOLFI, *Questioni in tema di regime giuridico dello sfruttamento commerciale dell'immagine,* secondo cui [i]l consenso alla divulgazione del proprio ritratto, almeno per quanto riguarda una certa categoria di persone, si concreta, normalmente, in un vero e proprio negozio avente per oggetto un *pati* in funzione di una controprestazione a carattere patrimoniale. Codesti negozi sono diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico. Salve le ipotesi di pubblicazione del ritratto in circostanze tali per cui possa profilarsi una lesione al decoro o alla reputazione (si tratta in questi casi di beni non patrimoniali del tutto indisponibili sì che relativamente ad essi si potrebbe parlare solo di consenso dell'avente diritto, sempre revocabile), non è più in discussione la compatibilità di negozi aventi per oggetto l'utilizzazione altrui di un proprio ritratto con i principi del buon costume".

[167] V. per tutti AGCM, AGCOM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui Big Data*, 10 febbraio 2020.

Nel 2014, la Commissione europea ha sottolineato l'importanza di rendere il mercato interno al passo con lo sviluppo dell'economia dei dati, indicando i passi da compiere per rendere l'area europea competitiva a livello internazionale[168].

Successivamente, nel 2016, il GDPR rafforza la libera circolazione dei dati[169], inserendosi all'interno della strategia per il mercato unico digitale annunciata nel maggio 2015 dalla c.d. Commissione Juncker[170] e affidata a Marija Gabriel dal 7 luglio 2017[171].

Successivamente, nel 2018, viene adottato il Regolamento 2018/1807 sulla libera circolazione dei dati non personali, ritenuto uno degli ultimi tasselli necessari alla creazione di regole giuridiche chiare, complete e prevedibili per il trattamento dei dati e il rafforzamento della competitività dell'industria dell'Unione. Nel GDPR si alternano dunque fattispecie e istituti tipici del diritto delle obbligazioni con altri istituti eccezionali (*e.g.* la revoca del consenso), che trovano una giustificazione nella sola natura del bene trattato[172]. Il problema del bilanciamento degli interessi, infatti, viene risolto dal GDPR; da un lato, rafforzando i diritti della persona e, dall'altro, liberalizzando i servizi tramite la tecnologia digitale. Quindi, sebbene in modo non del tutto lineare, la tutela dell'interessato è passata da una lettura personalista ad una patrimoniale[173].

Quest'ultima, infatti, si è affermata stabilmente solo con il GDPR che, ad esempio, nell'enunciare le condizioni di liceità del trattamento, come sopra esaminato, fa espresso richiamo alla fattispecie contrattuale. Questo profilo consente quindi di legittimare il trattamento dei dati personali, non solo in virtù di un contratto avente ad oggetto una prestazione diversa rispetto al trattamento, ma anche in virtù di un accordo che abbia ad oggetto lo stesso trattamento dei dati personali.

---

[168] v. In particolare, v. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Verso una florida economia basata sui dati*, COM(2014) 442 final. Tra i diversi punti, la Commissione si è concentrata su diversi temi quali, ad esempio, il *cloud computing*, le reti 5G, *Internet of Things* e nuove infrastrutture pubbliche.

[169] V, DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017; M. LILLÀ MONTAGNANI, *op. cit.*; R. MESSINETTI, *Circolazione dei dati e autonomia privata*, N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, pp. 137 ss 2019.

[170] COM (2015) 192 final http://ec.europa.eu/priorities/digital-single-market/.

[171] L'obiettivo è lo sviluppo di un'economia digitale in grado di espandere i mercati e di superare le barriere esistenti nell'Unione. V. anche A. DELLI PONTI, *Mercato unico digitale: la nuova normativa per la fornitura di servizi online dell'UE*, in https://www.ictsecuritymagazine.com, 10 ottobre 2019. Il mercato unico digitale è parte del programma Agenda digitale per l'Europa 2020 che rientra nell'ambito della strategia Europa 2020. I tre pilastri della strategia della Commissione europea sono: i) accesso a prodotti e servizi online; ii) condizioni per la crescita e lo sviluppo delle reti e dei servizi digitali; iii) crescita dell'economia digitale. L'attuazione di questa strategia è stata realizzata con l'introduzione della direttiva sul diritto d'autore nel mercato unico digitale (direttiva 2019/790).

[172] V. *supra* nota n. 81.

[173] Infatti, all'inizio della trattazione abbiamo visto come negli anni le due letture si sono alternate perché la direttiva del 1995 parlava già di circolazione dei dati, direttiva che poi è stata disattesa in fase di recepimento nazionale dapprima con la legge di recepimento del 1996 e, successivamente, nel 2003 con l'emanazione del nostro Codice della privacy, il quale aveva l'obiettivo di proteggere l'identità personale dei consumatori non comprendendo che solo riconoscendo la commercializzazione dei dati personali si sarebbe potuto iniziare a tutelare seriamente il consumatore.

Ulteriore conferma viene data dall'art. 1 co. 3 del GDPR, dove si legge che: "*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Dunque, il dato personale inizia ad essere considerato alla stregua di un bene che ha un suo valore economico, una ricchezza; coerentemente, gli istituti disciplinati dal GDPR acquistano una maggiore valenza patrimoniale.

Ed è proprio da qui che infatti sono partite due proposte di Direttive della Commissione Europea[174] che rientrano, insieme alle direttive 2019/770/UE e 2019/771/UE, nel c.d. "New deal per i consumatori", completato da ultimo dalla sopra menzionata direttiva *Omnibus*, entrata in vigore il 7 gennaio 2020[175] e che si inserisce in un'ottica di unificazione della disciplina sulla tutela dei consumatori.

Tale pacchetto, si inerisce all'interno della strategia per il mercato unico digitale, partendo dal presupposto che la disciplina vigente non è adatta ad assicurare una effettiva tutela ai consumatori che contrattano *online*. Il pacchetto mira, quindi, al rafforzamento delle regole che operano in una pluralità di contesti[176], adeguandole all'evoluzione degli strumenti digitali.

In un quadro europeo, si è iniziato così a parlare di contratti che hanno ad oggetto anche i dati di natura personale, nell'ottica della costituzione di un mercato unico digitale.

Pertanto, l'impresa che svolge un'attività economica mediante il trattamento e la circolazione dei dati personali, deve valutare anche i rischi e i costi derivanti dal diritto della protezione dei dati.

In quest'ottica negoziale e consumeristica c'è però un paradosso, in quanto colui che vuole ottenere il bene-dato personale risulta essere la parte forte del contratto, mentre colui che fornisce il dato personale medesimo è la parte debole. Tale paradosso trova fondamento nell'effettiva possibilità di rifiutare o meno il consenso al trattamento o di negoziarne i termini e le condizioni.

In altre parole, il rapporto negoziale vede contrapporsi, da una parte, il titolare del trattamento, ovvero l'impresa che desidera trattare il bene-dato personale e, dall'altra parte, l'interessato-parte debole, il quale è invece in grado di fornire il dato consistente in quella "particolare ricchezza"

---

[174] Le proposte sono state presentate l'11 aprile 2018 e sono due: una [COM (2018) 184]relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori che abroga la Dir. 2009/22/CE; l'altra [COM(2018) 185] sulla modifica di 4 direttive(la Dir. 93/13/CEE del Consiglio sulle clausole abusive nei contratti con consumatori, la Dir. 98/6/CE del Parlamento europeo e del Consiglio sui prezzi dei prodotti offerti ai consumatori, la Dir. 2005/29/CE del Parlamento europeo e del Consiglio sulle pratiche commerciali scorrette e la Dir. 2011/ 83/UE del Parlamento europeo e del Consiglio sui diritti dei consumatori) relativa agli interessi dei consumatori.

[175] Gli Stati membri dovranno adottare e pubblicare le disposizioni necessarie per conformarsi alle relative disposizioni entro il 28 novembre 2021. Le misure di attuazione, in ogni caso, inizieranno ad applicarsi a decorrere dal 28 maggio 2022.

[176] Per un approfondimento v. A. CILENTO, *"New deal" per i consumatori: risultati all'altezza delle ambizioni?* in *Contratto e impresa*, 2019, fasc. 3, p. 1208.

patrimonialmente valutabile[177].

In tal senso, quindi, il diritto alla protezione dei dati personali può rappresentare un requisito di tutela del consumatore, in quanto consente il governo del dato personale[178], ossia il governo dell'elemento costitutivo nell' "economia del prezzo-zero".

Ecco che quindi, mediante i *Big Data Analytics,* i nostri dati, raccolti per le finalità più disparate, concorrono a ridefinire le nostre identità: quelle "transattive" derivanti dalla ricostruzione del profilo di consumatore di ognuno; e quelle "predittive" che anticipano comportamenti, scelte e responsabilità[179]. Inoltre, è possibile constatare, sul piano economico prima ancora che giuridico, la non reale gratuità di una cessione di dati.

Basti pensare come con le moderne tecnologie, ad esempio gli *smartphone*, con l'uso di un semplice tasto è possibile ottenere giochi elettronici o altri servizi, sia dietro il pagamento di piccole somme, sia "gratuitamente". Si pensi altresì ai contratti stipulati per l'utilizzo dei *social network* (*e.g. Facebook, Instagram, Linkedin* ecc.) o dei motori di ricerca (*e.g. Google, Safari, Youtube*), dove si possono usare i loro servizi di ricerca in apparente gratuità e senza un'apparente controprestazione contrattuale[180]; in queste ipotesi, infatti, l'utente fornisce i propri dati in cambio dell'utilizzo del motore di ricerca o del *social network*[181].

In termini economici, c'è chi ha quantificato il valore medio quotidiano di un singolo dato personale intorno ad un dollaro[182], ma tale importo irrisorio non impedisce di ragionare in termini di un'operazione di scambio; tale assunto diventa ancora più comprovato quando si parla di Big Data, e cioè quando i dati personali oggetto di scambio sono raccolti, trattati e gestiti in massa. Infatti, se si

---

[177] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato, cit.*, p. 118.

[178] Cfr. A. SORO, *L'universo dei dati e la libertà della persona, cit. p. 8.*

[179] *Id.* p. 19.

[180] Tuttavia, il punto di partenza indiscusso è l'esistenza di un interesse economico a offrire "gratuitamente" i servizi in questione. In proposito cfr. P. SAMMARCO, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0,* in *Dir. inf.*, 2010, 639; F. ASTONE, *Il rapporto tra gestore e utente: questioni generali,* in *Aida*, 2011, 114, il quale, descrivendo la struttura dei *social networks*, sostiene che "*l'attività del gestore trova così giustificazione nello scambio che, in ragione dell'attività degli utenti, si realizza con l'inserzionista; allo stesso modo, la gratuità del servizio fornito agli utenti è funzione di quel medesimo scambio ed è – come prima già si diceva – una gratuità interessata, giustificata dal collegamento causale che si realizza tra prestazioni del gestore, prestazioni dell'inserzionista, attività degli utenti"*; R. CATERINA, *Cyberspazio, social network e teoria generale del contratto,* Aida, 2011, 96, secondo il quale*"[i] contratti per i servizi di social network di norma non prevedono il pagamento di un corrispettivo da parte degli utenti. Non sono evidentemente, contratti liberali: i fornitori di servizi di social network perseguono un interesse economico, attraverso la vendita di spazi pubblicitari e la commercializzazione di attività di profilazione dell'utenza. Si può parlare di contratti gratuiti interessati (a meno che non si voglia configurare l'autorizzazione a trattare i dati personali come un vero e proprio prezzo per la fruizione dei servizi)"*; W. VIRGA, *Inadempimento di contratto e sanzioni private nei social network,* Aida, 2011, 232, il quale evidenzia il fatto che "*per il gestore del servizio gli utenti, in realtà, non rappresentano altro che la contropartita offerta agli inserzionisti a fronte del loro investimento*".

[181] C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014, 88; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete,* cit., 416 s.

[182] MALGIERI e CUSTERS, *Pricing Privacy: The Right to Know the Value of Your Personal Data,* in *Computer Law & Security Review*, 2018, 34, p. 289 ss, p. 294

considerasse la grande quantità di dati a disposizione del singolo *social network* o motore di ricerca si potrebbe comprendere l'immenso valore economico degli stessi.

Questo trattamento in massa di dati consente all'impresa di gestirli, selezionarli e usarli per comprendere – mediante l'utilizzo di algoritmi da parte delle nuove tecniche di *Data analytics* – le esigenze, preferenze, spostamenti e tendenze del singolo soggetto, al fine di poterle anticipare e da poter offrire sul mercato ciò che quello specifico soggetto cerca in quello specifico momento di vita.

In tal senso, si esprime anche il legislatore europeo nella Direttiva UE 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche, il quale al *Considerando* n. 16, dopo aver definito nella prima parte il servizio di comunicazione elettronica, precisa che: *"Nell'economia digitale i partecipanti al mercato sempre più spesso ritengono che le informazioni sugli utenti abbiano un valore monetario. I servizi di comunicazione elettronica sono spesso forniti all'utente finale non solo in cambio di denaro, ma in misura sempre maggiore e in particolare in cambio della comunicazione di dati personali o di altri dati. Il concetto di remunerazione dovrebbe pertanto ricomprendere le situazioni in cui il fornitore di un servizio chiede all'utente finale dati personali ai sensi del regolamento (UE) 2016/679 o altri dati, e questi glieli trasmette consapevolmente, per via diretta o indiretta."*

In altri termini, il riferimento alla controprestazione contrattuale colloca la tematica del trattamento e della circolazione dei dati personali nell'alveo del diritto delle obbligazioni e dei contratti.

Tuttavia, il parere del 14 marzo 2017 del Garante europeo per la protezione dei dati personali (*European Data Protection Supervisor*) sui contratti per la fornitura di contenuto digitale, pur ammettendo l'esistenza di un mercato dei dati, manifestava seri dubbi sull'uso della nozione stessa di "controprestazione", sostenendo che un diritto fondamentale come il diritto alla protezione dei dati personali non possa esser considerato merce e ridotto a semplice interesse del consumatore[183].

In un parere successivo, il Garante europeo, in occasione del "New deal per i consumatori" sopra menzionato, da una parte si compiace di una proposta del legislatore europeo che possa garantire

[183] Così il Garante europeo per la protezione dei dati personali, Opinion 4/2017 in www.edps.europa.eu, p. 3, che prevede: "*However, one aspect of the Proposal is problematic, since it will be applicable to situations where a price is paid for the digital content, but also the where digital content is supplied in exchange for a counter-performance other than money in the form of personal data or any other data. The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be not be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity. The recently adopted data protection framework (the "GDPR") is not yet fully applicable and the proposal for new e-Privacy legislation is currently under discussions. The EU should avoid therefore any new proposals that upset the careful balance negotiated by the EU legislator on data protection rules. Overlapping initiatives could inadvertently put at risk the coherence of the Digital Single Market, resulting in regulatory fragmentation and legal uncertainty. The EDPS recommends that the EU apply the GDPR as the means for regulating use of use of personal data in the digital economy. The notion of "data as counter-performance" - left undefined in the proposal - could cause confusion as to the precise function of the data in a given transaction. The lack of clear information from the suppliers in this regard may add further difficulties. We therefore suggest considering, as a way of resolving this problem, the definition of services under the TFEU and the provision used by the GDPR to define its territorial scope may assist in".*

maggiori protezioni ai consumatori, dall'altra però conferma ancora una volta le sue preoccupazioni in merito all'utilizzo, nei contratti per la fornitura di contenuto digitale, del termine "controprestazione", che implica necessariamente una considerazione economica dei dati personali, sostenendo appunto che tale approccio non terrebbe conto della natura giuridica fondamentale della protezione dei dati stessi. [184]

Il legislatore europeo della Direttiva omnibus sembra accogliere le istanze e preoccupazioni del Garante europeo e, nella parte del *considerando* n. 31, stabilisce che: "*Data la loro somiglianza e la loro interscambiabilità, i servizi digitali a pagamento e i servizi digitali forniti contro dati personali dovrebbero essere soggetti alle stesse norme ai sensi di tale direttiva*".

Similmente, sempre all'interno del pacchetto legislativo "New deal per i consumatori" al *considerando* 24 della Direttiva UE 2019/770 si prevede che:" *La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali. I dati personali potrebbero essere forniti all'operatore economico al momento della conclusione del contratto o successivamente, (…). La presente direttiva dovrebbe applicarsi ai contratti in cui il consumatore fornisce, o si impegna a fornire, dati personali all'operatore economico. (…) La presente direttiva dovrebbe altresì applicarsi nel caso in cui il consumatore acconsenta a che il materiale che caricherà e che contiene dati personali, come fotografie o post, sia trattato a fini commerciali dall'operatore economico. Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale"*.

A parere di chi scrive questa sembra una lettura ipocrita del fenomeno visto che: da un lato, si riconosce l'esistenza di un mercato e di modelli commerciali[185] aventi ad oggetto dati personali,

[184] Così lo stesso Garante europeo per la protezione dei dati personali nell'Opinion 8/2018 del 5 ottobre 2018.

[185] Si parla a proposito di *Personal data economy models*, ossia di quei modelli di ricchezza basati sui dati personali, diffusi in particolare negli Stati Uniti e consentono agli operatori economici di acquistare i dati direttamente dai consumatori. Questi modelli possono comprendere due tipi di dati: i *data-insight models* tramite i quali le società offrono agli utenti piattaforme in cui raccogliere, gestire e commerciare i propri dati personali e; i *data-transfer models* attraverso cui le imprese a fronte di un corrispettivo acquistano le informazioni direttamente dagli utenti e, dopo averle catalogate e dopo avergli assegnato un valore, le mettono sul mercato dove terzi possono acquistarle.

dall'altro, si fa fatica a parlare di "valore economico" o di "prezzo" dei dati personali come controprestazione[186]. Lo stesso EDPB, con linee guida 2 del 2019, ha precisato che i dati personali non possono essere considerati come merce scambiabile[187]; gli interessati possono, dunque, accettare il trattamento dei propri dati personali, ma non possono commerciare i loro diritti fondamentali[188].

Il paradosso sorge però ogni qual volta i titolari del trattamento, e non gli stessi interessati, cedono i dati personali per motivi economici; sarebbe infatti un controsenso lasciare il diritto di "commercializzazione" dei dati a tutti, eccetto agli interessati al trattamento.

Inoltre, se da una parte si è restii a vedere il dato come una merce, dall'altra si riconosce l'esigenza di estendere i rimedi contrattuali ai servizi digitali forniti contro dati personali.

In altri termini, da una parte, il legislatore europeo fa un distinguo terminologico tra servizi digitali a pagamento e servizi digitali forniti contro dati personali, dall'altra, riconosce la loro interscambiabilità e l'applicabilità della direttiva in oggetto per entrambe le tipologie di servizi; insomma, cambierebbe la forma ma non la sostanza.

Infine, il legislatore europeo rimette ai singoli Stati membri e al diritto nazionale la scelta del rapporto individuale, a prescindere che esso sia di natura contrattuale.

La dottrina più accorta però si era già espressa nel senso di riconoscere una struttura giuridica di tipo contrattuale[189], escludendo così, con riferimento al rapporto tra titolare e interessato, altre fattispecie come i rapporti di mero fatto o altri tipi di obbligazioni.

Le ragioni addotte da tale dottrina a fondamento delle sue conclusioni sono diverse.

In primo luogo, lo stesso GDPR sembra richiamare rapporti giuridici di natura obbligatoria aventi ad oggetto dati personali e fa più volte espresso riferimento al contratto quando, all'art. 20 del GDPR e al *considerando* 68, tratta dei due presupposti per l'applicabilità del diritto alla portabilità dei dati; per l'esercizio di quest'ultimo, infatti, il GDPR presuppone un diritto di natura relativa che ha la propria fonte nel consenso o in un fenomeno patrimoniale, oltre a riconoscere anche il trattamento

---

[186] Dello stesso avviso anche RESTA e ZENO ZENCOVICH *op. cit.*

[187] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf

[188] In particolare, al punto 51 (vedi anche nota 28) delle linee guida citate, l'EDPB afferma che: "*Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity. Data subjects can agree to processing of their personal data but cannot trade away their fundamental rights. Besides the fact that the use of personal data is regulated by the GDPR, there are additional reasons why processing of personal data is conceptually different from monetary payments. For example, money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained*".

[189] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato, cit.*, p. 124; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit.; S. SCALZINI, *L'estrazione di dati e di testo per finalità commerciali dai contenuti degli utenti. Algoritmi, proprietà intellettuale e autonomia negoziale* in *Analisi Giuridica dell'Economia,* 2019, fasc. 1, pp. 395-423.

con mezzi automatizzati come i *Big Data Analytics.*

In secondo luogo, sempre nell'ambito del diritto alla portabilità dei dati, ciò che più rileva ai fini della natura contrattuale del rapporto è che l'interessato ha il diritto di ottenere che il trasferimento dei dati personali passi direttamente ad un terzo da parte del primo titolare (c.d. trasferimento diretto). Infatti, la pretesa, imposta dall'interessato al titolare originario, di trasferire i dati ad un altro operatore economico, non può che ricondursi alla nozione di obbligazione di cui all'art. 1174 c.c.

Tuttavia, non deve rilevare a tal fine il fatto che il rapporto tra titolare-impresa e interessato-consumatore sia disciplinato da una legge, il GDPR. Infatti, com'è noto, nel recente diritto dei contratti non mancano casi d'integrazione del contenuto del contratto e di determinazioni del rapporto che hanno titolo nella legge, come ad esempio l'integrazione del contratto dell'art. 1374 c.c.[190] e l'istituto della sostituzione automatica di clausole invalide dell'art. 1339 c.c.[191]

Relativamente invece alla tipologia contrattuale occorre dire che l'operazione economica avente ad oggetto i dati è elastica e flessibile, in coerenza con i nuovi modelli commerciali in oggetto; dunque, non deve commettersi l'errore di circoscrivere tali operazioni economiche in una specifica tipologia contrattuale[192].

Sul punto occorre distinguere la cessione del dato personale quando è fatta per fini commerciali (indipendentemente dall'esistenza di una corresponsione di denaro) dalla cessione del dato personale, per poter accedere a servizi digitali. Ebbene, se il primo caso di cessione è all'interno di una struttura contrattuale, il secondo caso è al di fuori della struttura contrattuale; infatti, il rapporto di trattamento può essere accessorio a quello di fornitura e acquisto di un determinato bene di consumo. Tuttavia, sebbene si tratti sicuramente di accessorietà economica, non è detto che si tratti di accessorietà giuridica.

La struttura contrattuale della compravendita viene esclusa da autorevole dottrina dato che l'interessato non perde mai il controllo sul bene-dato personale, come si evince ad esempio dal diritto alla cancellazione dei propri dati, così come dal diritto di accesso sopra menzionati.

Tale struttura contrattuale si esclude, dato che nulla impedisce ad altri titolari di trattare lo stesso dato personale. Piuttosto che parlare di trasferimento in capo al titolare, si parla di un diritto soggettivo in capo a quest'ultimo, che gli consente di trattare il dato e di utilizzarlo ai fini di uno sfruttamento economico sul mercato.

---

[190] C.M. BIANCA, *Il Contratto,* Milano. 2019, p. 453 ss.; GALGANO, *Effetti del contratto. Rappresentanza. Contratto per persona da nominare,* in *Comm. Scialoja-Branca*, a cura del medesimo Art. 1372-1405, 65; RODOTÀ, *Le fonti di integrazione del contratto,* Milano, 1969; D'ANGELO, *Contratto e operazione economica*, Torino, 1992.

[191] C.M. BIANCA, *Il Contratto,* cit., p. 465; CASELLA, *Nullità parziale del contratto e inserzione automatica di clausole*, Milano, 1974; SARACINI, *Nullità e sostituzione di clausole contrattuali*, Milano, 1971; GIAQUINTO DI MAJO, *L'esecuzione del contratto*, Milano, 1967.

[192] Così V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato, cit.,* p. 124.

Diversamente, ci si potrebbe avvicinare maggiormente ai diritti reali nel caso dei *Big Data* dove il titolare trasforma e utilizza l'originario dato personale ricavandone – grazie alla tecnologia di *Data Analytics* – dati di "secondo grado", alla luce di una profilazione dell'interessato e di una conseguente categorizzazione in classe di dati. Infatti, in questo caso, si potrebbe assistere alla produzione di un "nuovo bene", ricavato grazie allo sfruttamento dell'originario dato personale, sempre che quest'ultimo abbia perso la sua "personalità" e dunque, ai sensi della definizione di dato personale dell'art. 4 n.1 del GDPR[193], l'informazione riguardante la persona fisica a cui apparteneva non sia più identificabile[194].

Pertanto, acquisita la consapevolezza che alla base della circolazione dei dati personali possa esserci un contratto, occorrerà, a livello nazionale, valutare la tipologia dello stesso, visto e considerato che, né il GDPR, né la direttiva omnibus per la protezione dei consumatori online si esprimono in tal senso.

1.3.6 *Segue* – Un breve cenno al *Digital Services Act* e ai nuovi obblighi di trasparenza per *Big Tech*

Il "*Digital Services Act*" (di seguito, DSA) è una proposta di regolamento della Commissione europea e, come tale, dovrà subire un *iter* legislativo che, come per il GDPR, prenderà probabilmente anni, anche data la sua portata e gli interessi in ballo.

Già dal titolo risulta chiaro come la proposta in questione andrà a modificare il quadro normativo previsto dalla *Direttiva sul Commercio Elettronico (2000/31/EC)*, nonostante mantenga pienamente saldi i suoi principi cardine (*e.g.* sulla responsabilità e sulla clausola del mercato interno) e i diritti fondamentali degli utenti.

Tale proposta regolamentare non pregiudica inoltre quanto previsto dal GDPR, dalla direttiva *Omnibus*, dalla Carta dei diritti fondamentali dell'UE e dalla Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU).

L'obiettivo della Commissione europea sembra essere diretto a fornire un nuovo quadro giuridico dei servizi digitali che sia in grado di rafforzare il mercato unico digitale e garantire il rispetto dei diritti e dei valori dell'Unione, tutelando i diritti fondamentali che sempre più sono influenzati dalla *governance* dei soggetti privati nella società dell'informazione.

In assenza di tale intervento, infatti, è probabile che gli Stati membri adottino strategie nazionali che porterebbero ad un incremento della frammentazione giuridica e alla creazione di ostacoli allo sviluppo delle imprese europee, rafforzando il potere dei *Big Tech*. L'emanazione di misure nazionali

[193] È dato personale "*qualsiasi informazione riguardante una persona fisica identificata o identificabile [...]*" (art. 4, lett. 1, GDPR).

[194] Sulle tecniche di anonimizzazione e pseudonimizzazione in materia di Big Data v. G. D'ACQUISTO, M. NALDI, *Big Data e Privacy by design*, Torino, 2017.

e indipendenti rischierebbe di non dare effettiva tutela ai diritti e alle libertà nell'Unione europea.
Tale contesto normativo mostra il ruolo dei diritti fondamentali nella società dell'informazione, specialmente ai tempi della pandemia di COVID-19. Risulta inoltre dirimente comprendere se l'ambito di applicazione di tale proposta regolamentare ricomprenda non solo gli attori pubblici, come tradizionalmente accade, ma anche soggetti privati, quando questi ultimi esercitano funzioni para-pubblicistiche. Quest'ultima ipotesi, infatti, risulta essere un'opzione praticabile al fine di evitare che l'esercizio di libertà fondamentali si trasformi in un potere che sfugga alla cornice costituzionale.
In particolare, il DSA adatta il diritto civile e commerciale dell'Unione europea agli operatori digitali, ai fini di garantire maggiore equità, trasparenza e responsabilità relativamente alla fornitura di servizi digitali. Il DSA reagisce anche all'utilizzo di sistemi di intelligenza artificiale da parte di attori pubblici e privati, rispettando gli impegni presi dalla Commissione europea nel documento "*Shaping Europe's Digital Future*"[195], con riferimento agli obblighi e responsabilità per i fornitori di servizi digitali, quali le piattaforme *online*.
Sebbene l'introduzione di nuovi diritti potrebbe portare alla compressione delle libertà economiche e di altri diritti fondamentali, il DSA colma una lacuna ventennale nel regime di responsabilità delle piattaforme, tutelando i diritti e la democrazia nell'Unione europea.
In altri termini, la proposta contenuta nel DSA costituisce un passaggio fondamentale per colmare il divario tra individui e poteri privati, prevedendo strumenti di tutela nei confronti di questi ultimi.
In particolare, il DSA mantiene le regole di responsabilità per gli intermediari *online*, ormai stabilita come fondamento dell'economia digitale e strumentale alla tutela dei diritti fondamentali.
Il DSA è volto ad introdurre nuove regole in materia di pubblicità personalizzata *online* e raccomandazioni: gli utenti avranno diritto ad una maggiore trasparenza, a sapere perché hanno visto una certa pubblicità o un certo contenuto raccomandato (e in base a quale profilazione). Questo incide anche sulla trasparenza e il modo di operare degli algoritmi di profilazione.
Nel DSA sono previsti obblighi aggiuntivi per quelle piattaforme che sono ritenute "*very large online platforms*" e che hanno oltre 45 milioni destinatari del servizio; in questo caso, è infatti previsto uno standard più elevato di trasparenza e responsabilità su come i fornitori di tali piattaforme moderano i contenuti, sulla pubblicità e sui processi algoritmici.
Tali piattaforme digitali saranno dunque obbligate a sviluppare strumenti di gestione appropriati e a ridurre i rischi sistemici connessi al proprio business; a tal riguardo, la Commissione europea vigilerà sul rispetto degli obblighi previsti. Inoltre, in caso di mancato rispetto di questi ultimi, sono previste sanzioni fino al 6% del fatturato su scala globale nell'anno precedente.

[195] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

1.3.7 Segue – Il GDPR come *benchmark* internazionale: il caso californiano e quello cinese

Lo Stato della California ha emanato di recente il c.d. *California Consumer Privacy Act* (CCPA) che è stato firmato il 28 giugno 2018 ed è entrato in vigore a gennaio 2020. Sebbene esso sia applicabile solo per i cittadini dello Stato della California, anche società come *Facebook*[196] e *Google* devono adeguarsi, per evitare di imbattersi in due regimi molto diversi (quello della California e quello del resto degli USA) e, di conseguenza, aumentare i costi d'impresa, come quelli di *compliance*.

Il CCPA pare essere in parte ispirato al GDPR europeo, sebbene parli in modo più espresso di diritti dei consumatori.

A ciò si aggiunga che, in occasione delle ultime elezioni americane, questa legge è stata potenziata con l'introduzione di una nuova autorità che, sul modello europeo del Garante della privacy, prenderà in carico le segnalazioni degli utenti quando i propri dati personali non sono trattati in conformità alla legge. La decisione è frutto del referendum sulla c.d. "*Proposition 24*", che si è tenuto lo stesso giorno delle elezioni presidenziali.

Ebbene, la CCPA, pur aggiungendo nuove misure di protezione per i dati sensibili (e.g. quelli sulla salute, la razza o la religione), è ancora ben lontana dagli *standard* del GDPR; essa prevede ad esempio che siano gli utenti a dover navigare tra le impostazioni per fare *opt-out,* invece di dover dare il consenso preventivo al trattamento dei propri dati.

Anche in Cina, uno dei paesi con più largo uso di telecamere per la videosorveglianza e il riconoscimento facciale, qualcosa sta cambiando.

Infatti, anche nella sede del gigante dell'*e-commerce* cinese Alibaba, si sta facendo largo la proposta di vietare la raccolta di dati personali con le telecamere installate nei complessi residenziali.

Mentre i cinesi non si oppongono troppo all'idea che il governo possa avere accesso ai propri dati personali, quando questo garantisce ordine e sicurezza, non si può dire che la stessa fiducia sia riposta nelle imprese private; infatti, è stata pubblicata una bozza di legge sulla protezione dei dati, con l'obiettivo di regolare la gestione dei dati personali da parte delle imprese[197].

Come abbiamo già visto per il CCPA, anche nella bozza cinese è evidente l'ispirazione al GDPR e, sembra ci sia l'intenzione di fare molti passi avanti nella tutela della *privacy*; si prevede, per esempio, la creazione di una struttura statale che promuova l'educazione alla *privacy* e veda convergere

[196] Mark Zuckerberg, dopo l'audizione al Congresso americano, apriva all'intervento legislativo con obiettivo di cristallizzare le norme sul trattamento dei dati personali, stabilendo ciò che le piattaforme possono fare, oppure no, per aumentare nei soggetti la sicurezza di poter disporre a proprio agio dei dati personali e del profilo, finalmente nella consapevolezza del loro valore.

[197] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/?s=09. Per il testo in lingua originale cfr. https://npcobserver.files.wordpress.com/2020/10/personal-information-protection-law-draft.pdf.

pubblico e privato.

Inoltre, come nel caso del GDPR, la legge si applicherà anche a quelle società che, pur essendo stabilite fuori dal territorio cinese, offrono i loro servizi ai cittadini in Cina. Il trattamento dei dati deve essere collegato a scopi precisi e deve seguire il principio della minimizzazione dei dati (non devono essere richiesti più dati di quelli strettamente necessari per perseguire lo scopo). Gli utenti potranno negare il proprio consenso dopo averlo concesso, mentre le imprese non potranno impedire l'accesso al servizio in caso di mancato consenso, salvo che quest'ultimo non sia necessario.

È prevista l'obbligatorietà di un'informativa sui dati e la loro conservazione per il minor tempo necessario; inoltre, qualora l'impresa titolare del trattamento si avvalesse di fornitori, essa dovrà stipulare un accordo che regoli i limiti e gli scopi dell'uso dei dati.

Nella bozza è richiesta l'adozione di misure di sicurezza idonee e, in alcuni casi, la nomina di una figura simile al nostro responsabile per la protezione dei dati.

Ulteriore novità degna di nota, tanto più in un paese come la Cina in cui esiste il c.d. *social score*, è l'introduzione, all'articolo 25, di una norma che prevede la possibilità di opporsi alle decisioni prese in base a un trattamento automatizzato dei dati.

L'articolo 35 disciplina invece il trattamento dei dati da parte dello Stato, che deve richiedere il consenso degli interessati, salvo non sia previsto il segreto di legge o il consenso sia necessario per scopi simili.

Ciò nonostante, è difficile dire fin dove possa estendersi tale nuova disposizione, dato che il sistema costituzionale e di valori e le garanzie che esso offre ai cittadini, sono ben diversi da quelli europei.

Ferma restando la tendenza a trattenere i dati sul territorio cinese, quelle imprese che volessero trasferire i dati personali verso stati terzi, dovrebbero prima superare positivamente la valutazione del Dipartimento di Stato sulla *Cybersecurity*. Inoltre, è previsto che qualora i paesi terzi dovessero adottare misure restrittive nel campo della protezione dei dati verso la Cina, la Repubblica cinese potrà fare lo stesso. In caso di violazione, sono inoltre previste multe fino a 6 milioni di euro o il 5% del fatturato. È previsto inoltre che all'impresa titolare possa essere ritirata la licenza commerciale e possano essere confiscati tutti i proventi derivanti dal trattamento illecito dei dati; a ciò si aggiunge, differentemente dal GDPR, una sanzione anche per la persona in carica.

Non c'è dubbio che la legge cinese stia andando nella giusta direzione, mostrandosi per certi versi anche più rigida e garantista del GDPR, ma occorre sempre ricordare che gli ampi poteri della Repubblica Popolare Cinese allungano di molto la distanza da colmare con il regolamento europeo, che rimane ancora oggi il *benchmark* di riferimento o, come sostengono altri, "*gold standard*" a livello

internazionale[198].

In altri termini, il GDPR avrebbe stimolato una *race to the top* nella regolamentazione del diritto alla protezione dei dati[199].

1.4 – Il fenomeno dei Big Data come modello commerciale nella società digitale

Quella sopra delineata è la cornice entro cui ci si muoverà al fine di introdurre qui il tema dei Big Data e di esaminare, anche nei capitoli che seguono, le sfide e le problematiche giuridiche più stimolanti ed attuali del nuovo mercato digitale.

In altri termini, le considerazioni sopra esposte consentono di contestualizzare lo scenario dei Big Data, valutando l'equilibrio tra protezione dei dati personali e innovazione nella società dell'algoritmo, che usa tecniche di *Data analytics*[200].

La dottrina più attenta già aveva previsto la trasformazione della corporeità della persona umana in flussi di comunicazioni elettroniche, con una crescente integrazione dell'intelligenza artificiale[201].

Nello scenario dell'*Internet delle cose (c.d. Internet of Things)*[202], i Big Data sono stati opportunamente definiti "i giacimenti petroliferi del terzo millennio", e nella *sharing economy* la loro condivisione è "il carburante per la produzione successiva di informazioni".

Tuttavia, c'è chi la pensa diversamente, in quanto i dati non sarebbero tanto una risorsa scarsa destinata ad esaurirsi, ma piuttosto risorse potenzialmente disponibili in grande quantità e riutilizzabili al pari delle energie rinnovabili[203].

Sicuramente l'*Internet of Things* è in grado di apportare notevoli benefici all'interno della società, tanto per il singolo, quanto per il settore pubblico.

A fronte di tali benefici, tuttavia, l'impiego di tali tecnologie importa anche una serie di rischi, per lo più relativi alla *privacy* e alla sicurezza dei consumatori che ne fanno uso.

I soggetti che utilizzano i *Big Data*, nonostante l'assonanza, non sono solo le *Big Tech Firm* ossia i giganti del *web* (*Google, Facebook, Amazon, Microsoft, Apple*); come vedremo, i Big Data sono

---

[198] A. MANTELERO, *The future of data protection: Gold standard vs. global standard, Computer Law & Security Review*, disponibile *online* dal 9 November 2020, in www.sciencedirect.com. In particolare, l'autore sostiene invece che, mentre il GDPR possa essere usato come *gold standard*, la Convenzione 108+, firmata dai paesi membri del Consiglio d'Europa, debba essere usata come *global standard* (o *koinè*) tra le diverse culture, ordinamenti giuridiche ed interessi economici dei vari paesi a livello internazionale.

[199] GREENLEAF G., '*A World Data Privacy Treaty? "Globali- sation" and "Modernisation" of Council of Europe Convention 108'* in David Lindsay et al. (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014), 136-137.

[200] Tramite l'uso di tecniche di *machine learning* e computazionali all'interno di modelli psicometrici gli algoritmi consentono di confrontare l'accuratezza dei giudizi espressi circa la personalità degli individui con le valutazioni delle macchine computazionali. Così DELMASTRO E NICITA, op. cit., 36.

[201] RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, 2004, p. 185.

[202] Si tratta di imprese che producono oggetti digitali "intelligenti" (come, ad esempio, elettrodomestici o *smartwatches*) che sono connessi alla rete e in quanto tali sono capaci non solo di generare dati digitali ma anche di restituirli ai loro produttori.

[203] GOBBATO S., *"Big data" e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo* in *Rivista di diritto dei media*, 2019, *fasc. 3*, 150.

rinvenibili sia nel settore privato, sia in quello pubblico[204], e nei più disparati comparti economici (*e.g.* banche e assicurazioni, energia, trasporti, grande distribuzione)[205].

Accanto a questi soggetti, nella nuova linea di *business* della *Data Monetization*, si muovono ormai i nuovi intermediari del mercato digitale: i *Data broker*, entità che raccolgono informazioni *online* sugli utenti da fonti pubbliche, le interpretano e le analizzano per poi venderle ad altri broker, imprese e/o individui, costituendo parte integrante della *Big Data economy*.

A tal proposito, c'è chi ha parlato anche di "capitalismo immateriale", descrivendo così l'avvento di una nuova società (quella digitale), dove l'acquisizione di dati è diventata un'attività a costo zero, nonostante la conservazione e l'elaborazione comportino costi elevati [206]. Nel settore digitale, infatti, elevati costi fissi, come quelli dei motori di ricerca, sono accompagnati da ridotti, o addirittura nulli, costi variabili; ciò ha cambiato le regole del gioco, tanto che le più grandi compagnie di intermediazione (*Facebook*, *Amazon*, *Google*, *Apple*[207], *Uber* e molti altri meno noti) sono le imprese che in generale raggiugono i più alti fatturati, tuttora in continua crescita.

Le informazioni sono ormai un'infrastruttura essenziale per operare nel mercato digitale, e chi arriva ad ottenerne l'esclusivo controllo, può costituire una vera e propria barriera all'ingresso di nuovi soggetti nel mercato stesso.[208]

I Big Data si differenziano dai dati normali per la loro natura massiva, non selettiva, il loro trattamento viene effettuato in maniera automatizzata mediante algoritmi[209] e altre tecniche avanzate, al fine di individuare correlazioni, modelli o tendenze mediante una profilazione di "massa".

Questi dati vengono poi processati tramite tecnologie automatizzate per restituire successivamente

---

[204] L'istituzione di una piattaforma per la valorizzazione dei dati della PA costituisce uno degli obiettivi perseguiti sin dal *Piano triennale per l'informatica nella PA 2017-2019*, confermato nel successivo Piano 2019-2021 attraverso l'implementazione della Piattaforma Digitale Nazionale Dati che mira ad «aprire il mondo della Pubblica Amministrazione ai benefici offerti dalle moderne piattaforme per la gestione e l'analisi dei big data» (in tal senso, AgID, *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021*, 19 marzo 2019, 71). Le azioni intraprese in Italia si inseriscono all'interno della strategia di *eGovernment* concepita a livello europeo nell'ambito della *Digital Single Market Strategy* (sul tema si veda, per il periodo in corso, la Comunicazione della Commissione europea, *Piano d'azione dell'UE per l'eGovernment 2016-2020. Accelerare la trasformazione digitale della pubblica amministrazione*, COM(2016) 179 final).

[205] S. GOBBATO, *op.cit.*, 151.

[206] S. QUINTARELLI, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, 2019.

[207] Recentemente, Apple ha tuttavia cercato – dopo aver sanzionato in precedenza la commercializzazione dei dati sulla localizzazione dei dispositivi - di contrastare il mercato delle applicazioni gratis che scaricano dati e rubrica degli utenti da rivendere ai broker, vietando espressamente agli sviluppatori tale pratica.

[208] A.G. PARISI, op.cit., 131.

[209] BURRELL, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms* in *Big Data & Society*, 2016; S. M. BENJAMIN, *Algorithms and Speech*, in *University of Pennsylvania Law Review*, 2013, 161, 1445 ss. L'intenzione di implementare le nuove tecniche di analisi emerge anche dalla comunicazione della EUROPEAN COMMISSION, *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions: A European strategy for data*, in https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, Brussels, 19 febbraio 2019 (data di ultima visita: 28 marzo 2020).

dati informativi nuovi che consistono in valutazioni e previsioni probabilistiche derivate dai dati originari[210].

Il valore dei dati non è quindi intrinseco, ma deriva dall'abilità delle compagnie di organizzarli, analizzarli, misurarli, ricavarne dei fattori e assumere decisioni.

Il paradigma statistico dell'intelligenza artificiale consente infatti di governare più efficacemente la società odierna, una società dell'informazione digitalizzata (conosciuta anche come società dell'algoritmo), grazie a valutazioni e previsioni calcolate matematicamente, così da garantire sicurezza, velocità ed economicità[211].

Gli elementi essenziali dei Big Data sono riassumibili nelle c.d. "cinque *v*" corrispondenti a *volume*, *velocity*, *variety*, *veracity* e *value*[212]. Tuttavia, non manca chi è arrivato a contare oltre 70 "*v*".

La "V" più importante è "*value*" intesa come la capacità di estrarre valore dai Big Data, in cui l'aspetto preponderante è l'attività di raccolta pubblicitaria *online* (c.d. *digital advertising*), in relazione alla commercializzazione di prodotti e servizi, indirizzata ad una domanda già precedentemente profilata. Oltre a tale accezione di valore, inteso come valore privato (per le imprese e per i singoli consumatori), c'è anche il valore pubblico dei dati che possono essere impiegati per la creazione di politiche dirette a migliorare il benessere complessivo della società (c.d. benessere sociale)[213].

Dunque, all'interno del fenomeno dei Big Data, la psicometria e il *marketing* offrono una straordinaria possibilità di manipolare l'informazione di massa.

Secondo l'*Osservatorio Big Data Analytics & Business Intelligence* della *School Management* del Politecnico di Milano[214], i *Big Data* hanno raggiunto solo in Italia un valore complessivo di 1,7 miliardi di euro nel 2019. Negli ultimi tre anni, il loro valore è cresciuto rispetto all'anno precedente in media del 23%, oltre il doppio rispetto al 2015, con un tasso medio annuo di crescita del 21,3 %.

Ad investirci sono soprattutto le grandi società, che coprono il 93% della spesa, mentre le Pmi rappresentano il restante 12% del valore.

---

[210] R. MESSINETTI *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019. p. 167 ss, p. 175.

[211] LASICA, *Identity in the Age of Cloud Computing – The Next Generation Internet's Impact on business governance and social interaction*, Washington DC, 2009.

[212] Così B. RABAI, *I "big data" nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, 2017, fasc. 3, p. 405.

[213] In questo senso si era già espresso, nel 2015, l'*European Data Protection Supervisor* (EDPS) sul caso *Cambridge Analytica* affermando che: "I Big Data, se usati responsabilmente, possono portare benefici significativi alla società. (…) I Big Data potrebbero essere usati per prevenire azioni che probabilmente si realizzeranno ma che non si sono ancora verificate…anticipando il rischio di suicidio e di commettere un crimine."

[214] Si veda Politecnico di Milano School of Management Osservatorio Big Data Analytics & Business Intelligence, Strategic Data Science: time to grow up, novembre 2019, disponibile su: https://www.osservatori.net/it_it/osservatori/comunicati-stampa/big-data-analytics-italia-mercato-2018 (visitato il 18 aprile 2019).

Il fenomeno dei Big Data ha invaso diversi settori: dal settore sanitario a quello bancario e finanziario, dal settore energetico a quello della grande distribuzione, dal settore del trasporto e della logistica a quello agricolo.

Il rapporto dell'*Osservatorio* indica la suddivisione della spesa in *Big Data* Analytics tra i vari settori merceologici, indicando come primo settore quello bancario (28% della spesa), seguito dal comparto manifatturiero (24%) e dal settore telecomunicazioni e media (14%), mentre il restante è coperto da servizi, grande distribuzione e *retail* (8%), assicurazioni (6%), *utility* (6%) e pubblica amministrazione e sanità (5%).

Nel mondo inoltre sono state censite ben 790 *startup* operanti nel *Big Data Analytics*, per un totale di investimenti raccolti pari a 6,4 miliardi di dollari.

Come si può vedere, sono solo pochi numeri, che però danno un'idea circa l'importanza del fenomeno economico e la crescita esponenziale del mercato in questione.

È un mercato in continuo divenire caratterizzato dalla presenza di diversi soggetti: fornitori di *software* (c.d. infrastrutture), fornitori di *analytics*, piattaforme *online* e così via; l'ambito economico e tecnologico è multiforme e complesso.

In questo ecosistema ci sono relazioni economiche e contrattuali tra cittadini utenti e imprese, le quali acquisiscono i dati digitali in rete in qualsiasi modo, in qualsiasi circostanza e a qualsiasi titolo.

Parlare di valore economico dei dati personali, quanto meno dal punto di vista sostanziale, è dunque possibile ma solo in modelli di *business* basati sull'uso commerciale degli stessi, e non in altri casi dove i dati personali forniti dal consumatore sono utilizzati per obblighi di legge o per la mera fornitura di contenuti o servizi digitali agli utenti.

Con riferimento all'utilizzo dei dati per fini commerciali, la cessione del dato personale costituisce la prestazione principale, entrando propriamente nella struttura di un contratto; mentre, negli altri casi di utilizzo, la prestazione resta al di fuori del rapporto contrattuale, e non può dunque avere natura patrimoniale.

Il fenomeno dei Big Data è quindi un tipico caso di modello commerciale in cui, grazie all'utilizzo di algoritmi, i dati personali si confondono facilmente con altre categorie di dati[215].

Nella stessa Indagine conoscitiva sui Big Data, pubblicata il 10 febbraio 2020 e svolta dalle tre Autorità indipendenti di settore coinvolte (*i.e.* AGCM, AGCOM e Garante per la protezione dei dati personali), si parla di valore economico del *set* di dati personali e non[216].

[215] Si parla a tal fine di monetizzazione di dati, con riguardo a servizi apparentemente gratuiti ma pagati dai consumatori con i propri dati personali. Pertanto, è la privacy stessa che diviene risorsa economica nel momento in cui sono gli stessi utenti a cederla in cambio di servizi gratuiti.

[216] J. MANYIKA et al., *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, maggio 2011; AGCM, AGCOM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui Big Data*, 10 febbraio 2020.

Le tre Autorità hanno contribuito, ciascuna per le proprie competenze e in coordinamento tra loro, a fronteggiare le principali criticità relative ai Big Data, nella consapevolezza del fatto che l'evoluzione economica del mercato digitale necessita di una regolamentazione giuridica.

Anche l'offerta gratuita di un'*App* può fornire opportunità di guadagno, lì dove i ricavi provengono dalla vendita di spazi pubblicitari agli inserzionisti, o dalla vendita dei dati agli utenti.

Tali pratiche, pur sembrando all'apparenza gratuite, fondano dunque il proprio *business* sulla raccolta e monetizzazione dei dati degli utenti (si pensi ad esempio a *Instagram*, *Facebook* e *Twitter*), formando veri e propri mercati dove la forza di queste imprese è direttamente proporzionale al loro bacino di utenti. Più l'impresa ha utenti, più ci sono interazioni (*like,* condivisioni, visualizzazioni, commenti) nella piattaforma *social* e più ci saranno inserzionisti intenzionati ad acquistare spazi pubblicitari in modo da poter attingere a quel bacino di utenza, pubblicizzando i propri prodotti o servizi. È qui che entra in gioco la c.d. pubblicità comportamentale (c.d. *behavioural targeting*), tecnica utilizzata nel *marketing* e nella pubblicità *online* per incrementare l'efficacia di una campagna pubblicitaria; essa utilizza le informazioni raccolte dall'attività dell'utente (pagine seguite e ricercate, *like*, condivisioni ecc) al fine di individuare gli interessi degli utenti e, su tale base, erogare pubblicità relativa a prodotti o servizi ricercati dagli stessi utenti.

Ciò ovviamente, come si vedrà meglio nel paragrafo successivo, pone seri dubbi sul rispetto del principio di trasparenza del GDPR, in quanto l'utente per poter essere profilato avrebbe diritto di ricevere un'informativa sul trattamento dei dati e di poter esprimere il proprio consenso in modo consapevole. In questa nuova epoca digitale, alcuni economisti parlano della c.d. "economia del dato profilato", in cui l'informazione relativa alla persona diventa essa stessa un bene di mercato[217].

Mentre nel capitalismo tradizionale la conoscenza dell'informazione consente e facilita la formazione del prezzo di scambio dei prodotti tra domanda e offerta, nel capitalismo digitale si agevola lo scambio di informazioni mediante l'accesso a servizi o prodotti gratuiti.

Il vero valore della transazione non è dunque il prodotto consumato o il servizio fruito, ma le informazioni che spesso indirettamente o implicitamente vengono cedute a tal fine; in altri termini, il meta-mercato di riferimento è proprio quello dell'informazione[218].

Il nocciolo economico della questione e la grande novità del fenomeno dei Big Data stanno nel fatto che, da una parte, attraverso questo "scambio implicito", anche coloro che rilasciano i propri dati ottengono in cambio servizi, dall'altra parte, lo scambio resta però implicito, non misurato dunque attraverso prezzi dedicati e trasparenti; quindi, lo scambio non è internalizzato dal mercato[219].

---

[217] A. NICITA, *Il mercato del dato profilato tra privacy, concorrenza e potere contrattuale nella prospettiva economica, in I dati personali nel diritto europeo,* a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1167.
[218] *Id.*
[219] DELMASTRO E NICITA, *op.cit,* 33.

Si comprende allora come non basti dire che il dato personale deve essere sottratto al mercato in quanto inalienabile (c.d. *inalienability rule*), se poi la sua natura lo trasforma comunque in bene privato, consegnandolo al mercato grazie ad uno scambio implicito.[220]

Pertanto, l'analisi del fenomeno dei Big Data con il solo paradigma della *privacy*, con riferimento ai soli dati personali, rischia di ignorare tutti i fattori in gioco.

Il valore economico dei Big Data è infatti riconosciuto soprattutto perché essi contengono informazioni di carattere generale, non solo personale, fornendo così informazioni sul comportamento dei singoli individui e offrendo indicazioni predittive grazie alla *Big Data Analytics*.

Paradossalmente, le predizioni fatte tramite l'uso del *machine learning* sono molto più esaustive delle informazioni rilasciate dagli utenti, in quanto i *Big Data Analytics* consentono di ricostruire i dati personali indipendentemente dal loro originario rilascio, superando così la tradizionale classificazione tra dati personali e non personali, o tra dati strutturati e non strutturati.

1.4.1 Segue – I *Big Data Analytics*, il *cloud computing* e l'Intelligenza Artificiale

Come si è visto i dati singolarmente considerati hanno un valore irrisorio, mentre se considerati in massa acquisiscono un valore importante. In quest'ambito, la fase dell'elaborazione dei Big Data consente l'organizzazione dei dati grezzi in informazioni suscettibili di essere utilizzate per finalità economiche.

Dopo una prima fase di estrazione e di successiva integrazione dell'informazione, interviene la vera e propria analisi dei dati che avviene per lo più tramite algoritmi[221]; tra questi ultimi si distinguono quelli di interrogazione, che mirano a rispondere alle richieste precise degli utenti, da quelli di apprendimento, che mirano ad estrarre nuova conoscenza avvalendosi di tecniche avanzate di a livello europeo

ificiale[222].

---

[220] *Id.*

[221] Il termine algoritmo indica la sequenza di istruzioni che deve essere effettuata per eseguire un'elaborazione o risolvere un problema.

[222] La tematica dell'intelligenza artificiale è sempre più attuale ed è oggetto di riflessione anche sui tavoli istituzionali, come emerge peraltro da recenti approfondimenti. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Creare fiducia nell'intelligenza artificiale antropocentrica, Bruxelles, 8.4.2019, COM (2019) 168 final; Commissione europea per l'efficienza della giustizia (Cepej) del Consiglio d'Europa, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, Strasbourg, 3-4 December 2018 nel quale si sono stabiliti i principi etici relativi all'uso dell'Intelligenza Artificiale (AI), in particolare nei sistemi giudiziari. La Carta intende fornire un quadro di principi destinati a policy maker, legislatori e i professionisti della giustizia con riguardo al rapido sviluppo dell'IA nei procedimenti giudiziari nazionali. L'opinione del CEPEJ, come si evince dalla Carta, è che l'applicazione dell'IA nel campo della giustizia può contribuire a migliorare l'efficienza e la qualità e deve essere attuata in modo responsabile e conforme ai diritti fondamentali garantiti, in particolare nella Convenzione europea sul Diritti umani (CEDU) e la Convenzione del Consiglio d'Europa sulla protezione dei dati personali. Per il CEPEJ, è essenziale garantire che l'IA rimanga uno*

In altri termini, alla luce dell'Indagine sui *Big Data* pubblicata nel febbraio 2020 è emerso che l'analisi dei *Big Data* può avvenire tramite due tipologie di algoritmi: i) gli algoritmi *analytics*, che organizzano le informazioni al fine di anticipare le scelte delle persone, determinandone almeno in parte i comportamenti e; ii) gli algoritmi di *machine learning*, anche conosciuti come algoritmi di apprendimento, che man mano che fanno esperienza forniscono informazioni sempre più precise grazie ad un apprendimento automatico da parte del sistema informatico. Il funzionamento di questi ultimi dunque evolve e migliora sulla base dell'esperienza ottenuta, in quanto è la disponibilità di nuove fonti di dati che consente il miglioramento degli algoritmi impiegati.

Il dato dunque rappresenta l'origine stessa dell'evoluzione degli algoritmi, visto che la loro caratteristica è quella di essere variabili nel tempo, ottimizzando i modelli sulla base dei dati analizzati.

Per tale motivo si dice che gli algoritmi di *machine learning* abbiano una certa autonomia di comportamento.

L'implementazione di algoritmi può a sua volta richiedere modelli informatici di calcolo come il modello del *cloud computing*[223], dove risorse *hardware* e *software* sono disponibili in *data center* remoti, rilasciati agli utenti che possono condividerli.

Il *cloud computing* può ricondursi ad un approccio a tre livelli: i) il c.d. *Infrastructure as a Service* (IaaS), nel quale solo i dati dell'impresa finiscono nei *datacenter* di un soggetto terzo; ii) il c.d. *Platform as a service* (PaaS), dove l'impresa si appoggia alla piattaforma tecnologica esterna per sviluppare e far funzionare le applicazioni che rimangono al suo interno; e iii) il c.d. *Software as a service* (SaaS), in cui sono le applicazioni stesse ad essere esternalizzate.

Inoltre, sia i motori di ricerca (e.g. Google[224], Microsoft), sia i giganti dell'*e-commerce* (*e.g.*

---

strumento al servizio dell'interesse generale e che il suo uso rispetti i diritti individuali. In questa prospettiva, il CEPEJ ha identificato i seguenti principi fondamentali da rispettare nel campo dell'IA e della giustizia: a) principio del rispetto dei diritti fondamentali, al fine di assicurare che la progettazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali;b) principio di non discriminazione, al fine di prevenire lo sviluppo o l'intensificazione di qualsiasi discriminazione tra individui o gruppi di individui; c) principio di qualità e sicurezza, in relazione al trattamento delle decisioni giudiziarie e dei dati, utilizzando fonti certificate e dati non modificabili con modelli concepiti in modo multidisciplinare, in un ambiente tecnologico sicuro; d) principio di trasparenza, imparzialità ed equità, al fine di rendere i metodi di trattamento dei dati accessibili e comprensibili, autorizzando audit esterni; e) principio "under user control" ("sotto il controllo dell'utente"), al fine di prevenire un approccio "prescrittivo" ed assicurare che gli utenti siano attori informati e in controllo delle loro scelte .Per il CEPEJ, il rispetto di questi principi deve essere assicurato nell'elaborazione delle decisioni giudiziarie e dei dati mediante algoritmi e nell'uso fatto degli stessi.

Ulteriori materiali di approfondimento possono essere rinvenuti al link: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment.

[223] Anche con riferimento al *cloud computing*, in caso di trattamento di dati personali, può essere necessaria l'adozione di adeguate cautele: v. in merito, le indicazioni contenute nel Parere 05/2012 sul *cloud computing* adottato dal gruppo art. 29 il 1° luglio 2012 WP 196, *sub* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf.

[224] Nei primi nove mesi del 2020, Google ha incrementato i ricavi di *Google Cloud* del 7,4% arrivando a 9,2 miliardi di dollari. Fonte: ilSole24ore, 16 dicembre 2020, articolo di Vittorio Carlini, p 10.

Amazon[225] e Alibaba) hanno compreso come il *cloud* non è più solo una questione di ricavi, ma piuttosto di un elemento essenziale del mondo imprenditoriale; il business dell'impresa è infatti sempre più esternalizzato, e le imprese non vogliono più gestire internamente attività troppo complesse.

Ecco che quindi l'intelligenza delle tecniche di analisi, congiuntamente alla voluminosità e alla varietà dei dati, costituiscono un'importante innovazione nel processo di estrazione delle informazioni; a tal proposito, si parla di un nuovo paradigma analitico (c.d. *data driven*), in cui i dati concorrono a scoprire nuova conoscenza, attraverso gli algoritmi dell'intelligenza artificiale.

Si tratta di un nuovo metodo di acquisizione di informazioni, in grado di generare conoscenza mettendo al centro i dati.

L'innovazione è tanto rilevante, che alcuni sostengono che si stia assistendo ad una vera e propria rivoluzione scientifica rispetto all'approccio tradizionale "ipotesi–modello–esperimento"[226].

Tuttavia, i miglioramenti registrati nei diversi settori e mercati non sono dovuti solo alle nuove tecniche di analisi basate sugli algoritmi, ma anche alla disponibilità di immense quantità di dati.

Per queste ragioni: da una parte, le *Big Tech* appaiono godere di un vantaggio competitivo rispetto alle imprese dei settori tradizionali, in quanto oltre a possedere enormi quantità di dati, esse sono le prime ad aver sviluppato tecniche avanzate di analisi[227]; dall'altra parte, sembra doversi escludere che le imprese che non dispongano di tali tecniche di analisi ed elaborazione versino in una condizione di svantaggio competitivo, in quanto potrebbero acquisire facilmente in *outsourcing* i servizi di *cloud computing.*

L'utilizzo dei *Big Data* e dell'Intelligenza Artificiale ha dunque dato vita ad un processo decisionale delle imprese guidato dai dati (c.d. *data-driven decision making*), secondo il quale le decisioni sono prese sulla base dei dati e della correlazione tra gli stessi; in altri termini, le decisioni sono prese in una prospettiva di utilizzo commerciale dei dati.

Alla luce di questo nuovo approccio, la disponibilità dei dati acquista un'importanza fondamentale, visto e considerato che, tramite una grande e variegata mole di dati, gli algoritmi di intelligenza artificiale possono individuare complessi schemi (o *pattern*) di relazioni, che possono invece sfuggire ai ricercatori che seguono il tradizionale metodo scientifico. In questo modo, le tecniche di *machine*

[225] Amazon infatti ha ben compreso la sua importanza in quanto primeggia nello Iaas e Paas dove detiene il 33% del relativo mercato. È seguita a debita distanza da Microsoft (18%), Google (9%) e Alibaba (6%). Inoltre, la redditività operativa nel *cloud* di Amazon, nei primi 9 mesi del 2020, ha accellerato a quota 9,97 miliardi di dollari. Fonte: ilSole24ore, 16 dicembre 2020, articolo di Vittorio Carlini, p 10.

[226] CERI S., "*On the role of statistics in the era of big data: A computer science perspective*" *Statistics & Probability Letters*, 136, 68-72, 2018.

[227] Secondo dati PwC, Amazon, Google, Microsoft ed Apple rientrano tra le prime 10 imprese per spesa complessiva in ricerca, mentre Facebook si colloca a ridosso di questo primo gruppo (in 14a posizione). Cfr. https://www.strategyand.pwc.com/innovation1000.

learning possono arrivare a svolgere una serie di attività che prima richiedevano esclusivamente l'intervento dell'uomo.

Ebbene, nonostante tale approccio trovi applicazione nei più diversi settori economici, è possibile trovare alcuni aspetti comuni.

In primo luogo, i *Big Data* possono contribuire al miglioramento dei processi decisionali, gestionali ed operativi, così da consentire di individuare i punti di scarsa produttività.

In secondo luogo, i *Big Data* possono offrire prodotti e servizi innovativi, come quello di offrire condizioni del traffico grazie ai dati di posizione e di spostamento di milioni di utenti.

In terzo luogo, i *Big Data* consentono alle imprese di possedere una conoscenza molto dettagliata sui bisogni e le preferenze dei consumatori; tale conoscenza può inoltre essere utilizzata per personalizzare i prodotti e i servizi offerti, e per la comunicazione pubblicitaria *online*. Lo stesso accade nel mondo dell'*e-commerce,* dove si propongono ai propri utenti beni e servizi in linea con le preferenze individuali, e con una possibile differenziazione dei prezzi; trattasi di pratiche di *price discrimination,* che potrebbero condurre ad una revisione dei modelli ed istituti giuridici inerenti all'autonomia contrattuale delle parti negoziali.

In altri termini, ove il prezzo sia deciso da una macchina, in base all'analisi del profilo individuale o di gruppo, il costo del bene non sarà più determinato sulla base di trattative, bensì in ragione di una classificazione automatica attribuita da un algoritmo, sfruttando le preferenze individuali dell'utente precedentemente profilato (c.d. pratiche di *profiling*).

Infatti, queste imprese, attraverso le elaborazioni algoritmiche, possono captare una serie di informazioni inerenti i comportamenti dei clienti come: le abitudini di consumo, la disponibilità economica del singolo consumatore e i suoi bisogni consci e inconsci.

Infine, i *Big Data* trovano sviluppo anche nell'offerta di nuovi servizi pubblici, contribuendo a migliorare la qualità della vita della collettività, come ad esempio ha cercato di fare in Italia la *app* "Immuni", una piattaforma che ha consentito di tracciare gli spostamenti dei singoli utenti che, su base volontaria, si sono scaricati l'applicazione sul loro *smartphone*[228]. Inoltre, anche le istituzioni pubbliche possono migliorare la loro capacità di azione, facendo leva sulla quantità e varietà dei dati riguardanti le preferenze e le scelte degli agenti economici[229].

Peraltro, la raccolta ed analisi di una grande mole di dati non è limitata solo alle piattaforme *online,* ma costituisce un'importante fonte di vantaggio anche per gli operatori tradizionali, i quali sempre

[228] Sul punto cfr G. ATTARDI - N. MARINO - E. SANTUS, *Contact tracing, perché è così importante* contro il covid (anche in Italia), Agendadigitale.eu. 21 aprile 2020; P. CLARIZIA E E. SCHNEIDER, *Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19*, IRPA - Osservatorio sullo Stato digitale. 19 aprile 2020.

[229] Sul punto si veda ad esempio l'intervento di apertura al Workshop "*Harnessing Big Data & Machine Learning Technologies for Central Banks*" del Vicedirettore Generale della Banca d'Italia Fabio Panetta, Roma, 26 maggio 2018.

più stanno capendo l'importanza dei *Big Data*, spesso acquisiti anche attraverso un'attività *offline*. Tuttavia, la maggior parte dei dati è concentrata nelle mani dei grandi *players* come le *Big Tech*, che hanno sede fuori dall'Unione europea. Infatti, nell'ambito dell'"*European strategy for data*, l'*European Data Protection Supervisor* si auspica un *data economy model* alternativo, più aperto e democratico in modo da poterlo usare per tutte le realtà economiche[230].

1.4.2 Segue – Alcuni esempi dell'utilizzo dei Big Data nei vari mercati

Come si è visto, l'utilizzo dei Big Data è diffuso in una varietà di settori economici.

In considerazione del grado di rilevanza dei *Big Data* nei processi competitivi è possibile distinguere almeno tre macro categorie di settori o mercati:

i) in primo luogo, ci sono quei mercati dove l'utilizzo dei Big Data è di scarso rilievo nella fornitura del bene/servizio, come ad esempio per migliorare l'efficienza produttiva, senza però incidere sul processo competitivo[231] (*e.g.* sviluppo di campagne di *marketing*, gestione di *call center*);

ii) in secondo luogo, ci sono mercati dove l'utilizzo dei *Big Data* incide sulle condizioni di offerta del servizio (ad esempio in termini di qualità), investendo in maniera diretta il rapporto fornitore-utente. È questo il caso dei mercati caratterizzati da importanti asimmetrie informative, come quelli finanziari, bancari ed assicurativi, dove l'analisi di una mole sempre maggiore di dati porta ad una conoscenza sempre più approfondita dei processi e dei clienti, con il fine di migliorare ogni aspetto dell'attività di impresa (*e.g. design* di prodotti e servizi, *marketing*, vendita);

iii) in terzo luogo, ci sono mercati dove l'utilizzo dei *Big Data* è di fondamentale importanza, in quanto da esso dipendono le caratteristiche essenziali del bene o servizio offerto. Si tratta di beni e servizi che rivestono un ruolo centrale nell'economia digitale, e che non potrebbero operare senza l'utilizzo dei *Big Data*, come ad esempio il *marketing online*, che tramite le informazioni raccolte dai singoli utenti individua determinati *target* di consumatori a cui indirizzare messaggi pubblicitari mirati. In questa terza macro categoria possiamo far rientrare: la commercializzazione diretta dei dati stessi raccolti e organizzati, l'utilizzazione dei dati nell'ambito di programmi di gestione societaria e dei relativi servizi di consulenza e l'utilizzazione dei *Big Data* per fornire nuovi servizi (*e.g. ranking* di beni e servizi). Poi ci sono le infrastrutture di gestione dati, che operano sul "*cloud*" e forniscono servizi di conservazione ed elaborazione; in particolare, il sistema *cloud* consente l'interconnessione delle banche dati, attraverso la condivisione dei patrimoni informativi.

Questi mercati sono caratterizzati da un elevato livello di concentrazione. A contribuire a ciò non è solo la disponibilità dei *Big Data*, ma anche altri fattori che – insieme ad economie di scala, di scopo

[230] *European Data Protection Supervisor*, Opinion 3/2020 on the *European strategy for data, 16 June 2020.*
[231] Cfr., al riguardo, audizione di *Amazon* (26 novembre 2018).

e alle esternalità di rete – contribuiscono all'esistenza di barriere all'entrata nei mercati digitali e, di conseguenza, svolgono un ruolo importante nello spiegamento del potere di mercato.

L'utilizzo dei *Big Data* assume un certo rilievo in una specifica struttura di mercato (c.d a più versanti). In quest'ambito si distinguono le piattaforme c.d. di attenzione, come i motori di ricerca *online* o *social network* (*e.g. Facebook, Instagram, Linkedin* ecc.), dalle piattaforme di scambio, come i *marketplace* del commercio elettronico (*e.g. Amazon, Alibaba ecc*).

Nelle piattaforme di attenzione, chi ha più utenti dispone di più dati per migliorare il proprio servizio, rendendo più difficile l'ingresso di nuovi operatori.

Un particolare mercato che è interessante analizzare è quello bancario – creditizio in cui l'approccio alle tecnologie *Big Data* deve essere necessariamente "prudenziale", in quanto non si è compreso se vi possa essere un concreto ed effettivo ritorno economico.

I *Big Data* sono infatti di per sé dati di qualità mediocre, che acquisiscono una loro rilevanza solo se si possiedono professionalità specifiche per poterli elaborare ed analizzare. In Italia, ad esempio, a differenza di quanto accade in altri contesti europei, non è possibile utilizzare i c.d. dati alternativi[232]e i dati s*ocial* per la valutazione del merito creditizio, in quanto va rispettato il Codice di condotta[233], di recente approvato dall'autorità garante della *privacy,* e aggiornato con le nuove sfide della *digital economy.*

Di recente, all'interno del mercato finanziario abbiamo assistito all'innovazione di prodotti e servizi in ambito *FinTech* quali ad esempio i servizi di pagamento digitale e i c.d. *mobile payment*, che verranno analizzati più in dettaglio nel corso del quarto capitolo, la cui diffusione è stata incrementata anche alla luce della Direttiva (EU) 2015/2366 del 25 novembre 2015 sui servizi di pagamento nel mercato interno (c.d. PSD2), recepita nel nostro ordinamento dal d.lgs. 15 dicembre 2017, n. 218. Infatti, tali nuovi fonti di informazione possono alimentare nuove elaborazioni fondate su tecnologie *Big Data*, e il mercato dei pagamenti digitali è uno di quelli che, come vedremo, più di altri sta assistendo all'emersione di nuovi *players* come grandi società, *startup e scaleup fintech*, che entrano in concorrenza con le banche e ed altri intermediari che finora hanno dominato il mercato *de quo.*

Per quanto riguarda invece il mercato assicurativo, l'elaborazione dei *Big Data* consentirà di personalizzare le offerte, al fine di costruire il prodotto assicurativo più congeniale per le esigenze

[232] Per "dati alternativi" ci si riferisce a quei dati riguardanti il comportamento nei pagamenti ovvero, più in generale, al comportamento economico finanziario di famiglie ed imprese, la cui disponibilità consentirebbe di avere un quadro più chiaro del soggetto che accede al credito.

[233] Si tratta del *"Codice di condotta per i sistemi di informazione gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*" approvato dal Garante il 12 settembre 2019 (doc. web 9141941) dopo un lavoro di revisione del vecchio Codice deontologico reso non più attuale dalle novità introdotte in materia di protezione dei dati personali dal GDPR. Le nuove regole prevedono tra l'altro un'estensione fino a 10 anni del termine di durata per la conservazione dei dati per la conservazione dei c.d. dati *off line* che potranno essere utilizzati per analisi statistiche e per la costruzione di modelli predettivi attraverso "*opportune tecniche di cripting o pseudoanonimizzazione*".

della clientela, anche alla luce del nuovo quadro regolamentare caratterizzato dalla *Product Oversight Governance* (c.d. POG), introdotta dalla direttiva 2016/97/UE (*Insurance Distribution Directive* – IDD)[234]. Infatti, fino ad oggi, l'uso delle nuove tecnologie è consistito essenzialmente nella diffusione di polizze *online*, attraverso il ricorso anche a siti comparatori.

La diffusione delle nuove tecnologie basate sui *Big Data* nei mercati assicurativi, mostra dunque importanti prospettive, sia nello sviluppo di nuove modalità di erogazione di prodotti e servizi assicurativi, sia nel miglioramento ed ottimizzazione dei processi interni e nella gestione di polizze.

Inoltre, i dati usati dalle imprese operanti nei diversi mercati sono tendenzialmente dati anonimizzati, in quanto si riesce ad ottenere le informazioni di cui si necessita per la pianificazione delle strategie di mercato, senza però violare la normativa sulla protezione dei dati personali.

Infine, alla luce delle dichiarazioni di alcuni operatori di mercato, sembrerebbe che si proceda con lo sviluppo di politiche che prevedono procedure standardizzate di anonimizzazione dei dati di identità personale[235].

1.5 – Rilievi conclusivi preliminari: la regolazione del mercato grazie alla regolazione di singoli rapporti individuali

Alla luce del quadro sopra riportato e delle nuove frontiere della società dell'informazione digitale si è potuto riscontrare, come avvenuto altre volte nella storia, che al mutamento della società è seguito l'intervento del legislatore, al fine di dare delle risposte in termini di maggiore tutela agli utenti e ai consumatori-interessati al trattamento dei dati.

Per far ciò però, il legislatore e le autorità di settore non hanno potuto far altro che riconoscere un nuovo mercato, quello digitale, nel quale le informazioni sono diventate di grande valore economico per le imprese, le quali hanno iniziato ad investire sempre più nei *Big Data* e nelle nuove tecniche di analisi dei dati basati sull'algoritmo.

Tali ultime novità tecnologiche hanno inoltre confermato un approccio olistico del dato, da sempre presente nella regolamentazione europea, ma di recente accolto anche nel dibattito statunitense, che cerca di approcciare la materia della protezione dei dati personali a livello federale, e non più solo a livello statale. Anche in Cina si è assistito a recenti sviluppi normativi, sulla falsa riga del GDPR, sebbene si segua un approccio non basato sulla protezione dell'individuo, ma basato sul rafforzamento dello stato sociale e del controllo dello stato sull'economia.

Sotto altro profilo, si è potuto riscontrare anche in materia di principi e diritti fondamentali, come ci

[234] Pe un quadro generale cfr. L. FARENGA, *Manuale di diritto delle assicurazioni private*, Torino, VI ed, 2019, 121 ss.
[235] AGCM, AGCOM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui Big Data*, cit, 24.

sia stato uno spostamento dell'attenzione del legislatore verso la libera circolazione dei dati e la loro commercializzazione in determinati modelli di *business*. Si è entrati quindi sempre più in un'ottica consumeristica, vedendo il dato come un bene immateriale e quindi come un prodotto interscambiabile. Basti pensare al diritto alla portabilità dei dati, previsto espressamente nello stesso GDPR.

Ovviamente con il tempo sono cambiate le tecniche di acquisizione, di utilizzo e di analisi del dato.

L'algoritmo, nella nuova società dell'informazione digitale, è diventato uno strumento fondamentale per catalogare ed utilizzare i dati con l'obiettivo di avere un insieme di dati aggregati (c.d. *data set)* che rappresenti i desideri, le personalità, i comportamenti e i tipi di spostamenti degli utenti, al fine di poter capire cosa desiderano, perché e quando.

L'identità della persona si è digitalizzata ed è diventata così funzionale a nuovi modelli di business, i quali utilizzano la pubblicità comportamentale e il *digital advertising*, con lo scopo di offrire al consumatore un determinato prodotto o servizio dopo averlo previamente profilato, spesso a sua totale insaputa.

Da una parte, l'utilizzo dei dati personali aumenta il benessere dei singoli consumatori per via dell'innovazione dei servizi, della qualità e varietà degli stessi, dall'altra parte, questo utilizzo riduce il benessere dei singoli consumatori, come ad esempio in situazioni dove all'attività di ricerca *online* dell'utente non segue subito l'acquisto di quel bene o servizio ricercato e, in questo caso, il titolare può sfruttare il tracciamento del consumatore per proporgli quel prodotto o servizio ad un prezzo maggiorato[236].

Infine, ci sono scenari particolari, dove l'utilizzo di dati personali aumenta il benessere dei singoli consumatori ma riduce il benessere sociale; ad esempio, questo avviene quando la personalizzazione dei contenuti giornalistici proposti agli utenti dalle piattaforme di ricerca o dai *social network* può essere gradita dal singolo utente, ma allo stesso tempo non è desiderabile dalla società a causa della riduzione del pluralismo informativo, con un impatto sulla sfera politica e sociale[237].

Per queste ragioni, tali decisioni automatizzate mediante gli algoritmi sono utilizzate in particolare dai giganti dell'*e-commerce* e dalle grandi compagnie o *social network* per profilare gli utenti, al fine di capire qual è il nuovo prodotto da creare e per chi, o per orientare la scelta degli utenti stessi.

Come quindi è già avvenuto nel mondo finanziario, bancario e assicurativo, viene fatta una profilazione dell'utenza; con la differenza però che in questi mercati, il più delle volte, il consumatore esprime una volontà *ex ante* di acquistare quel determinato prodotto finanziario o assicurativo, per il quale viene successivamente profilato al fine di poter ricevere il prodotto più appropriato e adeguato

[236] *Id.* cit, 87.
[237] *Id.*

alla sua esperienza finanziaria e alle sue esigenze.[238] Diversamente, nel mercato dei dati, quello dell'*Internet of Things (IoT)* e dei *social network*, l'utente viene, spesso e volentieri, profilato prima di manifestare la volontà di acquistare un determinato prodotto o servizio. Nel caso dell'IoT, le imprese accedono ai dati registrati da dispositivi venduti a terzi, mentre, nel caso dei *social*, le imprese tengono traccia di tutte le azioni che gli utenti compiono sulle loro piattaforme. In entrambi i casi però gli individui non registrano il proprio operato, che invece viene mappato dalle imprese, e non sempre l'individuo ha espresso uno specifico consenso ad essere profilato o, diversamente, non è sempre conscio di averlo espresso, seppur distrattamente.

Tuttavia, ora i Big Data sono utilizzati anche dal mondo bancario che ha compreso il loro valore tanto da esser diventato, come abbiamo visto, il primo mercato in termini di spesa per i *Big Data Analytics.* Ebbene, il legislatore ha compreso l'esigenza di tutelare gli individui, in particolare nel mondo *e-commerce,* dove il legislatore europeo, con la nota Direttiva *Omnibus,* ha concluso il c.d. "*New deal for consumer*", così estendendo la protezione dei consumatori anche al mercato digitale.

Ora la palla è passata quindi al legislatore nazionale, che avrà due anni di tempo per recepire le nuove norme del "New deal": le misure nazionali di attuazione dovranno essere adottate infatti entro il 28 novembre 2021, e dovranno entrare in vigore entro il 28 maggio 2022.

Non solo quindi non vi sono dubbi sul valore economico e commerciale dei dati, ma il legislatore europeo si è espresso qualificando tali dati – alla presenza di determinati comportamenti dell'operatore economico – come controprestazione o prezzo all'interno di un rapporto negoziale, rimettendo però al legislatore nazionale se e quale disciplina contrattuale applicare.

In questo panorama regolamentare, si inserisce anche il GDPR che, pur non facendo esplicitamente riferimento ai Big Data, non ha esonerato le grandi imprese titolari dei dati personali dal rispetto dei principi in esso espressi.

Si è visto come, nonostante tali principi siano messi a dura prova nel fenomeno dei Big Data, il legislatore europeo, mediante l'introduzione di due principi nel GDPR, noti come *privacy by design*[239] e *privacy by default,* abbia imposto alle imprese titolari di rispettare le disposizioni di detto Regolamento, con la predisposizione di una struttura organizzativa tale da rendere l'impresa stessa *compliant*.

---

[238] Per un approfondimento sulla formazione della volontà del consumatore nel mercato finanziario v. M. LIBERTINI, *La tutela della libertà di scelta del consumatore e i prodotti finanziari, in Mercati finanziari e protezione del consumatore*, a cura di M. GRILLO, Brioschi, Milano, 2010, 21-46. Con particolare riferimento alla rilevanza della trasparenza dell'intermediario nel momento della profilatura sia consentito il rimando a P. GRIECO, *La violazione degli obblighi informativi nell'intermediazione finanziaria tra disciplina civilistica e regolamentare*, in *Resp. civ. prev.*, n. 4/2017, p. 1265-1284.

[239] Tale principio è stato anche menzionato dalla Commissione europea, nella raccomandazione (EU) 2020/518 dell'8 April 2020 *"on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data"*, in https://ec.europa.eu/commission/presscorner/detail/it/ip_20_626.

Le problematiche legate alla protezione dei dati personali vengono così gestite e risolte nell'impresa a livello organizzativo, effettuando una valutazione di impatto della *privacy* per gestire i rischi legati al trattamento dei dati personali.

Tale approccio consente dunque di responsabilizzare l'operatore economico, in linea con il principio di *accountability.*

In altri termini, i dati, in base al punto di vista che si sceglie, possono esser visti come un costo, un rischio o un bene immateriale commerciabile.

In questo ampio contesto, la protezione del singolo interessato come consumatore pare strumentale alla tutela di interessi generali, già garantiti attraverso rimedi diversi da quelli individuali come, in particolare, l'imposizione di obblighi organizzativi posti a carico del titolare del trattamento, la cui violazione comporta sanzioni amministrative e penali.

Ecco che quindi abbiamo assistito, come comunemente accade, a interventi del legislatore europeo in materia di regolazione del mercato, grazie anche alla regolazione dei singoli rapporti individuali[240], seppur lasciando alcuni aspetti di questi ultimi alla determinazione dei singoli Stati membri[241].

Nel nostro caso, il mercato di riferimento è quello digitale che il legislatore europeo ha disciplinato tenendo in considerazione il delicato equilibrio tra libera circolazione dei dati e tutela del diritto alla protezione dei dati personali, tra libertà economica e diritti della personalità.

Le preoccupazioni maggiori non riguardano dunque solo lo sfruttamento in sé dei diritti della personalità, ma anche ulteriori attività poste in essere dal titolare.

Il diritto si occupa quindi non solo di tutelare la persona che dispone di sé stessa, del proprio nome o della propria immagine, ma anche – a seguito dell'oggettivizzazione delle informazioni attuata mediante le moderne tecnologie – delle conseguenze che possono derivarne.

Come abbiamo visto, però, chi intende trattare i dati, deve prima trovare il modo di raccoglierli, tanto che gli operatori economici, a tal proposito, hanno approfittato dell'erogazione di un servizio per chiedere contestualmente al consumatore di dare il proprio consenso al trattamento dei propri dati.

Riemerge così l'importanza della sfera individuale, dato che il condizionamento del servizio al consenso riguarda i singoli rapporti.

Anche nel fenomeno dei Big Data, la massa di dati si è pur sempre costituita grazie alla conclusione

---

[240] Cfr. sul punto osservazioni di V. ROPPO, *Giustizia contrattuale e libertà economiche: verso una revisione della teoria del contratto?,*in *Riv. crit. dir. priv.*, 2007, 602

[241] Vedi ad esempio, nell'ambito del "New deal per i consumatori", l'ultima parte del *Considerando* 24 della direttiva UE 2019/770 che prevede che: *Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale".* All'interno invece del GDPR si segnala ad esempio: l'art. 9 dedicato alle categorie particolari di dati, in cui ammette che gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute; l'art. 84 afferma che gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento.

di singoli "contratti", la cui disciplina si riflette sulla configurazione di tale massa.
Ecco che quindi i singoli rapporti negoziali hanno il potere di influenzare l'intero mercato digitale.
In altri termini, si può affermare che il concetto di dato come valore economico è stato considerato dal legislatore, sia sotto il profilo dell'organizzazione societaria, sia sul piano dei rapporti individuali ("contrattuali").
In quest'ottica la dicotomia mercato-persona diventa un falso problema, in quanto l'assunto dell'indisponibilità e dell'incommerciabilità degli attributi della persona, crolla innanzi alla consapevolezza che l'informazione, in un'economia complessa come quella attuale, gioca un ruolo fondamentale anche in termini economici.
Va in ogni caso ricordato che, attesa la natura di diritto fondamentale della protezione dei dati personali, gli ambiti di "negoziabilità" da parte dell'interessato devono trovare modalità di espressione nelle forme consentite dalla relativa disciplina, rispettando anzitutto i principi fondanti di protezione dei dati personali, compendiati all'art. 5 del GDPR, oltre che riscontrando la sussistenza di una delle condizioni di liceità del trattamento indicate al successivo art. 6 del Regolamento.
In una diversa prospettiva, la protezione dei dati personali può anche essere considerata in una dimensione qualitativa di un servizio, cosicché, a parità di prezzo ed eventualmente di altre caratteristiche, i consumatori (correttamente informati) dovrebbero tendere a scegliere il servizio che garantisca la minore fornitura possibile di dati o, comunque, un più elevato livello di controllo sui propri dati[242].
Ciò appare coerente con un'impostazione che vede il consumatore attribuire alla tutela dei dati personali a sé riferibili, anche un valore economico: come per altre caratteristiche qualitative, un livello maggiore di *privacy*, a parità di altre condizioni, dovrebbe corrispondere ad una maggiore utilità per il consumatore.
Ecco che quindi la coppia di soggetti rilevanti per la normativa consumeristica, si sovrappone alla coppia di soggetti rilevanti per la disciplina *data protection*; si avrà così un professionista che è anche titolare del trattamento, e un consumatore/utente che è anche interessato del trattamento.
In altri termini, accanto ad una approccio di natura "morale" della protezione dei dati personali, diretta alla tutela della riservatezza e dell'identità della persona, se ne affianca uno "negoziale"; quest'ultimo, comporta l'estensione delle tutele per l'interessato che potrà avvalersi, oltre che degli strumenti di tutela previsti dal GDPR, dei rimedi negoziali civilistici (*e.g.* nullità o annullamento del contratto) e delle tutele del diritto dei consumatori (*e.g.* clausole vessatorie o le pratiche commerciali

[242] Ciò è emerso, ad esempio, a seguito del messaggio di WhatsApp in cui ha proposto la modifica della sua privacy che, prevedendo una condivisione dei dati raccolti con altre piattaforme, ha generato il malcontento degli utenti che valutano sempre più il grado di protezione dei dati come grado qualitativo del servizio offerto e si registrano ad altre piattaforme di messaggistica istantanea come Telegram e Signal. Vedi § 1.3.2.

scorrette).

Con riferimento ai rimedi negoziali civilistici, ci si potrebbe ancora chiedere: cosa succede al trattamento di dati personali avvenuto sulla base di un consenso dichiarato nullo o annullato per vizi della volontà? Ebbene, nonostante la logica conseguenza dovrebbe essere l'invalidità derivata del trattamento, in questa fase non si può escludere la possibilità di pensare a una nullità di protezione che tenga in vita il rapporto negoziale.

Con riferimento invece alle tutele del diritto dei consumatori, con riferimento a quei termini contrattuali che, in relazione al trattamento dei dati personali, dovessero risultare iniqui nel rapporto tra titolare e interessato, si potrebbe effettuare il richiamo alla disciplina delle clausole vessatorie, con conseguente nullità solo di quella clausola.

Con riferimento invece alla materia delle pratiche commerciali scorrette, si rinvia la trattazione al terzo capitolo, in quanto prima è necessario comprendere le problematiche concorrenziali tipiche dell'economia digitale, esaminando come le autorità antitrust e le istituzioni stiano già reagendo alle condotte delle piattaforme digitali, operanti a livello internazionale.

CAPITOLO II

Il diritto antitrust contemporaneo nell'era digitale in una prospettiva comparata: un'analisi dei casi più recenti

Sommario: *Premessa* **2.1** *Abuso di posizione dominante* **2.1.1** La situazione americana e il caso Google **2.1.2** *La Cina e la condotta "choose one from two" di Alibaba* ***2.1.3*** *La situazione nell'Unione europea: i tre casi Google e il più recente caso Amazon* ***2.1.4*** *Il caso Facebook in Germania: una partita ancora aperta* ***2.1.5*** *L'enforcement dell'AGCM in Italia: i casi Google e il suo ruolo di apripista in Europa sul caso Amazon* ***2.1.6*** *Rilievi conclusivi in materia di abuso di posizione dominante* ***2.2*** *Le Concentrazioni e le "Killer Acquisition"* ***2.2.1*** *Stati Uniti* ***2.2.2*** *Un breve cenno agli ultimi sviluppi in Cina* ***2.2.3*** *Unione Europea* ***2.2.4*** *Questioni aperte in Italia ed eventuali divergenze con l'Europa* ***2.2.5*** *Rilievi conclusivi in materia di concentrazioni* ***2.3*** *Le intese orizzontali degli algoritmi di pricing e il "meeting of algorithms"* ***2.3.1*** *Stati Uniti* ***2.3.2*** *Lo stato dell'arte in Unione europea* ***2.3.3*** *Alcune idee conclusive sul "pricing algorithms" e i "new competition tools"* ***2.4*** *Riflessioni finali*

Premessa

Nel primo capitolo si è visto come il GDPR abbia rafforzato i diritti degli interessati nei rapporti individuali con l'impresa titolare, attribuendo così maggiore controllo sui loro dati personali.

Inoltre, si è visto come i *Big Data* costituiscano un *asset* strategico di rilevanza non solo economica ma anche personale, considerata la loro incidenza sulle libertà individuali di rango costituzionale [1].

In questo secondo capitolo, si analizzeranno i *Big Data* dal punto di vista del mercato digitale, e si cercherà di capire se e in quali casi essi possano costituire un vantaggio economico per le imprese che li posseggono e li gestiscono.

Il legame tra *Big Data*, *privacy* ed *enforcement* della disciplina a tutela della concorrenza può interessare tutti gli strumenti di intervento dell'autorità *antitrust*: abusi, concentrazioni ed intese.

Si analizzerà se e quando l'attività di generazione, raccolta ed acquisto di dati digitali possa essere considerata lesiva del buon funzionamento del mercato. Si cercherà di vedere quando e in che misura le condotte delle piattaforme digitali integrino un comportamento anti-competitivo, sia che si tratti di condotte unilaterali, che possono integrare un abuso di posizione dominante, sia che si tratti di condotte bi- o multilaterali, con l'eventuale applicazione della disciplina sulle concentrazioni o sulle

[1] S. GOBBATO, *"Big data" e "tutele convergenti"* tra concorrenza, GDPR e Codice del consumo in Rivista di diritto dei media, 2019, fasc. 3, pp. 150. Sul punto cfr. anche B. RABAI, *I "big data" nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, 2017, fasc. 3, pp. 405-422.

intese[2].

Inoltre, un'altra questione rilevante ai nostri fini è la correlazione tra la disciplina della *privacy* e il diritto *antitrust*.

In passato, si è sempre negato che la violazione di disposizioni sulla protezione dei dati personali potesse avere una certa rilevanza in materia di diritto della concorrenza[3]. Ciò, in considerazione del fatto che le due discipline mirano ad obiettivi differenti: (i) da una parte, la disciplina sulla protezione dei dati personali tutela gli individui dal controllo e l'interferenza da parte dei governi o delle imprese, garantendo i diritti e le libertà fondamentali delle persone; (ii) dall'altra, il diritto della concorrenza promuove invece l'efficiente distribuzione delle risorse e l'innovazione, a beneficio del consumatore. Pertanto, si è sempre pensato che gli strumenti propri del diritto *antitrust* non si sarebbero potuti usare per perseguire obiettivi diversi dalla protezione del processo concorrenziale.

Oggi, invece, si inizia ad accettare, sebbene con molta cautela, una influenza e relazione tra le due diverse materie. In altri termini, emerge come, a volte, una bassa qualità di protezione dei dati personali possa essere considerata in ambito concorrenziale, ovvero possa assumere rilevanza ai fini di un'analisi *antitrust*[4]. In questo capitolo, si analizzeranno anche le correlazioni e i rapporti tra il diritto alla protezione dei dati personali e il diritto *antitrust*, alla luce delle ultime novità giurisprudenziali e delle istruttorie attivate dalle diverse Autorità di settore, nell'eventualità che il diritto antitrust sia utilizzato per tutelare le identità digitali degli individui[5].

Il rischio però è anche quello che una medesima condotta possa essere vagliata da Autorità diverse, con il risultato di sottoporre l'impresa ad un ingiustificato doppio procedimento sanzionatorio, in

---

[2] Per una ricostruzione generale ed alcuni profili introduttivi cfr. G. AMATO, *Il potere e l'antitrust*, Il Mulino, 1998, 93.; V. BAGNOLI, *The big data relevant market (Il mercato rilevante dei "big data")*, in *Concorrenza e mercato*, 2016, pt. 1, pp. 73-94; G. COLANGELO, *"Big data", piattaforme digitali e "antitrust" (Big data, digital platforms and antitrust)*, in *Mercato concorrenza regole*, 2016, fasc. 3, pp. 425-460; DELMASTRO E NICITA, *Big data: come stanno cambiando il nostro mondo*, il Mulino, 2019; F. DI PORTO, *La rivoluzione "big data". Un'introduzione*, in *Concorrenza e mercato*, 2016, pt. 1, pp. 5-14; A. GIANNACCARI, *La storia dei "Big Data", tra riflessioni teoriche e primi casi applicativi (The Big Data antitrust story: theoretical approaches and the first enforcement cases)*, in *Mercato concorrenza regole*, 2017, fasc. 2, pp. 307-332.; M. MAGGIOLINO, *Big data e diritto Antitrust*, Egea, 2; G. MUSCOLO, *Big data e Concorrenza Quale rapporto?*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, 173; R. NAZZINI, *Online Platforms and Antitrust: Where Do We Go From Here? (Piattaforme "online" e "antitrust": dove andiamo da qui?)* in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2018, fasc. 1, pp. 18; MARIA OREFICE, *I "big data". Regole e concorrenza (Big Data. Rules and Competition)* in *Politica del diritto*, 2016, *fasc. 4*, pp. 697-743; G. PITRUZZELLA, *Big data, competition and privacy: a look from the antitrust perspective ("Big Data", concorrenza e riservatezza: uno sguardo dalla prospettiva "antitrust")* in *Concorrenza e mercato*, 2016, pt. 1, pp. 15-27; E. PROSPERETTI, *Algoritmi dei Big Data: temi regolamentari, responsabilità, concorrenza, in Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini, G. Olivieri, Milano, 2018.

[3] Sul punto cfr. P. MERLINO, *Antitrust and Data protection Law: a relationship in search of clear boundaries* in E.A. RAFFAELLI, *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019, 391 ss.

[4] P.P. SwiRe, Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall, 18 October 2007, p.4, available at www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf .

[5] Vedi ad esempio caso Facebook in Germania trattato al § 1.2.3.

apparente violazione del divieto di *ne bis in idem.* Del resto, finora la Corte di giustizia e la Commissione europea, così come la *Federal Trade Commission* (FTC) statunitense[6], hanno sempre escluso che il diritto *antitrust* potesse intervenire per sanzionare o prevenire forme illecite di trattamento dei dati personali[7]. Tuttavia, non tutte le autorità nazionali sono state dello stesso avviso, come vedremo nel riferire sul caso Facebook in Germania.

L'accumulo dei *Big Data* può produrre anche effetti pro-competitivi, stimolando la concorrenza tra imprese sulla base del merito, e promuovendo l'innovazione a vantaggio dei consumatori finali[8].

Un'impresa che controlla i *Big Data* non è però a priori più efficiente rispetto ai propri concorrenti, quindi lo studioso di diritto *antitrust* dovrà procedere caso per caso.

Siamo nell'ambito di quello che viene definito come diritto *antitrust* contemporaneo che: tutela il processo concorrenziale rivolto al benessere del consumatore, contribuisce a proteggere i singoli individui dall'invasione della *privacy,* e opera contro il potere delle imprese e la manipolazione dell'informazione diffusa dalle stesse nel mercato[9].

Il vero potere di mercato può infatti essere attribuito a soggetti che non sono ancora presenti nel mercato, ma che in poco tempo potrebbero essere in grado di entrarvi e distruggere l'attuale assetto[10]: Google, nei primi anni 2000, è divenuto in pochissimo tempo uno dei *leader* del settore tecnologico, in un mercato che fino ad allora era dominato da *Microsoft* e; Amazon, con il recente acquisto dei diritti audiovisivi sulle partite di *Champions League* e il loro inserimento nel pacchetto *Amazon Prime,* si prepara a fare lo stesso in un settore completamente diverso dal suo *core business*[11].

Si tratta di una strategia di espansione, meglio nota come "*cross-markets*", operata dalle *BigTech* al di fuori dei mercati rilevanti sui quali esse sono già dominanti; lo scopo di tale strategia sembrerebbe essere quello di costruire un "ecosistema" in continua espansione, entro il quale l'utente può soddisfare i propri bisogni senza dover rivolgersi ad altro operatore[12].

In altri termini, queste piattaforme digitali possono esercitare il loro potere, non solo nei mercati dove sono già presenti, ma soprattutto nei mercati dove non sono ancora attivi, e che, grazie alla grande

---

[6] In *Google/Doubleclick* 20 dicembre 2007, la FTC ha chiarito che *"the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition." - Statement of Federal Trade Commission Concerning Google/doubleClick*, FTC file no. 071-0170 (Dec. 20, 2007).

7 Così anche P. MERLINO, *Antitrust and Data protection Law: a relationship in search of clear boundaries* op.cit, 392.

[8] Cfr. OECD, *Data Driven Innovation for Growth and Well-Being: Interim Synthesis Report,* October 2014.

[9] Cfr. F. Jenny, Chair of OECD Competition Committee; OECD Competition Open Day, 27 February 2019, https://oecd.streamakaci.com/cod2019/ .

[10] Cfr. audizione del dott. Quintarelli (13 settembre 2018) e audizione dei Proff. Preta, Maggiolino e altri (30 gennaio 2018) in (SEDE).

[11] Non è la prima condotta di questo tipo per Amazon che, tempo fa, aveva deciso di acquisire la catena di negozi di cibi freschi *Whole Foods.*

[12] Così M. MAGGIOLINO, *Big data e diritto Antitrust, cit.* 63 e 265; S. GOBBATO *op.cit*., p. 152.

disponibilità di dati e alla elevata capacità di elaborarli, potrebbero agevolmente dominare.[13]

In altri termini, la disponibilità di *Big Data* sembrerebbe attribuire alle grandi piattaforme la capacità di esercitare contemporaneamente un potere concorrenziale su più mercati, tanto da esser considerati come soggetti dotati di un notevole potere di mercato, ancor prima di avervi fatto ingresso.

Non a caso, infatti, gli operatori dei settori bancario-assicurativo, delle informazioni creditizie e delle telecomunicazioni, comunemente soggetti ad una regolamentazione particolarmente strutturata e stringente, hanno manifestato il bisogno che venga loro assicurato un *level playing field*, al fine di consentire alle imprese tradizionali di competere con gli *Over The Top – OTT (Amazon, Facebook, Google*), senza il vincolo di asimmetrie regolatorie[14].

La *data driven economy* porta infatti a disintermediare gli operatori tradizionali, ad accentrare nel potere dei *Big Tech* tutto il mercato dei servizi – con il rischio di estromettere gli operatori tradizionali – e a lasciare l'intero mercato dei servizi in mano agli OTT.

I timori tipici dell'accumulo dei dati non nascono solo da un rischio *antitrust,* ovvero di preclusione anti-competitiva, ma anche dal fatto che i *Big Data* incrementano il potere delle imprese di invadere la *privacy* degli individui. Tuttavia, le imprese, pur favorendo l'esistenza di asimmetrie informative, non dispongono di un potere di mercato per il solo fatto di detenere i *Big Data.*

A tal proposito, occorre mettere in discussione concetti di base, come la nozione di impresa e di accertamento del potere di mercato. Inoltre, i *Big Data,* quando utilizzano effettivamente l'analisi algoritmica per influenzare le scelte d'acquisto dei consumatori e superare la concorrenza delle imprese rivali, possono fungere da barriera protettiva dei mercati a valle.

Negli ecosistemi digitali, i rapporti tra gli operatori che detengono le piattaforme e gli operatori che le utilizzano – o sono comunque soggetti all'attività di intermediazione svolta da tali piattaforme – sono particolarmente complessi. Tuttavia, i rischi *antitrust* sono analoghi a quelli che emergono in filiere di mercato "tradizionali", in cui un operatore in posizione dominante – che eroga un servizio "essenziale" per l'attività a valle – è verticalmente integrato.

Anche con riferimento alle condotte multilaterali, come si vedrà più avanti, è rilevante la correlazione tra *Big Data* e struttura dei mercati delle piattaforme digitali, caratterizzati da un alto livello di concentrazione; in particolare, ci si interrogherà circa l'adeguatezza del sistema di controllo delle concentrazioni, senza il timore di mettere in discussione i punti fermi del diritto *antitrust*.

Da ultimo, si analizzeranno le intese di natura orizzontale basate sull'utilizzo degli algoritmi di prezzo

[13] È quello che ad esempio è accaduto con il mercato dei pagamenti da sempre guardato con un certo interesse da questi giganti vista il gran numero di transazioni commerciali che avvengono in queste piattaforme (es. Amazon).

[14] Cfr. audizioni di Unicredit (8 marzo 2018), Intesa San Paolo (23 febbraio 2018), Generali (21 marzo 2018), Experian (28 novembre 2017), CRIF (18 dicembre 2017), Allianz (17 novembre 2017), Vodafone (7 dicembre 2018), Wind-Tre (29 novembre 2018), Fastweb (7 dicembre 2018), TIM (7 dicembre 2018).

(o *pricing algorithms*)[15]. A tal proposito, ci si interrogherà anche sull'adeguatezza dello strumentario legislativo e investigativo delle autorità, e sulla necessità di introdurre nuove figure professionali all'interno delle autorità - in grado a loro volta di utilizzare *Big Data* e algoritmi per migliorare le attività di scoperta e investigazione dei cartelli.

2.1 Abuso di posizione dominante

Le grandi piattaforme digitali sono spesso descritte come dominanti, in ragione della loro rilevanza e del fatto che operano su economie di scala, sia dal lato della domanda sia da quello dell'offerta.

Tali piattaforme hanno scardinato molti dei riferimenti di diritto *antitrust*, come quello sintetizzato nello slogan "*competition is a click away*". Infatti, la persistenza del loro potere di mercato non sembra avvertire alcuna minaccia dagli altri operatori che, sebbene investano in innovazione, non riescono a smantellare il potere di mercato delle *Big Companies* digitali.

Come si vedrà, gli effetti (o esternalità) di rete e la disponibilità di informazioni dettagliate sui consumatori rendono il potere di mercato di questi grandi operatori verosimilmente persistente.

Infatti, i modelli di *business* fondati sui *Big Data* sono caratterizzati da elevati livelli di concentrazione e dalla presenza di grandi operatori, che detengono posizioni dominanti.

Però, la disponibilità di *Big Data* è solo uno dei diversi fattori che contribuiscono, cumulativamente all'elevato grado di concentrazione e all'esistenza di barriere all'entrata, a formare una posizione dominante sul mercato. A tal proposito, occorre infatti considerare altri fattori: sia quelli nuovi, come gli investimenti per sviluppare gli strumenti di analisi e gestione dei dati; sia quelli più tradizionali, come le economie di scala e di scopo, e le esternalità di rete[16] che, in ragione del loro effetto cumulato sulle dinamiche concorrenziali, acquisiscono un particolare rilievo nei mercati digitali.

L'utilizzo dei *Big Data* assume inoltre un ruolo importante nella struttura di mercato c.d. "a due o più versanti", caratterizzata dalla presenza di due o più gruppi distinti di utenti[17].

In quest'ambito, gli effetti di rete assumono grande rilevanza con riferimento alle piattaforme di attenzione (*i.e.* motori di ricerca *online* e *social network*), in quanto la piattaforma che ha più utenti dispone di più dati, con i quali può offrire un servizio migliore, e attirare a sé più utenti. Di conseguenza, le piattaforme avranno barriere all'uscita e gli altri operatori avranno difficoltà a fare

[15] Sul punto, si parla della c.d. collusione algoritmica che consiste nell'utilizzare i *Big Data* e l'intelligenza artificiale, per praticare prezzi personalizzati e/o per impedire alle imprese concorrenti di accedere ai propri *Big Data*.

[16] A tal proposito è opportuno fare una distinzione tra: i) le esternalità dirette di rete sussistono quando il beneficio che a un consumatore deriva dall'acquisto di un bene o di un servizio aumenta con il numero dei consumatori che acquistano lo stesso bene o servizio; ii) le esternalità indirette di rete derivano, invece, dal fatto che esistono due separati gruppi di utenti nei mercati a due versanti (gli utilizzatori privati e i pubblicitari).

[17] Si tratta quindi di piattaforme online che, come abbiamo visto già nel primo capitolo, danno luogo a mercati a più versanti c.d. di attenzione o di scambio.

ingresso nel mercato[18].

Un ulteriore elemento che può incidere sul processo competitivo è dato dall'eventuale presenza dei c.d. *switching costs,* ovvero limitazioni tecniche o economiche che derivano dagli effetti di rete e che l'utente subisce nel passaggio da un operatore ad un altro. Gli *switching costs* possono essere ridotti per alcuni servizi digitali grazie alla diffusione del c.d. *multi-homing*[19]*,* che consiste nell'utilizzare alternativamente più piattaforme per un unico servizio. Un esempio frequente è quello dei servizi di *social network* - sebbene il *multi-homing* sia disincentivato spesso dal costo/opportunità (ad esempio il tempo necessario per curare il proprio profilo sul *social network*[20]) che gli utenti dovrebbero eventualmente sostenere per utilizzare attivamente e contemporaneamente una pluralità di piattaforme.

A causa della scarsa diffusione del *multi-homing,* dell'effetto cumulato degli *switching costs,* degli effetti di rete diretti e indiretti, della struttura dei costi e dell'importanza sempre maggiore dei dati, i mercati digitali tendono ad essere particolarmente concentrati e con elevate barriere all'entrata, determinando il c.d. effetto "*the winner takes all*: "chi vince prende tutto". Queste sono solo alcune delle caratteristiche strutturali dei mercati digitali che alimentano l'acquisizione di una posizione dominante, spesso conseguenza di una maggiore produttività o innovatività del prodotto o servizio offerto. Infatti, molti servizi digitali offerti in Internet sono controllati da operatori dominanti che non appaiono soggetti a pressioni competitive significative (*e.g*. Google nei servizi di ricerca *online* e nei servizi operativi per dispositivi mobili, Facebook nei *social network* e Amazon nell'intermediazione del commercio elettronico). A tal proposito, si parla dei c.d. GAFA(M) (Google, Apple, Facebook, Amazon e Microsoft) e si tratta di operatori che hanno una rilevanza sistemica, i cui servizi hanno un ruolo centrale nelle interazioni e transazioni digitali.

Il controllo di questi portali consente di esercitare un'influenza significativa sulle interazioni economiche e sociali, che hanno luogo su Internet e che incidono sulla visibilità e la reputazione delle imprese terze, oltre che sulle loro relazioni con i consumatori.

Il potere di mercato detenuto da tali operatori digitali dipende anche dalla loro integrazione verticale e conglomerale, che gli consente di avere una profilatura estremamente puntuale mediante la combinazione di dati sul comportamento digitale di un soggetto.

Nell'integrazione verticale, l'operatore dominante fornisce un servizio all'impresa terza, con la quale compete in un diverso livello della filiera, situazione che potrebbe favorire l'emergere di condotte

[18] Commissione Europea (2016), "*M.8124 Microsoft/Linkedin",* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf , par. 345.
[19] Commissione Europea (2014), "M.7217 Facebook/Whatsapp", http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf , par. 188/189.
[20] Commissione Europea (2016), "*M.8124 Microsoft/Linkedin",* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf , par. 345.

discriminatorie di natura escludente.

In quest'ambito, si inserisce anche la natura strategica dei servizi offerti ai consumatori e alle imprese. La tipologia dei questi servizi –come sistemi operativi, social *network*, motori di ricerca – riveste una rilevanza particolare, sia per la loro elevata capacità di acquisizione dei dati da parte degli utenti, sia per la loro influenza in una moltitudine di transazioni economiche e sociali. A questo proposito, è stata già accertata da parte di autorità *antitrust* europee l'esistenza di diverse posizioni dominanti[21].

L'ampia varietà di servizi offerti consente a tali operatori di intercettare i dati relativi alle abitudini di consumo degli utenti, pur rispettando il principio della finalità dei dati, oggetto di analisi nel primo capitolo.

Tali operatori (come Google Analytics e Facebook Analytics) offrono servizi non solo ai consumatori, ma anche alle imprese per l'acquisizione, la gestione e l'elaborazione di dati; queste ultime, in cambio, offrono ai grandi operatori l'accesso ai dati raccolti nei siti *web*[22], che acquisiscono dati relativi all'utilizzo dei siti/*app*, per poter avere tutte le statistiche sull'accesso alle pagine, ai contenuti visualizzati e alla provenienza degli utenti[23].

Un'altra caratteristica del potere di mercato di queste piattaforme è la loro interoperabilità con servizi terzi e complementari, presenti nella filiera dei *Big Data*[24].

Le normative *antitrust* non colpiscono la dominanza in sé, ma gli abusi di posizione dominante, ovvero quei comportamenti messi in atto dalle imprese dominanti che hanno il fine di sfruttare la loro posizione di forza nei confronti dei consumatori, delle imprese intermedie (c.d. abuso da

[21] Commissione Europea (2019), "*AT.40411 Google Search (AdSense)*", cfr. http://europa.eu/rapid/press-release_IP-19-1770_it.htm; Commissione Europea (2018), "*AT.40099 Google Android*", cfr. http://europa.eu/rapid/press-release_IP-18-4581_it.htm; Commissione Europea (2017), "*AT.39740 Google Search (Shopping)*", cfr. http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf; Bundeskartellamt (2019) B6-22/16 *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, cfr. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22- 16.pdf?__blob=publicationFile&v=4.

[22] Cfr., al riguardo, la menzionata sentenza della Corte di giustizia (Grande Sezione) 1° ottobre 2019, causa C- 673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV c. Planet49 GmbH* nella quale sono esplicitate le condizioni (con particolare riguardo al consenso dell'interessato).

[23] S. Englehardt & A. Narayanan, 2016, *Online Tracking: A 1-million-site Measurement and Analysis*, ACM CCS. Per considerazioni in ordine alla contitolarità del trattamento che si viene così ad integrare v. Corte di giustizia, 5 giugno 2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH.*

[24] Ad esempio, con riferimento agli *standard* tecnologici per le piattaforme *cloud*, sono emerse due principali soluzioni concorrenti: *Amazon Web Services Compatible Solutions*, offerta direttamente da Amazon, e *OpenStack*, un progetto *open source* supportato da imprese del settore come IBM.

sfruttamento[25]) o delle imprese concorrenti (c.d. abuso da impedimento[26]).

Una fattispecie intermedia tra l'abuso da sfruttamento e l'abuso da impedimento, nota solo in USA, è il c.d. *attempt to monopolize*: il "tentativo di monopolizzazione"[27]. In Europa, tale fattispecie non era punita, poiché veniva considerato ragionevole per un'impresa il voler espandere la propria posizione sul mercato, salvo il caso in cui vi fosse già una posizione dominante o un abuso della stessa.

Per comprendere lo stato dell'arte sarà necessario analizzare i casi più importanti di cui si è parlato nei vari paesi. Come segue.

2.1.1 La situazione americana e il Caso *Google*

Posner, con riferimento all'America, in una conferenza allo *Stigler Center* nel 2017, diceva "*Antitrust is dead, isn't it?*", denunciando la corruzione del Congresso americano da parte delle *Big Companies*. Infatti, Posner collegava i loro finanziamenti alle campagne elettorali al fatto che la *Federal Trade Commission* – FTC non avesse sanzionato Google per il noto caso che, come vedremo, lo vede come protagonista.

Gli Stati Uniti hanno sempre primeggiato sull'Intelligenza artificiale e il Governo americano ha sempre difeso le *Big Tech*, dato che contribuivano a mantenere tale primato, lasciando alla Cina il ruolo di inseguitore.

Tuttavia, sebbene a metà del '900, con la terza rivoluzione industriale, le grandi società tecnologiche fossero considerate indispensabili - non solo economicamente, ma anche per fronteggiare la guerra

[25] Con riferimento ai casi di abuso da sfruttamento, essi originano dal potere di mercato che alcuni operatori detengono nei c.d. mercati senza prezzo. Sebbene questi casi costituiscano una dimensione residuale dell'*enforcement* antitrust "tradizionale", nel mercato digitale il loro rilievo è assai più esteso. Oltre al tema connesso al rapporto tra piattaforme e utenti finali con specifico riferimento al trattamento dei dati personali e, dunque, alla possibilità di configurare possibili abusi di posizione dominante anche con riferimento a tale aspetto, il potere di mercato degli operatori digitali può essere esercitato anche attraverso l'imposizione di prezzi (o altre condizioni contrattuali) eccessivamente gravosi.
L'esistenza di posizioni dominanti nell'attività di intermediazione tra una pluralità di soggetti, fa sì che le preoccupazioni possano riguardare uno solo dei versanti della piattaforma e, dunque, una sola categoria di utenti. Ad esempio, alcune recenti iniziative (legislative e di *enforcement)* pongono l'accento sulla relazione tra le piattaforme di intermediazione nel commercio elettronico e gli utenti non consumatori di tali piattaforme. Si tratta, dunque, di fattispecie il cui trattamento richiede una chiara definizione degli obiettivi che l'*enforcement* persegue, soprattutto in considerazione del fatto che tali iniziative possono comportare la necessità di un bilanciamento tra il benessere degli utenti dei diversi versanti della piattaforma, ovvero più direttamente tra i soggetti imprenditoriali che si avvalgono delle piattaforme e i consumatori finali.

[26] L'articolo 102 TFUE trova applicazione anche nei casi in cui il detentore di un'*essential facility* opponga un rifiuto a contrarre a un'impresa con la quale compete in un mercato a valle. Anche nel caso in cui l'*essential facility* sia costituita da dati, un eventuale rifiuto a concedere a terzi l'accesso a tali dati ha una rilevanza antitrust, se e nella misura in cui è idoneo a ridurre la concorrenza in un mercato complementare/a valle. Pertanto, ai fini dell'applicazione dell'art. 102 TFUE, assume particolare peso la finalità alla base di una richiesta di accesso ai dati detenuti da un'impresa dominante. Le richieste di accesso ai dati potenzialmente più rilevanti in una prospettiva concorrenziale sono quelle relative ai dati: i) necessari per offrire un bene/servizio al consumatore nel mercato in cui i dati sono acquisiti, in concorrenza con l'operatore (dominante); ovvero; ii) necessari per competere in un mercato contiguo; o iii) in un *aftermarket* in cui è attivo l'operatore in posizione dominante.

[27] DELMASTRO E NICITA, *Big data: come stanno cambiando il nostro mondo*, il Mulino, 2019, 70.

fredda sul controllo delle informazioni - oggi, durante quella che molti chiamano la quarta rivoluzione industriale (o Industria 4.0), la situazione sembra essere in parte cambiata, in quanto si cerca di responsabilizzarle sempre di più.

La disciplina *antitrust* statunitense, il c.d. *Sherman Antitrust Act* del 1890, si basa su tre parametri per supportare la tesi della posizione dominante; questi però, come vedremo, appaiono inadeguati per fronteggiare il mercato digitale.

Il primo parametro è quello che ha come riferimento il prezzo di beni e servizi, ovvero quando si può dimostrare che le società abbiano approfittato della loro posizione dominante per far salire i prezzi e limitare gli investimenti in un determinato mercato. Questo parametro è inadeguato nelle imprese tecnologiche, che spesso offrono servizi "gratuiti" ai loro utenti.

Il secondo parametro è la legalità con cui un'impresa acquisisce la sua posizione monopolistica; come sappiamo le società tecnologiche non sono monopoli naturali[28], beneficiando dell'agevolazione di ingresso con un costo elevato nel mercato e dei noti effetti di rete che hanno dominato e sfruttato a loro favore. Pertanto, non è semplice per le autorità competenti dimostrare l'illegalità di tali posizioni monopolistiche.

Infine, il terzo parametro è il benessere del consumatore, ma non è facile dimostrare una condotta contraria a tale parametro, dato che queste società sfruttano la massiccia raccolta di dati proprio a beneficio dei consumatori, per perfezionare la loro offerta di servizi gratuiti.

Con riferimento alla casistica, il primo caso che conosciamo (risalente agli anni '90) è quello di Microsoft, quando l'impresa è stata accusata di imporre il proprio sistema operativo Windows ai propri utenti. Per questi ultimi risultava difficile installare simultaneamente un *software* della concorrenza insieme ad Internet Explorer, il *browser* di Microsoft. In questo frangente, il Dipartimento di giustizia americano (*Department of Justice – DOJ*) ha cercato di scindere Microsoft per impedirgli di tenere insieme *Internet Explorer* con il sistema operativo Windows. Il provvedimento venne tuttavia impugnato da Microsoft, che ne ottenne così l'annullamento. Ciò nonostante, si è costituito un precedente, tanto che molti legislatori hanno suggerito la medesima impostazione anche per Amazon, mediante la divisione in due entità: una per l'*e-commerce*, e l'altra per *Amazon Web System*.

Se da una parte il caso si è risolto con un accordo amichevole tra il DOJ e la società americana,

[28] Di questo avviso, tra tutti, il Prof. Herbert Hovenkamp dell'Università di Pennsylvania secondo il quale non sarebbero configurabili come monopoli naturali in quanto, ed è questa la grande differenza rispetto ai servizi di pubblica utilità che vengono tradizionalmente regolati, i servizi offerti dalle piattaforme digitali sarebbero servizi differenziati. Per dimostrare tale tesi ha portato l'esempio dei siti di incontri, dove una importante impresa che ne ha acquisiti diversi negli ultimi anni, anziché aggregarli in un unico servizio, li ha tenuti separati. Il video dell'intervento del Prof. Hovenkamp è disponibile al seguente link: https://www.youtube.com/watch?v=1yHyWssaTzs&feature=youtu.be; l'intervento si basa su una bozza dell'articolo Hovenkamp, Herbert, Antitrust and Platform Monopoly (September 23, 2020). *Yale Law Journal*, Vol. 130, 2021, U of Penn, Inst for Law & Econ Research Paper No. 20-43, Available at SSRN: https://ssrn.com/abstract=3639142.

dall'altra parte si è creata una situazione in cui non solo *Microsoft* venne screditata agli occhi degli utenti ma, anzi, si creò un ambiente favorevole all'emergere di una delle più grandi *Big Tech* di oggi, *Google*.

Qualcosa è iniziato a cambiare già nel 2011 quando la FTC aprì un'istruttoria contro Google relativamente all'utilizzo di *cookies* di tracciamento in Safari, il *browser* di Apple, la quale si concluse con una multa di 22,5 miliardi di dollari[29]. In particolare, Google aveva violato la *privacy policy*, risultando responsabile per aver rappresentato in modo errato la garanzia di *privacy* agli utenti di Safari.

Successivamente, la FTC iniziò nuovamente un'investigazione su Google che, risultando vittorioso, poté continuare a gestire i suoi risultati di ricerca sul proprio *browser*, sponsorizzando i suoi servizi, sia pure promettendo di fare piccoli aggiustamenti nel *search advertising*. Questa vittoria di Google non fu di poco conto, perché consentì alla società di imporsi come uno dei nuovi *leader* del settore tecnologico, generando miliardi di dollari di profitti annui dall'*advertising*, ed espandendo il proprio *business* anche in altri ambiti, come quello delle mappe.

A detta del DOJ, dopo oltre un anno di indagine, le promesse di Google sull'*advertising* non sembrano essere state rispettate, in quanto nell'ottobre 2020 Google è stata accusata di proteggere illegalmente il suo monopolio nei motori di ricerca (c.d. *search*) e nella pubblicità digitale (c.d. *search advertising)*, attraverso accordi e contratti di distribuzione nei quali la stessa pagherebbe ad altre imprese milioni di dollari. Si tratta del business di una società holding, *Alphabet Inc*, fondata nel 2015 come holding a cui fanno capo Google LLC e altre società controllate. A tale iniziativa del DOJ, che è la diretta conseguenza di un rapporto del Congresso, si sarebbero uniti undici Stati repubblicani.

In particolare, il DOJ ha denunciato un comportamento anti-competitivo di Google, in violazione della *Section 2* del *Sherman Antitrust Act*, consistente nell'aver stipulato accordi commerciali esclusivi e condotte anti-competitive, al fine di sbarrare i canali distributivi ed escludere le imprese rivali falsando la libera concorrenza. L'accusa sostiene che Google abbia pagato miliardi di dollari ogni anno a distributori (*e.g.* Apple, LG, Motorola, and Samsung) e sviluppatori di *browser* (Mozilla, Opera, and UCWeb), al fine di assicurarsi di rimanere l'impresa di *default* come motore di ricerca generico e, in molti casi, anche proibendo alle sue controparti di fare affari con i suoi concorrenti.

In alcuni di questi accordi, secondo l'accusa, Google avrebbe obbligato le sue controparti ad avere le sue App, come quelle di ricerca, mantenendole nelle prime posizioni sui loro dispositivi, in modo che gli utenti fossero maggiormente invogliati ad iniziare le ricerche sul *web* tramite Google.

Alla luce di tali condotte, secondo il Dipartimento di Giustizia, Google avrebbe inoltre precluso la concorrenza nella ricerca su Internet.

[29] *United States v. Google Inc*., No. 3:12-cv-04177 (N.D. Cal. Nov. 16, 2012)

La dominanza del colosso americano è testimoniata anche dal fatto che il nome "*Google*" non è solo usato per identificare la società ed il motore di ricerca, ma anche come verbo utilizzato per far riferimento all'attività di ricerca su internet. Google monetizza questo monopolio sulla ricerca in Internet nei mercati per il *search advertising* e per il *text advertising.* In quest'ambito, Google usa le richieste di ricerca dei consumatori e le loro informazioni per vender loro pubblicità. Quest'ultima, muove un importo pari a 40 miliardi di dollari all'anno, che vengono corrisposti a Google per l'*advertising* nei risultati di ricerca. Tale importo viene spartito da Google con i distributori, in cambio della loro fedeltà e come disincentivo a contrattare con altri concorrenti. In altri termini, tali pagamenti verso i distributori creano barriere all'entrata per i rivali di Google, con particolare riferimento alle imprese innovative che non possono permettersi di competere con questi alti costi d'entrata. In questo modo, Google avrebbe creato continui e rinforzati monopoli in diversi mercati.
Inoltre, i diversi tipi di *search advertising* richiedono particolari algoritmi di *self-learning* in grado di analizzare i dati estrapolati dalle ricerche degli utenti e di imparare costantemente dagli stessi, adattandosi ai diversi bisogni e richieste dei consumatori. Tali algoritmi vengono inoltre accelerati dal volume, dalla varietà e dalla velocità dei dati raccolti che Google, come pochi altri, può vantare.
La causa verte anche sugli accordi commerciali del sistema operativo Android, di proprietà di Google, che prevede appunto il suo *browser* come predefinito, e non eliminabile dai dispositivi.
La società americana, in risposta alle accuse del Dipartimento di giustizia, afferma che il suo obiettivo è quello di rendere disponibile *Google Search* a chiunque. Dunque, il motivo del loro utilizzo dipenderebbe dall'effettiva preferenza da parte degli utenti, rispetto ad altre piattaforme di ricerca. Inoltre, Google a difesa della sua posizione dominante e del suo comportamento, richiama anche l'oramai anacronistico principio "*competition is a click away*" che, come già rilevato, consiste nell'elevata mutabilità ed innovazione a cui è soggetto il mercato, che può facilmente vedere l'ingresso di nuovi operatori.
Però, sebbene, da una parte, le autorità statunitensi abbiano mostrato recentemente un atteggiamento più aggressivo nei confronti degli operatori digitali, e quindi più in linea con l'Unione Europea, dall'altra parte, gli Stati Uniti manifestano ancora forti perplessità rispetto ad una regolazione *ex-ante* nei confronti degli operatori digitali.
Nella conferenza dell'ICN (*International Competition Network*), tenutasi nell'ottobre 2020 e alla quale hanno partecipato i vertici delle autorità di concorrenza statunitensi e della Direzione Generale Concorrenza della Commissione Europea, il tema trasversale è stato proprio l'impatto della digitalizzazione dell'economia sulle attività di *enforcement* e *advocacy* delle autorità di concorrenza. In particolare, le autorità statunitensi hanno espresso riserve sulle iniziative intraprese dalla Commissione, in tema di nuovi rimedi per i mercati digitali, ritenendo sufficiente la legislazione

attualmente vigente[30]. Tali autorità, hanno sottolineato la complessità dei mercati digitali che, essendo tutti diversi, non si prestano necessariamente ad un approccio comune, Le stesse hanno ribadito, al contempo, la flessibilità del loro sistema di *enforcement* nell'adattarsi alle diverse condotte dei grandi operatori digitali. Inoltre, hanno rilevato la necessità di essere cauti prima di intervenire con una regolamentazione del settore, dal momento che sarebbe previamente opportuno valutare la capacità dell'intervento *antitrust* quale risposta alle criticità emerse nel settore digitale. I miglioramenti all'approccio *antitrust* possono derivare dalle analisi *ex post* sul proprio operato - come quelli in corso da parte della FTC sulla valutazione delle concentrazioni nel settore digitale - senza avere paura di fare emergere criticità.

Inoltre, nell'ottobre 2020, il Congresso americano ha pubblicato gli esiti di una lunga investigazione (durata più di 16 mesi) sulla concorrenza in materia di economia digitale e, in particolare, sulle nuove sfide emerse a seguito della posizione dominante di Apple, Amazon, Google e Facebook.

Il rapporto, intitolato "*Investigation of Competition in the Digital Marketplace: Majority Staff Report and Recommendations"*[31], totalizza più di 400 pagine, segnando il culmine di un'indagine che comprende sette udienze congressuali, la produzione di quasi 1,3 milioni di documenti interni e comunicazioni, contributi da 38 esperti di antitrust e interviste a oltre 240 partecipanti al mercato, ex dipendenti delle piattaforme indagate e altri individui.

In particolare, il Presidente della Commissione giudiziaria, insieme al Presidente della Sottocommissione di Antitrust, hanno dichiarato che: "*Our investigation leaves no doubt that there is a clear and compelling need for Congress and the antitrust enforcement agencies to take action that restores competition, improves innovation, and safeguards our democracy. This Report outlines a roadmap for achieving that goal*".

Dopo aver delineato le sfide presentate a causa della posizione dominante di Amazon, Apple, Google e Facebook, il rapporto esamina una serie di possibili rimedi per: (i) ripristinare la concorrenza nell'economia digitale; (ii) rafforzare le leggi *antitrust*; e (iii) rinforzare l'*enforcement* dell'*antitrust*.

Nella lista delle raccomandazioni, si trovano tra le tante: i) separazioni strutturali per vietare alle piattaforme di operare in linee di business, che dipendono o interagiscono con la piattaforma; ii) chiedere alle piattaforme di rendere i propri servizi compatibili con le reti concorrenti per consentire l'interoperabilità e la portabilità dei dati[32]; iii) rafforzare la FTC e la Divisione Antitrust del

[30] Il programma della conferenza è disponibile sul sito ICN al link: https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/09/2020ICNConferenceAgenda.pdf. Inoltre, tutte le sessioni sono registrate e accessibili al seguente link: https://icn-2020.videoshowcase.net/

[31] Cfr. https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

[32] Vi è una relazione di corrispondenza biunivoca inversa tra portabilità e antitrust, nel senso che quanto maggiore sia la garanzia del (l'esercizio efficace del) diritto alla portabilità dei dati personali, dunque di ubiquità dei dati degli utenti sui mercati digitali, tanto minori rischi vi saranno per la concorrenza.

Dipartimento di Giustizia (DOJ).

2.1.2 La Cina e la condotta "*choose one from two*" di *Alibaba*

La legge antimonopolistica in Cina, meglio conosciuta nel mondo occidentale come *Anti-Monopoly Law* (AML), è entrata in vigore nell'agosto del 2008[33].

In particolare, l'AML vieta: i) gli accordi monopolistici; ii) l'abuso di posizione dominante; iii) le concentrazioni e; iv) i monopoli delle amministrazioni cinesi[34].

Questi quattro pilastri costituiscono inoltre le basi sostanziali del contenzioso *antitrust* cinese: nei primi tre casi si tratta di contenzioso civile, mentre nell'ultimo caso di contenzioso amministrativo, a cui si uniscono le impugnazioni alle sanzioni emesse dell'Autorità cinese.

Alibaba è il colosso cinese dell'*e-commerce* e la sua piattaforma *retail*, Tmall, ha raggiunto un volume di affari di circa 74 miliardi di dollari in un giorno solo[35].

Il suo più grande concorrente si chiama JD.com e, durante la stagione annuale cinese dello *shopping*, la c.d. "Double 11" (l'equivalente del nostro *Black Friday*), si è affermata la *practice* del c.d. "*choose one from two*" ("二选一" in cinese)[36].

Tale pratica è diventata così comune in Cina che l'autorità *antitrust* cinese, la *State Administration for Market Regulation* (SAMR), deve avvertire in anticipo quasi prima di ogni stagione delle vendite.

La *Supreme People's Court* (SPC), l'organo di giurisdizione civile cinese, a seguito di un'azione contro Alibaba, da parte del concorrente JD.com e di altri più piccoli, sarà chiamata a pronunciarsi sulla condotta del "*choose one from two*", ovvero se questa costituisca o meno un abuso di posizione dominante in violazione della AML.

Va detto che in Cina tra le centinaia di casi di *public enforcement* dal 2008 (anno in cui è entrata in vigore l'AML) ad oggi, solo poche dozzine riguardano casi di abuso di posizione dominante. E, tra

---

[33] Per un'informazione generale in materia di abuso di posizione dominante e piattaforme digitali in Cina cfr. Adrian Emch/Wendy Ng, Wang Xiaoye Liber Amicorum - The Pioneer of Competition Law in China, https://www.concurrences.com/en/all-books/wang-xiaoye-liber-amicorum; The BRICS Competition Law and Policy Centre, BRICS Report on Digital Era Competition, http://www.bricscompetition.org/upload/iblock/6a1/brics%20book%20full.pdf; Public Enforcement of Antitrust Law in China: Perspective of Procedural Fairness (Abstract) (2015), https://mp.weixin.qq.com/s/xurWTl2lt9txKmSDW-39Cw Jet Deng e Ken Dai, A practical Review of The Draft Amendment to The Anti-Monopoly Law of China: Highlighting Six Areas with Eighteen Changes (2020), https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/february/27/a-practical-review-of-the-draft-amendment-to-the-antimonopoly-law-of-china; Antitrust Sanctioning in China: How Can The NDRC Guidelines Be Further Improved (2017), https://www.competitionpolicyinternational.com/antitrust-enforcement-in-the-chinese-automobile-industry-observations-and-future-perspectives/.

[34] Così Jet Deng e Ken Dai, *Antitrust Litigation in China: From the Pespective of Lawyer Practice,* https://whoswholegal.com/features/antitrust-litigation-in-china-from-the-perspective-of-lawyer-practice;

[35] PYMNTS, *Alibaba Single's Day 2020: $74.1 Billion New Record Setting Performance,* in https://www.pymnts.com/news/retail/2020/alibaba-singles-day-2020-sales-records-broken-but-new-chinese-regs-spoil-the-party/.

[36] Così Jet Deng e Ken Dai, *Antitrust Enforcement Against Digital Platforms in China: Anatomy of "Choose One from Two"* , https://whoswholegal.com/features/antitrust-enforcement-against-digital-platforms-in-china-anatomy-of-choose-one-from-two.

questi, nessuno riguarda una piattaforma *e-commerce*. Ciò, anche per il discorso più generico secondo cui stabilire una posizione dominante nel mercato digitale, a differenza dei mercati tradizionali, è più complicato per via degli effetti di rete, dei mercati a due o più versanti e del *multi-homing* che può contribuire a ridurre gli *switching costs* derivanti dagli effetti di rete stessi.

Tuttavia, la situazione sta cambiando, a seguito delle nuove proposte regolamentari avanzate nel novembre 2020 nella bozza dell'*Antitrust Guidelines on the Field of Platform Economy* (di seguito "*Draft Guidelines*")[37].

Infatti, il Consiglio di Stato ha varato una nuova *task force* di 17 entità governative ministeriali o dipartimenti, che dovranno vigilare per evitare lo sfruttamento di posizione dominante da parte di protagonisti come Alibaba. Quel che si sa, per ora, è che la SAMR farà da capofila, seguita da agenzie di livello ministeriale, dalla Banca centrale, dalla *China Banking and Insurance Regulatory Commission*, dalla *China Securities Regulatory Commission*, fino al ministero della Pubblica sicurezza. Si tratta di un passo ulteriore nella revisione cinese della AML del 2008 per metterla al passo con i tempi, tarandola sul dominio dei giganti *online* cinesi. La bozza estende i criteri adottati per valutare il controllo di un mercato da parte di una società, e menziona per la prima volta gli attori del *web*, le loro economie di scala, gli effetti di blocco dei loro prodotti o servizi e la loro capacità di gestire ed elaborare i dati[38].

Sul punto, la SAMR ha affermato nel novembre 2020 che investigherà sulla condotta "*choose one from two*" di Alibaba, per valutare se possa integrare una restrizione della concorrenza, tramite accordi di esclusiva avvenuti per iscritto, telefonicamente, o negoziati verbalmente con la controparte, nonché attraverso ostacoli di qualsiasi natura contenuti nel regolamento della piattaforma.

Tornando al caso di specie, si tratta di una condotta tramite la quale ai venditori viene richiesto di chiudere i negozi sulla piattaforma concorrente, in modo tale che i consumatori non siano più diretti sui loro prodotti all'interno della piattaforma, e la vendita di questi venga interamente sospesa.

Si tratta di una condotta che *prima facie* sembrerebbe violare il divieto di esclusiva, previsto in Cina come una delle condotte abusive ai sensi della AML.

Il c.d. *exclusive dealing* non è di per sé illecito, e può essere scusato da giustificazioni di *business* che, secondo la AML, possono consistere, a titolo esemplificativo, in sicurezza del prodotto, protezione della proprietà intellettuale ecc.

Secondo un'altra lettura, questa condotta poteva rientrare in un rifiuto a contrarre sulla base

[37]Così Chris Gill, *China's Alibaba, JD.com and Tencent could face break-up,* https://www.asiatimesfinancial.com/china-s-alibaba-jd-com-and-tencent-could-face-break-up.

[38] Il CEO del Gruppo Alibaba, il 16 novembre 2020, alla *World Internet Conference* ha dichiarato che "*development and government supervision is a relationship that promotes and relies on each other, so that platform enterprises cannot only develop well themselves, but also serve the sustainable and healthy development of the whole society*".

dell'*Essential Facilities Doctrine (di seguito anche EFD)* di origine statunitense[39], che prevede che i monopolisti che detengono una risorsa essenziale, sono obbligati a metterla a disposizione dei concorrenti, i quali hanno diritto di utilizzarla in base alle loro capacità, alla luce di una concorrenza basata sul merito[40].

Non è questa però la strada comunemente preferita dagli *enforcers*, in quanto non è facile per le autorità provare l'"essenzialità" della risorsa, tanto più in un mercato come quello digitale, caratterizzato dal *multi-homing* degli utenti.

Da ultimo, secondo un'altra tesi, la condotta di Alibaba sarebbe potuta rientrare in una condotta escludente, tipica dell'integrazione verticale, in cui l'operatore dominante fornisce un servizio all'impresa terza, con la quale compete in un diverso livello della filiera; tale situazione potrebbe favorire l'emergere di condotte discriminatorie di natura escludente.

Ebbene, ad aprile 2021 la SAMR ha sanzionato Alibaba con una maxi-multa da 18,2 miliardi di yuan (pari a 2,78 miliardi di dollari) per abuso di posizione dominante, superando così i 975 milioni di dollari pagati nel 2015 dal produttore di *chip* americano Qualcomm[41].

Tale decisione rappresenta il primo caso di abuso di posizione dominante nell'economia digitale cinese, a testimonianza del cambio di rotta dell'amministrazione cinese nei confronti delle condotte delle grandi piattaforme digitali.

2.1.3 La situazione nell'Unione europea: i tre casi *Google* e il più recente caso *Amazon*

Una priorità nell'*enforcement* dell'art. 102 TFUE è costituita dalla repressione degli abusi di natura escludente. Le recenti esperienze applicative della Commissione europea mostrano come tale norma sia idonea a contrastare diverse pratiche escludenti legate all'utilizzo dei *Big Data* - dirette a frapporre ostacoli ai soggetti terzi nell'acquisizione dei dati degli utenti - o consistenti in pratiche leganti o discriminatorie. In particolare, la Commissione ha concluso ben tre procedimenti istruttori nei confronti di *Google* per abusi di posizione dominante, aventi ad oggetto condotte escludenti nei mercati delle ricerche generiche sulla rete e in quello parallelo dell'intermediazione pubblicitaria dei motori di ricerca. Infatti, grazie a queste condotte, Google ha potuto negli anni acquisire una mole sempre più significativa di dati degli utenti, che sono serviti sia per le sue attività di ricerca, sia per quelle di pubblicità digitale.

[39] BARIATTI-SODANO, Gli abusi di posizione dominante, in Frignani-Bariatti (a cura di), Disciplina della concorrenza nella UE, in Tratt. dir. comm. dir. pubbl. econ. Galgano, Padova, Cedam, 2012, 318-321.
[40] Con riferimento all'*essential facility doctrine* vedi § 1.2.5.
[41] A. ANNICCHIARICO, *Tech sotto tiro in Cina. Alibaba rischia una multa da un miliardo, colpite Tencent e Baidu,* disponibile su https://www.ilsole24ore.com/art/alibaba-rischia-multa-un-miliardo-lascia-ceo-ant-group-simon-hu-ADRNDlPB, 12 marzo 2021.

1. Il primo caso risale al giugno 2017. La Commissione ha accertato un abuso di posizione dominante di Google nel mercato dei servizi di ricerca generica, e le ha comminato un'ammenda pari a 2,42 miliardi di euro[42]. In particolare, la società aveva riservato al proprio servizio di acquisti comparativi un trattamento più favorevole rispetto ai servizi concorrenti, in termini di posizionamento e di visualizzazione nelle sue pagine generali dei risultati di ricerca. In dettaglio, il servizio di Google non era soggetto agli algoritmi specifici, che rendevano probabile la retrocessione dei servizi di acquisti comparativi, concorrenti all'interno delle pagine di ricerca generica di Google. Inoltre, il servizio di acquisti comparativi di Google veniva visualizzato con funzionalità migliorate, in cima ai risultati della prima pagina di ricerca generica, o comunque tra i primi risultati, e tali funzionalità non erano accessibili ai concorrenti.
2. Il secondo caso è del luglio 2018, nel quale la Commissione europea ha inflitto a Google un'altra ammenda, pari a 4,34 miliardi di euro, per abuso di posizione dominante[43].

   In questo caso, la Commissione accertava che la società, nella fase di transizione dall'utilizzo dei computer *desktop* a quello di Internet *mobile*, aveva implementato una strategia, per far sì che gli utenti continuassero ad usare *Google Search* sui propri dispositivi mobili.

   Google aveva infatti imposto ai produttori di dispositivi Android, e agli operatori di reti mobili, condizioni contrattuali illegittime, al fine di consolidare la propria posizione dominante nel mercato delle ricerche generiche su Internet.

   Tali condotte avevano reso possibile pre-installare il motore di ricerca e il *browser* di Google, sulla quasi totalità dei dispositivi *Android* dello stesso, a scapito dei motori di ricerca dei concorrenti[44].
3. Infine, nel terzo caso, a marzo 2019, è stata comminata a Google una sanzione pari a 1,49 miliardi di euro, per aver abusato della propria posizione dominante sul mercato dell'intermediazione pubblicitaria nei motori di ricerca, dove Google è attiva tramite la piattaforma *AdSense for Search*. Attraverso questa piattaforma, Google agiva come un intermediario pubblicitario tra inserzionisti e proprietari di siti web, che intendevano trarre profitto dallo spazio attorno alle pagine dei risultati

[42] Commissione Europea (2017), "AT.39740 Google Search (Shopping)", http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.
[43] Commissione Europea (2018), "AT.40099 Google Android", http://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf.
[44] In particolare, Google aveva: i) imposto ai produttori di dispositivi mobili intelligenti di preinstallare l'applicazione Google Search e la sua applicazione di browsing *(Chrome*) come condizione per la concessione della licenza relativa al portale di vendita di applicazioni di Google (*Play Store*); ii)concesso significativi incentivi finanziari ad alcuni grandi produttori e operatori di reti mobili affinché preinstallassero a titolo esclusivo l'applicazione Google *Search* sui loro dispositivi e; iii) impedito ai produttori che desiderassero preinstallare le applicazioni Google la vendita di dispositivi mobili funzionanti con versioni alternative di Android non approvate da Google (le cosiddette "*Android forks*").

della ricerca[45].

Dall'istruttoria condotta dalla Commissione europea, emergeva che Google, come prima cosa, imponeva ai principali siti *publisher* un obbligo di fornitura esclusiva, in modo da impedire ai concorrenti di inserire annunci pubblicitari collegati alle ricerche sui siti web, più significativi dal punto di vista commerciale, e poi adottava una strategia di "esclusiva non rigida", tramite la quale riservava per i propri annunci gli spazi migliori, e controllava le prestazioni degli annunci degli operatori concorrenti.

In tutti e tre i casi, sopra analizzati, si tratta di condotte escludenti contestate nel diritto *antitrust* tradizionale, e che vanno interpretate alla luce del diritto *antitrust* contemporaneo, che deve tener conto delle specificità dell'economia digitale[46].

Infatti, anche nel primo caso, il più risalente, riguardante l'uso dell'algoritmo come principale strumento di discriminazione, l'accertamento della condotta di abuso si fondava, in particolar modo, sulla portata escludente della strategia di Google.

Inoltre, altro caso rilevante ai fini della presente analisi è quello di Amazon che, come noto, ricopre un importante ruolo nel mercato del commercio *online*[47]*;* qui l'accusa della Commissione è duplice: la società avrebbe sia usato i dati di fornitori terzi a proprio beneficio, sia garantito a questi ultimi una via preferenziale ai suoi servizi[48].

Tale strategia dell'impresa integrerebbe, secondo la Commissione, gli estremi di una condotta di abuso di posizione dominante.

Il caso ha ad oggetto la posizione ambigua e "duale" di Amazon, la quale ricopre al tempo stesso sia il ruolo di intermediario *online* per terzi, sia quello di fornitore di prodotti/servizi propri e concorrenti con quelli che vengono intermediati.

Un'indagine preliminare ai danni della società in questione era iniziata già a luglio 2019. In tale occasione, la Commissione europea per la concorrenza, Margrethe Vestager, ha affermato che:

---

[45] Quando un utente effettua una ricerca utilizzando questa funzione, insieme ai risultati della ricerca, il sito web propone annunci pubblicitari collegati alla ricerca. Dal momento che i concorrenti nella pubblicità collegata alle ricerche, come Microsoft e Yahoo, non hanno la possibilità di vendere spazi pubblicitari nelle pagine dei risultati di ricerca di Google, i siti web di terzi rappresentano un importante punto di accesso per tentare di competere efficacemente con Google.

[46] M. RICOLFI, *IoT and the ages of Antitrust ("IoT" e le età di "Antitrust")* in *Concorrenza e mercato*, 2017, pt. 1, pp. 215-232. Infatti, si può osservare come nell'economia digitale la definizione dei mercati rilevanti e l'accertamento del potere di mercato siano indubbiamente più complessi che nell'economia tradizionale. Ciò posto, impregiudicata l'utilità di una comprensione del contesto in cui le condotte oggetto di analisi si sviluppano e producono i loro effetti, una maggiore attenzione può essere prestata direttamente alla portata escludente di tali condotte, in particolare se fondate sulla centralità e non replicabilità dei dati nella disponibilità dell'impresa dominante che possono interessare contemporaneamente una varietà di mercati.

[47] Il valore del commercio *online* è pressochè raddoppiato negli ultimi cinque anni in Europa raggiungendo nel 2020 i 720 miliardi di euro. In tutto ciò ha influito senz'altro il confinamento provocato dall'epidemia influenzale.

[48] La commissaria alla Concorrenza Margrethe Vestager ha infatti dichiarato che le regole della piattaforma *online* non devono favorire artificialmente le offerte al dettaglio di Amazon o le offerte dei rivenditori che utilizzano i servizi logistici e di consegna della stessa Amazon. Cfr. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077.

"*Secondo conclusioni preliminari, Amazon ha abusato della sua posizione in Germania e in Francia*"[49].

Il comportamento di *self-preferencing,* realizzato anche attraverso l'accesso privilegiato a dati non disponibili ai concorrenti diretti, costituisce uno dei comportamenti anticoncorrenziali che vengono solitamente contestati alle nuove piattaforme digitali, che al ruolo di intermediazione affiancano quello di una integrazione conglomerale dei diversi versanti dei mercati intermediari. In altri termini, la Commissione contesta all'impresa un vantaggio non replicabile dai concorrenti.

Si tratterrebbe di un vantaggio strutturale che non sembra essere risolvibile, se non con impegni verificabili che siano in grado di assicurare la rimozione degli effetti concorrenziali contestati dalla Commissione[50].

Sul piano dei rimedi si è discusso anche nella conferenza ICN, sopra menzionata, dove la Vestager ha sostenuto che, man mano che la digitalizzazione pervade sempre più la nostra economia, si rende necessaria l'introduzione di una regolazione e di strumenti correttivi *ex ante*, per assicurare un più corretto funzionamento dei mercati, che possono in alcuni casi presentare delle criticità dal punto di vista concorrenziale[51].

Ritornando al caso di Amazon, il vantaggio dell'impresa consisterebbe nell'accesso esclusivo ai dati di terze parti, relativo a prodotti e servizi concorrenti, al fine di anticipare le strategie di prezzo e spiazzarne la domanda, indirizzandola presso i propri prodotti e servizi piuttosto che quelli della concorrenza.

Nello specifico, ciò avverrebbe anche attraverso il *placement* privilegiato di propri prodotti e servizi in appositi box utilizzati dagli utenti (c.d. "*Buy Box*").

L'impresa si è difesa affermando che il suo *business* rappresenterebbe solo l'1% del mercato mondiale del commercio al dettaglio.

L'America, come abbiamo visto, ha da sempre protetto le imprese nazionali come Amazon e, nonostante ultimamente gli USA stanno cambiando approccio, rimane sempre forte questa tentazione.

Mentre l'Europa vorrebbe presentare una modifica delle regole *antitrust* e consentire alla Commissione di agire *ex ante,* dinanzi al rischio di abuso di posizione dominante da parte di una *Big Tech,* la FTC americana rimane ancora contraria a detti interventi.

Infatti, da ultimo, il *Digital Markets Act* propone: da una parte, la definizione di una serie di regole

[49] L'Italia viene lasciata fuori per il lavoro, iniziato in anticipo, avviato già dall'AGCM contro Amazon.

[50] Il commissario UE alla Concorrenza Margrethe Vestager ha infatti riconosciuto che, sebbene negli anni lei stessa abbia irrogato sanzioni severissime nei confronti di questi giganti, queste grosse multe ai BigTech non possono consistere in un rimedio alla loro posizione dominante. Infatti, anche i casi di multe significative non riescono a modificare in modo strutturale le dinamiche competitive in questi mercati né il ruolo di "gatekeeper" di queste piattaforme.

[51] In particolare, durante la conferenza la Vestager ha messo l'accento su come in Europa ci si stia muovendo nella direzione di introdurre forme di regolamentazione ex ante in maniera complementare agli interventi antitrust tradizionali per fronteggiare la tendenza dei mercati digitali alla concentrazione e all'innalzamento di barriere all'entrata.

orizzontali *ex ante* che mettono al centro l'utente, la trasparenza degli algoritmi di mercato e l'uso economico del dato; dall'altra parte, il rafforzamento delle competenze *antitrust*, anche mediante la definizione e imposizione di rimedi strutturali (*e.g.* divieto di esclusive, condivisione dei dati o forme di separazione strutturale). A livello europeo, si propone di considerare come c.d. *gatekeeper*, le società che son presenti in almeno tre Stati membri e che hanno una clientela pari ad almeno il 10% della popolazione europea (circa 45 milioni di persone), o 10 mila imprese. Oltre a questi presupposti, si aggiunge quello secondo cui la società deve avere un *turnover* superiore a 6,5 miliardi di euro, o una capitalizzazione di borsa superiore a 65 miliardi di euro. In caso di violazioni, potranno essere applicate multe pari al 10% del fatturato mondiale. In altri termini, i giganti dell'economia digitale dovranno garantire a società terze l'interoperabilità dei loro servizi, ed assicurare l'accesso ai dati, raccolti in quanto *gatekeeper*.

Secondo una prima analisi, rientrerebbero nella figura di *gatekeeper:* Amazon, Google, Facebook, Samsung ed Alibaba. Queste imprese, in qualità di *gatekeeper*, dovranno rispettare una serie di divieti e obblighi tra i quali: i) il divieto di discriminazione a favore dei propri servizi; ii) l'obbligo di garantire l'interoperabilità con la propria piattaforma ad altre piattaforme concorrenti; e iii) l'obbligo di condividere, nel rispetto delle norme sulla *privacy*, i dati che vengono forniti o generati attraverso le interazioni degli utenti commerciali e dei loro clienti sulla piattaforma dei *gatekeeper*.

2.1.4 Il caso *Facebook* in Germania: una partita ancora aperta

Il caso Facebook in Germania è quello che, tra tutti, presenta maggiori complessità[52].

In Germania, il *Bundeskartellamt* (in seguito, anche, BKartA o autorità tedesca) è intervenuto nel 2016, avviando un procedimento *antitrust* nei confronti di Facebook, per accertare se i termini di servizio, che riducono la protezione della privacy dei propri utenti, possano costituire un abuso di posizione dominante.

Si noti che, al riguardo, nell'ultima sessione del *Competition Committee* dell'OCSE di novembre 2016, l'OCSE ha rilevato il fatto che fra i dati raccolti dalle piattaforme *online* vi siano anche dati personali può rappresentare un elemento rilevante ai fini della analisi di eventuali comportamenti anticoncorrenziali, posti in essere dalle principali piattaforme *online*. Ad esempio, può accadere che,

[52] Per un'analisi diffusa, v., *ex multis*, il *Report* (del George J. Stigler Center for the Study of the Economy and the State e della University of Chicago Booth School of Business) del Commit- tee for the Study of Digital Platforms, Market Structure and Antitrust Subcommitte, pubblicato il 15 maggio 2019. Inoltre, una, sebbene non aggiornata, disamina del caso così come discusso in dottrina cfr. A. GIANNACCARI, *Facebook e l'abuso da sfruttamento al vaglio del Bundesgerichtshof*, in *Mercato concorrenza regole*, 2020, fasc. 2, pp. 403-409; OSTI - PARDOLESI, *L'Antitrust ai tempi di Facebook*, in *Mercato, concorrenza e regole*, 2/2019, p. 195- 218; C. COLANGELO, M. MAGGIOLINO, *Big Data, data protection and antitrust in the wake of the "Bundeskartellamt" case against Facebook (Big Data, protezione dei dati e "antitrust" sulla scia del caso "Bundeskartellamt" contro Facebook)*, in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2017, fasc. 1, pp. 9; A. GIANNACCARI, *Facebook, tra privacy e Antitrust: una storia (non solamente) americana* in *Mercato, concorrenza e regole*, 2/2019,p. 285.

in presenza di effetti di rete collegati alla disponibilità di dati degli utenti, gli operatori possano essere indotti a ridurre i livelli di *privacy* dei singoli utenti, esercitando il proprio potere di mercato. In linea di principio, il deterioramento del livello di *privacy* non è di per sé un aspetto negativo di un mercato, in quanto potrebbe essere correlato ad un aumento nella qualità di un prodotto/servizio offerto. Al tempo stesso, dal punto di vista regolamentare, potrebbe essere opportuno intervenire qualora la riduzione del livello di *privacy* sia contraria all'interesse pubblico.

Adottando tale approccio, le valutazioni preliminari dell'autorità tedesca, pubblicate a dicembre 2017, individuano il danno nella *"perdita del controllo: [i consumatori] non sono più capaci di controllare come i propri dati personali sono usati. Gli utenti di Facebook sono all'oscuro circa quali dati e da quali fonti sono combinati con quelli che Facebook già possiede al fine di sviluppare un dettagliato profilo dell'utente e della sua attività online. In ragione della combinazione dei dati, questi assumono un valore che l'utente non può prevedere. Allo stesso tempo, proprio a causa del potere di mercato di Facebook, gli utenti non hanno altra scelta per evitare tale combinazione. La combinazione da parte di Facebook di tali dati costituisce altresì una lesione del diritto costituzionalmente garantito ci ciascun utente di autodeterminarsi in maniera informata"* [53].

Con decisione del 6 febbraio 2019[54], pubblicata il 7 febbraio 2019[55], Facebook è stato ritenuto dominante nel mercato tedesco dei *social networks*, che comprendeva soltanto la stessa Facebook, a seguito dell'uscita dal mercato di Google+ (che comunque deteneva una quota di mercato prossima al 5%). Le contestazioni avevano ad oggetto la capacità di Facebook di combinare i dati degli utenti, raccolti direttamente in quanto Facebook (c.d."*on-Facebook*"), con quelli acquisiti tramite le altre società del gruppo (*in primis* Instagram e WhatsApp) e quelli relativi alla navigazione su terze parti attraverso il profilo utente Facebook (c.d."*off-Facebook*").

Il caso è stato avviato ai sensi della *Gesetz gegen Wettbewerbsbeschränkungen* (di seguito anche GWB o legge federale sulla concorrenza) e in particolare dell'art. 19 (1) sull'abuso di posizione dominante. Previsione certamente non dissimile dalla (anche se certamente non sovrapponibile alla) lett. a) dell'art. 102 TFUE, che individua un abuso "*nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque*". La giurisprudenza della

[53] Bundeskartellamt, Background information on the Facebook proceeding, 19.12.2017.

[54] Decisione del 6 febbraio 2019, *Facebook Inc., Menlo Parc, U.S.A., Facebook Ireland Ltd., Dublin, Ireland, Facebook Deutschland GmbH/Verbraucherzentrale Bundesverband e.V., Berlin.*

[55] Per una presentazione in inglese del caso da parte della stessa BKartA, si veda: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6.

Corte Federale tedesca (casi *VBL-Gegenwert*[56] e *Pechstein*[57]) afferma che, ai fini della valutazione del carattere abusivo di una condotta ai sensi dell'art. 19 (1) GWB, si può fare riferimento ad altre norme o principi del codice civile (come il principio di buona fede[58]), intesi a proteggere una parte contrattuale che versi in una situazione di squilibrio negoziale (c.d. abuso da sfruttamento da condizioni negoziali). Ciò posto, il BKartA ha ritenuto che il GDPR sulla protezione dei dati potesse essere utilizzato ai fini della valutazione dell'appropriatezza dei termini e delle condizioni di servizio di Facebook relative al trattamento dei dati[59]. In tale contesto, l'autorità tedesca ha osservato che: (i) i dati richiesti da Facebook eccedevano quelli tecnicamente necessari ad assicurare un'ottimale fruizione del servizio; (ii) gli utilizzatori non esprimevano un esplicito consenso, in quanto, sebbene la fruizione del servizio offerto da Facebook richiedesse l'accettazione dei termini e delle condizioni di servizio, gli utenti non erano consapevoli del fatto che i dati acquisiti da Facebook si estendevano ben oltre quelli relativi alla loro attività su Facebook.

Alla luce di tali presupposti, il BKartA ha concluso che il bilanciamento di interessi tra Facebook e i suoi utenti può ritenersi equilibrato soltanto limitatamente ai dati *on-Facebook*. In questo sottoinsieme, lo scambio tra acquisizione dei dati e gratuità del servizio risulta coerente con il modello di *business* di Facebook, prevedibile da parte dell'utente. Viceversa, l'abbinamento di tali dati a quelli *off-Facebook*[60], esubera il modello di *business* di Facebook, costituendo un vantaggio indebito e non conosciuto dai fruitori del servizio.

Nella decisione del BKartA non sono state imposte sanzioni pecuniarie ma, per contro, sono stati imposti rimedi inibitori, che limitano la possibilità di Facebook di raccolta ed elaborazione ai soli dati *on-Facebook*. L'abbinamento con i dati *off-Facebook* potrà essere effettuato esclusivamente previo esplicito consenso da parte dell'utente. Inoltre, Facebook dispone di quattro mesi di tempo per

---

[56] VBL-*Gegenwert II*, 24.1.2017, KZR 47/14, che segue a VBL-*Gegenwert I*, 6.11.2013, KZR 58/11. Nel primo il BGH ravvisava l'abuso nella violazione degli artt. 307 ss. del codice civile germanico, BGB (come modificati attraverso la ricezione della direttiva n. 93/13 in tema di clausole abusive): in particolare quando tale violazione – nella specie, l'imposizione, da parte di un ente pubblico cruciale per i partecipanti al mercato, di condizioni generali che rendevano irragione- volmente più difficile il recesso da contratti di durata – è la manifestazione del superiore potere contrattuale della parte che impone i termini in questione.

[57] *Pechstein/International Skating Union*, 6.16.2016, KZR 6/15. Il caso in questione riguardava la sottoscrizione, da parte di un'atleta, di una clausola arbitrale nella domanda di partecipazione ai campionati del mondo, monopolizzati da un'organizzazione sportiva: abuso, nella specie, negato. Qui, il BGH estendeva tale ragionamento, osservando che nell'applicazione della "clausola generale" dell'art. 19 (1) GWB occorre tener conto anche della violazione, ad opera della controparte contrattuale dotata di forza preponderante, dei diritti costituzionali delle parti.

[58] In particolare, la violazione del principio di buona fede sta nell'imposizione di un obbligo che, in sostanza, non corrisponde ad una controprestazione.

[59] C'è chi sostiene che all'origine dell'iniziativa dell'autorità antitrust tedesca vi fosse una forte convinzione «politica» tesa ad assicurare un intervento incisivo in un'area in cui il quadro regolamentare e la prassi applicativa sembravano molto deboli, a fronte di minacciose e indisturbate manipolazioni di masse ingentissime di dati (ad opera, prevalente, di multinazionali statunitensi). Così OSTI - PARDOLESI, *L'Antitrust ai tempi di Facebook, cit.* p. 202.

[60] Il BKartA ha dunque imposto a Facebook di rinunciare a raccogliere dati relativi agli utenti attraverso i servizi prestati dai siti terzi e da Facebook Business Tools, nonché la loro aggregazione ai dati presenti sulla piattaforma *senza il consenso degli utilizzatori.* Stesso discorso quando i dati vengono raccolti attraverso i *cookies*: si è così imposto a Facebook di modificare anche la sua politica al riguardo.

predisporre un piano di attuazione dei rimedi, che dovranno poi essere introdotti entro un anno dalla decisione.

Dalla giurisprudenza delle Corti europee non sembrerebbe emergere un orientamento equivalente a quello delle Corti Federali tedesche, sull'utilizzabilità di altri principi del codice civile come parametro per l'accertamento dell'appropriatezza di una condotta, per poi dedurne un'illegittimità di natura concorrenziale[61].

Relativamente al contenzioso, a seguito del ricorso presentato da Facebook ex art. 65(3) della Legge sulla concorrenza, con decisione interinale del 26 Agosto 2019[62], l' *Oberlandesgericht Düsseldorf* (di seguito anche OLG o Alta Corte Regionale di *Düsseldorf*) ha sospeso il provvedimento del BKartA affermando che: (i) la decisione è priva di una teoria del danno convincente; (ii) le questioni affrontate dalla decisione attengono alla protezione dei dati personali e non presentano alcun elemento concorrenziale; (iii) non è stato dimostrato alcun nesso causale tra la raccolta di dati da parte di Facebook e i danni alla concorrenza, in nessuno dei mercati individuati (*social network* e *online advertising*).

Volendo ulteriormente sintetizzare il ragionamento seguito dall'OLG, si potrebbe concludere che non sussiste: (1) un abuso da esclusione, in quanto il BKartA non prova gli effetti di deterrenza nei confronti dei concorrenti; (2) un abuso da sfruttamento, in quanto i) il comportamento di Facebook non ha nulla a che fare con la concorrenza; ii) la *policy* di Facebook può essere comune ad imprese completamente prive di posizione dominante; iii) infine, è dubbio che riguardi un caso di sfruttamento, in quanto è evidente che, per la grande maggioranza degli utenti, si tratta di un prezzo risibile da pagare per ottenere un servizio così utile e molto comune.

Successivamente, il 23 giugno 2020, la Corte di giustizia federale[63] (c.d. *Bundesgerichtshof)* ha ribaltato la decisione di primo grado, rigettando il provvedimento cautelare disposto dall'*Oberlandesgericht Düsseldorf* ed affermando che: i) è irrilevante il fatto che i termini e le condizioni del servizio di Facebook siano in linea con la normativa a tutela della *privacy* (GDPR); ii) non ci sono dubbi sul fatto che Facebook abbia una posizione dominante nel mercato dei *social network* in Germania), fondata su *network effects;* da ciò discende una speciale responsabilità; iii) non può essere dubitato che Facebook abbia abusato della sua posizione, privando gli utenti della possibilità di scelta in merito alla raccolta e all'utilizzo dei dati *off-Facebook*; iv) il modello di

[61] Sul punto anche autorevole dottrina come W.P.J. Wils, *The Obligation for the Competition Author- ities of the* EU *Member States to Apply* EU *Antitrust Law and the Facebook Decision of the Bunde- skartellamt*, www.ssrn.com, luglio 2019, a cui avviso «*conduct such as that found in the Facebook Decision of the Bundeskartellamt arguably also falls under Article 102 TFEU. If the applicability of Article 102 TFEU were to be confirmed, it would follow that the Bundeskartellamt has infringed Article 3(1), second sentence, of Regulation 1/2003 by not also applying Article 102 TFEU in its Facebook Decision*».

[62] Oberlandesgericht Düsseldorf 26 agosto 2019, VI-Kart 1/19 (V)

[63] *Bundesgerichtshof, Beschluss vom* 23 Juni 2020, Kvr 69/19, Facebook.

business di Facebook (ossia, l'acquisizione e l'elaborazione dei dati degli utenti), per com'è strutturato, impedisce la concorrenza, incrementando *lock-in effects*, le barriere all'entrata del mercato e la posizione di mercato di Facebook.

La trama argomentativa della Corte di giustizia federale ha preso le mosse proprio dalla definizione del mercato rilevante, e dall'accertamento della dominanza di Facebook. A tal riguardo, la Corte ha fatto affidamento sui consolidati criteri di sostituibilità dei prodotti e servizi dal lato della domanda (quanto a caratteristiche, usi cui sono destinati, e fasce di prezzo) e ciò anche in relazione a servizi erogati in assenza di corresponsione di denaro. In tal senso, si è inteso parimenti valorizzare la prassi applicativa della stessa Commissione europea, che si analizzerà in seguito con riferimento alle concentrazioni Facebook/WhatsApp e Microsoft/LinkedIn, concludendo sia nel senso di ritenere che Facebook non sia sostituibile con piattaforme alternative (i.e. Twitter, YouTube, Snapchat o LinkedIn), ma anche nella prospettiva di considerare i due versanti del mercato (utenti ed inserzionisti pubblicitari) come appartenenti a due segmenti differenti, difficilmente considerabili all'interno di un unico mercato rilevante[64].

Ciò premesso, e come sarà dato osservare, la Corte di giustizia federale ha implicitamente sconfessato larga parte della trama argomentativa sviluppata dal BKartA, ma il giudizio rappresenta una vittoria proprio per il BKartA, posto che la relativa decisione era stata oggetto di un riesame, ancorché in via interinale, oltremodo corrosivo in sede d'appello.

Si tratta di una torsione sostanzialmente completa rispetto alle conclusioni dell'Alta Corte di Düsseldorf, da cui discende l'operatività delle misure rimediali imposte dal BKartA.

Infatti, se l'autorità tedesca aveva sostanzialmente rintracciato l'abuso di posizione dominante, in termini di violazione di disposizioni estranee al diritto della concorrenza - quelle sul trattamento dei dati personali definite nel GDPR - la Corte di giustizia federale riporta il riscontro dell'illecito antitrust in un alveo più tradizionale, almeno per la dottrina e giurisprudenza teutonica.

Viene fatto obbligo a Facebook di porre fine alle pratiche volte alla collazione dei dati degli utenti attraverso fonti differenti, in assenza di un esplicito consenso. Ma la società dovrà altresì modificare i termini e le condizioni sull'uso della piattaforma (in Germania), entro dodici mesi.

Sembra potersi constatare che l'autorità tedesca abbia voluto farsi carico, sulla scia della rivoluzione indotta dalla nota scuola di Chicago, di un'impotenza che il diritto della concorrenza tradizionale dimostra rispetto all'economia digitale, in cui si sono affermati le *multi-sided media platforms* che operano in una dimensione, dove lo SSNIP test (criterio principe sulla sostituibilità dei prodotti per definire il potere di mercato) sembra non essere più attuale, in un'economia caratterizzata da mercati

[64] Così A. GIANNACCARI, *Facebook e l'abuso da sfruttamento al vaglio del Bundesgerichtshof, cit.*, p. 406.

multi versante[65].

Da ultimo, il provvedimento della Corte di giustizia federale rappresenta solamente un pronunciamento in sede cautelare. L'Alta Corte Regionale di Düsseldorf è infatti chiamata ad operare le proprie valutazioni nel procedimento principale. In sostanza, è possibile che la controversia sia destinata a riapprodare alle cure della stessa Corte di giustizia federale, così come, è parimenti probabile, che i giudici di appello optino per il rinvio pregiudiziale dinnanzi alla Corte di giustizia Ue.

Si segnala come le diverse autorità nazionali abbiano reagito alle condotte di Facebook con modalità diverse, ed è quindi interessante vedere come una stessa condotta sia stata affrontata dalle varie autorità. Questo discorso sarà oggetto di disamina più avanti nel terzo capitolo con riferimento alle pratiche commerciali scorrette.

Sul punto, infatti, occorre ricordare che il diritto *antitrust* non si occupa di quanto siano informate le scelte dei consumatori e, dunque, non valuta se l'informazione sia a loro volta corretta, valida o veritiera[66].

Da una parte, il diritto *antitrust* si occupa dell'offerta delle imprese, dall'altra, la *disclosure regulation* e la disciplina a tutela dei consumatori si avvicinano ai mercati dal lato della domanda, garantendo che i consumatori siano in grado di orientare consapevolmente le loro scelte[67]. Anche qui però si rinvia il discorso al capitolo seguente.

2.1.5 L'*enforcement* dell'AGCM in Italia: i casi *Google* e il suo ruolo di apripista in Europa sul caso *Amazon*

L'AGCM è stata l'autorità nazionale che in tema di abuso di posizione dominante è intervenuta per prima nel sanzionare le condotte dei giganti tecnologici. In particolare, si fa riferimento a due recenti casi: quello di Google sul *display advertising,* e quello di Amazon che ha usato a proprio beneficio i dati di fornitori terzi, garantendo una via preferenziale ai suoi servizi.

Con riferimento al primo caso, l'AGCM nell'ottobre 2020 ha aperto un'istruttoria nei confronti di Google per abuso di posizione dominante nel mercato italiano del *display advertising*[68], contestando l'utilizzo discriminatorio dei dati, raccolti attraverso le proprie applicazioni, che impedisce ai

[65] Si veda infatti come ad es. in MAGGIOLINO, *op. cit.*, p. 252 ss. si faccia riferimento ad un nuovo test, il c.d SSNDQ test che valuta più la qualità dei prodotti.

[66] M. MAGGIOLINO, *Big data e diritto Antitrust*, Egea, 2018, 140.

[67] Relativamente alla complementarità tra *disclosure regulation* e diritto antitrust si veda: ROBERT BALDWIN, MARTIN CAVE, MARTIN LODGE, *Understanding Regulation* (2012).

[68] 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.

concorrenti di competere in modo efficace, con forti ricadute anche sui consumatori.

Nell'ambito del *display advertising*, l'incontro fra domanda e offerta degli spazi pubblicitari avviene per mezzo del c.d. *programmatic advertising*, ovvero la compravendita di spazi pubblicitari *online* in tempo reale, tramite piattaforme tecnologiche (*software*) automatizzate che mettono in comunicazione acquirenti e venditori di spazi pubblicitari. Si parla quindi da una parte di *demand side platform* e dall'altra di *supply side platform.* In altri termini, le due piattaforme possono definirsi come "agenti di acquisto" e "agenti di vendita" elettronici, rispettivamente di inserzionisti e operatori che offrono spazi pubblicitari.

Le piattaforme tecnologiche di vendita sono le c.d. *Supply Side Platform* (di seguito "SSP") che sono utilizzate da concessionarie e editori/operatori, e permettono a questi ultimi di procedere alla vendita dei loro spazi pubblicitari, secondo un meccanismo di allocazione automatizzato.

Invece, dal lato della domanda di spazi pubblicitari, gli inserzionisti e le agenzie media si avvalgono delle piattaforme tecnologiche di acquisto di spazi pubblicitari, le c.d. *Demand Side Platform* (DSP), che sono imprese che, fornendo strumenti tecnologici, consentono a *media agency* e inserzionisti di accedere alla contrattazione di spazi pubblicitari in modalità automatizzata.

Ebbene, queste piattaforme sono capaci di ottimizzare il processo di vendita e acquisto di spazi pubblicitari, consentendo di mostrare un contenuto pubblicitario, totalmente personalizzato a un utente nell'esatto momento in cui questo vuole visualizzarlo.

In pratica, ogni volta che un utente clicca su un indirizzo Internet di una pagina con spazi pubblicitari, disponibili nell'*ad exchange* (mercato virtuale, incontro tra DSP e SSP), l'editore proprietario di quella pagina, tramite la SSP, comunica agli inserzionisti o alle *media agency,* che un utente con determinate caratteristiche sta per accedere alla sua pagina web. La SSP mette all'asta lo spazio pubblicitario a tutte le DSP interconnesse, con un processo di negoziazione che dura millesimi di secondo. In particolare, le società *Alphabet Inc., Google LLC e Google Italy S.r.l.* avrebbero violato l'art. 102 del TFUE[69], rifiutandosi di fornire ai concorrenti le chiavi di decriptazione dell'ID Google, ed escludendo i pixel di tracciamento di terze parti.

In altre parole, Google non consente di associare l'attività di un determinato utente in termini di visualizzazione di un determinato messaggio pubblicitario.

La condotta di Google è stata segnalata da *Interactive Advertising Bureau* Italia (IAB) che è un'associazione di categoria di imprese attive nel settore del *digital advertising,* e che rappresenta

[69] L'articolo 102 del TFUE vieta lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una sua parte sostanziale, nella misura in cui ciò possa arrecare un pregiudizio al mercato intraeuropeo. Tra le pratiche che possono costituire un abuso di posizione dominante viene menzionata la limitazione della produzione, degli sbocchi o dello sviluppo tecnico a danno dei consumatori (lettera b), nonché l'applicazione nei rapporti commerciali con i contraenti di condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio concorrenziale (lettera c).

società di comunicazione e pubblicità attive in Italia.

Da come si legge nel provvedimento dell'AGCM, secondo IAB: "*le condotte di Google – facenti parte di un'unica e complessa strategia escludente – si sostanziano in: (i) interruzione, dal 25 maggio 2018, delle chiavi di decriptazione dell'ID utente Google; (ii) interruzione, dal 6 agosto 2015, degli spazi pubblicitari su YouTube (piattaforma di condivisione video di Google) venduti da intermediari terzi; (iii) interruzione, dal 21 maggio 2018, dei dispositivi di tracciamento degli utenti (cookie, pixel di tracciamento) di operatori terzi su YouTube. Le condotte segnalate sarebbero finalizzate a escludere gli altri player dal mercato del display advertising e avrebbero come effetto quello di privare i clienti inserzionisti ed editori della possibilità di scegliere i propri interlocutori commerciali e controparti contrattuali.*[70]"

Pertanto, tale comportamento discriminatorio consisterebbe in una condotta interna-esterna e cioè, da una parte, nel rifiuto di fornire ai concorrenti le chiavi di decriptazione dell'ID Google e, dall'altra, nell'escludere i concorrenti in merito alla possibilità di tracciamento dei pixel, che gli permetterebbero di competere con Google sulla base delle proprie capacità di "targhettizzazione".[71]

Si tratta di condotte discriminatorie poste in essere da un operatore in posizione dominante, che svolge un'attività di intermediazione, e al tempo stesso, è attivo come "utente" in (almeno) uno dei versanti della piattaforma in questione.

Tale provvedimento dell'AGCM sembra in linea con gli ultimi orientamenti della Commissione europea in tema di abuso di posizione dominante di tipo escludente.[72]

Come si legge anche nell'indagine sui *Big Data* pubblicata nel febbraio 2020: "*il rischio paventato da alcuni osservatori è che tali posizioni dominanti possano impedire in futuro l'entrata di nuovi operatori e ridurre gli incentivi all'innovazione e al miglioramento dell'offerta per gli incumbent, con effetti negativi sull'efficienza e il dinamismo delle imprese. Alcuni recenti studi, ad esempio, suggeriscono che, nei paesi OCSE e con particolare riguardo al settore digitale, a fronte di un margine di profitto medio conseguito dalle imprese in crescita, si assiste già ad una riduzione del tasso di entrata medio di nuove imprese nel mercato.*[73]"

---

[70] Cfr. Provvedimento AGCM n. 542 del 20 ottobre 2020, https://www.agcm.it/dotcmsdoc/allegati-news/A542_avvio%20istruttoria.pdf .

[71] La targhettizzazione, o anche *targeting*, è ben radicata nel marketing on-line, dove l'espressione "approccio mirato al target" ricorre frequentemente. Le imprese investono ingenti somme per campagne di marketing con l'obiettivo di promuovere un prodotto il più possibile e aumentare così le vendite. Non sempre l'articolo pubblicizzato è di pari interesse per tutte le persone. Pertanto, ricorrendo al *targeting*, i banner pubblicitari, i video e gli annunci sui motori di ricerca sono visualizzati solo dai potenziali clienti.

La targetizzazione è infatti in grado di individuare il pubblico che potrebbe essere interessato al rispettivo prodotto o servizio tra tutti gli utenti di un sito web. Quanto più precisa è la restrizione del filtro, tanto minore è la dispersione che la campagna registra.

[72] Vedi punti 19 e 30 della *Comunicazione della Commissione — Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti - 2009/C 45/02.*

[73] AGCM, AGCOM, Garante per la protezione dei dati personali, Indagine conoscitiva sui Big Data, p.79.

Esaminando il caso di specie, secondo l'autorità, le condotte di Google sembrano avere un significativo impatto sulla concorrenza, nei diversi mercati della filiera del *digital advertising,* con ampie ricadute sui *competitor* e sui consumatori. Infatti, l'assenza di concorrenza nell'intermediazione del *digital advertising,* potrebbe ridurre le risorse destinate ai produttori di siti *web* e agli editori, impoverendo così la qualità dei contenuti diretti ai clienti finali.

Si rileva al riguardo che, sebbene l'autorità italiana abbia volutamente evitato di parlare di "risorsa essenziale"[74] – per evitare di avere l'onere di provare l'essenzialità della risorsa nella sede giudiziaria – il caso in questione ricorda, per certi versi, un tipico esempio di dominanza nel diritto *antitrust* tradizionale, ovvero quello dell'impresa *leader* che controlla una *essential facility* o infrastruttura essenziale.[75]

In quest'ambito, l'art. 102 TFUE trova applicazione nei casi in cui il detentore di un*'essential facility* opponga un rifiuto a contrarre ad un'impresa concorrente, con cui compete in un mercato a valle[76]. Quindi, anche nel caso in cui un'*essential facility* sia costituita da dati, un ipotetico rifiuto a concedere a terzi l'accesso a tali dati, ha una rilevanza *antitrust,* nella misura in cui è idoneo a ridurre la concorrenza in un mercato complementare.[77]

Ai fini dell'applicazione dell'art. 102 TFUE, la finalità alla base di una richiesta di accesso ai dati,

[74] Prima del provvedimento dell'AGCM, l'altra idea proposta in dottrina per aggirare la prova della risorsa essenziale è stata quella dell'abuso di dipendenza economica. Cfr. F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, I, p. 1070. Si evidenziava come: "*a differenza dell'abuso di posizione dominante — in cui si dovrebbe fornire la prova sia dell'insostituibilità della risorsa essenziale sia del rapporto non direttamente concorrenziale tra le imprese — nell'abuso di dipendenza economica il rifiuto di vendere, o dare in licenza la risorsa posseduta, potrà considerarsi abusivo ove si dimostri che non vi sia una reale possibilità sul mercato di reperire alternative soddisfacenti. Dunque, se il titolare dei big data a cui venga richiesto il rilascio di una licenza pur non essendo l'unico a disporre di quei dati abbia i data-set notoriamente più vasti, aggiornati e completi presenti sul mercato, questo potrà essere sufficiente a ritenere insoddisfacenti le altre alternative reperibili sul mercato*".

[75] Alcuni esempi sono le telecomunicazioni fisse, i servizi energetici quali elettricità e gas o il trasporto ferroviario. Infatti, non a caso queste tipologie di settori sono spesso soggetti ad una regolamentazione pro-concorrenziale e ad un controllo da parte di Autorità indipendenti di settore.

[76] Su un eventuale obbligo dei *BigTech* di fornire le informazioni digitali cfr. B. MÄIHÄNIEMI, *Competition Law and Big Data: Imposing Access to Information in Digital Markets*, Elgar Publishing, 2020. Come è noto, un rifiuto a contrarre costituisce una violazione della normativa antitrust se ricorrono le seguenti condizioni cumulative: i) il rifiuto si riferisce ad un prodotto o ad un servizio obiettivamente necessario per poter competere in maniera effettiva su un mercato a valle, ii) è probabile che il rifiuto determini l'eliminazione di una concorrenza effettiva sul mercato a valle, e iii) è probabile che il rifiuto determini un danno per i consumatori. Quando il rifiuto a contrarre concerne l'esercizio di diritti di proprietà intellettuale, la giurisprudenza euro-unitaria ha aggiunto la condizione ulteriore che il rifiuto si debba riferire all'offerta di un prodotto o servizio nuovo per il quale sussiste una potenziale domanda. Così la Corte di Giustizia dell'Unione Europea, C-241/91 P e C-242/91, *Radio Telefis Eireann (RTE) e Independent Television Publications (ITP)/ Commission (Magill); C-418/01, IMS Health/NDC Health; T-201/04, Microsoft/Commission.*

[77] Ai fini dell'analisi dell'indispensabilità tipica della dottrina antitrust dell'*essential facility* nel settore dei Big Data, almeno tre aspetti specifici appaiono potenzialmente rilevanti: i) la natura personale o meno dei dati oggetto della richiesta di accesso; ii) se i dati in questione siano stati: a) volontariamente forniti dal soggetto a cui si riferiscono; b) rilevati dall'operatore dominante; c) ricavati tramite attività di analisi dei dati svolte dall'operatore in questione (*analytics*); iii) il grado di aggregazione dei dati oggetto della richiesta di accesso potendo distinguere, dunque, tra dati a livello individuale, aggregati o *bundled.*

detenuti da un'impresa dominante, assume una particolare importanza[78].

Pertanto, i *Big Data Analytics*[79] possono costituire, solo in circostanze eccezionali, una risorsa "essenziale" per operare in un mercato ed essere soggetti ad un obbligo a contrarre, ai sensi della normativa a tutela della concorrenza[80]. La nozione legale di *essential facility* va oltre il mero riconoscimento della rilevanza dei *Big Data* nel processo competitivo. Infatti, anche quando una risorsa è un'importante fonte di vantaggio competitivo, e costituisce una barriera all'entrata, la normativa *antitrust* non impone necessariamente alle imprese di condividere tale risorsa con i propri concorrenti. Altrimenti, ciò si tradurrebbe in un forte disincentivo per tali imprese ad investire nei *Big Data,* a detrimento dei consumatori che non beneficerebbero più dei servizi innovativi connessi. Pertanto, per poter ricadere in un rifiuto di cui all'art. 102 TFUE, la società: i) deve essere in posizione dominante; ii) deve far riferimento a dati oggettivamente necessari per poter competere nel mercato a valle; e iii) deve poter condurre all'eliminazione di una concorrenza effettiva nel mercato a valle e a danno del consumatore finale.[81]

Inoltre, non è tanto la raccolta dei dati in sé a rappresentare la vera risorsa scarsa alla base di rilevanti posizioni dominanti, quanto piuttosto la capacità di estrarre informazioni utili da grandi volumi e varietà dei dati.[82] In quest'ambito, bisognerebbe *a latere* considerare anche la relazione tra l'eventuale obbligo dei giganti digitali di fornire i dati e il GDPR, almeno sotto due aspetti: a) con riferimento al diritto alla portabilità dei dati personali, analizzato nel primo capitolo, che consente ad un'impresa di acquisire i dati direttamente dai soggetti a cui fanno riferimento, senza farseli fornire dall'impresa in posizione dominante[83]; b) con riferimento alla possibile tensione tra l'accesso ai dati

---

[78] Sul rapporto tra finalità del trattamento dei dati e diritto antitrust cfr. G. D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra "data protection" e antitrust. Il caso dell'uso secondario di "big data"" (The principle of purpose limitation between data protection and antitrust, regarding to the so called "secondary use of big data")* in *Il Diritto dell'informazione e dell'informatica*, 2018, fasc. 6, pp. 943-987.

[79] Con la locuzione "Big Data" si fa riferimento, in prima approssimazione (nell'assenza di definizioni normativamente vincolanti), alla raccolta, all'analisi e all'accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale (nell'accezione fornita dall'art. 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisicheconriguardoaltrattamentodeidatipersonali,nonchéallaliberacircolazioneditalidatie che abroga la direttiva 95/46/CE, di seguito anche "RGPD"), in ipotesi provenienti anche da fonti diverse. La natura massiva delle operazioni di trattamento reca con sé la necessità che tali insiemi di informazioni (sia memorizzate, sia in *streaming*) siano oggetto trattamento automatizzato, mediante algoritmi e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e/o modelli. Cfr. Provvedimento AGCM n. 28051 del 20 dicembre 2019.

[80] G. PITRUZZELLA, *Big Data and Antitrust Enforcement*, in *Rivista Italiana di Antitrust*, n.1/2017, p. 79-81.

[81] Cfr. Communication from the Commission: Guidance on its enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45, 24.2.2009 and the case law in Oscar Bronner (C-7/97, judgement of 26 November 1998), IMS Health (C- 418/01, judgement of 29 April 2004) and Microsoft (T-201/94, judgement of 17 September 2007).

[82] OCSE (2016), *"Big data: bringing competition policy to the digital era - Background note by the Secretariat",* https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf, p. 22.

[83] Con riferimento al rapporto tra diritto alla portabilità e diritto antitrust cfr. M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 2018, fasc. 2, pp. 223-245; S. FAMILIARI, *Il diritto alla portabilità dei dati: origine e prospettive per il futuro (The rights to data portability: origin and perspectives for the*

da una parte, e il diritto alla *privacy* e alla protezione dei dati dall'altra[84].

Anche in passato le Corti UE e la Commissione europea non hanno considerato tali dati come risorse essenziali in termini generici, ma solo con riferimento alla creazione di alcune innovazioni specifiche.[85]

Inoltre, la risorsa è essenziale quando servirebbe unicamente ad offrire un prodotto o un servizio specifico e, questo nuovo requisito del prodotto è diretto a garantire la caratteristica innovativa del bene o servizio, così da creare un equilibrio tra gli interessi privati alla tutela del diritto di proprietà intellettuale e l'interesse generale per la protezione della concorrenza.

Fatta questa breve ma dovuta digressione, la disponibilità dei *Big Data* è essenziale quando da essi dipendono caratteristiche fondamentali del servizio reso, in particolare in termini di innovazione e/o di personalizzazione, come rilevato nella recente Indagine conoscitiva.

È evidente, infatti, che la caratteristica distintiva della pubblicità *online,* risiede proprio nella capacità di utilizzare le informazioni raccolte sui singoli utenti, per consentire agli inserzionisti pubblicitari di raggiungere *target* specifici di consumatori, indirizzando loro messaggi mirati, con crescenti livelli di personalizzazione (e di misurare in modo più preciso l'efficacia della campagna pubblicitaria).

Inoltre, al fine di valutare un'ipotesi di abuso di posizione dominante, occorre definire anche l'ambito merceologico e geografico nel quale si svolge la concorrenza tra le imprese (mercati rilevanti)[86], il potere di mercato detenuto dalle imprese (posizione dominante[87]) e la condotta suscettibile di integrare la fattispecie anticoncorrenziale.

Con riferimento al caso in esame, ove vengono in rilievo mercati digitali, la principale leva concorrenziale è rappresentata dalla fruibilità di un numero elevato di dati e dalla loro rilevanza.

La disponibilità dei *Big Data* è però solo una delle caratteristiche che contribuiscono cumulativamente all'elevato grado di concentrazione e all'esistenza di barriere all'entrata nei mercati

---

future), in *Ciberspazio e diritto*, 2016, fasc. 3, pp. 403-434; J. MOSCIANESE - F. DI BENEDETTO, *Privacy, portability and interoperability regarding data produced by the consumer. The role of competition law and market regulation*, in E.A. RAFFAELLI, *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019.; WEBER, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, in *Concorrenza e Mercato*, 2016, 23, 59, p.67 ss.

[84] Tale tensione, come abbiamo già visto nel primo capitolo può essere risolta attraverso tecniche di anonimizzazione dei dati o ai sensi dell'art. 6 GDPR.

[85] In merito al dibattito europeo corrente cfr., Joseph Drexl, Reto M. Hilty, Luc Desaunettes, Franziska Greiner et al., Data ownership and Access to Data (2016), https://ssrn.com/abstract=2833165

[86] Si segnala inoltre che in dottrina c'è chi aggiunge alle tradizionali due categorie del mercato merceologico e di quello geografico, anche il criterio dell'orizzonte temporale. Cfr. BAGNOLI, *op.cit.*, 81. Tuttavia, in senso critico, F. VESSIA, *op.cit.* 1064. che osserva come:" *l'evanescenza del criterio temporale e la difficoltà di stima e valutazione dello stesso suggeriscono di escluderne la natura di terza dimensione (intesa come variabile) all'interno della nozione di mercato*".

[87] Ai fini dell'applicazione dell'articolo 102 del TFUE, la posizione dominante consiste in una situazione di potere economico grazie alla quale l'impresa che la detiene è in grado di ostacolare il persistere di una concorrenza effettiva nei mercati rilevanti e di agire in maniera significativamente indipendente rispetto ai suoi concorrenti, ai suoi clienti e, in ultima analisi, ai consumatori. Si veda Comunicazione della Commissione "*Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti*" (2009/C 45/02).

digitali. Infatti, altri fattori (oltre agli investimenti per sviluppare le capacità di analisi ed elaborazione dei dati), come le economie di scala e di scopo e le esternalità di rete, continuano ad avere un ruolo importante nello spiegare il potere di mercato. Si tratta di aspetti che, pur non essendo nuovi nell'ambito dell'analisi *antitrust*, acquisiscono un particolare rilievo nei mercati digitali, per il condizionamento significativo che il loro effetto cumulato è in grado di esercitare sulle dinamiche concorrenziali.

Anche l'integrazione verticale e conglomerale che caratterizza i principali operatori digitali come Google è stata un elemento di particolare rilievo nella valutazione del potere che tali operatori detengono nei singoli mercati rilevanti in cui sono attivi, nella misura in cui amplifica la loro capacità di acquisire, elaborare e sfruttare i dati nella fornitura dei servizi a consumatori e imprese.

In tale prospettiva, l'AGCM ha tenuto conto anche di altri indicatori, a partire innanzitutto dall'ampiezza della gamma dei servizi offerti ai consumatori (e alle imprese), e del correlato uso delle piattaforme abilitanti alla raccolta di tali dati.

La condotta di Google, a dire dell'Autorità, appare essere contraria alle regole poste a tutela della concorrenza basate sul merito, e scoraggerebbe l'innovazione tecnologica per lo sviluppo di tecnologie pubblicitarie meno invasive per i consumatori.

In particolare, sembra che Google, soggetto verticalmente integrato e presente nei diversi mercati che compongono la filiera della pubblicità *online*, abbia posto in essere condotte commerciali suscettibili di ostacolare i propri concorrenti non integrati e di mantenere e rafforzare ulteriormente il proprio potere di mercato nel *display advertising*, oltre che nei singoli mercati in cui esso va segmentato, in violazione dell'articolo 102 del TFUE. Le condotte dell'impresa, potendo ostacolare significativamente l'ingresso e l'operatività di concorrenti attuali e potenziali, anche esteri, sul mercato nazionale, appaiono suscettibili di alterare il commercio tra Stati membri.

Da ultimo, a maggio 2021, Google è stata sanzionata dall'AGCM per oltre 100 milioni di Euro per non aver consentito l'interoperabilità dell'app JuicePass[88] di Enel X con Android Auto con il fine di favorire la propria app Google Maps e quindi in violazione dell'art. 102 del TFUE[89].

In particolare, Google, rifiutando a Enel X Italia di rendere disponibile JuicePass su Android Auto, avrebbe ingiustamente limitato le possibilità per gli utenti di utilizzare la app di Enel X Italia quando sono alla guida di un veicolo elettrico e hanno bisogno di effettuare la ricarica. In tal modo Google, secondo l'Autorità, avrebbe favorito la propria app Google Maps, che può essere utilizzata su Android

[88] Juice Pass è una specifica funzionalità di Android che consente di utilizzare le app quando l'utente è alla guida nel rispetto dei requisiti di sicurezza e di riduzione della distrazione. JuicePass permette una vasta gamma di servizi funzionali alla ricarica dei veicoli elettrici, che vanno dalla ricerca di una colonnina di ricarica alla gestione della sessione ricarica passando per la prenotazione di una colonnina; quest'ultima funzione garantisce l'effettiva disponibilità dell'infrastruttura una volta che l'utente l'abbia raggiunta.

[89] Cfr. Provvedimento AGCM n. 529 del 13 maggio 2021.

Auto e consente servizi funzionali alla ricarica dei veicoli elettrici, attualmente limitati alla ricerca di colonnine di ricarica e alla navigazione ma che in futuro potrebbero comprendere altre funzionalità, per esempio la prenotazione e il pagamento.

Secondo l'Autorità, infatti, il perdurare di questa condotta da parte di Google potrebbe, *inter alia*, compromettere definitivamente la possibilità per Enel X Italia di costruire una solida base utenti, in una fase di crescita significativa delle vendite di veicoli elettrici. Inoltre, la app JuicePass potrebbe uscire dal novero delle applicazioni utilizzate dagli utenti causando una riduzione significativa delle possibilità di scelta dei consumatori e un ostacolo al progresso tecnologico.

L'AGCM ha quindi imposto a Google di rendere disponibile l'app JuicePass di Enel X su Android Auto che consente di usufruire di servizi connessi alla ricarica di veicoli elettrici.

Con riferimento invece al secondo caso sopra segnalato, l'AGCM nel 2019 ha aperto un'istruttoria contro Amazon per una condotta identica a quella precedentemente vista, e che ha impegnato la Commissione europea nell'ottobre 2020[90]. Tale similitudine è anche stata riconosciuta dalla stessa Commissione che, per una delle due condotte investigate, ha aperto la procedura in tutti i paesi dell'area economica europea tranne l'Italia, per la quale l'AGCM stava già investigando.

Amazon, infatti, incentivava questi terzi rivenditori a usufruire del suo servizio di logistica, in cambio di particolari benefici come quello di poter apparire nei primi risultati di ricerca del *BuyBox*.

Il modello adottato da Amazon era infatti di tipo ibrido o duale (al tempo stesso gestore del *marketplace* e *seller* su di esso). Pertanto, per evitare ulteriori ripetizioni si rinvia al caso così come discusso nel paragrafo relativo all'Unione europea.

2.1.6 Rilievi conclusivi in materia di abuso di posizione dominante

Come si è visto, la crescente interdipendenza dei mercati e dei sistemi economici fa sì che le questioni sollevate dall'economia dei dati assumano spesso carattere sovra-nazionale.

Dall'analisi in materia di abuso di posizione dominante, è emerso come il legislatore e le diverse autorità di concorrenza si stiano adoperando, sia dal punto di vista regolatorio, sia dal punto di vista di ampliamento di organico e di strumentazione tecnologica, per poter fronteggiare le nuove sfide dell'economia digitale e dei *Big Data*.

Sul fronte più propriamente organizzativo, dalla sessione plenaria del gruppo di lavoro sull'efficienza delle autorità di concorrenza (*Agency Effectiveness Working Group* o AEWG[91]), è emerso che molte autorità hanno rafforzato il proprio organico per includere nuove figure professionali, creando in

[90] Per il caso italiano cfr. Provvedimento AGCM n. 528 del 10 aprile 2019.

[91] Si ricorda che tutte le sessioni della conferenza ICN sono state registrate e sono accessibili al seguente link: https://icn-2020.videoshowcase.net/

alcuni casi una nuova unità, o riorganizzando quelle esistenti. Diverse le figure professionali prese in considerazione: esperti di *Big Data* e algoritmi per il *data mining* o *market intelligence* (come nel caso del progetto "*Brain*" dell'autorità brasiliana focalizzato sull'analisi di cartelli nelle gare pubbliche[92]), investigatori e informatici forensi per le attività ispettive (come nel caso della Korea del Sud), ingegneri di dati per sviluppare tecniche di analisi di migliaia di documenti e file, quali il *predictive coding* (come nel caso della autorità di concorrenza inglese che ha utilizzato tali tecniche per esaminare le migliaia di segnalazioni di consumatori a seguito dell'emergenza Covid-19).

Dal punto di vista dell'*enforcement*, gli ultimi anni sono stati densi di interventi delle autorità *antitrust*: a livello nazionale (e.g. caso Facebook in Germania e Casi Google e Amazon in Italia), a livello europeo (e.g. caso Amazon) e nel panorama internazionale (e.g. Cina e Stati Uniti). Pertanto, in questo scenario nuovo ed evolutivo, un coordinamento fra le autorità della concorrenza non è solo auspicabile, ma necessario.

A tal proposito, a livello europeo, l'AGCM ha aderito alla Rete Europea della Concorrenza (*European Competition Network* - ECN), alla quale partecipano la Commissione europea e le autorità *antitrust*, istituite in ogni Stato Membro dell'Unione Europea, competenti ad applicare le regole di concorrenza stabilite dal TFUE. In particolare, nell'ambito dell'ECN, è stato costituito un gruppo di lavoro, denominato "ECN *Digital Markets*", in cui le Autorità europee espongono le attività in corso sull'applicazione delle regole di concorrenza relative ad operatori digitali. La creazione di tale gruppo di lavoro è volta, da una parte, a favorire la cooperazione tra le autorità degli Stati Membri, dall'altra, a promuovere la corretta allocazione di procedimenti istruttori riguardanti l'economia digitale. Inoltre, in ragione della rapida evoluzione dei mercati digitali, è stata emanata la Direttiva UE 2019/1 (anche denominata ECN+) che conferisce alle autorità garanti della concorrenza degli Stati Membri poteri di applicazione più efficaci. Il dialogo transfrontaliero europeo non è, dunque, soltanto legato a temi di concorrenza, ma vi è anche un coordinamento interdisciplinare.

Con riferimento alle proposte regolamentari, invece, non sembra esserci omogeneità a livello globale. Ad esempio, da una parte, l'Europa, con le proposte contenute nel *Digital Markets Act* pubblicate a dicembre 2020, sta andando verso una regolazione *ex ante*, mentre gli Stati Uniti, con i risultati dell'investigazione del Congresso americano, pubblicati nell'ottobre 2020, sono ancora critici verso questo tipo di soluzione.

In particolare, come noto, l'Europa procederà verso una regolazione *ex ante* attraverso tre strumenti tra loro complementari: i) usare meglio i poteri *antitrust* attualmente a disposizione, come le misure cautelari, che la Commissione ha di recente applicato nel caso *Broadcom*; ii) pensare a nuovi

[92] Per maggiori informazioni sul progetto Brain, cfr. contributo dell'autorità brasiliana alla tavola rotonda OCSE 2018, disponibile al link: https://one.oecd.org/document/DAF/COMP/GF/WD(2018)21/en/pdf.

strumenti come, ad esempio, avviene nel Regno Unito, che risolvano le criticità concorrenziali che sono generate non da una condotta specifica, ma riconducili ad assetti di mercato quali effetti di rete e economia di scala; iii) affrontare con una regolazione *ex ante*, le criticità poste dalle piattaforme con significativo potere di mercato (c.d. operatori *gate-keeper*), che approfittano della loro posizione dominante per precludere l'accesso in un altro mercato ai loro concorrenti (come nel caso *Google Shopping* della Commissione), o per imporre agli stessi clausole contrattuali non eque.

Con riferimento agli Stati Uniti, invece, tutto dipenderà anche da come la nuova amministrazione americana, da poco insediatasi, intenderà contrastare questa tipologia di condotte perpetrate dai giganti tecnologici, spesso americani.

In Italia, anche l'AGCM intende prestare una particolare attenzione alle condotte delle piattaforme digitali che possono potenzialmente determinare effetti restrittivi della concorrenza, come dimostrano le istruttorie *antitrust* recentemente avviate.

In questa prospettiva, inoltre, per perseguire l'obiettivo di tutela del benessere del consumatore, diventa opportuno non confinare l'analisi ai tradizionali parametri legati a prezzi e quantità, ma, con l'ausilio degli strumenti propri del diritto *antitrust*, estenderla anche alla qualità, all'innovazione e all'equità.

Un'efficace politica pubblica per i *Big Data* e l'economia digitale richiede non solo l'*enforcement*, ma anche un'adeguata attività di *advocacy*, di cui l'iniziativa congiunta dell'Indagine Conoscitiva sui *Big Data* è testimonianza.

Appaiono infine necessarie, quantomeno con riferimento alle piattaforme digitali globali, misure volte ad incrementare la trasparenza dell'utente circa la natura della propria profilazione, nonché meccanismi di *opt-in* circa il grado di profilazione prescelto, e ciò anche ai fini della tutela del pluralismo *on-line*, in relazione alla selezione dei contenuti profilati.

Il punto di frontiera, forse il più innovativo, riguarda la centralità dell'algoritmo e dello spazio informativo in cui il consumatore esprime la sua doppia libertà: nella scelta dei contenuti e nel grado di esposizione dei propri dati da una parte, e nella esposizione "passiva" operata dall'algoritmo dall'altra.

Di certo, l'Europa si è candidata al ruolo di *standard setting* a livello globale, attraverso processi decisionali aperti alla consultazione con tutte le parti, un'attenta valutazione degli impatti regolatori e mediante un nuovo disegno istituzionale per la *governance* dell'ecosistema digitale.

2.2 Le Concentrazioni e le "*Killer Acquisition*"

La crescente rilevanza assunta dai *Big Data* in alcuni settori suggerisce di guardare alle acquisizioni di natura conglomerale con un'attenzione maggiore di quella che tradizionalmente era stata loro

riservata.

La disponibilità di dati e la capacità di analizzarli può infatti consentire il rafforzamento del potere di mercato, anche in mercati apparentemente lontani tra loro.

Come accade in diversi settori, le acquisizioni giocano un grande ruolo nel dare forma alla struttura dei mercati digitali.

Negli ultimi anni, le trasformazioni digitali in ambito di tecnologie di *Big Data Analytics*, *Cloud*, *mobile*, e di *social networks* hanno riguardato acquisizioni di grande valore[93].

Per tali motivi, il controllo sulle concentrazioni è l'area del diritto *antitrust* che ha avuto maggiore testimonianza dello sviluppo delle relazioni: da una parte, tra *Big Data* e potere di mercato; dall'altra, tra teoria del danno e raccolta di una grande mole di dati.

Nell'area delle concentrazioni, c'è una stretta connessione con il diritto alla protezione dei dati personali. In particolare, il livello di protezione dei dati personali offerto dai vari operatori tecnologici può effettivamente rappresentare un importante parametro, slegato dalle dinamiche di prezzo dei prodotti e servizi. In altre parole, accanto al prezzo, che può anche essere nullo, assumono importanza anche il grado di innovazione e il livello di qualità dei prodotti/servizi offerti, anche con riguardo al livello di tutela dei dati offerto.

Con riferimento alle analisi delle concentrazioni, dunque, occorre garantire che l'analisi degli effetti delle operazioni sia adeguata a cogliere le peculiarità dei mercati *zero-price*, in cui assumono importanza centrale altre dimensioni del confronto competitivo quali: il grado di innovazione, il livello di qualità dei servizi e il livello della protezione dei dati degli utenti.[94]

Approfondire l'impatto dell'innovazione e della qualità sulla concorrenza, oltre agli effetti sui prezzi, rappresenta una sfida importante per l'analisi delle concentrazioni, e ciò anche grazie alla relazione complessa tra pressione concorrenziale e qualità. Pertanto, introdurre l'analisi di aspetti diversi dal prezzo monetario all'interno della valutazione degli effetti delle operazioni di concentrazione, costituisce una sfida da affrontare.

Con riguardo all'innovazione, ad esempio, l'estesa letteratura economica evidenzia come il rapporto con la concorrenza dipenda da una varietà di aspetti particolarmente complessi a livello analitico[95], anche a causa di mercati caratterizzati da un notevole dinamismo.

---

[93] Vedi ad esempio: *Google/Doubleclick*, Commission Decision of 11 March 2008, Case No. COMP/M.4731; *Microsoft/Yahoo!*, Commission Decision of 18 February 2010, Case No. COMP/M.5727; *Intel/Mcafee*, Commission Decision of 26 January 2011, Case No. COMP/M.5984*; Facebook/Whatsapp*, Commission Decision of 3 October 2014, Case No. COMP/M.7217; *Microsoft/Skype*, Commission Decision of 7 October 2011, Case No. COMP/M. 6281.

[94] Cfr. OCSE (2018), *Quality Considerations in Digital-Zero Price Markets, Background note by the Secretariat*, Parigi, 28 novembre.

[95] Ad esempio, occorre considerare il tipo di attività innovativa svolta dalle parti, la struttura dei mercati del prodotto connessi a tale attività innovativa, le caratteristiche della concorrenza di natura dinamica, e la capacità delle imprese di appropriarsi dei benefici dell'innovazione.

È possibile che un'operazione di concentrazione possa incrementare la capacità innovativa di un'impresa, ad esempio ingrandendo quest'ultima e combinando attività complementari, anche in rapporto ad una riduzione degli incentivi derivanti dall'eventuale perdita di una pressione competitiva.

Dato che il livello di *privacy* offerto da una piattaforma è uno dei parametri che indirizzano la scelta degli utenti - e le imprese sono in concorrenza anche su questo - la fusione tra due imprese può avere l'effetto di ridurre il livello di protezione dei dati e, quindi, della qualità del servizio offerto agli utenti [96]. Infatti, anche la qualità può rappresentare un elemento rilevante del benessere del consumatore, al pari del prezzo, e un fattore fondamentale per la competitività delle imprese, soprattutto nei mercati *zero-price* come quelli *data-driven* [97]. Tuttavia, alcune operazioni di concentrazione possono portare ad una riduzione della qualità al pari di un incremento dei prezzi, sebbene in un contesto in cui assume particolare rilievo il fenomeno della differenziazione strategica del prodotto[98].

Pertanto, da una parte, ci si interroga sull'adeguatezza dell'attuale sistema di controllo delle concentrazioni, senza temere di mettere in discussione i tradizionali punti fermi del diritto *antitrust*, dall'altra, le dimensioni sempre più sovra-nazionali dell'economia richiedono un ulteriore impulso al processo di convergenza dei diritti nazionali con il diritto dell'UE e, allargando lo sguardo oltreoceano, con il diritto statunitense.

Consentire un controllo delle concentrazioni efficace e rigoroso nei mercati digitali costituisce un obiettivo di *policy* che deve essere ampiamente condiviso, sia a livello nazionale, che a livello internazionale. In particolare, il recente dibattito internazionale sull'adeguatezza di un controllo preventivo delle operazioni di concentrazione, il cui ambito è definito esclusivamente o quasi, da un sistema di notifica basato su soglie di fatturato e sulla opportunità di colmare eventuali *gap*, ha portato Germania ed Austria a introdurre criteri di notifica basati sul valore della transazione, e il requisito che l'impresa oggetto di acquisizione sia attiva in maniera considerevole in tali Paesi.

Più in generale, in un'economia caratterizzata dalla crescente importanza dei *Big Data,* occorre forse ripensare a diversi istituti del diritto *antitrust* e meglio adeguarli alla realtà che cambia.

Il fatto che il controllo sulle concentrazioni sia basato su soglie di fatturato, non consente alle autorità

[96] Cfr. nota n. 55

[97] Con particolare riguardo ai mercati *data-driven*, la protezione dei dati individuali, la trasparenza e le informazioni necessarie per una scelta consapevole del consumatore possono rappresentare fattori qualitativi rilevanti per il confronto concorrenziale tra piattaforme digitali, soprattutto in mercati caratterizzati da prezzi nulli. I consumatori possono, infatti, preferire soluzioni che consentano di fornire la quantità minore di dati possibile o di mantenere il maggior controllo possibile sull'utilizzo dei dati personali forniti.

[98] Cfr. G. FEDERICO et al. (2017), "*A simple model of mergers and innovation", Economic Letters*, Vol. 157; E. ARGENTESI, et al. (2016), The effect of retail mergers on prices and variety: an ex-post evaluation, DICE Discussion Paper, 225.

antitrust di scrutinare le acquisizioni dove i *Big Data* giocano un ruolo cruciale.

In alcuni casi, la creazione o il rafforzamento di potere di mercato in mercati *data-driven* derivano da fenomeni di crescita esterna. Si tratta di operazioni che possono sfuggire al controllo delle concentrazioni, previsto dalle norme a tutela della concorrenza, e che riguardano principalmente acquisizioni da parte di operatori dominanti di *start-up* potenzialmente *disruptive* (le "*killer acquisitions*"), soprattutto quando oggetto dell'acquisizione sono i dati e la capacità di analizzarli.

Dal 1998 ad oggi, Amazon, Facebook, Apple e Google hanno tutte insieme acquisito più di 500 società emergenti. [99] Per tali ragioni, l'area delle concentrazioni è quella dove le autorità potranno intervenire maggiormente nei mercati digitali.

Inoltre, la combinazione dei dati dopo la fusione tra due società, può avere un impatto sul potere di mercato della società risultante dalla operazione di concentrazione, sulle barriere all'entrata e sull'espansione nel mercato dei concorrenti attuali o potenziali.

Non si ha in questa sede la pretesa di dare risposte definitive a questi interrogativi, ma si ha piuttosto l'intenzione di proseguire una riflessione già aperta e attualmente in corso.

Prima di provare a tracciare alcuni rilievi conclusivi, come si è fatto per l'abuso di posizione dominante, sarà necessario analizzare i casi più importanti di cui si è parlato nei vari paesi. Come segue.

2.2.1 Stati Uniti

La disciplina americana in merito alle concentrazioni è la c.d. *U.S. Merger Policy*, la quale viene introdotta dalle c.d. *Horizontal Merger Guidelines*, emanate il 19 Agosto 2010 dal DOJ congiuntamente con la FTC.[100] Inoltre, il 30 giugno 2020 sono entrate in vigore anche le *Vertical Merger Guidelines*[101].

La FTC è incaricata per legge di svolgere la sua attività di *enforcement* su due aree: *antitrust* e tutela dei consumatori. I doveri della FTC in materia di concentrazioni sono messi in pratica dal *Bureau of Competition*, la cui autorità deriva dal *Clayton Act*, che vieta "*corporate acquisitions that may tend to substantially to lessen competition*" [102].

La Section 7 del Clayton Act prevede che: "*No person engaged in commerce or in any activity affecting commerce shall acquire, directly or indirectly, the whole or any part of the stock or other*

[99] Cfr. U.S. House of Representatives - The House Judiciary Committee's Antitrust Subcommittee, *Investigation of Competition in the Digital Marketplace, Washington, 6 ottobre 2020, p. 406.*

[100] https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

[101] https://www.ftc.gov/system/files/documents/reports/us-department-justice-federal-trade-commission-vertical-merger-guidelines/vertical_merger_guidelines_6-30-20.pdf.

[102] FTC Office of the General Counsel – Cfr. http://www.ftc.gov/ogc/brfovrvw.shtm, (last visited Nov. 28, 2007). Vedi Clayton Act, 15 U.S.C. § 18 (2007).

share capital and no person subject to the jurisdiction of the Federal Trade Commission shall acquire the whole or any part of the assets of another person engaged also in commerce or in any activity affecting commerce, where in any line of commerce or in any activity affecting commerce in any section of the country, the effect of such acquisition may be substantially to lessen competition, or to tend to create a monopoly."

Mentre prima del 1976 molti casi erano contestati con riferimento alla Section 7, dopo il 1976 il *Hart-Scott-Rodino Antitrust Improvements Act of 1976* ha segnato il passaggio delle indagini, prima condotte dalle corti distrettuali, in mano all'agenzia della FTC. Inoltre, il § 5 del FTC Act vieta "*unfair methods of competition*" che racchiude tutte le condotte vietate dal *Sherman Antitrust Act*[103]. Ebbene, uno dei doveri più importanti della FTC è proprio quello relativo all'approvazione delle fusioni, ed esiste grazie al *Hart-Scott-Rodino Antitrust Improvements Act of 1976.*

Tale atto richiede la notifica delle concentrazioni di una certa dimensione, ed è previsto un periodo di attesa di 30 giorni, durante il quale la transazione non può essere conclusa.

Durante questo periodo il FTC e il DOJ analizzano la transazione per determinare se essa è di natura anti-competitiva. In questo caso possono verificarsi due scenari: (i) la natura non viene considerata come anti-competitiva, la transazione è automaticamente autorizzata e può essere conclusa non appena il periodo di 30 giorni arriva al termine; (ii) la transazione è invece preliminarmente considerata problematica dal punto di vista *antitrust*, e la FTC può estendere il periodo di 30 giorni per richiedere ulteriori informazioni e documentazione relative all'acquisizione proposta (c.d. *Second Request*). In questo secondo scenario, la FTC ha tre opzioni: i) autorizzare l'operazione; ii) negoziare un accordo risultante in un decreto di consenso; iii) ritenere l'accordo non raggiunto e affidare la questione all'*United States District Court* che può vietare preliminarmente l'operazione[104].

Il caso *Google/DoubleClick* è il primo in cui l'integrazione tra due società ha avuto effetti nella riduzione del livello di protezione dei dati personali e, dunque, sulla qualità del servizio offerto agli utenti. In questo caso, la FTC ha investigato sulla possibilità che la transazione potesse distorcere i parametri della concorrenza che non fossero basati sul prezzo (e.g. la *privacy* del consumatore). Di conseguenza, l'autorità ha concluso l'indagine in esame affermando che non ci fosse sufficiente evidenza che potesse confermare tale distorsione.[105]

DoubleClick era la più grande società di *advertising*, e la sua acquisizione da parte di Google per 3,1 miliardi di dollari veniva sfidata da Microsoft e altri operatori; questi allegavano violazioni non solo

---

[103] "*Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade of commerce among the several States, or with foreign nations, is declared to be illegal."* Fed. Trade Comm'n Act, 15 U.S.C. § 1 (2006).

[104] Cfr. 15 U.S.C. § 18a (2006); 15 U.S.C. § 25 (2006).

[105] TROTTA, T. CHRISTINA, *The Google-Doubleclick Merger, the FTC, and the Future of Transactional Privacy Inquiries in the United States* (December 13, 2007). Available at SSRN: https://ssrn.com/abstract=1071823 or http://dx.doi.org/10.2139/ssrn.1071823.

della disciplina *antitrust*, ma anche di quella a protezione dei dati personali[106].

Il 20 aprile 2007 l'*Electronic Privacy Information Center* (EPIC), un centro di ricerca nato a Washington nel 1994 per sensibilizzare l'attenzione sulle libertà civili e la tutela della *privacy*, ha ricevuto un reclamo insieme alla FTC, nel quale veniva richiesto di vietare la fusione tra Google e DoubleClick, e di avviare un'indagine relativamente alle circostanze della fusione[107].

La FTC ha notato come l'operazione non sottraesse ai concorrenti di Google l'accesso ai dati relativi ai consumatori, in quanto i rivali già disponevano di un proprio bacino di dati da utilizzare e accrescere nel tempo. In altre parole, né i dati disponibili a DoubleClick né i dati disponibili a Google, potevano considerarsi un *input* essenziale per fare ingresso o operare nel mercato dell'intermediazione pubblicitaria.

Un'altra conferma che anche le operazioni di concentrazione sono annoverabili tra gli strumenti utilizzabili dalle imprese per avere accesso ai dati digitali, la troviamo nel caso *Microsoft/Yahoo* del 2010.

In particolare, il DOJ consentiva alle due imprese di disporre una scala di *input* sufficienti a contrastare la concorrenza di Google nel mercato dei motori di ricerca generalisti.

Durante la propria indagine, il DOJ accettava la versione delle parti secondo cui l'accumulo di dati avrebbe portato ad un aumento di efficienza e, dunque, avrebbe reso l'offerta di Microsoft competitiva rispetto a quella di Google, che era l'impresa di maggior successo sul mercato.

Infine, altro caso è del 2014, quando la FTC ha approvato l'operazione *CoreLogic/DataQuick*, sempre relativa a servizi informativi, con l'impegno a dare in licenza i dati a un nuovo entrante.

In mercati altamente innovativi è essenziale che gli impegni siano di facile implementazione; in caso contrario, ci si può chiedere se sia più opportuna una decisione di autorizzazione in fase I: gli investimenti potrebbero essere rallentati dall'intervento *antitrust*, considerata la rapida evoluzione dei mercati e il fatto che la posizione dominante potrebbe non risultare persistente.

La plenaria del gruppo di lavoro sulle concentrazioni, la c.d. *Merger Working Group* (MWG), anche con riferimento agli Stati Uniti, ha ripercorso le sfide principali per le autorità di concorrenza, che riguardano la necessità di aggiornare i criteri di analisi delle acquisizioni di *start-up* (o potenziali concorrenti in mercati nascenti) e i criteri valutativi, per tener conto di alcune caratteristiche dei mercati digitali (*i.e.* la natura multi-versante di molti operatori, gli effetti di rete, le economie di scala e scopo e il ruolo dei *Big Data*).

Invece, in materia di "*killer acquisition*", l'OECD (*Organisation for Economic Co-operation and Development*) ha pubblicato un documento in occasione del 133esimo OECD *Competition Committee*

[106] Miguel Helft & Louise Story, *Google Buys an Online Ad Firm for $3.1 Billion*, N.Y. TIMES, Apr. 14, 2007, at C1. Steve Lohn, *Microsoft Urges Review of Google' s Bid for Ad Company*, N.Y. TIMES, Apr. 16, 2007, at A14.

[107] Con riferimento al reclamo cfr. http://www.epic.org/privacy/ftc/google/epic_complaint.pdf

che si è tenuto dal 10 al 16 giugno 2020.

Infatti, il diritto *antitrust* statunitense riconosce le concentrazioni tra imprese concorrenti, incluse quelle con nascenti o potenziali concorrenti. Trattasi quindi di imprese che non sono ancora presenti sul mercato, ma che potrebbero avere l'abilità o l'incentivo ad entrarvi e concorrere con le imprese già presenti.

Per anni, quindi, sia la FTC che il DOJ hanno sfidato le concentrazioni verticali e orizzontali che riguardavano i concorrenti nascenti.

L'ultima concentrazione risale ad agosto 2019, quando il DOJ ha sfidato *Sabre Corporation* con riferimento alla proposta di acquisizione di *Farelogix*[108].

Il DOJ ha statuito che l'operazione potrebbe consentire a *Sabre* - la più grande impresa di fornitura di servizi di prenotazione di voli aerei negli Stati Uniti - di eliminare un concorrente innovativo, che aveva introdotto una nuova tecnologia, che stava crescendo in modo significativo.

Il reclamo prevedeva che l'operazione avrebbe comportato l'innalzamento dei prezzi, la riduzione della qualità dei servizi e una minore innovazione.

Il caso è finito davanti alla corte federale distrettuale, che statuiva che Farelogix era un concorrente "*disruptor*" e che "*evidence suggests that Sabre will have the incentive to raise prices…and stifle innovation*"[109] a seguito dell'acquisizione.

Ciò nonostante, la corte ha rigettato la richiesta del DOJ di bloccare l'operazione di acquisizione e, usando come precedente il caso deciso dalla Corte Suprema *Ohio v. American Express Co*[110], ha affermato che *Sabre* e *Farelogix* non competessero in un mercato rilevante.

Le agenzie americane (FTC e DOJ), per fronteggiare queste "*killer acquisition"* e comprendere meglio le dinamiche di mercato sottese a tali operazioni, hanno ampliato il loro *staff* con economisti (con il titolo di dottorato) ed esperti di tecnologia. Tali agenzie sono coscienti del fatto che tali tipi di operazioni possano ridurre significativamente la concorrenza, e hanno intenzione di utilizzare la Section 7 del Clayton Act e la Section 2 dello Sherman Act, come strumenti per proteggere i consumatori da acquisizioni e altre condotte che possano distorcere la concorrenza.

Infine, nel rapporto dell'ottobre 2020 del Congresso USA dal titolo "*Investigation of Competition in the Digital Marketplace"*[111], già analizzato precedentemente con riferimento all'abuso di posizione dominante, vengono incluse anche diverse raccomandazioni in materia di concentrazioni, come: i) la fissazione di uno standard per vietare acquisizioni strategiche che riducano la concorrenza e; ii) il

[108] Complaint, United States v. Sabre Corp., No. 1:19-cv-01548-LPS (D. Del. Aug. 20, 2019), https://www.justice.gov/opa/press-release/file/1196816/download.

[109] Opinion, United States v. Sabre Corp., 34, 87, Civil Action No. 1:19-cv-01548-LPS (D. Del. April 8, 2020).

[110] 138 S. Ct. 2274 (2018).

[111] U.S. House of Representatives - The House Judiciary Committee's Antitrust Subcommittee, *Investigation of Competition in the Digital Marketplace, Washington, 6 ottobre 2020.*

rafforzamento dell'art. 7 del *Clayton Act*[112] e dell'*enforcement* in materia di concentrazioni.

2.2.2 Un breve cenno agli ultimi sviluppi in Cina

L'industria digitale in Cina ha assistito ad un gran numero di fusioni ed acquisizioni nell'ultimo decennio, nonostante nessuna di queste abbiano coinvolto l'autorità *antitrust* cinese.

Il motivo è che le imprese tecnologiche cinesi solitamente danno vita alle c.d. "*VIE structure*", (struttura societaria stabilita in Cina e controllata dall'amministrazione cinese, sebbene sia totalmente o parzialmente posseduta da investitori stranieri) per aggirare le restrizioni agli investimenti stranieri (c.d. *Foreign Direct Investment* – FDI) che il Governo cinese impone in diversi settori, tra cui quello dei servizi di telecomunicazione.

Per molti anni, il Ministro del Commercio cinese è stato responsabile per il controllo sulle concentrazioni, e ha sempre temuto che un'autorizzazione *antitrust* sulle concentrazioni potesse essere vista come un *endorsement* a questi tipi di strutture societarie[113]. Per questi motivi, non ci sono stati casi di concentrazioni in Cina, e ciò l'ha portata - dopo i noti casi Google in Europa dal 2017 al 2019, e il più recente caso Google del 2020 avviato dal DOJ statunitense - ad essere criticata per non aver ancora utilizzato gli strumenti *antitrust* nei confronti delle grandi piattaforme digitali.

Nel novembre 2020, l'autorità *antitrust* cinese (*la State Administration for Market Regulation* – SAMR) ha pubblicato una bozza dell'*Antitrust Guidelines on the Platform Economy*, nella quale viene affermata la possibilità di notificare un'operazione di *VIE structure*. In particolare, l'art. 18 prevede che le concentrazioni delle attività rientranti nel *VIE structure* ricadano nel controllo sulle concentrazioni. Con questi nuovi presupposti, quindi, sembra che tali operazioni non possano più sfuggire da un controllo sulle concentrazioni da parte dell'autorità cinese. Inoltre, questa bozza delle *Guidelines* chiarisce anche il potere di indagine della SAMR sulle "*killer acquisitions*", che sono al di sotto delle soglie previste per il controllo sulle concentrazioni. In particolare, si tratta di acquisizioni di *start-up* o società emergenti in un mercato dominato da grandi società.

Queste società non hanno generato grandi ricavi e dunque, una volta acquisite, non comportano particolari obblighi. Tuttavia, società risultanti da tali acquisizioni possono minacciare la concorrenza per le informazioni tecnologiche e la forte innovatività che le caratterizza. Infatti, l'art. 19 delle *Draft Guidelines* prevede che la SAMR debba investigare anche su tali operazioni, qualora ci fosse la prova che esse possano comportare effetti potenzialmente anti-competitivi; questa nuova norma può condurre molte compagnie tecnologiche cinesi a segnalare all'autorità tali operazioni, sebbene esse

[112] Clayton Act, 15 U.S.C. § 18 (1914). L'art. 7 vieta infatti ogni operazione in cui "*the effect of such acquisition may be substantially to lessen competition, or to tend to create a monopoly*".

[113] Così Jet Deng e Ken Dai, *The Failure-to-File Antitrust Risks Rise Sharply for The VIEs*, https://www.mondaq.com/china/antitrust-eu-competition-/932588/the-failure-to-file-antitrust-risks-rise-sharply-for-the-vies

non siano notificabili.

2.2.3 Unione Europea

Come già evidenziato, l'area delle concentrazioni è quella dove emerge maggiormente il rapporto tra diritto *antitrust* e diritto alla *privacy*.

In Europa, fino a qualche anno fa, nell'ambito della valutazione degli effetti delle operazioni di concentrazione, si registrava una certa ritrosia ad introdurre esplicitamente considerazioni riguardanti la protezione dei dati.

Nella concentrazione *Facebook/WhatsApp*[114], autorizzata senza condizioni nel 2014, la Commissione europea ha ritenuto che la *privacy* non fosse un importante parametro nella scelta dei consumatori nel mercato delle *App* di comunicazione e che, quindi, una possibile degradazione della *privacy* - a valle dell'operazione di concentrazione - non avrebbe potuto danneggiare il benessere dei consumatori.

La Commissione affermava che una riduzione della qualità della *privacy*, come conseguenza della concentrazione dei dati a seguito dell'operazione di fusione, non rientrava nello scopo del diritto della concorrenza europeo, ma piuttosto in quello del diritto europeo alla protezione dei dati personali[115].

Ciò nonostante, non è mancato in dottrina chi già da allora sottolineava come la *privacy* potesse essere considerata come parametro della concorrenza capace di mitigare i rischi di esercizio del potere di mercato;[116]negli ultimi anni, tale orientamento si è fatto avanti anche nella pratica delle autorità di concorrenza. Questo si fonda su un'interpretazione ampia della nozione di benessere dei consumatori, tale da ricomprendere correttamente anche la dimensione della protezione dei dati personali.

Nella recente concentrazione *Microsoft/Linkedin* [117] , autorizzata con condizioni nel 2016, la Commissione ha concluso che la *privacy* è un parametro della concorrenza tra *social network* professionali, e che in assenza di rimedi adeguati, la concentrazione avrebbe potuto escludere concorrenti in grado di offrire una *privacy* maggiore di quella offerta da *Linkedin,* fermo restando il rispetto del quadro regolamentare in materia di protezione dei dati personali.

Di conseguenza, la Commissione concludeva che gli effetti di preclusione nel mercato per altri operatori dei *social network* potevano negativamente toccare i consumatori, in quanto comportava la marginalizzazione dei concorrenti, che avrebbero potuto offrire un grado di protezione dei dati

[114] Commissione Europea (2014), "M.7217 Facebook/Whatsapp", http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[115] Sul punto cfr. PITRUZZELLA, *op.cit.* p. 82.

[116] Cfr. *ex multis* P. MERLINO, cit, p. 394 che ha utilizzato come esempio proprio Facebook/Whatsapp nel punto in cui la Commissione affermava che "*after the announcement of WhatsApp's acquisition by Facebook and bacause of privacy concerns, thousands of users downloaded different messaging platforms, in particolar Telegram which offers increased privacy protection*".

[117] Commissione Europea (2016), "M.8124 Microsoft/Linkedin", http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

personali maggiore rispetto a *Linkedin*.

Al tal proposito, la Commissione considera due principali teorie del danno:

i) in un mercato ipotetico dell'offerta di dati personali, l'operazione avrebbe accresciuto il potere di mercato, o elevato barriere all'ingresso di altri concorrenti, i quali avrebbero dovuto raccogliere una elevata mole di dati per competere con l'entità risultante dall'operazione;

ii) in caso di impossibilità tecnica nell'unione dei *data set*, la concentrazione avrebbe eliminato la concorrenza tra le due società.

La Commissione alla fine propende per l'assenza di simili preoccupazioni poiché: (i) Microsoft e LinkedIn non rendono disponibili tali dati a terze parti per fini pubblicitari, e detengono in ogni caso una modesta quota di mercato nella pubblicità *online*; e (ii) la combinazione dei *data set* non sembra aumentare le barriere di mercato, in quanto molti utenti di internet - ai quali possono indirizzarsi le attività di *advertising* di operatori concorrenti – acquistano anche servizi di altri operatori.

Inserire considerazioni di *privacy* all'interno del controllo delle concentrazioni, costituisce solo uno dei diversi strumenti a disposizione dell'autorità di concorrenza per contribuire alla tutela di tale valore nell'esercizio delle proprie competenze. Come illustrato nell'Indagine 2020 sui *Big Data* e, in particolare, nella sezione 5.3 dedicata al rapporto tra concorrenza e *privacy*, infatti, una relazione virtuosa tra questi due ambiti può svilupparsi solo laddove i consumatori assumano scelte dei servizi digitali, anche sulla base di una effettiva consapevolezza e sensibilità rispetto alla tutela dei propri dati.

Con riferimento, invece, alla valutazione dell'operazione *Apple/Shazam*[118] (leader mondiale nel riconoscimento musicale), la Commissione ha ritenuto che l'integrazione dei *database* delle parti, contenenti dati sui rispettivi utenti, non avrebbe conferito alla nuova entità un vantaggio non replicabile. Si trattava, infatti, di *database* contenenti dati non unici e non qualificabili come *input* importanti per la fornitura dei prodotti a valle.

Oltre al problema delle soglie, un'altra questione riguarda i c.d. *remedies* nell'ambito di mercati fortemente innovativi.

Si pone l'esigenza di trovare misure idonee a risolvere gli effetti negativi associati all'aggregazione di dati tra società differenti, come nel caso in cui vi sia un'aggregazione di database. In taluni casi, le parti si sono impegnate a dismettere database a soggetti terzi, come nella fusione tra i fornitori di servizi di informazione Thomson Corporation e Reuters Group, esaminata dalla Commissione europea nel 2008. In risposta ad una delle preoccupazioni relativa al rischio di un impatto negativo

[118] Commissione Europea (2018), "M.8788 Apple/Shazam", http://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf.

dell'operazione, sui soggetti che utilizzano i contenuti forniti dalle due società nei propri prodotti offerti al mercato, le parti si sono impegnate a trasmettere una copia dei propri database ad un soggetto terzo.

Le implicazioni per il controllo delle concentrazioni determinate dalla diffusione degli algoritmi di prezzo richiedono ulteriori considerazioni: le evidenze relative alla portata ed i pro e contro del fenomeno; inoltre, sembra ragionevole sostenere che l'accresciuta possibilità di praticare strategie di prezzo discriminatorie, comporti una maggiore attenzione e sensibilità, sia sulla definizione del mercato rilevante del prodotto (che potrebbe anche collassare su quelli che, in assenza di algoritmi di prezzo, erano segmenti di un mercato più ampio), sia sulla valutazione degli effetti unilaterali.

Diversamente, lo sviluppo di algoritmi di prezzo pro-collusivi comporta, come vedremo nei paragrafi successivi, una maggiore attenzione nelle valutazioni dei rischi di coordinamento anche in mercati più frammentati.

Infine, in linea con quanto fatto dalle agenzie americane (FTC e DOJ), anche in Europa si sta assistendo ad un importante sviluppo: la creazione nel 2019 del *Gruppo Investigazioni Digitali e Intelligenza Artificiale*, che conferma la tendenza delle Autorità di concorrenza ad affiancare ai giuristi e agli economisti figure professionali come i *data scientist*, in grado di comprendere la relazione tra algoritmi, *Big Data*, intelligenza artificiale e il ruolo dell'individuo nella formazione di intese anticoncorrenziali.

2.2.4 Questioni aperte in Italia ed eventuali divergenze con l'Europa

In considerazione dei meccanismi di rinvio dei casi tra gli Stati membri e la Commissione, sono numerosi i casi di operazioni di dimensione comunitaria, notificate alla Commissione e poi esaminate dall'AGCM. Ad esempio, l'Autorità ha autorizzato con condizioni l'acquisizione del controllo di La Gardenia e Limoni da parte del gruppo CVC, a cui appartiene Profumerie Douglas, rinviata dalla Commissione all'Italia sulla base dell'articolo 4, paragrafo 4 del regolamento[119].

I rinvii stanno aumentando: nel 2017, sono state rinviate dalla Commissione all'Italia altre due operazioni: i) Holcim aggregati calcestruzzi-Colabeton, approvata dall'AGCM in fase 1; ii) Admiral Entertainment-Lottomatica, una *joint venture* rispetto alla quale l'Autorità ha ritenuto prevalenti gli aspetti di natura cooperativa.

L'AGCM ha in ogni caso privilegiato un'interpretazione evolutiva del test di dominanza, per porlo in linea con il test UE, con un approccio analitico robusto, un'analisi complessiva del rischio e del relativo impatto sulla concorrenza. Specie nei casi più recenti, l'Autorità ha prestato particolare

[119] In tal caso, l'Autorità ha integrato le misure proposte dalla parte richiedendo alla società acquirente la cessione a soggetti terzi ed indipendenti di alcuni punti vendita nelle aree in cui sono state riscontrate criticità concorrenziali.

attenzione ai potenziali effetti restrittivi dell'operazione, oltre che alla costituzione o rafforzamento di una posizione dominante, facendo spesso riferimento agli orientamenti comunitari sulle concentrazioni orizzontali[120].

Un'ulteriore differenza tra il test di valutazione comunitario e quello nazionale è che quest'ultimo non prevede espressamente l'analisi di bilanciamento degli effetti restrittivi con i vantaggi di efficienza dell'operazione.

L'AGCM ha tuttavia tenuto conto nella propria prassi delle argomentazioni poste dalle parti[121].

Il fatto che l'Autorità abbia cercato di avvicinarsi al test UE, pur in assenza di una modifica normativa, non risolve il problema, in quanto in ogni caso, specie nei casi di maggior rilievo, l'autorità ha minor forza nel richiedere o nell'imporre misure, purché queste siano fondate su un'analisi non perfettamente coincidente con quella prevista dal legislatore.

Sarebbe auspicabile, pertanto, la modifica dell'art. 6, comma 1, della legge n. 287/90, con l'introduzione di uno *standard* valutativo più adatto alle sfide dell'economia digitale, che faccia leva sul criterio dell'impedimento significativo della concorrenza effettiva (SIEC – *Substantial impediment to effective competition*).

In un'economia caratterizzata dalla crescente importanza dei *Big Data* occorre forse ripensare alcuni istituti del diritto *antitrust*, o meglio adeguarli alla realtà che cambia.

Altra peculiarità italiana riguarda la questione delle *joint venture* nell'ambito delle concentrazioni.

La disciplina nazionale relativa alle imprese comuni distingue tra imprese comuni di natura concentrativa ed imprese comuni aventi natura cooperativa, sottoponendo solo le prime alla disciplina sulle concentrazioni.

A livello comunitario, invece, sono configurate come concentrazioni, ed assoggettate al Reg. n. 139/2004, tutte le imprese comuni *full-function;* ciò implica, che la costituzione della medesima impresa comune *full-function*, configurabile come concentrazione secondo i parametri adottati dalla Commissione, potrebbe essere qualificata come una *joint venture* cooperativa e non dare luogo ad una operazione di concentrazione ai sensi dell'articolo 5, comma 3, della legge 287/90.

La valutazione circa la natura cooperativa o concentrativa di una operazione non è sempre immediata, e questo potrebbe dare luogo a incertezze applicative, anche in considerazione del sistema dei rinvii

[120] A titolo di esempio, nel provvedimento di autorizzazione condizionata del caso RTI/Finelco (2016), si evidenzia che la concentrazione avrebbe dispiegato, oltre ad effetti di sovrapposizione orizzontale, anche effetti di tipo conglomerale, in quanto Fininvest avrebbe potuto "sfruttare la naturale propensione degli inserzionisti a pianificare congiuntamente la pubblicità su mezzo televisivo insieme alla pubblicità su mezzo radiofonico".

[121] Cfr. M-DIS, Servizi stampa Liguria, 2013, in cui sono stati esaminati gli effetti orizzontali, verticali dell'operazione e le efficienze evidenziate dalle parti e l'operazione è stata autorizzata; per contro, nel caso SEL, Società elettrica altoatesina, 2015, l'Autorità ha escluso che le efficienze fossero *merger specific* e autorizzato l'operazione con condizioni.

previsto dal reg. 139/2004[122].

Per superare tali problematiche, l'Autorità aveva chiesto nella segnalazione per la legge annuale del 2 ottobre 2012 una modifica della relativa disciplina; la questione dovrebbe essere senz'altro tenuta a mente in una riconsiderazione della disciplina nazionale. La legge sulla concorrenza n. 124/2017 ha infatti risolto la questione delle soglie di fatturato ai fini della notifica per le *joint venture* di nuova costituzione, mentre resta ancora aperto il profilo in questione.

Da ultimo, meritano un cenno le ulteriori differenze tra il nostro ordinamento e quello comunitario, su cui è opportuno riflettere.

Con riferimento alle restrizioni accessorie: nel sistema europeo, il provvedimento autorizzativo non deve esaminare le singole restrizioni accessorie, che si considerano automaticamente approvate qualora presentino i requisiti previsi; a livello nazionale, invece, le vigenti modalità di comunicazione prevedono che tali accordi devono essere comunicati all'Autorità, che ne valuta la eventuale natura accessoria.

Nei provvedimenti, l'AGCM si pronuncia in merito all'esito di tale verifica, chiarendo se le clausole rientrino nella nozione di restrizioni accessorie e possano ritenersi automaticamente approvate, o se le restrizioni non presentano i requisiti della connessione diretta/necessarietà. Questo significa che l'autorizzazione non le protegge da altre norme di diritto della concorrenza e spetterà alle parti valutare autonomamente se queste ultime sono violate o meno. A tal proposito, si potrebbe infatti valutare se modificare il punto.[123]

Per concludere, si rileva come le differenze ad oggi esistenti tra l'ordinamento comunitario e quello nazionale, seppur numerose, non sembrano aver causato nella prassi divergenze applicative di rilievo significativo.

L'interpretazione evolutiva del test di dominanza privilegiata dall'AGCM ha consentito esiti valutativi sostanzialmente convergenti con il test europeo, minimizzando i rischi di interpretazioni divergenti e incertezza giuridica per le imprese. Ciò non riduce la necessità di un pieno adeguamento alla normativa UE.

Nella propria prassi, l'AGCM ha inoltre prestato particolare attenzione agli *standard* UE e delle Autorità degli altri Stati membri, affinando nel tempo la propria analisi.

Si pensi, a titolo di esempio, alla definizione dei mercati geografici locali, dove l'Autorità si è

[122] Si pensi al caso *Admiral Entertainment*-Lottomatica, relativo all'acquisizione del controllo congiunto di un'impresa comune attiva nella gestione delle sale per la raccolta del gioco. Tale caso è stato rinviato dalla Commissione all'Italia a seguito dell'istanza formulata dalle parti.
L'Autorità ha deliberato il non luogo a provvedere ritenendo che l'operazione non potesse qualificarsi come concentrazione e, contestualmente, ha aperto un procedimento per asserita violazione dell'articolo 101 TFUE. Il procedimento si è chiuso con un non luogo a provvedere dopo che le parti hanno dichiarato di rinunciare all'operazione.

[123] Cfr. anche TAR Lazio, n. 3252/2011, Bain Capital Investors, secondo cui gli "accordi accessori" non devono "essere previamente notificati all'Autorità" che non avrebbe quindi un obbligo di pronunciarsi.

allineata alla prassi seguita a livello europeo, in particolare dall'Autorità inglese e da quella francese. Infatti, mentre in passato a livello nazionale il mercato veniva definito facendo perlopiù ricorso ad un approccio di tipo "amministrativo", ossia con riferimento ai confini amministrativi provinciali o regionali, più recentemente è stato adottato un approccio economico, che guarda le c.d. *catchment area*[124]. In altri termini, si è assunto come punto di riferimento la disponibilità a muoversi dei clienti per raggiungere il punto vendita, nell'ipotesi in cui, quanto più questa è ridotta tanto più circoscritto è l'ambito competitivo rilevante.

2.2.5 Rilievi conclusivi in materia di concentrazioni

Alla luce delle considerazioni sopra esposte bisogna innanzitutto constatare come la privacy e la tutela dei dati personali sia divenuta sempre più un parametro della concorrenza[125].

Inoltre, occorre considerare l'opportunità di introdurre a livello normativo criteri di notifica delle concentrazioni, che consentano il controllo preventivo di operazioni di fusione e acquisizione di imprese innovative da parte dei grandi operatori digitali, le quali oggi possono sfuggire al vaglio dell'Autorità a causa della natura e del livello delle soglie previste per le comunicazioni.

La Commissione, dopo l'adozione del Libro bianco nel 2014[126], ha preso atto, anche nella Consultazione pubblica del 2016[127], della presenza di un dibattito tra gli *stakeholders* e gli esperti di concorrenza con riferimento all'efficacia delle attuali soglie di fatturato su cui si basa il controllo delle concentrazioni, soglie stabilite dall'art. 1 Reg. n. 139/2004, per determinare quali transazioni abbiano rilevanza comunitaria. A tal proposito, è stato osservato che questo parametro non consente l'attrazione nell'ambito di competenza della Commissione di tutte operazioni che potenzialmente abbiano impatto sul mercato unico, specie in relazione alle operazioni concluse nella *digital economy*, dove le acquisizioni sebbene non generino sempre utili tali da ricadere all'interno delle soglie di fatturato prefissate, abbiano un valore rilevante e costituiscano, o costituiranno, un importante fattore competitivo nel mercato rilevante, capace di generare nel corso del tempo extra-profitti per l'impresa[128].

---

[124]Cfr. tra gli altri, casi La Gardenia, 2018 e Coop Centro Italia, 2015, entrambi rinviati dalla Commissione.

[125] Commissione Europea (2016), "M.8124 Microsoft/Linkedin", http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

[126] Libro Bianco COM (2014) 449 final, Bruxelles, 9.7.2014, *Verso un controllo più efficace delle concentrazioni nell'UE*; In dottrina, cfr. FERRETTI, *Osservazioni sulle proposte di modifica contenute nel Libro Bianco intitolato: "Verso un controllo più efficace delle concentrazioni dell'UE*", in *Contr. impr. eur.*, 2015, 381 ss.

[127] European Commission, *Consultation on Evaluation of procedural and jurisdictional aspects of UE Merger Control*, 2016.

[128] In particolare, a pagina 2 della Consultazione (p. 2) si legge che: «*Some stakeholders have raised the question of whether the turnover- based jurisdictional thresholds allow capturing, under EU merger control rules, all transactions which can potentially have an impact in the internal market. This question may be particularly significant for transactions in the digital economy, but also in other industry sectors, such as pharmaceuticals, where acquisition targets may not have always generated substantial turnover yet, but nevertheless are highly valued and constitute, or are likely to become, an important competitive force in the relevant market(s)».*

Con la diffusione dei *Big Data*, il controllo delle concentrazioni assume una nuova centralità. Al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza, rispetto alle operazioni di concentrazione, sarebbe auspicabile una riforma a livello nazionale e internazionale, tale da consentire alle autorità di concorrenza di poter valutare pienamente anche quelle operazioni di concentrazione sotto le attuali soglie richieste per la comunicazione preventiva, ma che potrebbero risultare idonee a restringere sin dalla loro nascita importanti forme di concorrenza potenziale (come le acquisizioni da parte dei grandi operatori digitali di *start-up* particolarmente innovative anche soprannominate '*killing acquisitions'*); si pensi alle ricadute sul concetto di potere di mercato e alla necessità di individuare indici adeguati per valutare la rilevanza di un'operazione, nei casi in cui il fatturato è, di per sé, poco significativo. Ciò che può rilevare, in questi casi, sono gli *assets* di un'impresa, tra cui i dati che possiede.

Nell'analisi degli effetti prodotti da una concentrazione, il possesso di dati deve essere trattato alla stregua di un *input* che, in presenza di determinate condizioni, è idoneo a generare effetti di esclusione. Nel condurre tale analisi, si dovrà avere riguardo alla natura dei dati in oggetto, al fine di apprezzare se si tratta di un elemento chiave per il successo di un prodotto e la sua replicabilità.

In tale prospettiva, ci si dovrà anche interrogare in che misura la combinazione di più *data-set* possa risultare in un accrescimento del potere di mercato della nuova entità.

Occorre considerare l'opportunità di prevedere metodologie diverse dalle soglie di fatturato per fare scattare l'obbligo di notifica. Le soglie, infatti, vanno bene nell'ambito di una economia tradizionale, quando il rischio che si crei un potere di mercato eccessivo è dato dal fatto che due giganti si uniscono. Nell'economia digitale il rischio è diverso, dipende dalla possibilità che un *player* consolidato, che ha una posizione dominante, blocchi l'innovazione e l'ingresso di un concorrente nel mercato attraverso l'acquisizione di una *start up*. Queste operazioni in base al criterio di notifica sulla base delle soglie sfuggirebbero al controllo *antitrust*.

All'interno dell'Unione europea ci si interroga su possibili criteri differenti: la Commissione europea, nella consultazione pubblica avviata nel 2016 sul reg. 139/2004, ha considerato quale possibile criterio il valore dell'operazione; Germania e Austria, invece hanno già introdotto norme, entrate in vigore nel giugno 2017, in base alle quali l'operazione è soggetta a notifica se il valore è superiore a un determinato importo (400 milioni di euro in Germania e 200 milioni di euro in Austria) e la *target* opera in maniera significativa nel paese in questione.

Sulla base della nuova normativa austriaca, l'operazione Apple/Shazam, conclusa per un importo di circa 400 milioni di dollari, è stata notificata in Austria, mentre sfugge al vaglio preventivo *antitrust* negli altri Stati membri a causa del fatturato esiguo della società *target*. Tutti i mercati oggetto dell'operazione sono di dimensioni quantomeno comunitarie, e le imprese sono attive in tutti gli Stati

membri.

La divergenza tra il test comunitario e i test nazionali potrebbe esporre le imprese al rischio di incoerenze nella valutazione della compatibilità dell'operazione, specie nei casi di concentrazioni tra imprese di diversi Stati membri: nell'Unione europea vi sono ogni anno oltre 200 operazioni multi-giurisdizionali, ciascuna delle quali deve essere notificata in media a 3,5 autorità nazionali di concorrenza[129]. Pertanto, a tal proposito, ci si auspica un intervento a livello UE, prevedendo l'applicazione dei medesimi parametri di valutazione dell'operazione in occasione di concentrazioni multi-giurisdizionali.

Le soluzioni vanno trovate senza timori di mettere in discussione i tradizionali strumenti *antitrust*, con l'unico obiettivo di assicurare che la finalità del controllo sulle concentrazioni sia quella di garantire che i mercati restino competitivi e aperti.

L'obiettivo non è quindi quello di contenere la crescita dimensionale delle imprese.

Gli *Over The Top* e i "campioni nazionali" possono ben raggiungere posizioni di dominanza, anche in modo *disruptive*, purché ciò avvenga per crescita interna e grazie a una concorrenza basata sul merito.

In presenza di concentrazioni, va valutato attentamente che non si costruiscano posizioni poi difficilmente contendibili, bisogna riflettere se soglie di fatturato e quote di mercato siano ancora gli strumenti più idonei per affrontare realtà in cui il potere di mercato è conglomerale e travalica i confini dei singoli mercati.

Quindi, piuttosto che ricorrere a regole *ad hoc* per i mercati digitali si potrebbe avallare una forma di controllo *ex post* delle operazioni sotto soglia, come è già previsto negli Stati Uniti.

In alternativa, qualora si volessero mantenere i vantaggi legati al sistema di notifica e valutazione preventiva, si potrebbero definire delle soglie calcolate in termini di volume delle transazioni, o di valore delle acquisizioni.

Infine, le autorità antitrust saranno portate ad assumere decisioni orientate verso una indagine accurata degli effetti del comportamento delle imprese sulla base del loro potere di investire e di innovare, perciò indagini più mirate sugli effetti economici, prospettici e dinamici (e.g. lo strumento del *business plan* e similari), piuttosto che sullo stato delle cose al momento della decisione. In questo senso, negli Stati Uniti, si era già mossa la Commissaria Pamela Jones Harbour della FTC tramite una *dissenting opinion* sulla fusione Google/DoubleClick, la quale fu esaminata nel 2007 e poi autorizzata con il suo voto contrario.

[129]Cfr. rapporto commissionato dall'autorità di concorrenza francese al Ministero dell'Economia del 14 marzo 2014, *Making merger control simpler and more consistent in Europe, a 'win-win' agenda in support of competitiveness.*

2.3 Le intese orizzontali degli algoritmi di *pricing* e il *meeting of algorithms*

L'elevata trasparenza dei mercati e lo sviluppo di tecnologie - capaci di analizzare l'incredibile quantità di informazioni continuamente estratte dall'ambiente digitale - non agevolano la gestione e il reciproco controllo da parte delle imprese del rispetto di eventuali accordi anticoncorrenziali. Tuttavia, la trasparenza dei mercati e le nuove tecnologie rendono possibile il verificarsi di fenomeni collusivi fra algoritmi, benché tali forme di intelligenza artificiale non siano programmate per restringere la concorrenza ma, semplicemente, per massimizzare i profitti delle imprese[130].

La domanda che occorre porsi è se l'attuale nozione di intesa sia in grado di catturare le nuove forme di condotte multilaterali degli operatori digitali; senza soffermarsi sulla nozione di intesa, prevista all'art. 101 TFUE[131] e all'art. 2 della l. 287/90,[132] e sulle fattispecie - su cui molto si è scritto - dell'accordo[133], della decisione di associazione di impresa[134] e della pratica concordata[135], ben più rilevante è distinguere tra le forme di collusione che ricadono nel diritto *antitrust* e i semplici comportamenti paralleli leciti.

---

[130] Cfr. L. CALZOLARI, La collusione fra algoritmi nell'era dei big data: l'imputabilità delle imprese delle intese 4.0. ai sensi dell'art. 101 TFUE, *Media Laws* n.3, 2018, 224; M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency* (March 31, 2019). *Bocconi Legal Studies Research Paper* No. 3363178, SSRN: https://ssrn.com/abstract=3363178 or http://dx.doi.org/10.2139/ssrn.3363178; F. DI PORTO, M. MAGGIOLINO, *Algorithmic Information Disclosure by Regulators and Competition Authorities* (March 31, 2019). *Global Jurist*, 2019, Bocconi Legal Studies Research Paper No. 3363169, SSRN: https://ssrn.com/abstract=3363169 or http://dx.doi.org/10.2139/ssrn.3363169.

[131] "1. Sono incompatibili con il mercato interno e vietati tutti gli accordi tra imprese, tutte le decisioni di associazioni di imprese e tutte le pratiche concordate che possano pregiudicare il commercio tra Stati membri e che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza all'interno del mercato interno ed in particolare quelli consistenti nel: a) fissare direttamente o indirettamente i prezzi d'acquisto o di vendita ovvero altre condizioni di transazione; b) limitare o controllare la produzione, gli sbocchi, lo sviluppo tecnico o gli investimenti; c) ripartire i mercati o le fonti di approvvigionamento; d) applicare, nei rapporti commerciali con gli altri contraenti, condizioni dissimili per prestazioni equivalenti, così da determinare per questi ultimi uno svantaggio nella concorrenza; e) subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi. 2. Gli accordi o decisioni, vietati in virtù del presente articolo, sono nulli di pieno diritto. 3. Tuttavia, le disposizioni del paragrafo 1 possono essere dichiarate inapplicabili: — a qualsiasi accordo o categoria di accordi fra imprese, — a qualsiasi decisione o categoria di decisioni di associazioni di imprese, e — a qualsiasi pratica concordata o categoria di pratiche concordate, che contribuiscano a migliorare la produzione o la distribuzione dei prodotti o a promuovere il progresso tecnico o economico, pur riservando agli utilizzatori una congrua parte dell'utile che ne deriva, ed evitando di: a) imporre alle imprese interessate restrizioni che non siano indispensabili per raggiungere tali obiettivi; b) dare a tali imprese la possibilità di eliminare la concorrenza per una parte sostanziale dei prodotti di cui trattasi."

[132] "1. Sono considerati intese gli accordi e/o le pratiche concordati tra imprese nonché le deliberazioni, anche se adottate ai sensi di disposizioni statutarie o regolamentari, di consorzi, associazioni di imprese ed altri organismi similari. 2. Sono vietate le intese tra imprese che abbiano per oggetto o per effetto di impedire, restringere o falsare in maniera consistente il gioco della concorrenza all'interno del mercato nazionale o in una sua parte rilevante, anche attraverso attività consistenti nel: a) fissare direttamente o indirettamente i prezzi d'acquisto o di vendita ovvero altre condizioni contrattuali; b) impedire o limitare la produzione, gli sbocchi o gli accessi al mercato, gli investimenti, lo sviluppo tecnico o il progresso tecnologico; c) ripartire i mercati o le fonti di approvvigionamento; d) applicare, nei rapporti commerciali con altri contraenti, condizioni oggettivamente diverse per prestazioni equivalenti, cosi da determinare per essi ingiustificati svantaggi nella concorrenza; e) subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura o secondo gli usi commerciali, non abbiano alcun rapporto con l'oggetto dei contratti stessi.3. Le intese vietate sono nulle ad ogni effetto."

[133] *Ex multis* cfr. C. LO SURDO, *Accordo contrattuale e intesa ai sensi della normativa antitrust*, *I Contratti*, 299 (2001).

[134] *Ex multis* cfr. P. FATTORI, M. TODINO, *La disciplina della concorrenza in Italia, 86* (2010).

[135] *Ex multis* cfr. M. LIBERTINI, *Pratiche concordate e accordi nella disciplina della concorrenza* (*commento a C. St*., 29 novembre 1996, n. 1792), 5 *Giorn. dir. amm.*, 445 (1997).

Sotto il profilo dell'analisi *antitrust,* la collusione tacita è "qualcosa meno" di una pratica concordata[136]: i prezzi praticati dalle imprese sono infatti fra loro rigidamente interdipendenti, ma non per questo concordati[137]; a tal proposito, anche un'erronea caratterizzazione di un'intesa come accordo, decisione di associazione di impresa o pratica concordata, può essere rilevante ai fini del diritto *antitrust,* se l'autorità è in grado di dimostrare il concorso di volontà (il c.d. *meeting of minds* statunitense[138]) tra le imprese. In altri termini, è tale concorso a rappresentare il contenuto necessario e sufficiente della nozione di intesa, a prescindere dalla modalità secondo cui il concorso si estrinseca e si manifesta. Tuttavia, in dottrina sembra prevalere l'orientamento secondo il quale la collusione fra algoritmi rientrerebbe nel campo di applicazione dell'art. 101 TFUE, laddove assimilabile a un'ordinaria pratica concordata piuttosto che a un'ipotesi di collusione tacita[139].

Le autorità di concorrenza europee e nazionali, sulla scorta dell'esperienza statunitense, hanno escluso la c.d. "interdipendenza oligopolistica" dall'ambito di applicazione dell'art. 101 TFUE e dell'art. 2 della l. 287/90; con tale termine, si identificano quegli scenari in cui le imprese tengono comportamenti collusivi, ma non in ragione di un reciproco intendimento, ma in ragione del loro adattamento intelligente al mercato[140]. In altre parole, esistono dei contesti di mercato in cui le imprese, pur prevedendo i comportamenti dei loro rivali e convergendo in un equilibrio collusivo, agiscono autonomamente e indipendentemente tra di loro[141].

Gli algoritmi consistono in una serie di comandi necessari al raggiungimento di determinati fini e non è automatico considerarli in termini *antitrust*. Tuttavia, se tradizionalmente le imprese violano l'art. 101 TFUE quando condividono le modalità di calcolo dei loro prezzi, pare ragionevole ritenere che la medesima violazione si realizzi quando due o più imprese pongono in comune i propri *pricing algorithms*.

L'utilizzo dei *Big Data* può avere un impatto sul livello dei prezzi anche tramite l'utilizzo di algoritmi di *pricing*[142]; questi ultimi possono essere implementati dalle stesse imprese che vendono il

[136] M. FILIPPELLI, *Il problema dell'oligopolio nel diritto antitrust europeo: evoluzione, prospettive e implicazioni sistematiche*, in *Riv. Società*, ISSN 0035-6018. - 63:2-3(2018), pp. 567-614.

[137] Sull'importanza di una precisa distinzione fra tali nozioni ai fini di una corretta analisi antitrust delle fattispecie di collusione espressa e tacita, v. fra gli altri L. Kaplow, *On the Meaning of Horizontal Agreements in Competition Law*, in *California Law Review*, 2011, 683 ss.

[138] Cfr. in gurisprudenza, *American Tobacco Co. V. United States*, 328 *U.S.* 781, 809-10 (1946); *Monsanto Co. v. Spray-Rite Serv*., 465 U.S. 752,768 (1984); in letteratura, tra gli altri, Gregory J. Werden, *Economic Evidence on the Existence of Collusion: Reconciling Antitrust Law with Oligopoly Theory*, 72, *Antitrust Law Journal*, 719 (2004); William H. Page, *Objective and Subjective Theories of Concerted Action, 79 Antitrust Law Journal 215 (2013).*

[139] L. CALZOLARI, La collusione fra algoritmi nell'era dei big data: l'imputabilità delle imprese delle intese 4.0. ai sensi dell'art. 101 TFUE, op.cit.; MAGGIOLINO, op.cit., 299

[140] Così MAGGIOLINO, op.cit., 291

[141] C. OSTI, *Antitrust e oligopolio. Concorrenza, cooperazione e concentrazione: problemi giuridico-economici e proposte di soluzione*, 165 (1995).

[142] Un algoritmo di *pricing* è una procedura automatizzata usata per determinare i prezzi di vendita ottimali di prodotti e/o servizi sulla base delle condizioni del mercato e adeguarli in "tempo reale" alle variazioni di queste ultime.

prodotto/servizio, o da *software house* che offrono soluzioni complete per una gestione automatizzata della definizione dei prezzi. L'esistenza di prodotti di questo tipo fa sì che algoritmi di *pricing,* anche molto sofisticati, possano essere utilizzati da imprese di dimensione relativamente piccola.

Gli algoritmi di *pricing,* usando particolari sistemi di monitoraggio, acquisiscono i prezzi applicati dalle imprese concorrenti e, sulla base di questi, ricalcolano e aggiornano frequentemente i prezzi.

I dati elaborati da questa tipologia di algoritmo includono: i dati storici relativi a prezzi e profitti, i costi dell'impresa, le informazioni personali del consumatore, i prezzi dei concorrenti, ecc.

Gli algoritmi di *pricing* possono anche essere semplici e basarsi su regole predefinite: allinearsi al prezzo più basso del mercato, o rimanere al di sotto/sopra di una determinata soglia rispetto al prezzo più basso del "mercato" di riferimento; quelli più avanzati invece possono essere basati su modelli predittivi e sull'utilizzo di tecniche di *machine learning,* al fine di massimizzare i profitti dell'impresa.

Ebbene, l'utilizzo degli algoritmi può potenzialmente agevolare fenomeni collusivi, più o meno taciti, in ragione: *i)* dell'elevata trasparenza dei mercati *online,* ossia dell'ampia disponibilità di dati sui prezzi dei concorrenti e di altre informazioni rilevanti; *ii)* della frequenza di aggiustamento dei prezzi, ossia della capacità degli algoritmi di monitorare in tempo reale i mercati, potendo modificare istantaneamente e continuamente i prezzi; *iii)* delle capacità di apprendimento delle strategie di prezzo ottimali attraverso il *machine learning*. In particolare, nel caso di algoritmi caratterizzati da meccanismi di *machine learning,* appare assai difficile rintracciare lo scambio di volontà, che rappresenta l'ingrediente decisivo per una violazione dell'art. 101 TFUE.

È possibile rilevare, in linea generale, come accordi orizzontali tra imprese, che riducono il livello di *privacy* offerto sul mercato, possano essere considerati restrittivi della concorrenza, al pari di accordi idonei ad aumentare i prezzi. In una prospettiva più "tradizionale", anche accordi tra imprese aventi ad oggetto la condivisione di dati personali dei propri utenti, possono evidentemente presentare criticità, laddove siano idonei ad agevolare un coordinamento delle politiche commerciali delle imprese stesse.

Sotto il profilo dell'*enforcement antitrust*, la repressione di comportamenti abusivi e di intese restrittive della concorrenza - entrambi facilitati dallo sviluppo di nuovi *software* e algoritmi sofisticati - è una delle priorità dell'attività delle autorità di concorrenza nell'economia digitale.

Tra le autorità di concorrenza ha trovato autorevole sostegno l'idea che gli algoritmi favorirebbero la collusione aumentando la trasparenza e, quindi, facilitando l'individuazione del prezzo di cartello che, nei mercati *online,* può essere cambiato frequentemente[143].

[143] *Bundeskartellamt, Autoritè de la concurrence, Competition law and data (2016),* http://bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

In particolare, si parla di mercato asimmetricamente trasparente, in quanto le condotte delle imprese sono intellegibili solo per le imprese che dispongono di *Big Data*, escludendo così i consumatori da coloro che beneficiano della trasparenza[144]*;* tale esclusione avrebbe l'effetto di rendere più semplice la collusione facilitando il prezzo di cartello.

La diffusione di algoritmi di prezzo[145], anch'essa agevolata dalla disponibilità di grandi quantitativi di dati, può facilitare la stabilità di cartelli e la creazione di contesti di mercato favorevoli ad equilibri collusivi. Infatti, l'emergere di pratiche di discriminazione del prezzo, grazie all'utilizzo di raffinati algoritmi, rappresenta una delle principali fonti di preoccupazione per le autorità garanti della concorrenza; emerge l'inadeguatezza del diritto *antitrust* europeo e dell'art. 101 TFUE nel contrastare il potenziale impatto negativo dell'utilizzo degli algoritmi di prezzo nei mercati oligopolistici.

Questa impotenza del TFUE ha anche una spiegazione storica, perché tale trattato è stato concluso prima degli approfondimenti scientifici in materia di oligopolio collusivo tacito, generati dalla polemica tra *Turner* della Scuola di Harvard e *Posner* della Scuola di Chicago.

In particolare, una informazione dettagliata e diffusa sulle preferenze dei consumatori può consentire alle imprese di compiere una discriminazione di prezzo a proprio vantaggio. Dal punto di vista economico, si tratta di una pratica che assume effetti anti-competitivi, quando facilita la formazione e la sostenibilità di un accordo collusivo[146].

Da una parte, la diffusione degli algoritmi di prezzo ha un impatto positivo non solo sull'economia - in quanto sono funzionali al contenimento dei costi e al raggiungimento di migliori efficienze – ma anche sulla tutela del consumatore, consentendo a quest'ultimo di verificare rapidamente i prezzi e i beni disponibili sul mercato; dall'altra parte, però, possono creare una serie di problemi riconducibili a quattro macro-categorie: i) l'uso degli algoritmi di monitoraggio per facilitare il funzionamento di cartelli già esistenti; ii) l'uso degli algoritmi da parte di intermediari (agenti, distributori ecc) per coordinare interi settori dei loro fornitori (c.d. *hub and spoke*); iii) gli algoritmi paralleli (c.d. *parallel algorithms o predictable agent* [147]), ovvero algoritmi indipendenti utilizzati da parte di diverse imprese tra loro concorrenti, che tendono ad allineare i prezzi all'interno di una condotta collusiva tacita [148]; iv) algoritmi di *self learning*, dotati di strumenti di intelligenza artificiale, in grado di

[144] MAGGIOLINO, op.cit., 285.

[145] Con riferimento agli algoritmi di prezzo, Cfr. S. GAMBUTO, *Algorithms, big data and tacit collusion new challenges for competition law*, in E.A. RAFFAELLI, *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019; A. MASTRORILLI, *Algoritmo scellerato?*, in Mercato concorrenza e regole, 2/2019, pp. 343-352; COLOMBO – PIGNATARO, *Raccolta e condivisione di Big data: quali effetti sulla collusione?*, in Mercato, concorrenza e regole, 2/2019,p. 315 ss.

[146] COLOMBO – PIGNATARO, *op. cit.*, 315.

[147] L'algoritmo *predictable agent* non è dotato di intelligenza artificiale ma esegue meccanicamente secondo la frequenza preimpostata gli obiettivi che gli vengono dati come quello della massimizzazione del profitto. C'è chi riconduce tale collusione tacita all'intesa dell'art. 101 TFUE.

[148] Anche qui però va sanzionato il comportamento a monte in quanto gli algoritmi sono governati e settati dalle imprese stesse.

decidere da soli la migliore strategia di prezzo (c.d. capacità di *decision making*[149]), che dovrebbe condurre nella maggior parte dei casi, ad un equilibrio collusivo tacito e non concordato sui mercati[150].

Il problema più grande in quest'ultimo scenario riguarda la responsabilità; una delle ipotesi è quella di considerare l'algoritmo come dipendente dell'impresa che ne risponde per il suo comportamento collusivo. In particolare, c'è chi sostiene che ai fini dell'imputabilità dell'impresa si debba seguire il rapporto preponente-agente commerciale, dove l'impresa è preponente, e l'algoritmo è l'agente che agisce nell'interesse dell'impresa e stabilisce il prezzo nell'interesse di quest'ultima.

Nello scenario dell'*hub and spoke* invece, l'*hub* è il fornitore dell'algoritmo e il responsabile del comportamento collusivo, in quanto faciliterebbe il funzionamento del cartello.

2.3.1 Stati Uniti

Negli Stati Uniti gli algoritmi di prezzo possono essere interpretati con due diversi strumenti del diritto *antitrust*:

1. Il primo è quello della c.d. "*facilitating practice*" che, negli Stati Uniti, rientra nelle c.d. "*unfair practices"* ai sensi della *Section 5* della US *Federal Trade Commission Act*.

   All'interno dell'"*unfair methods of competition*" della *Section* 5, la FTC potrebbe fare un reclamo contro l'"*invitation to collude*", ovvero una comunicazione unilaterale contenente informazioni per i concorrenti con effetti anti-competitivi, anche se non c'è evidenza di un accordo o una comunicazione. In altri termini, l'invito a colludere è un atto unilaterale che sfugge dalla *Section* 1 dello Sherman Act ma, può essere perseguito agendo ai sensi della *Section* 5 della FTC Act. In particolare, affinchè la fattispecie sia integrata, in assenza di una prova di un accordo, la FTC deve dimostrare: i) che l'impresa sotto indagine intendeva agire al fine di ridurre la concorrenza sui prezzi; ii) che essa non può produrre alcuna giustificazione oggettiva per il comportamento tenuto[151]. Dunque, l'impresa indagata può considerarsi autrice dell'illecito se ha agito con l'intento di realizzare un equilibrio collusivo o se era consapevole degli effetti collusivi ("*meeting of minds*). Una condotta che utilizza algoritmi è considerata come illecita dalla FTC, quando: i) causa o può causare un danno sostanziale ai consumatori; ii) non può essere ragionevolmente evitata dai consumatori; e iii) non è compensata da altri benefici per i consumatori o per la concorrenza[152].

[149] In questo contesto, i meccanismi decisionali sono difficilmente conoscibili e ripercorribili dalle Autorità antitrust in quanto spesso sono indipendenti e autonomi rispetto alle imprese.

[150] In particolare, L'algoritmo *self learning* utilizzando l'intelligenza artificiale, prende le sue decisioni da sé operando come complemento dell'essere umano. In questo caso però, l'algoritmo, non essendo impostato dall'essere umano per la collusione è più difficile ipotizzare l'applicazione dell'art. 101 TFUE salvo che quest'ultimo si interpreti estensivamente, o che la collusione non fosse già stata prevista dall'impresa. Sul punto cfr. E. DONINI, *op.cit*.

[151] Cfr. E. I du Pont de Nemours & Co. v. FTC., 729 F.2d 128 (2d Cir. 1984).

[152] 15 U.S. Code, Section 45(n) (Standard of proof; Public policy considerations); Federal Trade Commission, Policy Statement on Unfairness (17 December 1980).

Tuttavia, come è emerso dai casi *Boise Cascade*[153] e in *Ethyl*[154] devono sussistere altri requisiti: in *Ethyl*, ad esempio, la FTC ha affermato che particolari condotte, come una comunicazione di cambiamento di prezzo o clausole "*most-favored-customer*", agevolano l'eliminazione di una concorrenza orizzontale.

Nell'applicazione della *Section 5*, si è adottato un approccio restrittivo: quando non c'è evidenza che le imprese tacitamente o espressamente siano d'accordo di evitare la concorrenza, la FTC potrebbe provare un intento anti-competitivo dell'impresa o l'assenza di un legittimo interesse di *business* dell'impresa.

Ebbene, applicando tali assunti in un'ottica algoritmica, l'impresa sarebbe responsabile ai sensi della Section 5: i) se l'impresa ha interesse ad ottenere uno scopo anti-competitivo o; ii) se l'impresa è consapevole delle conseguenze anti-competitive, derivanti dall'applicazione dell'algoritmo.

Tuttavia, non è facile provare la relazione causale tra l'intenzione anti-competitiva dell'impresa e l'impatto negativo dell'algoritmo; l'impresa, infatti, potrebbe avere un legittimo interesse ad adoperare la tecnologia dell'algoritmo per ragioni societarie e di *business*.

2. L'altro strumento di diritto *antitrust* statunitense, utilizzabile per gli algoritmi di prezzo, è quello della c.d. "*market manipulation*". A tal proposito, nel 2014, la *US Securities and Exchange Commission's* (SEC), l'equivalente della nostra CONSOB, ha aperto un caso nei confronti di *Athena Capital Research* (una società di *trading* attiva nella pratica meglio nota come "*marking the close*"); questa società, attraverso l'uso di un sofisticato algoritmo chiamato *Gravy*, vendeva e comprava azioni nei due secondi finali di ogni giorno di negoziazione in borsa, al fine di manipolare i prezzi di chiusura di migliaia di azioni quotate nel mercato NASDAQ.

   Dato che i dipendenti di *Athena* erano consapevoli dell'impatto che Gravy aveva sui prezzi delle azioni e sul mercato – come è emerso dalle *e-mail* interne alla società – l'autorità di vigilanza ha irrogato alla società una sanzione pari a un milione di dollari per "*market manipulation*". Perciò, l'intento anti-competitivo va provato anche per l'uso di questo secondo strumento legale.

   Infatti, premesso che l'uso dell'algoritmo può portare ad un aumento di prezzi e a dinamiche di mercato anti-competitive - allo stesso modo della collusione esplicita - anche negli Stati Uniti appaiono necessari interventi regolatori.

Nel recente caso statunitense *David Hopkins*[155], il DOJ ha contestato l'esistenza di un cartello a un individuo che, operando su Amazon, ha progettato e condiviso con altri venditori i rispettivi algoritmi

[153] *Boise Cascade Corp. v. Federal Trade Commission*, 837 F.2d 1127, 1148 (D.D.C. 1988).
[154] *E.I. du Pont de Nemours Company. v. Federal Trade Commission*, 729 F.2d 128, 142 (2d Cir. 1984).
[155]Cfr. DOJ, Former E-Commerce executive charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution (2015), https://www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace.

di prezzi dinamici, programmati per agire in conformità al loro accordo.

Allo stesso modo, se un'impresa svelasse il suo algoritmo ai suoi concorrenti, potrebbe configurarsi una condotta illecita se essi non se ne dissociano pubblicamente. In altri termini, si tratterebbe di un invito a colludere che potrebbe integrare uno scambio di informazioni strategiche[156], dunque una pratica concordata[157].

Rimanendo in ambito internazionale, l'art 6 (rubricato "*horizontal monopoly agreements"*[158]*)* delle già citate *Draft Guidelines* cinesi, pubblicate il 10 novembre 2020, fa riferimento alle pratiche concordate in relazione allo scambio di intenzioni e informazioni tra imprese tramite algoritmi.

2.3.2 Lo stato dell'arte in Unione europea

Con riferimento agli accordi di cooperazione orizzontale, la Commissione europea ha avviato il processo di revisione di due Regolamenti, quello sugli accordi di ricerca e sviluppo[159] e quello sugli accordi di specializzazione[160], entrambi in scadenza nel 2022. Sebbene considerati tra i più delicati sotto il profilo *antitrust*, gli accordi orizzontali possono, in taluni casi, ritenersi compatibili con il diritto della concorrenza, nella misura in cui consentano di realizzare incrementi di efficienza trasferibili ai consumatori senza che la concorrenza risulti inevitabilmente compromessa.

La Commissione, mediante la pubblicazione di una comunicazione sugli accordi di cooperazione orizzontale, ha fornito un quadro di analisi applicabile alle forme più comuni di accordi al fine di verificare se esse possano beneficiare di un'esenzione ai sensi dell'art. 101(3) del TFUE.

La consultazione pubblica sui due Regolamenti è stata avviata a novembre 2019 e si è conclusa a febbraio 2020[161]. La comunicazione della Commissione e il processo di revisione dei due Regolamenti costituiscono un'occasione per discutere delle nuove forme di cooperazione tra le imprese, favorite dallo sviluppo della digitalizzazione e di ecosistemi (come la *blockchain* e gli *smart contract*) e per valutare potenziali benefici e criticità concorrenziali sollevate, ad esempio, dallo

---

[156] I principi generali relativi alla valutazione dello scambio di informazioni sotto il profilo della concorrenza si trovano nella Comunicazione della Commissione del 12.01.2011 (2011/C 11/01) «Linee direttrici sull'applicabilità dell'art. 101 del Trattato sul funzionamento dell'Unione Europea agli accordi di cooperazione orizzontali» (§§ 55-104), che non contempla espressamente la *digital economy*. Cfr. Wish-Bailey, Competition Law, Oxford, 2012, 539 ss, spec. 547.

[157] L. CALZOLARI, La collusione fra algoritmi nell'era dei big data: l'imputabilità delle imprese delle intese 4.0. ai sensi dell'art. 101 TFUE, cit. 227.

[158] In particolare l'art 6 delle *Draft Guidelines* prevede che: "*Operators in the platform economy sector with competitive relationships may reach price-fixing, market division, production (sales) restriction, new technologies (products) restriction, group boycott or other horizontal monopoly agreements through the following methods: (1) Using platforms to collect or exchange price, sales or other sensitive information; (2) Using technical means to communicate intentions; (3) Using data and algorithms to achieve concerted practices; (4) Other methods that help to achieve concerted practices. Price referred to in this Guideline includes but not limited to product price, commissions, handling fees, membership fees and promotion fees."*

[159] Regolamento (UE) n. 1217/2010 della Commissione, del 14 dicembre 2010, relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a talune categorie di accordi ricerca e sviluppo.

[160]Regolamento (UE) n. 1218/2010 della Commissione, del 14 dicembre 2010, relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a talune categorie di accordi di specializzazione.

[161] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/11886-Evaluation-of-EU-competition-rules-on-horizontal-agreements/public-consultation.

scambio di informazioni sensibili tra operatori.

Nel caso *Container Shipping*[162], la Commissione europea ha espresso preoccupazione circa un sistema di annunci, per effetto del quale le parti regolarmente comunicavano al mercato - sui loro siti internet, sulla stampa o attraverso altre modalità - gli aumenti futuri dei prezzi praticati per i servizi di trasporto marittimo di container. Secondo la Commissione, questi annunci, anziché aiutare la clientela a organizzare meglio i suoi traffici, permettevano alle parti di esaminare le reciproche intenzioni di prezzo e di coordinare i loro comportamenti, testando i possibili effetti degli stessi e riducendo l'alea competitiva.

A tal proposito, dato che la segnalazione reciproca di ipotesi di prezzo costituisce, quando realizzata *off-line*, un illecito ex art. 101 TFUE, non si vedono le ragioni per cui una medesima condotta non dovrebbe essere qualificata come un'intesa, quando viene eseguita *online* per mezzo di macchine intelligenti e strumenti automatici.

Altro caso europeo degno di nota è il Caso *Eturas*[163] in cui alcune agenzie di viaggio lituane, impiegando il medesimo sistema di prenotazione online, avevano ricevuto dall'amministratore del sistema un invito a non fissare sconti superiori ad un certo livello, e avevano poi visto aumentata una restrizione tecnica che limitava gli sconti applicabili alle prenotazioni eseguite tramite il sistema.

Ebbene, la Corte di Giustizia ha correttamente osservato che, come accade nel mondo *offline*, l'intesa si sarebbe configurata qualora si fosse accertato che ciascuna agenzia avesse materialmente ricevuto il messaggio e non si fosse dissociata pubblicamente da questo. In particolare, parte della sentenza si sofferma sulla necessità di provare che le imprese abbiano ricevuto effettivamente l'invito a colludere; circostanza che deve essere provata dall'autorità antitrust.

Inoltre, con riguardo all'onere della prova, la Corte di giustizia ha applicato per la prima volta in un contesto algoritmico la c.d "presunzione Anic" secondo la quale l'impresa che partecipa meramente all'incontro collusivo viene considerata come facente parte del cartello. Conformemente a tale presunzione, il comportamento effettivo sul mercato può essere presupposto per quelle imprese che partecipano a pratiche collusive e rimangono attive sul mercato. Inoltre, nel presente caso, il comportamento sul mercato può essere desunto dal fatto che la limitazione della percentuale di sconto è stata attuata con mezzi tecnici, quindi applicata automaticamente a tutte le agenzie di viaggio che hanno continuato ad utilizzare il sistema Eturas.

Si tratta di una fattispecie di *hub and spokes,* analizzata in precedenza, dove gli *spokes* sono le imprese concorrenti che forniscono all'*hub supplier* le strategie di prezzi per le stesse *spokes*. A tal proposito, la Corte europea ha statuito che se si può dimostrare che gli *spokes* sono consapevoli del

[162] *CE*, 7 luglio 2016, Caso AT39850, *Container Shipping*, GU C327, 6 settembre 2016, 4.
[163] C-74/14 *Eturas UAB and Others v Lietuvos Respublikos konkurencijos taryba* (ECJ 21 January 2016).

comportamento collusivo operato dagli algoritmi, è possibile attivare il diritto *antitrust* come pratica concordata.

Di recente, in Italia, con riferimento alle intese di prezzo, il Consiglio di Stato ha inoltre confermato che "le indicazioni di associazioni di imprese di tenere un determinato livello di prezzi, anche laddove non vincolanti e costituenti una mera raccomandazione, costituiscono intese restrittive della concorrenza, anche nell'ipotesi in cui richiamino a giustificazione della propria condotta la dignità della professione o la qualità della prestazione".[164]

2.3.3 Alcune idee conclusive sul *pricing algorithms* e i *new competition tools*

Nonostante molti economisti abbiano già studiato la relazione tra discriminazione di prezzo e collusione[165], rimane ancora largamente inesplorata la stretta relazione tra la raccolta e condivisione di *Big Data* ed il raggiungimento di un accordo collusivo stabile nel tempo.

Alla luce del suddetto comportamento collusivo delle imprese mediante algoritmi di prezzo, si auspica che vengano effettuati degli interventi regolamentari, in modo da poter applicare più estensivamente l'art. 101 TFUE; così facendo, si considererebbero gli scambi di flussi informativi tra algoritmi come "scambio di informazione" o, quanto meno, come pratica facilitante contraria all'art. 101 TFUE. In alternativa, le autorità potrebbero servirsi loro stesse di algoritmi per fronteggiare le condotte collusive delle imprese che utilizzano i *pricing algorithms.*

Relativamente invece ai rimedi che il diritto *antitrust* europeo ha per fronteggiare tali comportamenti collusivi ci sono sei diverse ipotesi:

1. si discute della possibilità di intervenire *ex ante* sul Regolamento sulle concentrazioni n. 139/2004 (c.d. *Merger Regulation*) così da rinvenire, anche in un contesto algoritmico, gli effetti coordinati tra imprese in mercati non altamente concentrati e non strettamente oligopolistici;
2. si auspicherebbe la possibilità di intervenire *ex post*, in via più tradizionale, mediante l'applicazione dell'art. 101 TFUE, in modo da considerare l'accordo e il requisito del *meeting of minds* come un'offerta (l'algoritmo che segnala il prezzo collusivo) e accettazione tacita (l'algoritmo che si stabilizza su quel prezzo collusivo), o un'estensione del concetto di pratica concordata, rinvendo quel contatto diretto o indiretto che si richiede tra le imprese nel mero comportamento collusivo degli algoritmi, che tendono a decodificarsi l'uno con l'altro. In

[164]CdS, VI, 19 dicembre 2019, nn. 8588 e 8591, I792.

[165] Si vedano per esempio M.H. Chang (1991), *The Effects of Product Differentiation on Collusive Pricing, in «International Journal of Industrial Organization»*, 9, pp. 453-469; M. Helfrich e F. Herweg (2016), *Fighting Collusion by Permitting Price Discrimination, in «Economics Letters»*, 145, pp. 148-151; e Q. Liu e K. Serfes (2004), *Quality Information and Oligopolistic Price Discrimination, in «Journal of Economics & Management Strategy»*, 13, pp. 671-702.

alternativa, si possono considerare gli algoritmi come delle pratiche facilitanti[166] o come scambio di informazione violativi dell'art. 101 TFUE[167];

3. sempre *ex post* c'è chi applica l'art 102 TFUE e quindi l'abuso della posizione collettiva dominante. In questo terzo caso, occorrerebbe però dimostrare che i prezzi siano paralleli e che vi sia il livello ultra-competitivo dei prezzi stessi[168];
4. tra le proposte più moderne, c'è quella che suggerisce una *compliance by design* (una regolamentazione che si fonda sul *design* dell'algoritmo o sulla trasparenza dello stesso[169]), sulla farsa riga di quello che accade in materia di protezione dei dati personali - ovvero
5. altri propongono di agire direttamente sul mercato: proponendo l'inserimento di *policies* che lo destabilizzino, riducendo la trasparenza e la frequenza delle interazioni tra gli algoritmi stessi, o facilitando l'entrata di nuovi concorrenti nel mercato[170];
6. infine, lo scenario più futuristico è quello che vede l'introduzione delle c.d. contromisure "*smart*", le quali consisterebbero nell'utilizzo di algoritmi da parte delle *autorithies* o da parte degli stessi consumatori (c.d. consumatore algoritmico).

La Commissione europea parla di *New Competition Tool - NCT*[171] con riferimento a nuovi strumenti e rimedi regolamentari diversi da quelli tradizionali, e quindi non sanzionatori, di cui le autorità avrebbero bisogno al fine di fronteggiare i nuovi problemi strutturali, non legati a condotte e non fronteggiabili con gli artt. 101 e 102 TFUE. Però, questi nuovi strumenti possono eventualmente operare solo per quegli algoritmi considerati come parti della stessa struttura, e non come parte di *meeting of minds.* Infatti, in quest'ultimo caso, è difficile applicare l'art. 101 TFUE dato che non ci può essere intesa tra sé e sé.

Con riferimento a questi nuovi strumenti, vi sono problematiche di tipo procedurale non da poco che vanno tenute in considerazione dalla Commissione.

Per ragioni di certezza del diritto è necessario chiarire in anticipo la *policy* che le imprese devono

---

[166] Sull'annoveramento dello scambio di informazione nelle c.d. patiche facilitanti cfr. M. LIBERTINI, Concorrenza, in Enc. dir., Annali III, Milano, Giuffrè, 2010, 119 e 216 ss.

[167] L. CALZOLARI, op.cit., 227.

[168] Tale opinione è stata autorevolmente sostenuta dal *Department of Justice* degli Stati Uniti, secondo cui «*the implementation of pricing policies by one firm's employees is unilateral conduct (whether it factors in the prices of competitors or not) and is not actionable under Section 1 of the Sherman Act without evidence establishing an agreement with another firm over the purpose or effect of a pricing algorithm*» (cfr. *Algorithms and Collusion – Note by the United States*, OECD Roundtable on Algorithms and Collusion, 2017, § 6).

[169] Così A. MASTRORILLI op.cit., 350.

[170] Così AGCM, AGCOM, Garante per la protezione dei dati personali, Indagine conoscitiva sui Big Data, p.114

[171] European Commission, The New Competition Tool: its institutional set-up and procedural design, 2020.WHISH, *New Competition Tool: Legal comparative study of existing competition tools aimed at addressing structural competition problems, with a particular focus on the UK's market investigation tool, Study for the EU Commission, 2020;* LAROUCHE/DE STREEL, *Interplay between the New Competition Tool and Sector-Specific Regulation, Study for the EU Commission, 2020; and Fletcher, Market Investigation for Digital Platforms: Panacea or Complement, ccp Working Paper, 2020, p. 9, available on ssrn.com*

attuare per evitare di essere sanzionate dalle autorità.

Nella già citata conferenza ICN si è svolta anche la sessione plenaria del gruppo di lavoro sui cartelli (*Cartel Working Group* o CWG); questa è stata dedicata proprio alle questioni legate alle nuove forme di collusione basate sull'elaborazione dei *Big Data* grazie all'uso di algoritmi e intelligenza artificiale. La sessione ha messo in evidenza che non c'è consenso sulla rilevanza di tale fenomeno, mentre molte autorità di concorrenza sono ancora in una fase di apprendimento. Ad esempio, in maniera non dissimile da quanto già fatto in Italia dall'AGCM, il DOJ americano, sul fronte degli appalti pubblici, ha creato un coordinamento con le stazioni appaltanti e il *Federal Bureau of Investigation* (FBI), per l'uso di tecniche di analisi dei dati per l'individuazione di fenomeni collusivi. Tuttavia, dalla discussione non sono ancora emersi orientamenti su come le autorità intendano affrontare le questioni riguardanti: la responsabilità *antitrust*, lo standard valutativo, l'onere probatorio e la garanzia dei diritti di difesa nei casi che coinvolgono l'uso di algoritmi intelligenti da parte delle imprese.

2.4 Riflessioni finali

Fino ad oggi l'approccio *antitrust* alle questioni concorrenziali sollevate dai *Big Data* è stato: da una parte, dell'applicazione *case by case* di principi e regole generali sulla concorrenza (come nel caso europeo Google del 2017[172]), in linea con il *self-regulatory approach* adottato per tutto il mondo di Internet[173];dall'altra parte, di studio e di ricerca di nuovi strumenti valutativi e di *enforcement*[174], attraverso le numerose indagini conoscitive[175] e i report delle Autorità (europee e non) sull'impatto dei *Big Data* sulla concorrenza[176].

Le caratteristiche dell'economia digitale richiedono, come si è visto, la ricerca di un nuovo equilibrio tra il rischio di scoraggiare i processi innovativi e il rischio di *under-enforcement*.

Inoltre, non minori difficoltà sono quelle legate alla globalizzazione dei mercati digitali in contrasto con l'assenza di una regolamentazione uniforme e di strumenti globali di *enforcement*[177], dovendo anche fare i conti con il principio di territorialità che circoscrive le competenze delle autorità nazionali

[172] Commissione Europea (2017), "AT.39740 Google Search (Shopping)", http://ec.europa.eu/competition/anti-trust/cases/dec_docs/39740/39740_14996_3.pdf.

[173] Con riferimento all'autoregolamentazione degli utenti nella rete Internet cfr. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.*, 2012, 135 ss. spec. 142.

[174] Cfr. *ex multis* European Commission, *The New Competition Tool: its institutional set-up and procedural design*, 2020

[175] Cfr. *ex multis* AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020.

[176] Senza pretesa di esaustività si rinvia sommariamente ai seguenti Report: *Big data and differential pricing, by The Executive Office of the President of the US*, February 2015, disponibile su http://obamawhitehouse.archive.gov; UK Competition & Markets Authority Report (CMA38, June 2015), *The commercial use of consumer data*, in www.gov.uk; Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights, *Latest White House Report on Big Data*, 4th May 2016; il US Federal Trade Commission Report (January 2016), *Big Data. A tool for Inclusion or Exclusion?* in www.ftc.gov; il Report congiunto *dell'Autorité de la Concurrence* francese e del *Bundeskartellamt* tedesco, *Competition Law and Data*, May 10 th, 2016, in www.autoritedelaconcurrence.fr/doc/reportcompetitionlawdatafinal.pdf.

[177] A tal proposito cfr. PITRUZZELLA, *L'applicazione delle regole di concorrenza nel mercato globale: istanze di tutela, sfide ed opportunità*, in Benacchio-Carpagnano (a cura di), *L'applicazione delle regole di concorrenza in Italia e nell'Unione Europea*, Napoli, 2015, 1 ss.

in ambiti talvolta più ristretti rispetto a quelli di operatività delle piattaforme digitali.

A tal proposito, non mancano soluzioni volte ad affermare la competenza delle autorità nazionali anche di fronte a modelli di *business* attivi su scala mondiale, come si è scelto per legge di fare in Germania[178].

La constatazione delle conseguenze plurioffensive derivanti dal trattamento massivo di dati personali da parte delle imprese sta spingendo alcune Autorità e alcuni interpreti a promuovere un diverso approccio nell'*enforcement* di *privacy* e *antitrust*, che si potrebbe definire come combinato e sinergico.

In questo ambito è stata avanzata l'idea di considerare i "*personal data as a new antitrust tool*"[179] : i) utilizzando il numero degli utenti di una piattaforma (che forniscono spontaneamente i propri dati personali) come indicatore del potere di mercato delle imprese – alternativo al calcolo delle quote in base al fatturato – o quanto meno come parametro di valutazione della capacità di un'impresa di intaccare la concorrenza[180];ii) creando efficaci meccanismi d'integrazione delle procedure di *antitrust* e *privacy*, che potrebbero concretizzarsi in pareri obbligatori (vincolanti o non vincolanti) dell'Autorità di protezione dei dati personali, sia all'interno di istruttorie *antitrust* (sulle concentrazioni, intese e abusi di posizione dominante che coinvolgano imprese proprietarie di *data-set*), sia come condizioni per l'autorizzazione delle concentrazioni, come ad es. l'assunzione di impegni relativi al trattamento, trasferimento e riuso dei dati personali[181].

Sembrano andare in quest'ultima direzione anche le posizioni dell'AGCM e del *Bundeskartellamt*, rispettivamente la prima per avere avviato e pubblicato un'indagine conoscitiva sui Big Data congiuntamente al Garante per la protezione dei dati personali ed all'AGCom (Autorità per le Garanzie nelle Comunicazioni)[182], la seconda per aver espresso questa scelta prima nel *report* congiunto con *l'Autorité de la Concurrence*, poi in un *paper*[183], e infine nella già menzionata istruttoria per abuso di mercato condotta contro Facebook per violazione del Regolamento generale sui dati personali, nella quale ha scelto di farsi affiancare dall'Autorità tedesca per la protezione dei dati personali e dalle associazioni dei consumatori.

E sembra abbia dato segnali in tal senso anche la Commissione Europea nel caso di acquisizione

---

[178] In particolare, si fa riferimento al § 18.2, del GWB: «*Der räumlich relevante Markt kann weiter sein als der Geltungsbereich dieses Gesetzes*».

[179] MERIANI, *Digital platforms and spectrum of data protection in competition law analyses*, in ECLR, 2017, vol. 38, Issue 2, 93.

[180] Cfr. STAKHEYEVA-TOKSOY, *Merger control in the Big Data world: To be or not to be Revisited*? in ECLR, 2017, vol. 38, Issue 6, 270.

[181] *Id*., 270.

[182] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020.

[183] *Bundeskartellamt Paper, Big data und Wettbewerb*, Oktober 2017, 9-11, reperibile su http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2017/06_10_2017_Schriftenreihe_Digitales.html [accesso del 18.10.2017].

Microsoft/LinkedIn, autorizzata a dicembre 2016[184].

A quest'ultimo approccio si dovrà prestare sempre maggiore attenzione, d'ora in poi, non solo perché appare coerente con le esperienze del passato di applicazione del diritto *antitrust* a settori speciali sottoposti a vigilanza delle diverse autorità di settore (e.g. comparto bancario, assicurativo, radio-televisivo ecc.), ma anche perché la casistica internazionale sopra esposta ha dimostrato il fallimento delle posizioni "autonomistiche" espresse in passato, e una tendenza crescente alla disattenzione verso la tutela della *privacy* da parte delle piattaforme digitali.

Inoltre, anche i casi analizzati di sfruttamento abusivo della dominanza nei mercati digitali, specie se conseguenti a fenomeni concentrativi, testimoniano una certa contiguità e convergenza tra la disciplina della concorrenza e quella della *privacy*. Ciò richiede – nel caso in cui rilevanti violazioni nel trattamento dei dati personali integrino, al contempo, abusi del potere di mercato –non solo un ripensamento degli obiettivi e delle priorità *antitrust*, ma anche un approccio integrato e sinergico dei rispettivi problemi, per una maggiore efficacia dell'azione delle diverse autorità coinvolte e per evitare pericolosi vuoti applicativi.[185]

A tal proposito, dunque, potrebbe risultare opportuna l'adozione della funzione del *consumer welfare* quanto meno nella sua accezione negativa della prevenzione di un "danno al consumatore", già prescelta dalla Corte di Giustizia, in diverse pronunce sugli abusi di sfruttamento come anche sulle intese; tale accezione negativa valuta la presenza (effettiva o potenziale) di "fallimenti del consumatore", almeno come elemento sintomatico di un illecito antitrust[186].

In questo modo, la tutela dei dati personali potrebbe diventare uno strumento del diritto *antitrust*, efficace per l'emersione e la repressione delle più diverse pratiche abusive[187]; tanto più se si considerano i molti condizionamenti (involontari e irrazionali) che limitano la razionalità delle scelte di consumo degli utenti dei mercati digitali "iperconnessi", che sono spesso vittime di l*ock-in e bias*[188].

Le autorità di concorrenza sono consapevoli del fatto che l'attività di profilazione – resa possibile dall'acquisizione di una grande mole di dati - può agevolare comportamenti abusivi idonei a ridurre la contendibilità degli ecosistemi delle principali piattaforme, rendendo persistente il loro potere di mercato. In particolare, in ragione della natura multisettoriale dell'economia digitale e della presenza di grandi operatori digitali attivi su più mercati, la definizione del mercato rilevante ai fini

[184]Commissione Europea (2016), "*M.8124 Microsoft/Linkedin",* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf , par. 345.

[185] ZENO-ZENCOVICH, *Internet e concorrenza*, in *Dir. inf.*, 2010, 697 ss. spec. 704.

[186] C. OSTI, *La tutela del consumatore tra concorrenza e pratiche commerciali scorrette*, in Catricalà-Gabrielli (a cura di) *I contratti nella concorrenza, Trattato dei contratti* Rescigno - Gabrielli, Torino, Utet, 2011, 425 ss. spec. 437-442.

[187] ROSSI, *Social network e diritto antitrust*, in AIDA, 2011, 83.

[188] DI PORTO, *Dalla convergenza digitale-energia l'evoluzione della specie: il consumatore «iper-connesso»*, in *Merc. conc. reg.*, 2016, 67, spec. 68-77.

dell'accertamento del potere di mercato potrebbe essere ripensata, talvolta tenendo significativamente in considerazione anche altri elementi.

Da una parte, come sostengono alcuni[189], è vero che la grande concentrazione delle piattaforme digitali porti a aumentare il benessere del consumatore, che acquista così il prodotto a lui più congeniale e in totale comodità; dall'altra parte, è altrettanto vero che i *Big Tech* dovrebbero consentire alle altre imprese più deboli di operare senza barriere all'entrata e in modo da guadagnarsi, anche loro, la parte di mercato che gli spetta sulla base dei rispettivi meriti e capacità.

Credo infine che l'unico modo per unire le due parti della medaglia sia intervenire con strumenti di natura regolamentare.

È necessaria, inoltre, un'intesa tra l'Unione europea e gli Stati uniti sul tipo di regolamentazione da attivare (*ex ante o ex post*) e sull'atteggiamento delle diverse autorità competenti.

Guardando alla questione in un'ottica *antitrust*, non vi è dubbio che non ogni violazione della *privacy*, posta in essere da un'impresa in posizione dominante, rappresenta un illecito concorrenziale. Dobbiamo allora chiederci in quali circostanze è suscettibile di integrare un abuso e quali rimedi andrebbero richiesti.

La scelta dei rimedi è centrale in quanto può conformare lo sviluppo dei mercati interessati in modo significativo. In tale contesto, ci si chiede se i mercati digitali richiedano un diverso approccio - per la difficoltà di disegnare rimedi appropriati in mercati nascenti dagli sviluppi imprevedibili - e se ci sia spazio per eventuali rimedi strutturali, oltre a quelli comportamentali. Nei mercati digitali, un semplice ordine di cessare la condotta anti-competitiva può non essere sufficiente, ma, allo stesso tempo, le autorità possono non avere ancora acquisito gli strumenti adatti per intervenire senza la collaborazione delle imprese oggetto di istruttoria.

Infatti, a ben vedere, nei casi che si basano sulla imposizione illecita di un determinato utilizzo dei dati personali - reso possibile dalla particolare posizione di mercato dell'impresa in questione - la soluzione potrebbe essere quella di richiedere una maggiore informativa e un corretto modo di acquisizione del consenso, senza dover ricorrere al diritto *antitrust*.

D'altra parte, tanto più i consumatori sono informati e consapevoli in relazione alle proprie scelte di consumo, tanto più le imprese possono concorrere tra loro, differenziando le proprie offerte di servizi digitali in relazione al diverso grado di utilizzo dei dati personali.

Occorrerà inoltre vedere: i) intelligenza arti, come verranno recepite le proposte del *Digital Markets Act; ii)* in Cina, se verrà confermato il contenuto delle *"Draft Guidelines"*; e *iii)* negli Stati Uniti, come la nuova amministrazione Biden intenderà fronteggiare le condotte delle grandi piattaforme digitali, e se le agenzie americane (DOJ e FTC) continueranno ad essere critiche nei confronti di una

[189] B. THOMPSON, *Aggregation Theory*, in https://stratechery.com/aggregation-theory/.

regolazione *ex ante*.

Sotto il profilo dell'*enforcement*, considerata la velocità con cui cambia la realtà in esame, va sicuramente migliorata la tempistica dei procedimenti, per evitare che i tempi dell'economia non siano al passo con quelli del diritto.

Occorre che l'intervento *antitrust* arrivi tempestivamente e non a distanza di anni, in un contesto in cui i mercati sono ormai già significativamente mutati[190].

A tal proposito, l'Europa, con il *Digital Markets Act* e mediante una regolazione *ex ante*, si propone di: i) accorciare i tempi di intervento delle autorità, limitando o, addirittura, prevenendo i danni delle condotte anticoncorrenziali; ii) fornire maggiore trasparenza e maggiori dettagli sul funzionamento del mercato digitale e delle piattaforme che vi operano; iii) consentire un intervento mirato sui *gatekeeper*; iv) permettere alle autorità di raccogliere più dati sulle possibili condotte anticoncorrenziali, in quanto le piattaforme *online* sono restie a condividere i dati sul proprio funzionamento.

Nel frattempo, le autorità di concorrenza, come quella italiana, che godono delle doppie leve (antitrust-tutela dei consumatori) stanno intervenendo con gli strumenti in materia di tutela del consumatore, con i quali hanno senz'altro il vantaggio di avere procedimenti rapidi, che si concludono in pochi mesi. In altri termini, trattare la materia con gli strumenti della tutela del consumatore e delle pratiche commerciali scorrette, come si vedrà nel terzo capitolo, consente ad oggi un intervento più celere e tempestivo.

[190] Cfr. caso Intel, deciso dalla Commissione nel 2009, e in cui sono trascorsi 10 anni tra l'avvio, nel 2007, e la pronuncia della Corte di Giustizia che nel 2017 ha annullato la decisione.

CAPITOLO III

La disciplina delle pratiche commerciali scorrette nell'economia digitale e la complementarità con la disciplina della *privacy*

Sommario: *Premessa* **3.1** *– Un breve cenno agli Stati Uniti* **3.2** *Il quadro europeo e alcune iniziative della Commissione in materia di PCS e tutela dei consumatori* **3.3** *L'applicabilità della disciplina PCS nel caso di contratti senza esborso monetario* **3.4** *– I c.d. prezzi personalizzati* **3.5** *Segue – Le convergenze tra tutela del consumatore e protezione dei dati personali* **3.6** *– Un approfondimento sul caso Facebook in Italia e la sentenza del TAR* **3.7** *– I diversi strumenti utilizzati da altri Paesi europei e dal Regno Unito* **3.8** *– Le class action e il private enforcement* ***3.9*** *– Conclusioni*

Premessa

Nel capitolo precedente si è visto come il diritto *antitrust* non sempre sia lo strumento più efficiente per contrastare gli abusi commessi da parte dei giganti dell'economia digitale; in particolare, gli strumenti della tutela del consumatore sembrano fornire ad oggi una tutela più celere ed immediata.
Infatti, da una parte, il diritto *antitrust* si occupa dell'offerta di prodotti e servizi da parte delle imprese, dall'altra, la tutela dei consumatori e la *disclosure regulation*[1] si avvicinano ai mercati dal lato della domanda, garantendo che i consumatori siano in grado di informare consapevolmente le loro scelte. In altre parole, la seconda completa l'azione della prima.
La tutela del consumatore può intervenire su molti profili connessi al rapporto tra le piattaforme digitali e gli utenti nella fase di acquisizione, elaborazione e trattamento dei dati. A tal proposito, occorre ricordare che una parte importante del fascio di disposizioni a tutela del consumatore sono rappresentate dalle norme che difendono i consumatori dalle c.d. pratiche commerciali scorrette (di seguito PCS)[2], come ad esempio quelle ingannevoli[3].

[1] F. DI PORTO, *La regolazione degli obblighi informativi*, Napoli, Editoriale Scientifica, 2017.
[2] In termini generali, Ai sensi dell'art. 20 cod. cons. pratica commerciale è scorretta quando ricorrono due condizioni: i) è contraria alla diligenza professionale; ii) è idonea "*a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta o del membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori".* In dottrina cfr. SCOGNAMIGLIO, *Le pratiche commerciali sleali: disciplina dell'atto o dell'attività?* in C. RABITTI BEDOGNI – P. BARUCCI (a cura di), *20 anni di antitrust. L'evoluzione dell'Autorità garante della concorrenza e del mercato*, Torino, 2010, vol. II; F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, I, p. 106; MELI, *Diligenza professionale, consumatore medio e regola di de minimis nella prassi dell'AGCM e nella giurisprudenza amministrativa* in www.orizzontideldirittocommerciale.it; T. BROGGIATO, *La tutela del consumatore nel rinnovato contesto*, in *Fintech: diritti, concorrenza e regole*, a cura di G. Finocchiaro e V. Falce, Zanichelli, 2019.
[3] La categoria speciale delle pratiche ingannevoli (artt. 21 e 22 cod. cons.) prevede le condotte che inducono il consumatore a prendere una decisione che altrimenti non avrebbe preso, quelle che forniscono informazioni non vere oppure che, pur divulgando informazioni vere, inducono comunque il consumatore in errore, oppure creino confusione,

In altri termini, secondo la disciplina delle PCS, le piattaforme digitali non devono ingannare i consumatori su aspetti che possono incidere sulle loro decisioni di natura commerciale, e non devono occultare l'intento commerciale della pratica. Di conseguenza, se il consumatore non viene informato dal professionista sul fatto che i dati, che è tenuto a fornire per accedere al servizio, saranno usati a fini commerciali o che i prezzi del prodotto o servizio offerto sono personalizzati, potrebbero esserci gli estremi per applicare la disciplina delle PCS.

Possono altresì venire in rilievo condotte di carattere aggressivo, ove risulti che il professionista abbia operato indebiti condizionamenti nella scelta del consumatore, inducendolo a fornire i propri dati per usufruire del servizio. In altre parole, le clausole dei contratti siglati dai consumatori potrebbero essere valutate non solo come pratiche ingannevoli[4], ma anche in relazione alle regole riguardanti le pratiche aggressive[5]: trattasi di quelle condotte che – mediante molestie, coercizione o indebito condizionamento – sarebbero dirette a limitare in modo rilevante la libertà di scelta dei consumatori, inducendoli a prendere una decisione di acquisto che non avrebbero altrimenti preso.

L'indebito condizionamento del comportamento economico del consumatore non si configura dunque solo quando la piattaforma digitale sfrutta a proprio vantaggio condizioni di debolezza emotiva del consumatore, ma anche quando l'impresa non adempie agli obblighi informativi verso il consumatore idonei a consentire a quest'ultimo di compiere una scelta consapevole. In tal senso, come si vedrà in seguito, depongono due provvedimenti, nei quali l'AGCM ha applicato la disciplina delle PCS, nonché gli articoli del Codice del Consumo in materia di clausole vessatorie per sanzionare le condizioni imposte da WhatsApp, fornitore di un servizio di messaggistica istantanea[6].

Un problema analogo emerge con riferimento alla disciplina in materia di *privacy*, che prevede che

---

o siano contrarie alle regole di un codice di condotta al quale il professionista dichiara di aver aderito. Inoltre, ai sensi dell'art. 22, secondo comma, Cod. Cons., costituisce un'omissione ingannevole anche il caso del professionista che ometta di dichiarare il proprio intento commerciale in quei casi in cui lo stesso non è evidente. Sul tema cfr. R. CALVO, *Le omissioni ingannevoli 179*, Giovanni De Cristofaro (a cura di), *Le pratiche commerciali sleali tra imprese e consumatori. La direttiva 2005/29/Ce e il diritto italiano* (2007) e V. MELI, *Le pratiche sleali ingannevoli 87*, Anna Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette* (2008).

[4] Ai sensi dell'art. 21 Cod. Cons., per pratica commerciale ingannevole si intende: *"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 caso, lo induce o è idonea a indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".*

[5] Ai sensi dell'art. 24 Cod. Cons. è aggressiva quella 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*". In dottrina cfr. L. DI NELLA, Le pratiche commerciali sleali aggressive 215, Giovanni De Cristofaro (a cura di), *Le pratiche commerciali sleali tra imprese e consumatori. La direttiva 2005/29/Ce e il diritto italiano* (2007); G. DALLE VEDOVE, Le pratiche commerciali aggressive 117, Anna Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette* (2008); e M.A. CARUSO, Le pratiche commerciali aggressive, 2010.

[6] Cfr. Provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597 e cfr. Provvedimento AGCM CV154, – WhatsApp – Clausole Vessatorie, 11 maggio 2017 n. 26596, in Boll. 18/2017.

gli interessati abbiano informazioni sufficienti per poter dare il loro consenso al trattamento dei dati personali[7].

Però, il fatto che alle condotte delle imprese sia applicabile la normativa in materia di protezione dei dati personali, non le esonera dal rispettare la disciplina in materia di PCS, ponendosi le due discipline come complementari e non alternative[8]; le due discipline dunque si sovrappongono. Tale sovrapposizione attiene: al livello di trasparenza garantito, all'accuratezza delle informazioni presentate ai consumatori, nonché alla necessità che tali informazioni siano comprensibili.

La disciplina a tutela dei consumatori e quelle a tutela della *privacy* sono quindi componenti importanti ai fini di una concorrenza leale.

Le condotte finalizzate all'acquisizione del consenso alla condivisione dei dati personali – nel caso i dati siano utilizzati per fini commerciali, da parte di piattaforme digitali che si rivolgono a consumatori – possono integrare una PCS; quando una piattaforma non comunica agli utenti che i loro dati personali sono trattati per finalità economiche, essa omette informazioni rilevanti, utili per l'utente interessato a prendere una decisione consapevole di natura commerciale.

A tal proposito, la Commissione europea, negli orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle PCS, ha evidenziato come la violazione della normativa in materia di *privacy* possa rilevare ai fini della valutazione del carattere illecito di una condotta[9].

Tuttavia, tra la disciplina a tutela dei dati personali e la disciplina sulle PCS vi sono differenze sostanziali: nella prima, si guarda essenzialmente alle modalità e alla procedura di acquisizione del consenso e di trattamento dei dati; nella seconda, invece, il campo di indagine è più ampio, con la possibilità di esaminare più in generale la correttezza della condotta del professionista nella relazione commerciale con il consumatore, anche con riferimento ai dati richiesti. Quest'ultima può quindi risultare di aiuto nel limitare quello che è stato definito "abuso del consenso" in materia di *privacy*.

---

[7] Ciò è implicito nella direttiva sulla protezione dei dati personali e esplicito nella direttiva sulla e-privacy, artt. 6.3 e 9.1 relativi al trattamento dei dati in relazione al traffico e all'ubicazione da parte di servizi di comunicazione elettronica accessibile al pubblico.

[8] Sul punto cfr. S. GOBBATO, "*Big data" e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo* in *Rivista di diritto dei media*, 2019, fasc. 3, pp. 148-161; D'IPPOLITO, *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali personali* in A.A. Vv, *Consumerism 2019. Dodicesimo rapporto annuale. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?* Consumer's Forum e Università degli studi Roma Tre, 2020, 70 ss., spec. 73, disponibile in *https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf.* In giurisprudenza, cfr. *ex multis* TAR Lazio, sez. I, sentenza 18 dicembre 2019 – 10 gennaio 2020, n. 261.

[9] In particolare, "*la violazione, da parte di un professionista, della direttiva sulla protezione dei dati o della direttiva relativa alla vita privata e alle comunicazioni elettroniche non sempre significa, di per sé, che la pratica costituisca anche una violazione della direttiva sulle pratiche commerciali sleali. Tuttavia la violazione delle norme in materia di protezione dei dati andrebbe presa in considerazione quando si valuta il carattere sleale di una pratica commerciale ai sensi di quest'ultima direttiva, in particolare nel caso in cui il professionista esegua il trattamento dei dati dei consumatori in violazione degli obblighi in materia di protezione dei dati, cioè a fini di invio di materiale pubblicitario o per qualsiasi altra finalità commerciale, come la profilazione, i prezzi personalizzati o le applicazioni relative ai megadati".*

Da una parte, infatti, si ritiene che il consenso dell'utente costituisca un elemento sufficiente per il trattamento dei dati; dall'altra parte, però, l'utente non sempre comprende appieno l'estensione del consenso che gli è richiesto.

Come abbiamo visto già nel secondo capitolo, tenuto conto delle grandi dimensioni di molti operatori attivi nell'economia digitale, intervenire sul piano sanzionatorio con un aumento del massimo edittale è solo una delle strade percorribili; in questa direzione va ad esempio il *Digital Markets Act* (di seguito anche DMA).

La questione della potenziale efficacia degli strumenti di tutela del consumatore è ampiamente trattata negli studi economici più recenti che analizzano i mercati *data-driven.*

Secondo tali studi, infatti, la tutela del consumatore contribuirebbe a risolvere le inefficienze derivanti: i) dal valore pari a zero del prezzo e; ii) dalla mancanza di consapevolezza da parte degli utenti relativamente alla fornitura dei loro dati alle piattaforme digitali[10]. A tal proposito, sono di rilievo le condizioni di fruizione dei servizi offerti gratuitamente all'interno di una piattaforma digitale.

In Italia, l'AGCM è intervenuta in più occasioni nel sistema della "*data driven economy"* con azioni di *enforcement* del Codice del Consumo; in particolare, come si vedrà, l'autorità è intervenuta nei confronti di WhatsApp e Facebook, per tutelare i consumatori, soprattutto quelli fruitori di servizi digitali "pagati" con i dati personali. Nello specifico, l'Autorità ha ritenuto che i modelli commerciali incentrati sulla raccolta e l'elaborazione dei dati – anche quando l'utente riceve il servizio senza dover pagare un corrispettivo in termini monetari – rientrano nella nozione di attività economica ai sensi del diritto europeo. A tal fine, l'Autorità, dando concreta attuazione a principi ormai consolidati – sia a livello europeo che internazionale – ha interpretato estensivamente il concetto di rapporto di consumo, riconoscendo la natura economica del comportamento dell'utente, anche in relazione alle piattaforme digitali che offrono gratuitamente servizi. A questo riguardo, l'Autorità ha ritenuto ingannevole la schermata di registrazione di Facebook, nella quale mancava un'adeguata e immediata informazione circa le finalità commerciali della raccolta dei dati dell'utente, e ha ritenuto aggressive le modalità con cui la piattaforma procedeva all'acquisizione del consenso per lo scambio, per fini

[10] Cfr. AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020, 5, dove in sintesi: "*è stato rilevato che circa 6 utenti su 10 non solo sono consapevoli di generare, con le loro attività online, dati utilizzabili per attività di profilazione, ma anche che essi appaiono informati dell'elevato grado di pervasività dei sistemi di raccolta (es. geo-localizzazione, accesso a funzionalità come la rubrica, il microfono e la videocamera) e della possibilità di sfruttamento dei dati da parte delle imprese. Nel complesso è risultato che 4 utenti su 10 sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio. Dal sondaggio è emerso altresì che solo 1 utente su 10 è consapevole dei propri diritti in materia di portabilità dei dati e che circa la metà degli utenti mostra interesse ad ottenere una copia dei propri dati. Il basso interesse all'utilizzo della portabilità è dovuto alla scarsa propensione ad utilizzare altre piattaforme/applicazioni (41,1%), ad una limitata sensibilità sulla rilevanza di tali dati (36,1%), nonché alla percezione di un'elevata complessità degli strumenti tecnologici (30,4%).*"

commerciali, di dati dei propri utenti con siti *web* o *app* di terzi[11].

Sul punto, come vedremo, il giudice di prime dure ha però confermato il provvedimento dell'autorità solo con riferimento al profilo dell'ingannevolezza, in violazione degli artt. 21 e 22 del Codice del Consumo, per aver Facebook ingannevolmente indotto gli utenti consumatori a registrarsi sulla sua piattaforma, non informandoli adeguatamente e immediatamente, in fase di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti e, più in generale, delle finalità remunerative che sottendono la fornitura del servizio di social network enfatizzandone la sola gratuità. Alla luce di quanto precede, l'Autorità ha vietato l'ulteriore diffusione della pratica commerciale e, con il medesimo provvedimento, ha disposto la pubblicazione da parte di Facebook di una dichiarazione rettificativa, ai sensi dell'articolo 27, comma 8, del Codice del Consumo.

L'impresa, pur essendosi impegnata per allinearsi alle indicazioni dell'autorità, a detta di quest'ultima la pratica commerciale presenta tuttora il medesimo profilo di scorrettezza già accertato.

Inoltre, FB non ha pubblicato la dichiarazione rettificativa e, in sede di ricorso avverso la delibera del 29 novembre 2018, n. 27432, ha sostenuto l'esistenza di insormontabili difficoltà tecniche nella pubblicazione secondo le modalità indicate nello stesso provvedimento. Il TAR Lazio, nelle sentenze nn. 260/2020 e 261/2020, ha stabilito che quanto alle paventate difficoltà tecniche *"si tratta di questioni di carattere interpretativo che … potranno essere affrontate dalla parte e dall'Autorità in sede di verifica dell'ottemperanza al provvedimento stesso, entro il cui ambito l'Agcm sarà tenuta a fornire a Facebook ogni chiarimento necessario per consentire una compiuta esecuzione della misura*".

Pertanto, con provvedimento del 21 gennaio 2020, n. 28072, l'Autorità ha avviato un ulteriore procedimento, contestando a Facebook di aver violato la diffida di cui alla lettera a) del dispositivo della delibera del 29 novembre 2018, n. 27432, nonché l'obbligo di pubblicazione della dichiarazione rettificativa. Quest'ulteriore procedimento si è concluso con un provvedimento pubblicato il 17 febbraio 2021[12], con il quale l'autorità ha sanzionato per complessivi 7 milioni di euro Facebook Ireland Ltd. e la sua controllante Facebook Inc., per non aver attuato quanto prescritto nel provvedimento emesso nei loro confronti nel novembre 2018.

La tutela del consumatore può dunque intervenire, anche nella fase di acquisizione dei dati, su molti profili connessi al rapporto tra operatori e utenti. Tale intervento è mirato non solo a fornire una tutela diretta ai consumatori, ma anche a svolgere un ruolo pro-competitivo, nella misura in cui gli utenti sono posti nella condizione di esercitare in modo più consapevole e attivo le proprie scelte di consumo: pertanto, quanto più i consumatori sono informati, consapevoli e liberi nelle loro scelte,

[11] Cfr. Provvedimento AGCM PS11112 - Facebook-Condivisione dati con terzi, 29 novembre 2018 n. 27432.
[12] Provv. AGCM, IP330 del 17 febbraio 2021.

tanto più le imprese sono propense a competere tra di loro, differenziando le proprie offerte di servizi digitali gratuiti in relazione alla qualità nella forma di *privacy*.

Ad esempio, come si vedrà nel prosieguo, la tutela del consumatore e la disciplina sulle PCS può avere oggi un ruolo importante nel trattare i rischi derivanti dai prezzi personalizzati[13].

3.1 – Un breve cenno agli Stati Uniti

La regolamentazione americana, a differenza di quella europea, si è sempre più concentrata sugli interessi delle imprese, piuttosto che sugli interessi dei consumatori.

La *Federal Trade Commission* – FTC è l'agenzia preposta alla tutela dei consumatori e alla valutazione sulla legittimità delle pratiche commerciali delle imprese.

Infatti, la Section 5 del *Federal Trade Commission Act* – FTCA del 1914, intitolata "*Unfair methods of competition unlawful"*, prevede che la FTC può esprimersi sulla dichiarazione di illiceità delle pratiche commerciali scorrette. In particolare, il FTCA concedeva all'agenzia non solo il potere di dare una definizione di *unfair methods of competition,* ma anche quello di proibire tali pratiche qualora ritenesse che esse potessero falsare il commercio.

Ebbene, nei primi cento anni dall'approvazione del FTCA (dal 1914 al 2014), la FTC ha emanato solo una norma regolamentare contenente una definizione di *unfair methods of competition*[14].

Solo nel 2015, infatti, la FTC ha emanato una raccolta di "*Enforcement Principles*" in cui ha affermato che gli *unfair methods of competition* dovessero essere guidati dalla *promotion of consumer welfare;* un obiettivo di *policy* assente da qualsiasi orientamento legislativo della *FTC.*

Peraltro, dall'adozione di questa raccolta, la FTC ha condotto, utilizzando la Section 5, solo un caso[15].

Tuttavia, il Congresso americano, nel rapporto intitolato "*Investigation of Competition in the Digital Marketplace: Majority Staff Report and Recommendations*[16]*"* – pubblicato nell'ottobre 2020, agli esiti di una lunga investigazione (durata più di 16 mesi) sulla concorrenza in materia di economia digitale – ritiene che le agenzie americane (FTC e DOJ) abbiano fallito nell'utilizzare i loro poteri nei confronti dei giganti tecnologici, anche con riferimento alle *unfair methods of competition*. A tal riguardo, nell'esito dell'indagine, il Congresso ha sottolineato come la FTC sia stata istituita anche al fine di fronteggiare le *unfair methods of competition* e per studiare le *business practices*[17].

---

[13] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020, p. 101-102.

[14] *Discriminatory Practices in Men's and Boys' Tailored Clothing Industry*, 16 C.F.R. pt. 412 (1968).

[15] *Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act* (Aug. 13, 2015), https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

[16] Il rapporto in questione è disponibile su https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

[17] S. REP. NO. 63-597, 13 (1914) ("*The committee gave careful consideration to the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce and to forbid [them] . . . or whether it would, by a general declaration condemning unfair practices, leave it to the commission to determine what practices were unfair. It concluded that the latter course would be better, for the reason . . . that there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others*.").

A tal proposito, nel rapporto condotto dalla sottocommissione Antitrust del Congresso americano si raccomanda la FTC di rafforzare le sanzioni per le violazioni delle regole sull' *unfair methods of competition* e di creare una maggiore simmetria con le disposizioni sull' *unfair or deceptive acts or practices.*

In particolare, con riferimento a Google, la sottocommissione Antitrust, alla luce di diverse interrogazioni, ha preso atto di come l'impresa fosse coinvolta in pratiche commerciali scorrette.

Google, tramite *Google Search,* era già il primo motore di ricerca esistente, ma la società, quando nel 2008 ha lanciato Google Chrome, ha iniziato a pubblicizzare e promuovere quest'ultimo in bella vista sulla *homepage* di Google.com, con l'intento di farlo diventare il motore di ricerca predefinito degli utenti. Da una parte, il Congresso ha riconosciuto tale pratica come scorretta, dall'altra parte, ha preso atto però che la disciplina americana vigente non consente di sanzionare tale tipologia di pratiche[18].

Invece, con riferimento a Facebook, la FTC ha aperto un'indagine nel marzo 2014 in merito alla proposta di Facebook di acquisire WhatsApp; il direttore dell'ufficio della divisione *Consumer* Protection della FTC, ad aprile 2014 – e quindi ancor prima che la Commissione europea a settembre iniziasse ad investigare sulla concentrazione in esame – inviò una lettera alle imprese coinvolte in cui diceva che WhatsApp avrebbe dovuto continuare ad onorare i suoi impegni in materia di tutela e sicurezza della privacy nei confronti dei suoi utenti, e che la loro violazione avrebbe costituito una "*deceptive practice under section 5 of the FTC Act.*"

3.2 – Il quadro europeo e alcune iniziative della Commissione in materia di PCS e tutela dei consumatori

In Europa, a differenza che negli Stati Uniti, si sono susseguite diverse misure a tutela del consumatore, tra le quali rientrano anche quelle relative alle PCS. In particolare, la direttiva UE 2005/29/CE[19] del Parlamento europeo e del Consiglio in materia di PCS, emendata dalla direttiva omnibus (*consideranda* n. 16, 53, 54, 55 e art. 3 e 4) e dal GDPR, nonché temporaneamente derogata dalla proposta regolamentare del DSA[20], ha armonizzato per la prima volta in Europa la disciplina in tema di pubblicità ingannevole, senza però opporsi alla più ampia tutela dei consumatori garantita

[18] Submission at 2 ("If read broadly, the prohibitions on 'monopolization,' 'unfair means of competition,' and 'restraints on trade' could be used to handle the challenges of our time. But 'broadly' is manifestly not how the laws are read by the judiciary at this point. For the courts have grafted onto these laws burdens of proof, special requirements and defenses that are found nowhere in the statutes, and that have rendered the laws applicable only to the narrowest of scenarios, usually those involving blatant price effects. And it is this that makes the laws inadequate for the challenges presented by digital markets.")

[19] Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (GU L 149 dell'11.6.2005, pag. 22).

[20] Vedi infra § 1.3.5

dagli Stati membri.

A livello comunitario, interviene poi il nuovo pacchetto di proposte regolamentari contenente il DSA e il DMA, già analizzato nel secondo capitolo in relazione all'abuso di posizione dominante; esso propone, infatti, una regolamentazione *ex ante* con riferimento alle PCS messe in atto dai c.d. *gatekeeper* [21] e alle conseguenze negative che da queste derivano (*e.g.* una riduzione della concorrenza nei mercati digitali) senza però limitare gli interventi *ex post* già previsti a livello europeo e nazionale.

Un esempio di regolamentazione *ex ante* proposta dalla Commissione è quella di prevedere una "*blacklist"* di pratiche commerciali. Inoltre, il capitolo 3 del DMA (artt. 5 e ss.) prevede diversi obblighi per i *gatekeeper.*

Ad aprile 2018, la Commissione europea ha presentato un nuovo pacchetto di misure legislative, il *New Deal for Consumers,* con cui propone di modernizzare le direttive in tema di PCS e diritti dei consumatori, al fine di accrescere la tutela offerta e rispondere in maniera efficace alle sfide dell'economia digitale. In altre parole, tale pacchetto legislativo si pone l'obiettivo di rafforzare la tutela dei consumatori, consentendo di far valere in modo più efficace i propri diritti e riconoscendo loro anche la possibilità di agire dinnanzi ai giudici o alle autorità amministrative nazionali, a tutela di interessi collettivi lesi dalle pratiche commerciali illecite[22].

A chiudere tale pacchetto di misure legislative è stata la direttiva (UE) 2019/2161, altresì conosciuta come "*direttiva omnibus*"[23], che conclude un processo di modernizzazione della protezione dei consumatori dell'UE (il c.d. *New Deal for Consumers*).

Le principali novità introdotte dalla direttiva mirano ad assicurare l'efficacia delle regole vigenti rispetto alle sfide dell'economia digitale. Tra queste, emergono: a) la previsione, in caso di "*infrazioni diffuse aventi una dimensione unionale*" di cui al Regolamento (UE) 2017/2394, di un massimo edittale non inferiore al 4% del fatturato annuo realizzato dal professionista nei Paesi interessati; b) la possibilità per gli Stati membri di regolare in modo più stringente la disciplina dei contratti conclusi fuori dai locali commerciali, purché le restrizioni siano giustificate da ragioni di ordine pubblico o di protezione della vita privata; c) l'estensione dell'ambito di applicazione della direttiva 2011/83/UE

[21] Vedi infra § 2.1.3.

[22] Cfr. direttiva (UE) 2020/1828 del 25 novembre 2020 sulle azioni rappresentative a tutela degli interessi collettivi dei consumatori. In dottrina v. R. CHIEPPA, *Ruolo dell'AGCM nel private enforcement e possibili ambiti di cooperazione con il giudice civile*, E.A. RAFFAELLI, *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea, Bruylant ed.*, 2019, spec. p. 3.

[23] Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori. Invece nel maggio del 2019 sono state pubblicate sulla Gazzetta Ufficiale dell'Unione Europea la Direttiva (UE) 2019/771 del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita di beni e la Direttiva (UE) 2019/770 del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

ai contratti di fornitura di contenuto digitale e di servizi digitali che non prevedono la corresponsione di un prezzo, ma l'impegno del consumatore a rendere disponibili al professionista i propri dati personali, oltre alla previsione di obblighi informativi supplementari per i contratti conclusi sulle piattaforme *online*[24]. Le misure nazionali di attuazione dovranno essere recepite entro il 28 novembre 2021 e dovranno entrare in vigore entro il 28 maggio 2022.

In particolare, in relazione alla direttiva 2005/29/CE in materia di PCS, è stata aggiornata la disciplina della pubblicità non trasparente alla luce delle nuove tecnologie, imponendo al professionista di precisare quando, nell'esito di una ricerca *online* da parte del consumatore, l'inclusione o il posizionamento di un prodotto discenda in realtà da un contratto di committenza.

Inoltre, per le infrazioni di rilievo europeo, si stabilisce che gli Stati membri debbano prevedere sanzioni pecuniarie con un massimo edittale non inferire al 4% del fatturato annuo realizzato dal professionista nei Paesi interessati.

Invece, in relazione alla direttiva 2011/83/UE in materia di diritti dei consumatori, viene esteso l'ambito di applicazione della stessa anche ai contratti attraverso i quali i consumatori accedono a beni o servizi senza un esborso monetario, rendendo però i propri dati personali disponibili all'impresa. Vengono previsti inoltre nuovi obblighi informativi per le piattaforme *online*, tra cui l'indicazione dei principali parametri che determinano il posizionamento delle offerte presentate al consumatore in esito a una sua ricerca effettuata sulla piattaforma.

3.3 – L'applicabilità della disciplina PCS nel caso di contratti senza esborso monetario

Da tempo gli operatori c.d. *Over the Top* (OTT) offrono agli utenti servizi apparentemente gratuiti che, in realtà, sono finanziati tramite la raccolta dei dati personali degli utenti reimpiegati nel mercato della pubblicità *on line*. Peraltro, l'economia digitale è caratterizzata da contratti – attraverso i quali i consumatori accedono a beni o servizi – che spesso non prevedono un esborso monetario, ma i consumatori rendono disponibili all'impresa i propri dati[25].

Nonostante la qualificazione di dati come corrispettivo dei servizi possa apparire in conflitto con la filosofia sottostante gli obiettivi di protezione della *privacy*, i dati personali acquisiti dal fornitore di un servizio sono spesso visti dalla letteratura economica, e persino dalla più recente giurisprudenza, come il prezzo che un utente paga per la fruizione di un servizio. Da una parte, tale analogia evidenzia come i dati personali costituiscono di fatto il principale, se non l'unico, valore di scambio del servizio,

[24] AGCM, *Relazione annuale sull'attività svolta 2020*, 31 marzo 2020, p. 125.
[25] DE FRANCESCHI, *Il pagamento mediante dati personali*, in *I dati personali nel diritto europeo* (a cura di CUFFARO, D'ORAZIO e RICCIUTO), Torino, 2019, p. 1329 ss.

laddove quest'ultimo viene erogato dall'impresa gratuitamente; dall'altra parte, assimilare la fornitura dei dati ad un prezzo significa riconoscere implicitamente che essa determina una "concessione" per l'utente, al pari di un esborso monetario, e deve in ogni caso tenere in considerazione la natura di diritto fondamentale della protezione dei dati personali.

Tale approccio è stato sviluppato anche nell'ambito dell'*enforcement* delle norme a tutela dei consumatori. Infatti, nonostante le piattaforme digitali spesso non richiedono all'utente alcun esborso monetario in cambio dei loro servizi, è configurabile un rapporto di consumo nei casi in cui l'utente stesso metta a disposizione della piattaforma o di terzi una mole ingente di informazioni collegata al proprio *account,* inclusi i dati personali e quelli dei propri contatti in rubrica.

Tale massa di informazioni è infatti utilizzata per la profilazione degli utenti per finalità pubblicitarie e, di conseguenza, acquista un valore economico che costituisce, in assenza di corrispettivo monetario, la controprestazione del servizio fornito dalla piattaforma.

Però, mentre i consumatori hanno di norma piena consapevolezza del prezzo dei prodotti/servizi che consumano, il livello di *privacy* associato al consumo di determinati servizi costituisce uno degli aspetti meno percepibili e "quantificabili" dal consumatore[26].

In Italia ormai, ai fini dell'applicabilità della disciplina a tutela del consumatore, è irrilevante il fatto che la controprestazione sia monetaria o meno. Già dal 2000, l'AGCM ha infatti affermato che la gratuità del servizio offerto non esclude il sindacato dell'eventuale ingannevolezza della comunicazione commerciale, quando al consumatore sia richiesto di cedere – quale condizione della fruizione del servizio – "*dati personali, relativi ai propri interessi e alle proprie esigenze. Inoltre, il fatto che tali dati si presentino in una forma, per così dire, 'grezza', e che necessitino dell'elaborazione della piattaforma per essere sfruttabili economicamente, non impedisce che tale transazione abbia una rilevanza economica*"[27].

Invece, più recentemente, l'AGCM ha ribadito che "*il patrimonio informativo costituito dai dati degli utenti […] utilizzato per la profilazione degli utenti a uso commerciale e per finalità di marketing, acquista, proprio in ragione di tale uso, un valore economico idoneo […] a configurare l'esistenza di un rapporto di consumo tra il professionista e l'utente*", facendone logicamente discendere l'applicabilità alla fattispecie *de qua* della disciplina in materia di PCS e di clausole vessatorie[28].

In tale caso, Whatsapp aveva ammesso che l'attività di condivisione dei dati con Facebook avrebbe migliorato l'attività di *advertising* della medesima e avrebbe generato direttamente a Facebook i ricavi.

[26] A titolo di esempio: AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020.
[27] Provvedimento AGCM PI2671 - Libero Infostrada, 17 febbraio 2000 n. 8051.
[28] Provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597.

Peraltro, al di là di eventuali ulteriori profili di violazione della disciplina di protezione dei dati, una determinata condotta può integrare gli estremi di una pratica ingannevole quando la commercializzazione dei servizi viene presentata come 'gratuita' e i consumatori non vengono informati del modo con cui vengono utilizzati i dati relativi alle loro preferenze, i dati personali e i contenuti generati dagli utenti[29].

In altri termini, i principali interventi dell'AGCM hanno ad oggi riguardato l'accesso degli operatori ai dati degli utenti, piuttosto che il loro concreto utilizzo, in un'ottica però complementare alla tutela della *privacy*.

Anche a livello comunitario, la direttiva 2005/29/CE relativa alle PCS estende l'ambito di applicazione ai casi in cui il consumatore fornisce una controprestazione non pecuniaria. La Commissione europea ha infatti chiarito che "*i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto e vengono venduti a terzi*"; di conseguenza, "*se il professionista non comunica al consumatore che i dati che è tenuto a fornire per accedere al servizio saranno usati a fini commerciali, questa pratica può essere considerata un'omissione ingannevole di informazioni rilevanti*"[30].

Infatti, la Commissione europea riconosce che i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico *de facto* e che una piattaforma che si qualifica come 'professionista' deve in ogni caso rispettare le norme dell'UE in materia di diritto commerciale e dei consumatori nell'ambito delle proprie pratiche commerciali.

Inoltre, anche in ambito *antitrust*, la Commissione ha ribadito la natura di controprestazione non pecuniaria dei dati degli utenti dei *social media*. In particolare, con riferimento ai profili concorrenziali dell'acquisizione di WhatsApp da parte di Facebook, così come analizzata nel secondo capitolo[31], la Commissione ha fatto numerose considerazioni sul valore economico dei dati degli utenti di WhatsApp, sottolineando, ad esempio, come le piattaforme di *social network* offrano i loro servizi, in genere gratuitamente, ricavando dal *marketing* e dai servizi *premium* una remunerazione non pecuniaria.

La situazione "cambiava" invece con riferimento alla direttiva 2011/83/UE sui diritti dei consumatori. L'uso dell'imperfetto non è casuale in quanto, come vedremo, questa "ingiustizia" è stata di recente risolta dal legislatore europeo.

Infatti, le definizioni dei contratti di vendita e di servizi facevano riferimento a un "prezzo" che il consumatore si impegnava a pagare[32], e tale riferimento era inteso dalla Commissione esclusivamente

[29] Provvedimento AGCM PS11112 - Facebook-Condivisione dati con terzi, 29 novembre 2018 n. 27432.
[30] Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali, Bruxelles, 25.5.2016.
[31] V. § 2.2.3
[32] Cfr. art. 2, parr. 5 e 6 della Direttiva 2011/83/UE

come pagamento in denaro. La prestazione di servizi online che non prevede un pagamento in denaro non risultava quindi rientrare nel campo di applicazione della direttiva.

Per contro, con riferimento ai contratti per la fornitura di contenuto digitale *online*, la direttiva non menzionava alcun "pagamento"; la Commissione riteneva che la direttiva "*sembra perciò applicarsi ai contratti ... di contenuto digitale online, anche quando non comportano un pagamento: per esempio la direttiva si applica a un contratto per il download gratuito di un gioco da un app store*"[33].

Tale distinzione appariva tuttavia ingiustificata, considerato che i due servizi - prestazione di servizi online e contratti per la fornitura di contenuto digitale *online* - tendevano in realtà spesso a sovrapporsi.

Ebbene, il nuovo pacchetto di misure legislative, il *New Deal for Consumers*[34], concluso dalla c.d. direttiva *omnibus*, risolve la problematica in questione estendendo l'ambito di applicazione della direttiva 2011/83/UE in materia di diritti dei consumatori anche ai contratti per la fornitura di servizi digitali, attraverso i quali i consumatori accedono a beni o servizi senza un esborso monetario.

In particolare, la nuova Direttiva 2019/770, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, trova applicazione anche quando la controprestazione del consumatore è costituita non dal pagamento di un prezzo, ma dalla fornitura di dati personali.

Tale modello di *business* è usato nel settore coperto dalla direttiva, specificando che i dati personali non sono assimilabili a merci, in quanto oggetto dei diritti inalienabili previsti dal GDPR.

Pertanto, fatta salva l'applicazione di quest'ultimo, anche in questo caso il consumatore deve poter disporre di tutti i rimedi che la direttiva prevede in caso di mancata fornitura o di difetto di conformità e, in particolare, deve poter procedere alla risoluzione del contratto anche se il difetto di conformità è di lieve entità.

3.4 – I c.d. prezzi personalizzati

Tra le preoccupazioni antitrust derivanti dalla titolarità di *Big Data* potrebbe esserci, e in questo caso il condizionale è d'obbligo, anche quello della discriminazione dei prezzi derivante da offerte personalizzate che gli operatori della *digital market economy* sono in grado di formulare all'esito del processo di profilazione degli utenti, in base ai loro gusti, bisogni e propensioni di spesa.

L'uso del condizionale è dovuto al fatto che sia la dottrina[35] sia le Autorità che finora si sono espresse

[33] Documento di orientamento della DG giustizia concernente la direttiva 2011/83/UE, giugno 2014, disponibile in https://ec.europa.eu/info/sites/info/files/crd_guidance_it.pdf.

[34] Il "New Deal for Consumers" è completato dalla cosiddetta "Direttiva Omnibus" (direttiva (UE) 2019/2161), che integra e modifica la direttiva sulle clausole abusive nei contratti con consumatori (Direttiva 93/13/EEC), la direttiva sui prezzi dei prodotti offerti ai consumatori (Direttiva 98/6/EC), la direttiva sulle pratiche commerciali scorrette (Direttiva 2005/29/EC) e la direttiva sui diritti dei consumatori (Direttiva 2011/83/EU).

[35] Cfr. ARMSTRONG, *Price Discrimination*, in www.else.econ.ucl.ac.uk, 6 ss. spec. 14-17; LIBERTINI, Concorrenza, op.cit., 326 ss.

su questa prassi[36], hanno evidenziato una certa ambivalenza degli effetti, al contempo positivi e negativi, prodotti dalle offerte personalizzate.

La centralità della questione è data soprattutto dal fatto che la pubblicità comportamentale, come si è visto in più occasioni, è il *core business* dei mercati digitali[37].

Sul versante della domanda, in senso pro-concorrenziale viene riscontrata la tendenza all'aumento ed alla massimizzazione del benessere generale dei consumatori (*consumer welfare*), intesi nella loro totalità (c.d. *social welfare*), così da rendere "più poveri i più ricchi e meno poveri i meno ricchi"[38], nonché una maggiore rivalità tra le imprese[39]; mentre in senso anti-concorrenziale si registra una perdita di benessere individuale per alcuni consumatori (quelli disposti a pagare prezzi più alti per avere determinati beni) a fronte del risparmio di spesa riservato soltanto ad alcuni consumatori (quelli disposti a pagare prezzi più bassi per fruire di determinati beni).

In generale, tale prassi risulta "fastidiosa" per i consumatori, sia in ragione di dinamiche socioculturali (nella società dei consumi di massa la parità dei prezzi sul mercato viene percepito come un valore, la disparità come disvalore)[40], sia in forza della carenza di informazione e trasparenza per gli utenti circa l'uso specifico che verrà fatto dei dati personali raccolti, come quello della profilazione finalizzata ad offerte personalizzate.

Vi è senz'altro un problema di *privacy* che attiene alle misure informative necessarie per rendere lecito l'uso dei dati personali a scopo di profilazione; a tal proposito, ci si domanda se sia sufficiente l'informativa sui *cookies* già fornita dai siti *web*, o se sia necessario implementare tale informativa imponendo, in sede regolamentare, un consenso espresso aggiuntivo per le sole offerte personalizzate.

Nell'ottica del diritto della concorrenza, però, il problema di maggior rilievo è se possa considerarsi illecita, per abuso di posizione dominante o come PCS, la prassi della discriminazione dei prezzi in violazione del principio di parità di trattamento.

Certamente la discriminazione dei prezzi praticata da un'impresa in posizione dominante – o da due o più imprese all'esito di un accordo (i.e. intesa restrittiva della concorrenza) – se rivolta a danno di altre imprese sul mercato, costituisce un illecito antitrust sia comunitario, ai sensi degli artt. 101 e

---

[36] A titolo di esempio: AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020, p. 106; Report: *Big data and differential pricing*, by The Executive Office of the President of the US, February 2015, disponibile su http://obamawhitehouse.archive.gov, 4; Report congiunto dell'Autorité de la Concurrence francese e del Bundeskartellamt tedesco, Competition Law and Data, May 10 th, 2016, in www.autoritedelaconcurrence.fr/doc/reportcompetitionlawdatafinal.pdf, 21.

[37] MORERA, *Legislatore razionale versus investitore irrazionale: quando chi tutela non conosce il tutelato*, in AGE, 1/2009, 78 ss; LINCIANO, *Errori cognitivi e instabilità delle preferenze nelle scelte di investimento. Le indicazioni di policy della finanza comportamentale*, in *Quad. fin. Consob*, n. 66/2010; MORERA-F. VELLA (a cura di), *Finanza comportamentale. Investitori a razionalità limitata*, in AGE, 1/2012; GENTILE-LINCIANO-LUCARELLI-SOCCORSO, *Financial disclosure, risk perception and investment choices. Evidence from a consumer testing exercise*, in *Quad. fin. Consob*, 82/2015.

[38] M. MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, 2016, 95 ss, spec. 98.

[39] *Id.*, 114-115.

[40] *Id.*, 98, 109-110.

102[41] TFUE, sia nazionale, in applicazione degli artt. 2 e 3 L. n. 287/1990 (legge Antitrust).

Tuttavia, vi sono più dubbi nello spostamento del *target* dalle imprese (concorrenti) ai consumatori[42], sebbene autorevole dottrina sostenga che sia configurabile un illecito *antitrust* per discriminazione dei consumatori, sia in termini di abuso di dominanza, sia in termini di accordo collusivo[43].

Diversamente, qualora la condotta discriminatoria provenga da imprese che non rivestano una posizione dominante sul mercato, resta da chiedersi se si possa considerare quanto meno come PCS la violazione della parità di trattamento in sé, ovvero per la modalità occulta con la quale viene di regola praticata l'offerta personalizzata, al pari di una pubblicità subliminale.

Il legislatore ha posto espressamente l'obbligo di contrattare con chiunque, garantendo la "parità di condizioni" solo al monopolista legale (artt. 2597 e 1679 c.c.); pertanto, non vi è alcuna ragione per ritenere vietato alle imprese praticare prezzi diversi per prestazioni equivalenti, ove le condizioni di concorrenza sul mercato siano tali da garantire ai consumatori un'adeguata varietà di scelta.

Da una parte, c'è chi ritiene che i prezzi personalizzati non siano qualificabili in termini di PCS, per ragioni di inopportunità dell'e*nforcement* sulle PCS, e che il terreno migliore per la tutela dei dati personali sia quello della disciplina sulla privacy[44]; dall'altra parte, c'è chi, guardando ai prezzi personalizzati in un'ottica di PCS, qualifica come omissione ingannevole (ai sensi dell'art. 22, comma 1°, Cod. Cons.) l'offerta personalizzata di beni o servizi che non sia seguita dalla chiara manifestazione della sua natura personalizzata e discriminatoria[45].

Sebbene quest'ultima fattispecie non sia contemplata nella *black list* tra le ipotesi tipiche considerate "in ogni caso ingannevoli" dall'art. 23, Cod. Cons., essa presenta non solo entrambi i requisiti richiesti

[41] In questo contesto, l'art. 102 lett. c TFUE è stato, ad oggi, per lo più utilizzato con riguardo a questioni legate alla protezione del mercato interno relative a discriminazioni basate sul paese di residenza dei clienti e mai a prezzi personalizzati. Alternativamente, ci si potrebbe chiedere se simili pratiche possano essere perseguite nell'ambito dell'art. 102.a TFUE, dovendo però chiarire quale sia il test che andrebbe applicato in questa ipotesi. In particolare, appare assai complesso ipotizzare condotte di sfruttamento quando i prezzi personalizzati hanno, per un verso, un impatto negativo sul benessere di alcuni consumatori, quelli con la disponibilità a pagare maggiore, per altro verso, hanno un impatto positivo sul benessere di altri consumatori, quelli con la disponibilità a pagare minore. Così AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020, p. 106.

[42] Sul punto cfr. AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020, p. 106 dove si afferma che: "La normativa europea a tutela della concorrenza vieta esplicitamente solo le discriminazioni di prezzo nei confronti di imprese (in ragione delle loro implicazioni escludenti) e non anche dei consumatori finali. Non è, pertanto, del tutto chiaro fino a che punto le disposizioni relative a condotte discriminatorie si applichino anche ai rapporti *business-to-consumer*."

[43] Cfr. M. LIBERTINI, *La tutela della libertà di scelta del consumatore e i prodotti finanziari*, in *Mercati finanziari e protezione del consumatore*, a cura di M. Grillo, Brioschi, Milano, 2010, 21-46.

[44] M. MAGGIOLINO, *op.cit.*, 132.

[45] Sulle pratiche commerciali ingannevoli, ed in particolare quelle omissive, si rinvia a MELI, *Le pratiche sleali ingannevoli*, in Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette*, Padova, 2008, 87 ss. spec. 105; CALVO, *Le pratiche commerciali «ingannevoli»*, in De Cristofaro (a cura di), *Pratiche commerciali scorrette e codice del consumo*, Torino, Giappichelli, 2008, 223 ss.; PENNISI, *Considerazioni in merito alle pratiche commerciali ingannevoli*, in questa Rivista, 2012, I, 653 ss.; TESTA, Sub art. 22 Cod. Cons., in L.C. Ubertazzi, *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, 6 a ed., Padova, Cedam, 2016, 2686 ss.

alternativamente dall'art. 22 Cod. Cons.[46], ma anche quei caratteri comuni alle PCS e contenuti nella definizione generale[47] di cui all'art. 20, comma 2°, Cod. Cons[48]. Il fatto che non sia un'ipotesi prevista nella *black list* significa inoltre che occorre dimostrare che tale mancanza possa falsare la scelta di consumo in misura considerevole.

A detta dello scrivente appare evidente che la discriminazione dei prezzi operata all'insaputa del consumatore sia giudicabile come una pratica carente di trasparenza e contraria alla correttezza professionale; essa attiene ad un elemento essenziale (il prezzo del prodotto) capace di ledere la libertà di scelta del consumatore, ovvero di incidere sulle sue scelte di consumo, inducendolo all'acquisto inconsapevole, o non sufficientemente informato, di un prodotto o servizio[49]. Quest'ultimo, infatti, se fosse stata dichiarata la sua natura personalizzata e discriminatoria, non sarebbe stato acquistato o sarebbe stato acquistato a condizioni diverse; o, quanto meno, avrebbe indotto il consumatore ad assumere maggiori informazioni su altre offerte analoghe, allo scopo di compararle e giungere ad una decisione più ponderata.

Conferma di ciò si può trarre dagli studi di *marketing* condotti sui consumatori, che hanno evidenziato non soltanto la loro percezione delle offerte personalizzate come scorrette e sleali, ma anche la loro intenzione di modificare la decisione di acquisto una volta informati della natura personalizzata del prezzo che era stato loro praticato, specialmente i consumatori più ricchi, dopo esser venuti a sapere di aver pagato il bene ad un prezzo più alto rispetto a quello di mercato[50].

Pertanto, in primo luogo, l'applicazione di prezzi personalizzati in maniera non trasparente (o senza fornire ai consumatori la possibilità di *opt-out)* potrebbe essere valutato ai fini di una PCS. A tal proposito, le imprese, con riguardo alle proprie strategie di prezzo, forniscono informazioni per consentire ai consumatori di acquisire consapevolezza dell'esistenza di tali pratiche, ed adottare, ove necessario, specifiche azioni per eluderle. Inoltre, si è visto come la reazione dei consumatori varia a seconda che siano a conoscenza della raccolta dati, della personalizzazione e della possibilità di *opt-*

---

[46] Questi sono: "*Omette informazioni rilevanti di cui il consumatore medio ha bisogno (...) per prendere una decisione consapevole o è idonea ad indurre in tal modo il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso*".

[47] A tal proposito, "*una pratica commerciale è scorretta se è contraria alla diligenza professionale, ed è falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta*" (c.d. *materiality test*)

[48] Sulla relazione di integrazione (e non esclusione) tra la clausola generale e le disposizioni particolari nelle definizioni delle pratiche commerciali scorrette, la tesi qui accolta è già stata sostenuta da LIBERTINI, *Clausola generale e disposizioni particolari nella disciplina delle pratiche commerciali scorrette*, in Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette*, Padova, Cedam, 2008, 27 ss. spec. 39.

[49] Essenziale è dunque la predisposizione di strumenti di protezione avanzati, idonei a operare sia sotto il versante informativo, sia sotto il versante delle regole di condotta. Sul punto si rinvia a R. NATOLI, *Il contratto "adeguato". La protezione del cliente nei servizi di credito, di investimento e di assicurazione*, Milano, 2012.

[50] Studi citati in M. MAGGIOLINO, *op.cit.,108-110 e 130.*

out[51].

In secondo luogo, è possibile perseguire e sanzionare PCS ancillari ma capaci di accrescere gli effetti negativi dei prezzi personalizzati, come pratiche ingannevoli o omissive che limitano ulteriormente la trasparenza e la possibilità di scelta del consumatore[52].

3.5 Segue – Le convergenze tra tutela del consumatore e protezione dei dati personali

Mentre la disciplina consumeristica si basa sulla qualifica dei soggetti coinvolti nel loro peculiare "rapporto obbligatorio", nella normativa a tutela dei dati personali è tale rapporto che ne determina l'applicazione e ne qualifica i soggetti rilevanti. Questa distinzione nell'ambito applicativo rende sovrapponibili le coppie di soggetti coinvolti: un professionista può essere anche titolare di un trattamento di dati personali, mentre il consumatore può essere anche l'interessato del trattamento. La prassi applicativa ha confermato sempre più la convergenza e l'assimilazione delle due figure.

Interessante a tal proposito è l'emersione nella disciplina consumeristica della figura del c.d. *prosumer*: si tratta, in questo caso, di una figura figlia dell'interattività del mondo digitale, che racchiude in sé i tratti tipici del professionista con quelli peculiari del consumatore/utente. Si pensi al settore in cui più è emersa tale figura, quello della pubblicazione sulle piattaforme digitali dei contenuti generati dall'utente (i c.d. *User Generated Content*): ossia quello delle opere creative e dell'ingegno, spesso derivanti da altre opere protette da diritto d'autore. In tali casi il *prosumer* è quell'utente che, pur non ponendo in essere un'attività d'impresa (non essendo quindi un professionista), realizza attività altamente professionalizzate e astrattamente idonee a integrare un'attività lucrativa (in altri termini, un consumatore che realizza un'attività simile a quella del professionista)[53].

Si assiste così ad una sovrapposizione di due piani distinti ma incrociati: da una parte, si è indebolita la distinzione tra professionista e consumatore, anche a causa dell'emersione del soggetto ibrido del *prosumer*; dall'altra parte, come già evidenziato, la coppia di soggetti rilevanti per la normativa consumeristica si sovrappone alla coppia di soggetti rilevanti per la disciplina *data protection*. A tal riferimento, ci sarà un professionista che è anche titolare del trattamento, e un consumatore/utente che è anche interessato del trattamento.

---

[51] European Commission, "*Market study on online market segmentation through personalised pricing/offers in the EU*", 2018, https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through-personalised-pricing-offers-european-union_en.

[52] Ad esempio, affermare che un prezzo è il più conveniente mentre ad altri consumatori vengano offerti prezzi migliori, offrire un prezzo personalizzato scontato che è più elevato di quello pubblico, raccogliere dati per personalizzare i prezzi senza il consenso dei consumatori.

[53] Così, D'IPPOLITO, *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali personali* cit., 70 ss., spec. 71, disponibile in https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf.

Inoltre, lo schema sotteso alla figura del *prosumer* può essere replicato anche in materia di tutela dei dati personali. Un *prosumer* è qui rinvenibile se si pensa all'incremento di quei soggetti di difficile collocazione, a metà tra il titolare/responsabile e l'interessato, o a metà tra soggetti che svolgono o no un trattamento di dati personali rilevanti ai sensi del Regolamento. A confermare ciò è anche la Corte di Giustizia dell'Unione europea in materia di co-responsabilità del trattamento dei dati personali tra l'amministratore di una "pagina Facebook" e Facebook stessa, in relazione ai dati dei visitatori della pagina[54] o con riferimento alla responsabilità del gestore di un sito Internet corredato del pulsante "mi piace" di Facebook, che può essere considerato congiuntamente responsabile con Facebook della raccolta e della trasmissione dei dati personali dei visitatori[55]. In altre parole, si hanno dei soggetti che, a seconda del caso concreto, per il fatto di avvalersi degli strumenti posti in essere dalle piattaforme digitali, detengono una certa responsabilità sulla gestione di dati personali.

Dal punto di vista dei soggetti, considerare un operatore economico sia come professionista che come titolare del trattamento vuol dire contestargli non solo il rispetto della normativa in materia di protezione dei dati personali, ma anche di quella consumeristica in materia di trasparenza, PCS o clausole vessatorie.

La sovrapposizione c'è anche nell'attività delle autorità amministrative indipendenti preposte ad un certo settore. In particolare, in Italia, si è assistito all'intervento dell'AGCM nel sanzionare lo scorretto trattamento di dati personali, in quanto poco trasparente o ottenuto tramite pratiche ingannevoli.

In altre parole, anche nell'attività di *enforcement*, finora condotta in questo settore dall'AGCM, sono spesso venuti in rilievo profili di intersezione con il diritto alla protezione dei dati personali.

Partendo dal caso meno recente, nel gennaio 2017 l'Autorità ha concluso un procedimento nei confronti di Samsung avverso la cessione forzata di dati personali per finalità di *marketing*[56]. L'accertamento in questione ha riguardato, tra l'altro, una condotta relativa all'acquisizione, per finalità di *marketing*, di una serie di dati personali ultronei e indipendenti dalla specifica promozione di Samsung, e necessari per richiedere i premi; in particolare, il consumatore veniva informato del possibile utilizzo a scopo di *marketing* dei propri dati, ma solamente dopo avere acquistato il prodotto in promozione e con lo sconto.

A tal proposito, il TAR Lazio ha annullato il provvedimento dell'AGCM con riferimento a quest'ultima condotta, evidenziando che "*l'eventuale illegittima raccolta dei dati presenti nella piattaforma o la loro cattiva gestione da parte del professionista costituisce una possibile violazione*

[54] Causa C-210/16 - *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirt- schaftsakademie Schleswig-Holstein GmbH* del 5 giugno 2018.
[55] Causa C-40/17 - Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW e V del 20 luglio 2019.
[56] Cfr. provvedimento AGCM PS10207 Samsung-Mancato riconoscimento promozione, 25 gennaio 2017 n. 26387.

dei principi in materia di corretto trattamento dei dati personali, il cui accertamento non è di competenza dell'AGCM, trattandosi di una prerogativa rimessa ai sensi del d.lgs. 30 giugno 2003, n. 196 al Garante per la protezione dei dati personali. L'AGCM è, invece, chiamata a verificare se la richiesta dei dati sia avvenuta secondo modalità tali da condizionare la libertà di scelta del consumatore"[57].

In concreto, nelle proprie valutazioni, il TAR ha dato rilievo al fatto che fosse previsto uno specifico consenso per l'invio di comunicazioni pubblicitarie al consumatore e che, dunque, non risultasse provato un indebito condizionamento della clientela.

Va tuttavia rilevato che, secondo consolidata giurisprudenza[58], le questioni relative a pratiche aggressive non trovano regolazione nelle discipline settoriali, con conseguente competenza dell'AGCM. Sul punto si tornerà meglio in seguito con riferimento al criterio autonomo della c.d. incompatibilità delle norme, richiamato con riferimento alla questione sul divieto del *bis in idem* sollevata da Facebook nel ricorso al TAR.

Anche quest'ultimo caso infatti testimonia la sovrapposizione tra tutela del consumatore e tutela dei dati personali: l'AGCM ha contestato all'impresa la violazione degli artt. 21 e 22 del Codice del consumo consistente nell'aver indotto ingannevolmente gli utenti a registrarsi sulla piattaforma, senza prima informarli adeguatamente e immediatamente dell'attività di raccolta dei loro dati e delle finalità remunerative, che sottendono la fornitura del servizio di *social network*, enfatizzandone la sola gratuità[59].

Con riferimento invece a WhatsApp, l'AGCM ha aperto due distinti procedimenti: il primo ha considerato una pratica aggressiva quella di WhatsApp consistente nell'aver indotto gli utenti ad accettare integralmente i nuovi Termini di Utilizzo e, in particolare, la condivisione dei propri dati con Facebook[60]; il secondo, ha invece rilevato la presenza di clausole vessatorie nel modello contrattuale sottoposto all'accettazione dei consumatori, per usufruire dell'applicazione WhatsApp Messenger[61].

Con riferimento al primo procedimento[62], l'Autorità ha irrogato a WhatsApp una sanzione di 3 milioni di euro per una PCS di tipo aggressivo ai sensi degli artt. 20, 24 e 25 del Codice del consumo, concernente la modifica delle condizioni generali di contratto. In tale caso, la condotta aggressiva è consistita nell'invitare gli utenti ad accettare integralmente i nuovi Termini di Utilizzo, che

[57] TAR Lazio, n. 5043, 7 maggio 2018.
[58] Consiglio di Stato, Sezione VI Sentenza 11 novembre 2019, n. 7699; Corte di giustizia UE Sez. 2^, 13/09/2018 Sentenza cause riunite C-54/17 e C-55/17.
[59] Provvedimento AGCM PS11112 - Facebook-Condivisione dati con terzi, 29 novembre 2018 n. 27432.
[60] Provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597.
[61]Provvedimento AGCM CV154, – WhatsApp – Clausole Vessatorie, 11 maggio 2017 n. 26596, in Boll. 18/2017.
[62] Cfr. Provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597.

comprendevano in particolare la condivisione dei propri dati con Facebook, facendo loro credere che sarebbe stato, altrimenti, impossibile proseguire nell'uso dell'applicazione. L'AGCM ha respinto le difese di WhatsApp, che nel corso dell'istruttoria aveva sostenuto, tra l'altro, che l'Autorità dovesse sospendere il procedimento sin tanto che il Garante della Privacy non si fosse pronunciato sulla fattispecie in merito alla liceità del trasferimento dei dati. A tale riguardo, l'AGCM ha affermato che *"[i]n linea di principio, 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".*

Inoltre, l'AGCM ha esaminato le possibili sovrapposizioni tra Codice del Consumo e disciplina a tutela dei dati personali, precisando 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, comma 3 e 27, comma 1-bis, del Codice del Consumo spetta, in via esclusiva, all'Autorità Garante della Concorrenza e del Mercato*"[63].

Con riferimento invece al secondo procedimento, l'AGCM ha accertato la nullità ai sensi degli artt. 33 e 35 del Codice del consumo di alcune clausole del modello contrattuale sottoposto agli utenti, che assicuravano a WhatsApp: i) esclusioni e limitazioni di responsabilità ampie e generiche; ii) la possibilità di interrompere unilateralmente il servizio o di variare le condizioni d'uso senza motivo e senza preavviso; iii) l'applicazione della legge della California e l'individuazione dei Tribunali dello stesso Stato quali unici fori competenti per la risoluzione delle controversie.

Il caso WhatsApp, in generale, ha quindi evidenziato la forte correlazione che intercorre tra concorrenza e *privacy*, nella misura in cui la violazione delle norme a tutela della *privacy* possa dare luogo a PCS nei confronti dei consumatori (ai sensi degli artt. 20, comma 2, 24 e 25 Cod. Cons.), come acclarato anche dall'AGCM con provvedimento (anche sanzionatorio)[64]. In particolare, l'AGCM, ha sanzionato WhatsApp per aver indotto i consumatori ad accettare la clausola di condivisione dei propri dati con Facebook nella fase di accettazione dell'aggiornamento dei termini

[63] Paragrafi 51 e 52 del provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597.

[64] Provvedimento AGCM PS10601- Whatsapp -Trasferimento Dati A Facebook, 11 maggio 2017 n. 26597, in Bollettino, 15 maggio 2017, n. 18/2017.

di utilizzo, facendo credere agli utenti che senza l'accettazione di questa clausola non avrebbero più potuto continuare ad utilizzare il servizio.

Da un lato, il caso dimostra che i contratti conclusi per la fruizione di servizi gratuiti (come quelli offerti da WhatsApp) siano qualificabili come contratti dei consumatori[65]; la loro valuta di scambio non è il denaro ma i dati personali e, di conseguenza, vanno assoggettati alle norme del Codice del Consumo, ivi incluse le disposizioni sulle PCS. Dall'altro lato, il caso conferma che vi possano essere abusi conseguenti all'acquisita dominanza su un determinato mercato (i.e. quello dei *social network* per Facebook), capaci di estendersi su altri mercati – quello delle comunicazioni mediante messaggi di testo, vocali, fotografici e video chiamate in cui opera WhatsApp – per effetto della fusione realizzata tra i due colossi, che però nessuna Autorità ha saputo prevedere.

Ebbene, una condotta simile sembra essersi ripetuta anche nel 2021, quando WhatsApp ha inviato ai propri utenti un messaggio di accettazione della nuova *privacy policy*, obbligando gli utenti a dare il proprio consenso entro l'8 febbraio 2021 per poter continuare ad utilizzare il servizio[66]. La nuova *policy* prevedrebbe la condivisione dei dati raccolti sulla sua piattaforma di messaggistica con altre piattaforme dello stesso gruppo, al fine di avere profili utenti, sempre più completi, a cui poter inviare annunci pubblicitari personalizzati. Tale condotta dell'impresa potrebbe ben considerarsi come una pratica commerciale aggressiva e, dunque, ci si potrebbe aspettare anche qui un intervento dell'Autorità a riguardo.

In conclusione, la sovrapposizione tra diverse discipline crea sia vantaggi che svantaggi: da una parte, c'è un'estensione della normativa e una maggior tutela per gli utenti (consumatori e interessati al tempo stesso), dall'altra parte, c'è però ancora un'incertezza normativa, con diversi rischi: i) quello di attribuire oneri eccessivi al soggetto sbagliato; ii) quello di sovrapposizione di competenze e di violazione del divieto del *ne bis in idem* nell'applicazione delle sanzioni[67], riconosciuto dall'art. 4 del Protocollo n. 7 della Convenzione europea per i diritti dell'uomo e dall'art. 50 della Carta dei diritti fondamentali dell'Unione europea[68].

La conseguenza è stata quella di assistere a fenomeni tipicamente di *data protection* all'interno del plesso normativo preposto alla tutela della concorrenza.

Un esempio sono anche le pronunce del *Bundeskartellamt,* che in Germania ha contestato un abuso

[65] Così ZENO-ZENCOVICH-GIANNONE CODIGLIONE, *Ten legal perspectives on the "big data revolution",* in Di Porto (a cura di), *Big data e concorrenza*, in *Conc. merc*., 2016, 41.

[66] Per ulteriori considerazioni sulla pratica in questione si rinvia a § 1.3.2.

[67] In materia di *ne bis in idem* cfr. *ex multis M.* LIBERTINI, *Cumulative enforcement of European and national competition law and ne bis in idem principle - Case comment to the judgement of EU Court of Justice of 3 April 2019*, in *Yearbook of Antitrust and Regulatory Studies (University of Warsaw)*, 2019.

[68] L'art. 50 della Carta dei diritti fondamentali dell'Unione europea sancisce che «[n]essuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge».

di posizione dominante a Facebook in qualità di titolare del trattamento[69].

A tal proposito, risulta però ancora assente la valutazione del rilievo della qualità e del livello di tutela della protezione dei dati degli utenti nell'ambito delle procedure di concentrazione, per la trattazione delle quali si rinvia al secondo capitolo.

In conclusione, tra la normativa consumeristica e quella sulla protezione dei dati personali non c'è un rapporto di genere a specie, con conseguente disapplicazione della normativa generale a favore di quella speciale, ma piuttosto un rapporto di complementarità, con conseguente possibilità di applicare entrambe le discipline. Due normative trasversali e orizzontali, quindi, parallele nella teoria, ma più volte secanti nella pratica.

Dalla sovrapposizione delle figure emerge come, a prescindere dalla nomenclatura dei soggetti, quel che rileva è la presenza di una nuova asimmetria che, oltre a quella consumeristica tradizionale, sorprende un utente tecnologicamente poco consapevole. Ciò accentua quindi le distanze tra la figura del soggetto economicamente/informativamente forte e quella di un soggetto socialmente/ informativamente debole.

3.6 – Un approfondimento sul caso Facebook in Italia e la sentenza del TAR

Con un provvedimento del 2018[70], l'AGCM ha sanzionato Facebook per complessivi 10 milioni di euro per due distinte tipologie di PCS, entrambe poste in essere nei confronti degli utenti italiani in violazione del Codice del consumo e aventi ad oggetto la raccolta, lo scambio con terzi e l'utilizzo ai fini commerciali dei dati raccolti, incluse le informazioni sui loro interessi *on line.*

Nella prima pratica, Facebook avrebbe posto in essere una pratica ingannevole, vietata dagli artt. 21 e 22 del Codice del consumo, non avendo informato adeguatamente e immediatamente l'utente, in fase di attivazione dell'*account*, dell'attività di raccolta e utilizzo, a fini commerciali, dei dati che egli cede a terzi.

Nella seconda condotta, l'AGCM ha rilevato invece che Facebook avrebbe posto in essere una pratica aggressiva, vietata dagli artt. 24 e 25 del Codice del consumo, esercitando un indebito condizionamento nei confronti dei consumatori registrati; questi ultimi avrebbero prestato inconsapevolmente il loro consenso, tramite un sistema di preselezione dello stesso, al trasferimento dei loro dati ai siti *web/App* di terzi, in cambio dell'utilizzo del *social network* e per finalità di profilazione e commerciali dell'impresa[71].

[69] Provvedimento B6-22/16 del 15 febbraio 2019. Cfr. anche § 2.1.4.

[70] Cfr. Provvedimento AGCM PS11112 - Facebook-Condivisione dati con terzi, 29 novembre 2018 n. 27432.

[71]In dottrina cfr. V. VESCIO DI MARTIRANO, *Facebook e il valore dei dati. Cosa dice la sentenza del Tar del Lazio*, 2020 in https://www.key4biz.it/facebook-e-il-valore-dei-dati-cosa-dice-la-sentenza-del-tar-del-lazio/285228/ e S. GOBBATO, "*Big data" e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo, cit.* p. 157- 158.

Ebbene, il 10 gennaio 2020, il TAR Lazio si è pronunciato con sentenza che ha confermato la legittimità del provvedimento sanzionatorio emanato dall'AGCM, solo con riferimento alla pratica commerciale ingannevole e, di conseguenza, ha invece annullato lo stesso con riferimento alla pratica commerciale aggressiva[72].

Con riferimento alla prima pratica, considerata ingannevole, l'AGCM sosteneva che nella fase di prima registrazione dell'utente nella piattaforma *web/app,* Facebook forniva un'informativa – in cui diceva "l'iscrizione è gratis" – ritenuta dall'Autorità priva di immediatezza, chiarezza e completezza, in riferimento alla attività di raccolta e utilizzo, a fini commerciali, dei dati degli utenti. Inoltre, l'informazione era ritenuta non veritiera e fuorviante in quanto la raccolta e sfruttamento dei dati degli utenti a fini remunerativi si configurava come controprestazione del servizio offerto dalla piattaforma. L'Autorità affermava che: "*i ricavi provenienti dalla pubblicità on line, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd. e il 98% del fatturato di Facebook Inc*".

Ebbene, nella sentenza del TAR Lazio, si afferma che nonostante il potere sanzionatorio per illecito o non conforme trattamento dei dati ricada sul Garante Privacy, l'AGCM conserva un potere sanzionatorio posto a tutela dell'interesse economico degli interessati, in quanto consumatori.

A tal proposito, il giudice amministrativo smentisce la tesi difensiva della piattaforma di *social network* secondo cui per i dati personali non sussisterebbe alcun corrispettivo patrimoniale e, dunque, un interesse economico dei consumatori da tutelare[73]; in particolare, la parte ricorrente sosteneva che l'unica tutela del dato personale risiedesse nella sua accezione di diritto fondamentale e, quindi, che fosse limitata al corretto trattamento dei dati personali dell'utente.

Sul punto, il TAR Lazio ha affermato che questa fosse solo una visione parziale delle tutele consentite all'utente in caso di sfruttamento dei dati personali, che possono ben costituire un *asset* disponibile in senso negoziale e suscettibile di sfruttamento economico da parte del titolare del trattamento che, a sua volta, lo utilizza come controprestazione in senso tecnico di un contratto.

A tal proposito, il TAR afferma che: "*il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "social network*".

In altri termini, lo sfruttamento economico dei dati e la conseguente applicazione della disciplina del

[72] TAR Lazio, sez. I, sentenza 18 dicembre 2019 – 10 gennaio 2020, n. 261.

[73] V. VESCIO DI MARTIRANO *Si possono cedere i dati a pagamento da parte degli interessati?* 25 luglio 2019, disponibile in https://www.key4biz.it/si-possono-cedere-i-dati-a-pagamento-da-parte-degli-interessati/266715/.

consumatore non sono un "concetto innovativo" o "un'interpretazione estensiva" dei poteri sanzionatori dell'AGCM.

Inoltre, il giudice amministrativo, a sostegno della tesi sul valore economico dei dati, richiama: *i)* "*Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*" del 25 maggio 2016, in cui la Commissione Europea aveva affermato che "*i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto*"; *ii)* il provvedimento PS10601 dell'11 maggio 2017, con cui l'AGCM sanzionava un operatore di *social network*, per PCS nei confronti della propria utenza, osservando che il patrimonio informativo costituito dai dati degli utenti e la profilazione degli utenti medesimi a uso commerciale "*acquista, proprio in ragione di tale uso, un valore economico idoneo, dunque, a configurare l'esistenza di un rapporto di consumo tra il Professionista e l'utente*"[74]; *iii)* la decisione della Commissione Europea del 3 ottobre 2014 , pubblicata il 19 novembre 2014, che ha autorizzato la concentrazione relativa all'acquisizione da parte di Facebook di tale *social network* e nella quale erano presenti considerazioni sul valore economico dei dati degli utenti; iv) il *network* europeo di autorità nazionali per la cooperazione della tutela dei consumatori di cui al Regolamento 2006/2004/CE che, nell'affrontare il tema della possibile contrarietà delle Condizioni d'Uso della piattaforma Facebook alla direttiva 93/13/CEE, ha avuto modo di affermare che tale direttiva "*si applica a tutti i contratti tra consumatori e professionisti, a prescindere dalla natura onerosa di tali contratti, inclusi i contratti in cui il contenuto e la profilazione generati dal consumatore rappresentano la controprestazione alternativa al denaro*"[75].

Inoltre, il TAR spiega come la possibilità di uno sfruttamento economico del dato personale nell'ambito delle piattaforme di *social network,* e la conseguente necessità di tutelare il consumatore, non ricadono solo nella tutela apportata dal GDPR, ma anche da quella a tutela del consumatore.

A sostegno della non sovrapponibilità della tutela della protezione dei dati personali e la protezione del consumatore, il TAR rinvia alle considerazioni svolte dalla Corte di giustizia dell'Unione Europea[76], la quale statuisce che la disciplina consumeristica non trova applicazione "*unicamente quando disposizioni estranee a quest'ultima, disciplinanti aspetti specifici delle pratiche commerciali sleali, impongono ai professionisti, senza alcun margine di manovra, obblighi incompatibili con quelli stabiliti dalla direttiva 2005/29*". In altre parole, si rinvia al concetto, già esaminato sopra, della complementarità e non alternatività tra le due discipline.

Sul punto, infatti, il ricorrente sosteneva che tutte le condotte rientrassero esclusivamente nella

[74] Cfr. il par. 54 del richiamato provvedimento.

[75] Cfr. pag. 19 della lettera del 9 novembre 2016 inviata a Facebook con cui è stata trasmessa la Posizione Comune del Network, allegata alla memoria di parte ricorrente del 28 giugno 2019.

[76] Corte di giustizia UE Sez. 2^, 13/09/2018 Sentenza cause riunite C-54/17 e C-55/17.

materia trattata nel GDPR, con il contestuale rischio della violazione del principio del *ne bis in idem*, scongiurato solo per ora dal giudice di prime cure[77]. Per comprendere meglio tale contestazione, anche alla luce della sua eventuale analisi da parte del giudice di appello che sarà chiamato a decidere, si potrebbe far riferimento ad una recente sentenza del Consiglio di Stato[78], la quale si è occupata del potenziale contrasto del potere sanzionatorio dell'AGCM con quello di altre autorità indipendenti; in particolare, il Consiglio di Stato ha osservato come il divieto del *ne bis in idem* abbia non solo una valenza sostanziale[79], ma anche processuale[80]. La sentenza della Corte di giustizia UE[81], citata anche dal TAR, per stabilire quale sia l'autorità competente, fa riferimento al criterio autonomo della c.d. incompatibilità delle norme. Secondo quest'ultimo, se la condotta già sanzionata fosse compatibile con la regolamentazione di settore, come sembrerebbe nel caso di specie, si applicherebbero soltanto le norme sulle pratiche commerciali scorrette, con conseguente competenza esclusiva dell'AGCM. Ebbene, secondo tale assunto, si escluderebbe a priori l'intervento dell'autorità di settore, ovvero il Garante privacy; di conseguenza, se venisse irrogata una seconda sanzione, essa sarebbe illegittima sia sotto il profilo procedimentale, sia sotto quello sostanziale[82].

Per le stesse ragioni, inoltre, il TAR esclude anche un effetto pluri-sanzionatorio della condotta in quanto si tratta di due condotte differenti: da una parte, la corretta informativa all'interessato al trattamento dei dati personali ai fini dell'utilizzo della piattaforma; dall'altra, la corretta informazione da fornire al consumatore, al fine di consentirgli di effettuare una scelta economica consapevole.

---

[77] Sul punto, inoltre, si segnala che le sanzioni irrogabili ex art. 83 GDPR dal Garante Privacy sarebbero ben più gravi per la violazione degli ex artt. 13 e 14 GPDR sulla corretta informativa all'interessato al trattamento dei dati personali ai fini dell'utilizzo della piattaforma.

[78] Consiglio di Stato, Sezione VI Sentenza 11 novembre 2019, n. 7699.

[79] Con riferimento al piano sostanziale: "*si vieta che per una stessa condotta vengano irrogate, nell'ambito dello stesso processo, due sanzioni in applicazione di norme diverse. Questo risultato viene evitato ricorrendo ai criteri di specialità o di assorbimento-consunzione che stanno alla base del concorso apparente di norme*."

[80]Con riferimento al piano processuale: "*si vieta di iniziare un secondo procedimento una volta definito quello precedente per la stessa condotta. L'art. 649 Cod. proc. pen. prevede che: i) «l'imputato prosciolto o condannato con sentenza o decreto penale divenuti irrevocabili non può essere di nuovo sottoposto a procedimento penale per il medesimo fatto, neppure se questo viene diversamente considerato per il titolo, per il grado o per le circostanze» (comma 1); ii) «se ciò nonostante viene di nuovo iniziato procedimento penale, il giudice in ogni stato e grado del processo pronuncia sentenza di proscioglimento o di non luogo a procedere, enunciandone la causa nel dispositivo» (comma 2). L'art. 4 del Protocollo n. 7 della CEDU prevede che «nessuno può essere perseguito o condannato penalmente dalla giurisdizione dello stesso Stato per un reato per il quale è già stato assolto o condannato a seguito di una sentenza definitiva conformemente alla legge ed alla procedura penale di tale Stato». L'art. 50 della Carta di Nizza prevede che «nessuno può essere perseguito o condannato per un reato per il quale è stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge». Si tratta di un divieto espressione di un diritto fondamentale di civiltà giuridica il quale intende evitare che una persona possa essere esposta senza certezze allo svolgimento di plurimi procedimenti sanzionatori."* Sul punto v. anche Corte cost. n. 43/2018 che statuisce come segue: *"La complessità della tematica del ne bis in idem processuale attiene alla individuazione della nozione di «medesimo fatto» e, dunque, il rischio non è tanto che si applichi la stessa norma in momenti temporalmente diversi ma, all'esito del primo processo, una diversa norma che disciplini il «medesimo fatto». Questa è la ragione per cui anche il ne bis in idem processuale presenta profili di connessione con il concorso di norme. Un primo orientamento ritiene che venga in rilievo il cd. idem legale. Sarebbe sufficiente, pertanto, che cambi la sola qualificazione giuridica della condotta perché si possa iniziare un secondo processo in applicazione di una diversa norma.*

[81] Corte di giustizia UE Sez. 2^, 13/09/2018 Sentenza cause riunite C-54/17 e C-55/17.

[82] Consiglio di Stato, Sezione VI Sentenza 11 novembre 2019, n. 7699.

Ebbene, con riferimento a quest'ultima, il TAR precisa che: "*il valore economico dei dati dell'utente impone al professionista di comunicare al consumatore che le informazioni ricavabili da tali dati saranno usate per finalità commerciali che vanno al di là della utilizzazione del social network: in assenza di adeguate informazioni, ovvero nel caso di affermazioni fuorvianti, la pratica posta in essere può quindi qualificarsi come ingannevole*". In altri termini, il "*claim*" utilizzato da Facebook nella pagina di registrazione ("*Iscriviti è gratis e lo sarà per sempre*"), avente come fine quello di invogliare gli utenti a iscriversi, lasciava intendere l'assenza di una controprestazione richiesta al consumatore in cambio della fruizione del servizio.

Tale pratica, infatti, è stata sanzionata in funzione dell'incompletezza delle informazioni fornite all'utente in quanto consumatore, il quale avrebbe avuto diritto di sapere che il professionista utilizzava i dati dell'utente a fini remunerativi, perseguendo dunque un intento commerciale.

Inoltre, la tesi del ricorrente, secondo cui l'onere informativo imposto a Facebook imporrebbe, ai sensi del GDPR, uno *standard* inconciliabile con gli Orientamenti sulla trasparenza, rimane indimostrata e, anzi, contraddetta dagli "Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali" del 2016, che impongono altresì ai professionisti di non occultare l'intento commerciale di una pratica.

In altri termini, il TAR avalla la valutazione dell'AGCM circa l'ingannevolezza della prima pratica che, impedendo la formazione di una scelta consapevole, è considerata dunque idonea a trarre in inganno il consumatore.

Con riferimento invece alla seconda condotta, quella dove l'AGCM contesta una pratica commerciale aggressiva, il TAR considera errata la ricostruzione del modello di funzionamento del meccanismo di integrazione delle piattaforme riportata nel provvedimento dell'autorità e, di conseguenza, fa emergere l'assenza di elementi idonei a dimostrare l'esistenza di una condotta idonea a condizionare le scelte del consumatore[83].

[83] Così, il TAR Lazio, sez. I, sentenza 18 dicembre 2019 – 10 gennaio 2020, n. 261, che nella sentenza afferma che: "*al fine di realizzare l'integrazione, è necessario compiere numerosi passaggi, che si concludono solo quando, una volta raggiunta tramite il login di Facebook la "app" di terzi, l'utente decide di procedere alla sua installazione.*
Dunque, la "pre-attivazione" della piattaforma Facebook (vale a dire la "pre-selezione" delle opzioni a disposizioni) non solo non comporta alcuna trasmissione di dati dalla piattaforma a quella di soggetti terzi, ma è seguita da una ulteriore serie di passaggi necessitati, in cui l'utente è chiamato a decidere se e quali dei suoi dati intende condividere al fine di consentire l'integrazione tra le piattaforme. L'affermazione dell'Autorità secondo cui la piattaforma di Facebook era "automaticamente attivata con validità autorizzativa generale" non risulta, in definitiva, corretta, avendo di converso dimostrato il professionista che la piattaforma non rappresenta un mezzo attraverso cui gli utenti forniscono il consenso al trasferimento dei dati, dal momento che ciò avviene in un momento successivo, su base granulare per ogni singola "app/sito web".
Deve, poi, osservarsi, che il giudizio circa la presunta natura "aggressiva" delle locuzioni usate per disincentivare l'utente dal disattivare la piattaforma risulta non adeguatamente motivato o approfondito, nonché parzialmente contraddittorio, in quanto sono effettivamente presenti delle conseguenze negative in caso di disattivazione. L'utilizzo, poi, da parte di Facebook di espressioni in alcuni casi dubitative in relazione alle possibili limitazioni nell'uso della

Infine, il TAR afferma anche che la non pertinenza o eccedenza del trattamento dei dati dell'utente, rispetto alla finalità del trattamento stesso, sarebbero di competenza del Garante Privacy, trattandosi di profili che riguardano l'utente in qualità di interessato al trattamento dei dati personali, senza incidere quindi sulla libertà di scelta del consumatore.

Ebbene, a prescindere di cosa deciderà il Consiglio di Stato, il caso Facebook rende evidenti alcuni dei limiti: *i)* il numero delle diverse Autorità procedenti che operano, come vedremo nel seguente paragrafo, su analoga fattispecie in diversi Paesi; la durata delle istruttorie; *ii)* gli importi relativamente limitati (considerate le dimensioni economiche dell'impresa interessata) delle sanzioni cumulate nei vari procedimenti; *iii)* la marginale o carente valutazione della mole di dati oggetto delle condotte controverse.

In questo discorso, la possibile violazione del principio del *ne bis in idem*, rappresenta un rischio per la generalità delle imprese che intendono investire nei Big Data; il rischio riguarda il fatto che una stessa impresa possa essere chiamata a rispondere da più autorità anche all'interno della medesima giurisdizione nazionale, aumentando così il grado complessivo di incertezza ed i costi di *compliance* addossati sugli operatori economici.

A tal proposito, va peraltro aggiunto che il *ne bis in idem* non vieta che l'ordinamento giuridico nazionale possa prevedere risposte repressive complementari in relazione ad una medesima condotta lesiva di beni giuridici distinti, attribuendo le rispettive competenze ad Autorità fra loro autonome[84]. Infatti, la Corte europea dei diritti dell'uomo ha stabilito che l'imposizione di distinte sanzioni sulla medesima condotta, da parte di Autorità differenti, è compatibile con il suddetto principio. Tuttavia, occorre altresì verificare che i "procedimenti convergenti" perseguano obiettivi complementari, sia in astratto che in concreto, avendo cioè riguardo ai distinti aspetti oggetto di autonomo accertamento in merito alla singola condotta illecita[85].

"app" di terzi nel caso di disattivazione dell'integrazione si giustifica in ragione della circostanza che i dati in oggetto sono, per l'appunto, detenuti e trattati da soggetti terzi.
Anche nei casi in cui determinate applicazioni terze prevedano un meccanismo di integrazione diverso dal "Facebook login" (quali i "plug-in" "social" "Mi piace" o "Condividi") Facebook avverte nella Normativa sui dati della possibilità che questi possono ricevere informazioni su ciò che l'utente pubblica o condivide e che "le informazioni raccolte da tali soggetti terzi sono soggette alle loro condizioni e normative, non alle nostre".

[84] CEDU, A e B c. Norvegia, ricc. 24130/11 e 29758/11 (2016), spec. § 121: "*In the view of the Court, States should be able legitimately to choose complementary legal responses to socially offensive conduct (such as non-compliance with road-traffic regulations or non-payment/evasion of taxes) through different procedures forming a coherent whole so as to address different aspects of the social problem involved, provided that the accumulated legal responses do not represent an excessive burden for the individual concerned".*

[85] CEDU, A e B c. Norvegia, cit., §§ 131-132: "*As regards the conditions to be satisfied in order for dual criminal and administrative proceedings to be regarded as sufficiently connected in substance and in time and thus compatible with the bis criterion in Article 4 of Protocol No. 7, the relevant considerations deriving from the Court's case-law, as discussed above, may be summarised as follows. Material factors for determining whether there is a sufficiently close connection in substance include: (i) whether the different proceedings pursue complementary purposes and thus address, not only in abstracto but also in concreto, different aspects of the social misconduct involved; (ii) whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct (idem);*

L'effettiva applicazione degli strumenti di tutela in tema di *Big Data,* di natura anche personale, non può quindi prescindere dalla preliminare applicazione del divieto del *ne bis in idem,* al fine altresì di evitare che l'incertezza ed i conseguenti oneri per le imprese vanifichino ogni incentivo alla concorrenza ed all'innovazione.

3.7 – I diversi strumenti utilizzati da altri Paesi europei e dal Regno Unito

È interessante osservare come anche in altri Stati UE e nel Regno Unito, le condotte di Facebook e di altre società del gruppo siano state esaminate e fronteggiate con strumenti giuridici ed autorità nel settore della tutela dei dati personali.

Infatti, in Francia ad esempio, le questioni relative all'utilizzo di dati da parte dei giganti tecnologici, sono state risolte con gli strumenti del diritto alla *privacy.*

Il primo caso ha riguardato Facebook, che è stato sanzionato da *La Commission nationale de l'informatique et des libertés* (l'autorità francese per la protezione dei dati personali, di seguito anche CNIL), per l'uso del *cookie "datr"* [86] ; quest'ultimo ha consentito all'impresa di raccogliere informazioni sui cittadini francesi ed altri cittadini europei, utilizzando i dati raccolti dal pulsante "Mi piace" e da altri *widget,* per indirizzare meglio gli annunci ai propri utenti, a loro completa insaputa.

Con una decisione del 26 gennaio 2016[87], prima ancora dell'entrata in vigore del GDPR, il presidente della CNIL ha emesso un avviso formale a Facebook Inc. e a Facebook Ireland Limited, chiedendo loro di porre rimedio alle loro numerose violazioni della legge francese del 6 gennaio 1978 sulla protezione dei dati[88].

Quando l'autorità belga per la protezione dei dati ha citato in giudizio Facebook nel 2015, la società ha affermato che il *cookie datr* veniva utilizzato come funzionalità di sicurezza per bloccare spam,

---

(iii) whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection as well as the assessment of the evidence, notably through adequate interaction between the various competent authorities to bring about that the establishment of facts in one set is also used in the other set; (iv) and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent that the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall amount of any penalties imposed is proportionate".

[86] Il cosiddetto *cookie "datr"* è ciò che Facebook utilizza almeno dal 2010 per tracciare gli utenti sul Web, anche se sono disconnessi da Facebook e anche se non hanno un account Facebook. La società lo fa tramite il pulsante "Mi piace" utilizzato da milioni di siti web.

Non è stato Facebook a parlarne per la prima volta ai suoi utenti e al pubblico, ma un ricercatore olandese che ha scoperto alla fine del 2010 che il pulsante Mi piace di Facebook avrebbe trasmesso i dati degli utenti anche se quegli utenti non facevano clic su di esso. Facebook ha definito questo problema un bug e ha detto che avrebbe fornito una soluzione.

[87] CNIL, decisione 2016-007 del 26 gennaio 2016, disponibile in https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000031997148/.

[88] La CNIL ha sottolineato che, secondo la giurisprudenza europea (CGUE, 1° ottobre 2015, C-230/14, *Weltimmo*; e CGUE, 13 maggio 2014, C-131/12, Costeja), le due società sono vincolate dal *Data Protection Act* nella misura in cui Facebook France deve essere considerata uno "stabilimento" di queste due società ai sensi della direttiva 95/46 / CE del 24 ottobre 1995. La CNIL ha anche affermato che le due società sono responsabili in solido nella misura in cui entrambe determinano perché e come vengono elaborati i dati.

account falsi, *botnet* e così via. La società sosteneva che il *cookie* fosse necessario per la protezione dei suoi utenti e che l'agenzia belga non avrebbe dovuto vietarne l'uso.

A tal proposito, la CNIL si è unita ad altri quattro paesi (Belgio, Paesi Bassi, Spagna e Germania) in un'indagine europea sulle pratiche relative ai dati di Facebook; a tal riguardo, l'indagine della CNIL ha scoperto diversi vizi di conformità della piattaforma[89].

L'autorità francese non ritiene che il semplice fatto che gli utenti inseriscano i propri dati sensibili, costituisca un consenso espresso ai sensi dell'articolo 8 della legge sulla protezione dei dati; essa aggiunge, inoltre, che gli utenti devono essere in grado di dare tale consenso, spuntando una casella specifica dopo aver saputo come queste informazioni vengono utilizzate.

L'autorità francese accusa le società del gruppo Facebook di aver violato il loro dovere di informare le persone interessate al loro trattamento dei dati: in particolare, la CNIL fa presente che non solo il *form* per l'iscrizione al *social network* non contiene alcuna informazione sul trattamento dei dati personali, ma anche che le società non hanno informato gli utenti sull'inserimento dei *cookie* sul loro dispositivo al momento della registrazione. A tal proposito, la CNIL considera questa condotta come una violazione dell'articolo 32 della legge sulla protezione dei dati.

La CNIL ha riscontrato inoltre una violazione dell'obbligo di una giustificazione giuridica per il trasferimento dei dati negli USA, sottolineando che *Safe Harbor* non costituisce più un valido motivo giuridico per i trasferimenti di dati al di fuori dell'Unione Europea, in quanto è stato invalidato il 6 ottobre 2015[90].

L'autorità francese ha inoltre accusato Facebook: di non comunicare agli utenti come sarebbero stati utilizzati i loro dati nei moduli di registrazione, di non consentire agli utenti di bloccare i *cookie datr* (come richiesto dalla vecchia "*legge sui cookie dell'UE*") e di non dimostrare una reale necessità di conservarli a tempo indeterminato.

L'agenzia francese ha terminato l'indagine sanzionando Facebook per tali condotte perpetrate a danno degli utenti.

Allo stesso tempo, il 9 febbraio 2016, la Direzione generale francese per la concorrenza, i consumatori e la frode (DGCCRF) ha concesso a *Facebook Ireland* e *Facebook Payments International Ltd* due mesi per eliminare o modificare alcune clausole illecite nei loro Termini di servizio. Ebbene, dopo solo due settimane da questi avvertimenti, la clausola che concede la giurisdizione ai tribunali della California, è stata dichiarata abusiva dalla Corte d'Appello di Parigi, la quale ha stabilito che i

[89] La CNIL ha elencato non meno di nove violazioni del *Data Protection Act* commesse dalle due società di Facebook, riguardanti in particolare: i) l'obbligo di fornire una giustificazione giuridica quando si combinano i dati; ii) il principio di proporzionalità dei dati raccolti; iii) il principio della correttezza della raccolta e del trattamento dei dati personali; iv)l'obbligo di stabilire un periodo di conservazione proporzionato allo scopo del trattamento; v) l'obbligo di garantire la sicurezza dei dati; e vi) l'obbligo di espletare alcune formalità prima del trattamento dei dati sensibili.

[90] CGUE, 6 ottobre 2015, C-362/14, Schrems.

tribunali francesi hanno giurisdizione per esaminare eventuali controversie tra i *social* e un utente francese[91].

Altro caso francese ha riguardato lo scambio dei dati tra WhatsApp e Facebook, anch'esso oggetto di analisi da parte della CNIL.

L'indagine è partita dopo che il gruppo *Working Party 29 – WP29,* che comprende i capi di tutte le agenzie nazionali per la protezione dei dati nell'Unione europea, ha indagato sulla condivisione dei dati di WhatsApp con Facebook, a valle dell'acquisizione della prima da parte di questa seconda. Il WP29 ha osservato che WhatsApp ha trasferito i dati dei suoi utenti su Facebook per scopi di "*business intelligence*" e "sicurezza". Questi dati includevano i numeri di telefono degli utenti e le loro abitudini di utilizzo delle applicazioni.

Il presidente della CNIL ha ritenuto che, sebbene la raccolta dei dati a fini di sicurezza sembrasse accettabile, i dati raccolti per la *business intelligence* non erano conformi alle leggi dell'UE in materia di trattamento dei dati. La CNIL ha osservato che né il consenso degli utenti, né il "legittimo interesse" di WhatsApp, possono essere utilizzati come argomenti legali per questo tipo di raccolta dati.

In tale caso, l'accertamento si è tuttavia limitato ai profili relativi al corretto trattamento dei dati e al consenso dell'interessato: in particolare, la CNIL, nel dicembre 2017, ha rilevato che i trasferimenti di dati tra WhatsApp e Facebook, avvenivano in parte senza il consenso degli utenti, e ha stabilito tre mesi di tempo per bloccare ogni condivisione di dati, che avvenisse senza un consenso necessario e preventivo dell'utente. WhatsApp, inoltre, si è rifiutata di fornire alla CNIL un campione dei dati raccolti dai cittadini dell'UE in quanto, secondo la società, i dati venivano archiviati negli Stati Uniti. A tal proposito, il garante francese ha respinto le argomentazioni difensive di Whatsapp, secondo le quali la società sarebbe stata soggetta solo alla legge degli Stati uniti.

A differenza dell'atto amministrativo emanato dall'autorità antitrust italiana, quello emanato dal garante privacy francese non è stato un provvedimento sanzionatorio, bensì un mero odine di cessazione.

Nel Regno Unito, ad ottobre 2018, l'*Information Commissioner's Office*[92] (di seguito anche ICO) ha inflitto a Facebook una sanzione pecuniaria pari a 500.000 sterline[93] (il massimo edittale previsto in

[91] Corte d'appello di Parigi, 12 febbraio 2016, n. 15/05624.

[92] L'*Information Commissioner's Office* (ICO) è l'autorità di regolamentazione indipendente del Regno Unito per la protezione dei dati e la legge sui diritti di informazione, che sostiene i diritti di informazione nell'interesse pubblico, promuove l'apertura da parte degli enti pubblici e la privacy dei dati per le persone.
L'ICO ha responsabilità specifiche stabilite nel Data Protection Act 2018 (DPA2018), nel Regolamento generale sulla protezione dei dati (GDPR), nel Freedom of Information Act 2000 (FOIA), nei regolamenti sulle informazioni ambientali 2004 (EIR) e nei regolamenti sulla privacy e sulle comunicazioni elettroniche del 2003 (PECR).

[93] Maggiori informazioni sulla multa sono disponibile sul sito https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/#.

sede civile dalla normativa applicabile al tempo in cui si sono verificate le condotte[94]).

Ebbene, secondo l'indagine condotta dall'ICO, è emerso che, tra il 2007 e il 2014, Facebook avrebbe elaborato le informazioni personali degli utenti in modo non corretto, consentendo agli sviluppatori di applicazioni di accedere alle loro applicazioni, senza un consenso chiaro ed informato degli utenti stessi.

In particolare, Facebook non è stato in grado di mantenere le informazioni personali degli utenti al sicuro, in quanto non è riuscito ad effettuare gli adeguati controlli su *app* e sviluppatori che utilizzavano la sua piattaforma; i dati degli utenti sono stati raccolti da uno sviluppatore, il dottor Aleksandr Kogan e la sua impresa GSR, che li hanno usati e condivisi con altre organizzazioni, tra cui, SCL Group, la società *holding* di *Cambridge Analytica*, coinvolta nelle note campagne politiche statunitensi.

In particolare, l'autorità inglese ha scoperto che le informazioni personali di almeno un milione di utenti del Regno Unito, erano tra i dati raccolti e erano dunque a rischio di un ulteriore illecito utilizzo.

In Germania, invece, come abbiamo potuto esaminare nel precedente capitolo, il *Bundeskartellamt* è intervenuto nel 2016 nei confronti di Facebook, utilizzando gli strumenti di diritto *antitrust*[95].

A tal proposito, va precisato che quelle autorità antitrust che, come quella tedesca, non possiedono entrambi gli strumenti (il diritto antitrust e la tutela del consumatore) sono definite da alcuni studiosi come autorità "monche"[96], in quanto non sono in grado di far comunicare queste due anime tra di loro; infatti, se ci fosse stato dialogo tra queste due anime, probabilmente la corte di giustizia federale (il *Bundesgerichtshof)* avrebbe deciso diversamente il caso Facebook.

In conclusione, appare evidente che uno stesso fatto o una stessa condotta siano stati interpretati diversamente nei diversi paesi; pertanto, sarebbe necessario individuare standard di riferimento comuni ed omogenei, in grado di interpretare in modi uguali situazioni uguali. Al momento, lo sforzo che si è fatto con la proposta di regolamento europeo DMA non sembra sufficiente a dare questi tipi di risposte.

3.8 – Le *class action* e il *private enforcement*

Le azioni rappresentative risarcitorie o *class action* rientrano a pieno titolo nel pacchetto di riforme in orbita *Digital Single Market Strategy*. In particolare, con riferimento alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, è intervenuta di recente la direttiva (UE) 2020/1828

[94] Questa multa è stata scontata ai sensi del Data Protection Act 1998. È stata sostituita a maggio dal nuovo *Data Protection Act* 2018, insieme al GDPR. Questi forniscono una gamma di nuovi strumenti di applicazione per l'ICO, comprese multe massime di £ 17 milioni o il 4% del fatturato globale.

[95] Cfr. § 2.1.4

[96] Così *ex multis* v. M. MAGGIOLINO, *op.cit.*

del 25 novembre 2020, pubblicata il 4 dicembre 2020, che ha altresì abrogato la direttiva 2009/22/CE[97]. Inoltre, da ultimo, la proposta di regolamento del DSA pubblicata il 15 dicembre 2021 prevedrebbe all'articolo 72 emendamenti della direttiva 2020/1828.

Quest'ultima, mediante incisive modifiche alla Direttiva 2009/22/CE (concernente le azioni collettive inibitorie e recepita in Italia con gli artt. 139 e 140 del Codice del consumo), introduce dunque, per la prima volta sul piano unionale, la figura delle azioni rappresentative risarcitorie (*class action*)[98].

La direttiva, da una parte, prevede una nuova azione rappresentativa volta ad ottenere una tutela risarcitoria e, dall'altra parte, scoraggia eventuali abusi nelle iniziative legali, grazie al principio per cui la parte soccombente paga le spese. In altri termini, la direttiva cerca di creare un giusto bilanciamento tra i diversi interessi in gioco, proteggendo i soggetti deboli, senza però esporre i professionisti ad azioni abusive o pretestuose; ad esempio, l'azione a tutela dei consumatori non è esperibile da parte di studi legali. Solo gli enti legittimati, come le associazioni dei consumatori, possono infatti rappresentare gruppi di consumatori e agire per tutelarli. Inoltre, a differenza della direttiva del 2009, ora abrogata, il legislatore europeo ha aggiunto al rimedio inibitorio anche quello risarcitorio.

Tali azioni rappresentative sono volte ad assicurare il ristoro degli interessi economici dei consumatori, i quali subiscono un pregiudizio dalla violazione di norme a loro tutela, ivi comprese le disposizioni in materia di PCS, diritti dei consumatori nei contratti e clausole vessatorie, mediante l'emanazione di un provvedimento risarcitorio o inibitorio; si obbligherebbe altresì il professionista a provvedere, a seconda del caso, all'indennizzo, alla riparazione, alla sostituzione, alla riduzione del prezzo, alla risoluzione del contratto o al rimborso del prezzo pagato.

Relativamente all'ambito di applicazione della direttiva, all'art. 2 si legge che: "*Essa si applica alle violazioni nazionali e transfrontaliere, anche qualora tali violazioni siano cessate prima che sia stata avviata l'azione rappresentativa o qualora dette violazioni siano cessate prima della conclusione dell'azione rappresentativa*" e che: "*La presente direttiva non pregiudica le norme dell'Unione in materia di diritto privato internazionale, in particolare quelle relative alla giurisdizione degli organi giudiziari nonché al riconoscimento e all'esecuzione delle decisioni in materia civile e commerciale e alle norme sul diritto applicabile alle obbligazioni contrattuali ed extra-contrattuali*."

Tra le maggiori novità di questa direttiva troviamo: *i)* l'obbligo per gli Stati membri di istituire un sistema di azioni rappresentative per la protezione degli interessi collettivi dei consumatori contro violazioni del diritto dell'Unione, contemplando azioni relative sia a provvedimenti inibitori che a

[97] Cfr. GU L 409/1.

[98] In dottrina v. R. CHIEPPA, *Ruolo dell'AGCM nel private enforcement e possibili ambiti di cooperazione con il giudice civile*, E.A. RAFFAELLI, *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019; J. NISTICÒ, *La tutela collettiva*, in Catricalà A., Cazzato C.E., Fimmanò F. (a cura di), Diritto antitrust, Giuffrè, 2021.

provvedimenti risarcitori; *ii)* l'istituzione di appositi enti legittimati designati dagli Stati membri a chiedere provvedimenti inibitori e/o risarcitori, quali l'indennizzo o la sostituzione, per conto di un gruppo di consumatori danneggiato da un operatore economico che si presume abbia violato uno degli atti giuridici dell'UE in relazione ai servizi finanziari, ai viaggi e al turismo, all'energia, alla sanità, alle telecomunicazioni e alla protezione dei dati; *iii)* la distinzione tra enti legittimati che hanno il diritto di intentare azioni nello Stato membro in cui sono stati designati (azioni rappresentative nazionali), e quelli che hanno il diritto di intentare azioni in qualsiasi altro Stato membro (azioni rappresentative transfrontaliere): *iv)* l'imposizione sugli enti legittimati di una serie di obblighi di trasparenza, in particolare riguardo al loro finanziamento da parte di terzi.

Gli enti, per essere legittimati alle azioni rappresentative, devono altresì rispondere a determinati requisiti. Innanzitutto, non devono avere scopo di lucro, l'oggetto sociale deve riguardare la tutela dei consumatori ed è richiesta una certa solidità economica (l'ente non deve essere dichiarato insolvente). Infine, va rispettato il requisito di trasparenza, secondo il quale l'organizzazione deve essere indipendente da influenze di professionisti che abbiano un interesse economico a sostenere l'azione rappresentativa. Ogni Stato membro deve comunicare alla Commissione europea un elenco degli enti legittimati, i quali rispettano i criteri previsti nella direttiva.

La direttiva, dunque, si prefigge l'obiettivo di tutelare il consumatore nel mercato interno europeo inteso come uno spazio senza frontiere, nel quale, ai sensi dell'art. 26 c. 2 TFUE, è assicurata la libera circolazione delle merci e dei servizi. La direttiva si applica a diversi settori come: i servizi finanziari, la protezione dei dati, i viaggi, il turismo, l'energia, la sanità e le telecomunicazioni.

Da una parte, il mercato interno dovrebbe fornire teoricamente un valore aggiunto ai consumatori, ad esempio, per la qualità superiore o la maggiore varietà di beni e servizi offerti. Dall'altra parte, le politiche dell'Unione dovrebbero offrire un livello elevato di protezione ai sensi dell'art. 38 Carta dei diritti fondamentali dell'Unione europea – CDFUE (c.d. Carta di Nizza).

La nuova direttiva mira a concretizzare tali principi, ma bisognerà vedere se ciò accadrà anche nella pratica. Nel mentre, gli Stati membri dovranno adottare o pubblicare le disposizioni legislative, regolamentari e amministrative, necessarie per conformarsi alla presente direttiva, entro e non oltre il 25 dicembre 2022, e le relative disposizioni saranno applicate a decorrere dal 25 giugno 2023.

Una piena implementazione del decreto di recepimento della Direttiva è tanto più necessaria proprio in quelle giurisdizioni, come quella italiana, in cui i soggetti più esposti e al contempo meno consapevoli – ovvero consumatori, piccole-medie imprese e pubbliche amministrazioni – devono ancora acquisire un'effettiva cognizione delle potenzialità del *private enforcement*.

Sul piano nazionale, il 12 aprile 2019 è stata approvata la legge n. 31/2019, la quale trasferisce la disciplina dell'azione collettiva risarcitoria (e inibitoria) dal Codice del consumo al Codice di

procedura civile, con l'introduzione del Titolo VIII-bis rubricato "Dei procedimenti collettivi" e, in particolare, degli artt. 840bis - 840 *quinquisdecies* in materia di "azione di classe", disciplinata fino all'aprile di quest'anno dall'art. 140-bis del Codice del consumo.

La nuova *class action* nazionale può essere azionata sia da un'organizzazione o un'associazione senza scopo di lucro[99], sia da ciascun componente della classe. Tale azione è caratterizzata dal fatto che: a) non richiede un mandato per intentare l'azione rappresentativa; b) contempla una adesione c.d. rafforzata e; c) prevede un sistema di *opt-in* efficace per i soli consumatori aderenti.

Ebbene, alla luce della direttiva del 2020 sull'azione rappresentativa europea, l'azione disciplinata dalla legge 13/2019 non potrà che essere oggetto di una revisione, se non altro in relazione ai soggetti legittimati a esercitare l'azione e in relazione al sistema probatorio. Il legislatore nazionale, nel dare attuazione alla direttiva, dovrà infatti riconoscere efficacia vincolante alle "decisioni definitive[100]", adottate anche dalle autorità amministrative indipendenti (come l'AGCM in ambito consumeristico); peraltro, ordinamenti di altri Stati membri, come quello tedesco, riconoscono già da tempo l'effetto vincolante delle decisioni delle autorità di concorrenza, sia nazionali che degli altri Stati membri.

Tuttavia, nell'attuale versione dell'azione rappresentativa italiana molti limiti precedenti sono stati superati: i) l'ambito di applicazione soggettiva è stato ampliato, essendo la nuova azione esperibile non più soltanto dai consumatori, ma anche da professionisti, imprese, associazioni senza scopo di lucro, investitori, azionisti, lavoratori; ii) la legittimazione ad agire è stata attribuita, oltre che ai componenti della classe, anche alle associazioni e alle organizzazioni senza scopo di lucro; iii) le adesioni sono consentite non solo dopo il superamento del filtro di ammissibilità, ma anche dopo la sentenza con cui il tribunale accerta la violazione denunciata; iv) i costi da sostenere per promuovere l'azione collettiva sono stati sensibilmente ridotti e; v) è stato introdotto un sistema di incentivi per i difensori del ricorrente e per il rappresentante comune della classe.

Nonostante questi miglioramenti effettuati dalla riforma, e sebbene l'azione di classe ambirebbe a offrire uno strumento per gestire processualmente i contenziosi seriali e a disincentivare comportamenti opportunistici da parte delle imprese, tale azione non sembra al momento dare le

[99] I loro obiettivi statutari comprendono la tutela di diritti individuali omogenei e sono iscritte in un elenco pubblico istituito presso il Ministero della giustizia.

[100] Infatti, all'art. 3, n. 9 della direttiva (UE) 2020/1828 del 25 novembre 2020 si legge che per "decisione definitiva" si intende: "*una decisione di un organo giurisdizionale o di un'autorità amministrativa di uno Stato membro contro cui non si può o non si può più ricorrere con mezzi d'impugnazione ordinari*". Poiché la Direttiva, fa riferimento unicamente alle decisioni di accertamento dell'illecito, l'effetto vincolante va riconosciuto solo ai provvedimenti di condanna, non potendo riguardare ciò che non è stato accertato e, dunque, le lettere di archiviazione e le decisioni di accettazione degli impegni. Tant'è che, là dove il giudice amministrativo dovesse annullare il provvedimento dell'Autorità, anche per un vizio non meramente procedurale ma attinente al merito della decisione, il potere del giudice civile di valutare i fatti tornerebbe ad essere pieno e l'azione di risarcimento del danno diventerebbe stand alone, senza alcun effetto vincolante derivante dalla pronuncia del giudice amministrativo. Allo stesso modo, se l'autorità, o in seconda battuta il giudice, dovessero limitare temporalmente l'accertamento dell'illecito, la limitazione della durata non assume carattere vincolante e ben potrebbero essere fornite al giudice civile le prove di una durata più estesa.

risposte che ci si aspettava.

La Legge 31/2019 è entrata in vigore il 18 maggio 2021 e contestualmente all'entrata in vigore della nuova legge sono abrogate le corrispondenti disposizioni sull'azione di classe contenute nel Codice del Consumo (artt. 139, 140 e 141 d.lgs. n. 229/2003).

La legge introduce una disciplina organica dell'azione di classe, che dal Codice del consumo, dove attualmente si trova, viene riportata all'interno del Codice di procedura civile, in chiusura del Libro IV. In particolare, dopo il Titolo VIII dedicato alla disciplina dell'Arbitrato è inserito il nuovo Titolo VIII-bis "Dei procedimenti collettivi" (artt. da 840-bis a 840-sexiesdecies), nel quale è appunto disciplinata l'azione di classe.

Se si guarda allo sviluppo dei sistemi di risoluzioni delle liti, un ruolo decisivo lo hanno assunto nell'ultimo decennio le forme di mediazione o composizione delle controversie alternative al giudizio: l'Arbitro bancario e finanziario – Abf (in materia di diritto bancario) e l'Arbitro per le controversie finanziarie – Acf (in materia di diritto dei mercati finanziari), che rappresentano oggi un fondamentale strumento di accesso alla giustizia nella soluzione delle controversie tra intermediari finanziari e clienti. La pratica, dunque, sembrerebbe insegnare che l'azione collettiva non è stata finora uno strumento idoneo e sufficiente per risolvere i problemi del contenzioso seriale nel processo civile italiano.

Lo stesso ragionamento può replicarsi con riferimento alla regolazione del mercato; molto spesso il contenzioso seriale si inserisce infatti in mercati regolati, nei quali vi è un penetrante intervento delle autorità indipendenti che esercitano poteri *ex ante*.

Con riferimento ad esempio all'Autorità antitrust, essa esercita poteri preventivi con riguardo al mercato, alla liceità delle clausole contrattuali e alle pratiche commerciali poste in essere dalle imprese. Dunque, in termini regolatori, sarebbe ragionevole chiedersi se l'azione collettiva non finisca in realtà per generare costi che aumentano il prezzo finale a detrimento dei consumatori; sarebbe quindi necessaria una valutazione costi benefici, al fine di vagliare le conseguenze sul prezzo ultimo per i consumatori.

Infine, l'azione di classe funziona quando gli avvocati, come avviene negli Stati uniti con le c.d. *contigency fee*, hanno rilevanti incentivi economici a promuovere la causa e investono risorse proprie per portarla a termine con successo. Tuttavia, tale problematica non si porrebbe nella *class action* europea, così come delineata dalla direttiva del 2020 in attesa di recepimento, in quanto essa non sarebbe esperibile da studi legali. Sarà quindi curioso vedere come, alla luce del recepimento di quest'ultima direttiva, il legislatore nazionale intenderà rimettere mano alla Legge 13/2019, in particolare con riferimento ai soggetti legittimari ad esercitare l'azione.

3.9 – Conclusioni

La materia in esame pone nuove sfide, e sono ancora in fase di definizione i rapporti tra le diverse discipline ed approcci delle varie Autorità.

In Italia, l'AGCM ha affrontato la questione dell'accesso dell'operatore ai dati attraverso lo strumento del Codice del Consumo, in un'ottica complementare alla tutela della *privacy*. Il caso Facebook mostra altresì come altre Autorità abbiano affrontato il tema sotto diversi profili: l'Autorità tedesca si è attivata con i poteri di diritto *antitrust*, mentre in Francia e nel Regno Unito il tema è stato esaminato sotto il profilo del diritto della *privacy*.

La soluzione a tali condotte potrebbe certo essere quella di richiedere una maggiore informativa e un corretto modo di acquisizione del consenso, senza la necessità di ricorrere al diritto *antitrust*. Infatti, tanto più i consumatori sono informati e consapevoli in relazione alle proprie scelte di consumo, tanto più le imprese possono concorrere tra loro differenziando le proprie offerte di servizi digitali in relazione al diverso grado di utilizzo dei dati personali.

Anche dal punto di vista di tutela del consumatore, potrebbe essere opportuno un approfondimento dei rapporti con la disciplina della *privacy*.

Come si è visto sopra, le due aree si pongono essenzialmente su due piani paralleli ma complementari, dove la disciplina sulle PCS amplifica la tutela offerta dalla disciplina *privacy*: lo strumento dell'informativa per il consenso all'acquisizione, utilizzazione e trattamento dei dati non appare infatti sempre idoneo a garantire agli utenti un quadro conoscitivo chiaro, circa la raccolta e utilizzo dei relativi dati.

Forme di coordinamento AGCM e *Privacy* appaiono sicuramente idonee a rafforzare la tutela offerta, sembra altresì esservi spazio per andare in questa direzione, come dimostra la riflessione congiunta oggetto dell'indagine conoscitiva in materia di *Big Data* conclusa a febbraio 2020 da AGCM, Garante *Privacy* e AGCOM.

Sotto il profilo dell'*enforcement*, considerata la velocità con cui cambia la realtà in esame, va sicuramente migliorata la tempistica dei procedimenti, per evitare che i tempi dell'economia non siano al passo con quelli del diritto; occorre, ad esempio, che l'intervento *antitrust* arrivi tempestivamente, e non a distanza di diversi anni quando la realtà su cui l'intervento dovrebbe incidere è ormai radicalmente mutata. A livello comunitario, l'esito del contenzioso è infatti talvolta pervenuto dopo numerosi anni dal momento in cui si era verificata la condotta nel mercato, in un contesto in cui i mercati e la società erano già significativamente mutati[101].

Sotto questo profilo, affrontare la questione con i poteri in materia di tutela del consumatore ha

[101] V. caso Intel, in cui sono trascorsi 10 anni tra l'avvio, nel 2007, e la pronuncia della Corte di Giustizia che nel 2017 ha annullato la decisione.

senz'altro il vantaggio di consentire procedimenti rapidi, i quali si concludono in pochi mesi.

Se è vero che il massimale edittale attualmente previsto potrebbe non risultare un sufficiente deterrente, il nuovo pacchetto di misure legislative, di cui fanno parte anche il *New Deal for Consumers* e la nuova proposta di regolamento della Commissione (il DMA), prevede un sistema di calcolo della sanzione basato sul fatturato, che potrebbe aumentare l'effetto deterrente nei confronti delle grandi piattaforme digitali e, quindi, l'incisività dell'intervento.

Appare altresì opportuno il rafforzamento dei poteri di acquisizione delle informazioni da parte delle autorità di concorrenza, anche al di fuori dei procedimenti istruttori (indagini conoscitive, attività preistruttoria), con la possibilità di irrogare sanzioni amministrative in caso di rifiuto o ritardo nel fornire le informazioni richieste o in presenza di informazioni ingannevoli od omissive. In questa direzione è infatti orientata anche la cornice normativa in materia di protezione dei dati personali[102].

Possibili soluzioni per le criticità riscontrate sembrano altresì emergere dagli sviluppi che hanno interessato il caso Facebook negli ultimi mesi. Le autorità nazionali a tutela dei consumatori, riunite nel *Consumer Protection Cooperation Network* – CPC, hanno infatti avviato, ai sensi del Regolamento (CE) 2006/2004[103], un'azione coordinata che, ad aprile 2019, ha condotto Facebook ad impegnarsi formalmente dinanzi alla Commissione europea a modificare i termini d'uso del proprio servizio, per superare entro il mese di giugno 2019 le problematiche rilevate[104]. L'azione congiunta delle autorità nazionali, sotto il coordinamento della Commissione nell'ambito del CPC, può essere replicata in materia di diritto *antitrust* dallo *European Competition Network – ECN*, ed in materia di protezione dei dati personali dallo *European Data Protection Board – EDPB*.

A livello di Unione europea, l'instaurazione di meccanismi stabili di coordinamento sembra, dunque, la chiave per assicurare l'intervento efficace degli Stati membri di fronte ad operatori attivi su scala sovranazionale.

Nello stesso senso, quanto alla necessità del miglior coordinamento, in sede non solo di *public enforcement* ma anche di *advocacy*, depongono a livello nazionale sia le *Linee Guida e Raccomandazioni di Policy sui Big Data* sia la *Indagine conoscitiva sui Big Data (*a cui hanno preso parte AGCM, AGCOM e Garante per la protezione dei dati personali). In questi documenti, le Autorità coinvolte intendono istituire una cooperazione tra loro permanente a partire dalla

[102] Cfr. artt. 157 e 166, comma 2, del Codice in materia di protezione dei dati personali.

[103] Regolamento (CE) n. 2006/2004 del parlamento Europeo e del Consiglio, del 27 ottobre 2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori (*Regolamento sulla cooperazione per la tutela dei consumatori*), in GUUE L 364 del 9 dicembre 2004, 1–11.

[104] In proposito, si veda il seguente comunicato stampa della Commissione europea: *Su richiesta della Commissione europea e delle autorità di tutela dei consumatori, Facebook modifica le proprie condizioni d'uso e chiarisce come vengono utilizzati i dati dei consumatori*, IP/19/2048 del 9 aprile 2019.

sottoscrizione di uno specifico *memorandum of understanding*[105].

Ebbene, oltre che attraverso l'effettiva implementazione di procedure di coordinamento tra le diverse autorità settoriali, i rischi di violazione del principio del *ne bis in idem* potranno essere ridotti applicando un più intenso *standard* di motivazione dei provvedimenti adottati sui requisiti oggettivi distintivi posti a fondamento della rispettiva competenza. A tal proposito, rimane poi compito delle Corti – a conclusiva garanzia del sistema in sede di sindacato giurisdizionale dei provvedimenti assunti dalle autorità amministrative – vigilare sui limiti delle rispettive aree di intervento nell'interpretazione della legge, alla ricerca del miglior bilanciamento tra i diritti fondamentali dei consumatori e delle imprese. A tal riguardo, la nuova *class action* europea sarà senz'altro uno strumento utile da tenere in considerazione.

[105] Si vedano le già citate *Linee guida e Raccomandazioni di Policy sui big data*, ove al punto 11 si legge tra l'altro che "*le tre Autorità, nell'esercizio delle competenze complementari ad esse assegnate e che contribuiscono a fronteggiare le criticità dell'economia digitale, si impegnano a strette forme di collaborazione negli interventi che interessano i mercati digitali, anche attraverso la sottoscrizione di un memorandum of understanding*".

CAPITOLO IV

Il nuovo mercato dei servizi di pagamento dopo la PSD2: il ruolo dei Big Data ed il c.d. *mobile payment*

Sommario: *Premessa* **4.1** *Il nuovo quadro regolamentare della PSD2: l'introduzione di due nuovi servizi di pagamento e di nuovi operatori (i c.d. TPPs) tra protezione dei dati personali, responsabilità e concorrenza* **4.1.1** *Il nuovo mercato dei servizi di pagamento* **4.1.2** *Profili di protezione dei dati personali tra GDPR e PSD2* **4.1.3** *L'ingresso dei TPPs nel mercato dei servizi di pagamento: profili di diritto della concorrenza* **4.1.4** *Profili di responsabilità e di autorizzazione dei TPPs* **4.2** *Le ultime innovazioni tecnologiche legate al mercato dei pagamenti:* **4.2.1** *L'accesso ai conti tramite le Application Programming Interfaces (APIs)* **4.2.2** *I Big Data e i pagamenti digitali: il c.d. mobile payment* **4.2.3** *Modalità innovative di analisi dei dati nel mobile payment* **4.2.4** *L'utilizzo dei Big Data nel settore creditizio e questioni giuridiche in comune con il mobile payment: possibili soluzioni?* **4.3** *Conclusioni*

Premessa

L'innovazione tecnologica ha segnato non solo i mercati privi di regolamentazione, ma anche quelli regolamentati, come quello bancario e finanziario[1].

La rivoluzione digitale costituisce un elemento di forte discontinuità non solo per i mercati di beni e di servizi, ma anche per i rapporti tra imprese e consumatori/utenti[2].

Da una parte, gli operatori tradizionali del settore creditizio, ricompresi nel perimetro della vigilanza, hanno incrementato la qualità e la quantità dei servizi offerti, sviluppando nuove tecniche di gestione dei rischi e una più efficace e sicura gestione dei pagamenti. Dall'altra parte, operatori estranei al perimetro della vigilanza, quali le imprese operanti nel settore *FinTech*[3], hanno potuto offrire servizi (e.g. servizi di pagamento) che inizialmente erano ad esclusivo appannaggio del sistema bancario[4].

---

[1] EUROPEAN BANKING AUTORITY, *Report on Big Data and Advanced Analytics*, in https://eba.europa.eu/sites/default/documents/files/document_library//Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf, gennaio 2020 (data ultima visita: 14 marzo 2021); F. DI PORTO, G. GHEDINI, "*I Access Your Data You Access Mine". Setting a Reciprocity Clause for the "Access to Account Rule" in the Payment Services Market* in *www*.papers.ssrn.com, giugno 2019, p. 4.

[2] Si veda l'intervento di C. BARBAGALLO, Capo del Dipartimento Vigilanza Bancaria e Finanziaria della Banca d'Italia, presso il Convegno Invernale 2019 – Associazione dei docenti di economia degli intermediari e dei mercati finanziari e finanza d'impresa: *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, Napoli, 8 febbraio 2019.

[3] Con il termine inglese *FinTech* ci si riferisce alla *Financial Technology*, ossia all'offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica, che comportano forti spinte innovative nel mercato dei servizi finanziari. Sul tema, cfr. European Central Bank and Banca d'Italia joint conference, *Digital transformation of the retail payments ecosystem*, Intervento del Governatore della Banca d'Italia Ignazio Visco, Roma, 30 novembre 2017.

[4] G. BIFERALI, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Diritto inf. e inform.*, fasc. 3, giugno 2018, p. 487.

Il *FinTech* investe oramai ogni segmento dei mercati dei servizi bancari e finanziari, modificandone altresì la struttura ed eliminando le tradizionali barriere all'ingresso, al fine di agevolare l'accesso al mercato da parte di nuovi operatori, grazie anche all'abbattimento dei costi fissi d'impresa.

In altri termini, l'innovazione tecnologica è dunque il *passepartout* attraverso cui le imprese che in passato non avrebbero avuto possibilità alcuna di affermarsi in un mercato governato da regole tradizionali, ora assurgono al ruolo di nuovi ed aggressivi *players*, scardinando le posizioni dominanti. Ciò ha altresì costretto i tradizionali *incumbents* ad investire, a loro volta, nell'innovazione tecnologica ed a rinunciare a quote di mercato considerate in precedenza immutabili.

Infatti, il centro dell'innovazione, in relazione ai servizi finanziari, si sta rapidamente spostando verso nuovi attori non finanziari, che fino ad oggi non avevano mai presidiato questo tipo di servizi. Pertanto, la competizione non è più spinta solo dall'attività dei tradizionali *incumbent*, che da sempre dominano il settore, ma anche da nuove realtà imprenditoriali, specializzate in tecnologie innovative, che minacciano di sottrarre importanti fette di mercato ai *player* tradizionali[5].

Sono diversi gli elementi che stanno contribuendo a dare nuova forma alla competizione e all'offerta dei servizi finanziari: *i)* il crescente utilizzo delle tecnologie e delle soluzioni digitali da parte dei consumatori; *ii)* la volontà di questi ultimi di non essere più meri soggetti destinatari di prodotti, ma di essere al centro dell'offerta del servizio; e *iii)* l'evoluzione del quadro normativo in Europa, diretto ad abbassare le barriere all'entrata e ad agevolare l'ingresso a nuovi operatori.

Con particolare riferimento alle tecnologie legate al sistema dei pagamenti, sono state numerose le innovazioni introdotte: alcune riguardano l'utente finale, in quanto mutano profondamente il modo in cui viene effettuato un pagamento; altre, invece, invisibili all'utente finale, sono relative ai processi interni di trasferimento del denaro.

Il mercato dei pagamenti è fortemente legato al contesto tecnologico e, storicamente, è sempre stato sulla frontiera dell'innovazione; in diversi casi si è potuta osservare la trasformazione di alcuni operatori che, da fornitori di servizi attivi in altri settori (e.g. nelle telecomunicazioni), si sono affermati nell'offerta dei servizi di pagamento[6]. Tale trasformazione è giustificabile, oltre che da esigenze legate all'efficienza dei servizi, anche dall'esistenza di economie di rete e di scopo[7].

Di recente, all'interno del mercato finanziario abbiamo assistito all'avvento delle nuove tecnologie

[5] Con riferimento a tematiche di concorrenza legate al settore dei pagamenti cfr. M. LIBERTINI, *Regolazione e concorrenza nei servizi di pagamento*, in *Diritto della banca e del mercato finanziario*, 2013, 1-28.

[6] È il caso di American Express che originariamente era una società di trasporto; AMEX entra nel mercato dei pagamenti prima con l'introduzione dei traveller's cheques e poi con la emissione di carte di credito. Analoga evoluzione è quella di Western Union, società telegrafica che successivamente si è specializzata nel mercato delle rimesse di denaro.

[7] G. ARDIZZI, C. IMPENNA, P. MASI, *La teoria economica dei sistemi di pagamento*, in C. Tresoldi (a cura di), *Economia dei sistemi di pagamento*, Il Mulino, Bologna 2005, pp.81-132; il tema è ritornato di forte attualità nel dibattito sui big data e a tal fine si veda H. VARIAN , *Economie di rete e Big Data*, Aspen Institute Italia (https://www.aspeninstitute.it/system/files/private_files/2018.../Aspenia80_Varian.pdf).

digitali, in cui rientrano ad esempio i servizi di pagamento digitale e il c.d. *mobile payment*[8], la cui diffusione è stata incrementata anche alla luce della Direttiva (EU) 2015/2366[9] del 25 novembre 2015 sui servizi di pagamento nel mercato interno (di seguito anche PSD2[10]), recepita nel nostro ordinamento dal d.lgs. 15 dicembre 2017, n. 218, ed avente lo scopo di consentire pagamenti più sicuri ed innovativi.

Nel nuovo contesto economico e tecnologico, la PSD2 risponde all'esigenza di fornire una risposta concreta non solo all'evoluzione del mercato dei pagamenti, ma anche alle criticità riscontrate nella vigenza del precedente regime delineato dalla precedente Direttiva 2007/64/CE (di seguito anche PSD1[11]). Quest'ultima aveva da un lato già consentito l'ingresso ordinato sul mercato dei pagamenti di nuovi operatori – gli istituti di pagamento ("IP") – legati alle novità tecnologiche dell'epoca, e dall'altro aveva introdotto un quadro regolamentare in grado di rispondere alle esigenze poste dall'evoluzione tecnologica negli anni successivi[12]. In altri termini, PSD1 rispondeva già all'esigenza di definire e normare un quadro giuridico europeo tale da favorire la creazione di un mercato interno dei servizi di pagamento nell'Unione Europea[13].

La PSD2 ha invece l'obiettivo di favorire la concorrenza e l'innovazione nel settore dei pagamenti *retail*, garantendo al contempo una maggiore sicurezza dell'utente; questi obiettivi, inoltre, vengono

---

[8] Sul tema v. S. MONETI, *Mobile payments: gli sviluppi del mercato e l'inquadramento normativo,* in *Analisi giuridica dell'economia*, 2015, 101; E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo,* in *Riv. trim. diritto dell'economia*, 2016, p. 41; G. GIMIGLIANO e G. NAVA, *L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari*, in *Smart cities e diritto dell'innovazione* a cura di G. Olivieri e V. Falce, Milano, 2016, p.190.

[9] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

[10] Con riferimento alla direttiva in generale cfr. F. PORTA, *Obiettivi e strumenti della PSD2*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale,* F. MAIMERI, M. MANCINI (a cura di), in Quaderni di ricerca giuridica della Consulenza Legale, 5 dicembre 2019, p. 21-46; G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Diritto della banca e del mercato finanziario*, 4, 2018; F. CASCINELLI - V. PISTONI - G. ZANETTI , *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno,* in www.dirittobancario.it; GIORDANO G., *Lo sviluppo dei servizi di pagamento*, in *Diritto ed economia di banche e mercati finanziari* di F. VELLA et al., il Mulino, 2019, p. 98 ss; M. RISPOLI FARINA , *Informazione e servizi di pagamento*, in *Analisi giuridica dell'economia*, I, 2015, p. 175 e ss; M. RISPOLI FARINA , *La direttiva PSD2: novità e continuità nella disciplina dei servizi di pagamento* in BRUNELLA RUSSO, (a cura di), *I servizi di pagamento nell'epoca della digitalizzazione,* Atti del Convegno in onore di Giuseppe Restuccia, Taormina 15-16 febbraio 2018, Cedam, 2019, p. 30 e ss; S. VANINI , *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218*, in *Le nuove leggi civili e commerciali*, 4, 2018, p. 866 e ss. P. MONTELLA , *La Direttiva PSD 2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, 2018.

[11] La PSD1 è stata recepita nell'ordinamento nazionale con il d. lgs n.11 del 27 gennaio 2010, entrato in vigore il 1° marzo 2010.

[12] La PSD1, aveva definito un quadro giuridico comunitario rinnovato per i servizi di pagamento elettronici, ponendosi i seguenti obiettivi: *i)* regolamentare l'accesso al mercato per favorire la concorrenza nella prestazione dei servizi; *ii)* garantire maggiore tutela degli utenti e maggiore trasparenza; *iii)* standardizzare i diritti e gli obblighi nella prestazione e nell'utilizzo dei servizi di pagamento per porre le basi giuridiche per la realizzazione dell'Area unica dei pagamenti in euro (SEPA); *iv)* stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di inefficienti strumenti quali quelli cartacei e il contante.

[13] Sul passaggio dalla PSD alla PSD2 cfr. anche il contributo di F. PORTA , *Obiettivi e strumenti della PSD2, op.cit.*

perseguiti anche attraverso l'ampliamento del novero dei servizi di pagamento sotto riserva, sottoponendo pertanto a regolamentazione alcune attività già di fatto offerte al pubblico in precedenza, sebbene in assenza di specifiche tutele. In questo contesto, il comune denominatore dei lavori per la messa a punto della PSD2 e le successive attività della *European Banking Authority* (EBA) è stato quello di favorire il diffondersi dell'innovazione tecnologica per '*lo sviluppo di nuovi tipi di servizi di pagamento, garantendo pari condizioni operative ai prestatori di servizi di pagamento esistenti e ai nuovi prestatori*'[14].

Un ruolo fondamentale dell'economia digitale è ricoperto dalle fonti di informazione, acquisite grazie a nuove elaborazioni fondate su tecnologie *Big Data*, e il mercato dei pagamenti digitali è uno di quelli che, come vedremo, più di altri sta assistendo all'emersione di nuovi *players* come BigTech, startup e scaleup fintech, che entrano in concorrenza con le banche e ed altri intermediari che finora hanno dominato il mercato *de quo.*

Le nuove tendenze vedono dunque un forte attivismo sia dei grandi operatori tecnologici (comunemente indicati anche come OTT o GAFA[15]), sia di agili *start-up* innovative[16], nell'area dell'offerta di servizi finanziari[17], con un focus sui pagamenti.

In altri termini, le banche e gli intermediari finanziari si trovano sempre più a competere, con grandi società internazionali specializzate nei servizi digitali (*e.g.* Amazon e Google), con gli operatori di telecomunicazione, che godono di un'ampia base di clientela e di un'infrastruttura tecnologica

[14] Il considerando 33, PSD2, recita: "*La presente direttiva dovrebbe prefiggersi di garantire continuità nel mercato, consentendo ai prestatori di servizi nuovi ed esistenti di offrire i propri servizi in un quadro regolamentare chiaro e armonizzato, indipendentemente dal modello commerciale da essi applicato. Fino a che tali disposizioni non siano applicate e fatta salva l'esigenza di garantire la sicurezza delle operazioni di pagamento e la tutela del cliente dal rischio comprovabile di frode, gli Stati membri, la Commissione, la Banca centrale europea (BCE) e Autorità europea di vigilanza (Autorità bancaria europea), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio (1) (ABE) dovrebbero garantire la concorrenza leale su tale mercato evitando discriminazioni ingiustificate a danno degli operatori esistenti. Qualsiasi prestatore di servizi di pagamento, compresi i prestatori di servizi di pagamento di radicamento del conto dell'utente di servizi di pagamento, dovrebbe poter offrire servizi di disposizione di ordine di pagamento*".

[15] Cfr. BANK FOR INTERNATIONAL SETTLEMENTS (BIS), *BigTech and the changing structure of financial Intermediation*, in Working Papers N. 779, aprile 2019.

[16] Osservatorio FinTech Italia 2019, PWC, marzo 2019, in cui si registra che sono state 31 le uscite dal mercato nel corso del 2018 tra le FinTech in Italia. Di queste, il 13% è stata oggetto di acquisizione da parte di altre FinTech; sembra esserci, anche in Italia, una tendenza al consolidamento tra le FinTech, come strategia per competere in un mercato caratterizzato dalla presenza di grandi players.

[17] Al tema dell'impatto dell'innovazione sul sistema finanziario sono dedicati numerosi *papers* delle diverse autorità sovranazionali. Si segnala, senza alcuna pretesa di esaustività: Financial Stability Board (FSB), (2017b), "*Financial Stability Implications from FinTech - Supervisory and Regulatory Issues that Merit Authorities' Attention*", disponibile su: http://www.fsb.org/2017/06/fsb-issues-a- report-on-the-financial-stability-implications-from-fintech/; Financial Stability Board (FSB), (2017c), "*FinTech Credit: Market Structure, Business Models and Financial Stability Implications*", disponibile su: http://www.fsb.org/2017/05/fintech-credit-market-structure-business-models-and- financial-stability-implications/; Basel Committee on Banking Supervision (BCBS), (2017), "*Sound Practices: Implications of Fintech developments for banks and bank supervisors*", Bank for International Settlements (BIS), disponibile su: https://www.bis.org/bcbs/publ/d431.htm. Per il mercato italiano si veda F. Panetta, (2018), "*Fintech and banking: today and tomorrow". Intervento presso la "Annual Reunion of the Harvard Law School Association of Europe*", disponibile su: http:// www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2018/panetta-120518.pdf.

all'avanguardia (*e.g.* Apple e Samsung), ed infine, con le cc.dd. "*FinTech*", ossia le piccole e innovative *startup* che nascono con l'obbiettivo di portare l'innovazione nei servizi finanziari[18].

Il legislatore europeo della PSD2 ha quindi optato per l'apertura del mercato dei pagamenti anche ad altri operatori per due ragioni. La prima è stata quella di regolamentare un mercato che di fatto si stava già creando, in cui i dati di conti di pagamento erano già disponibili a operatori non tradizionali e non autorizzati; a tal proposito, il mercato da solo non produce sufficiente informazione per funzionare correttamente, essendo necessario l'intervento del legislatore per ristabilire l'equilibrio competitivo.

La seconda ragione è stata invece quella di aumentare il livello di efficienza e di qualità degli strumenti di pagamento offerti; infatti, ampliando gli operatori e i servizi, si è voluta dare all'utente una più ampia gamma di servizi e operatori tra cui scegliere.

Non è un caso, infatti, che gli operatori dei settori bancario/assicurativo, delle informazioni creditizie e delle telecomunicazioni, comunemente soggetti ad una regolamentazione particolarmente strutturata e stringente, abbiano manifestato il bisogno che venisse loro assicurato un *level playing field*, al fine di consentire agli operatori tradizionali (banche e intermediari finanziari) di competere con le BigTech senza il vincolo di asimmetrie regolatorie[19].

La *data driven economy* porta infatti a disintermediare gli operatori tradizionali, ad accentrare nel potere dei *Big Tech* tutto il mercato dei servizi – con il rischio di estromettere gli operatori tradizionali – e a lasciare l'intero mercato dei servizi in mano agli OTT.

Dato questo quadro complesso, alcuni quesiti sorgono spontanei: come sta cambiando la competizione nei servizi finanziari, in particolare nel segmento dei sistemi di pagamento? E come possono risolversi eventuali contrasti tra PSD2 e GDPR con riferimento all'accesso ai dati dei conti di pagamento da parte dei nuovi operatori?

In questo capitolo si cercherà di dare risposte a questi quesiti, dopo aver esaminato la disciplina

---

[18] In materia di *Fintech* cfr. FINANCIAL STABILITY BOARD, *FinTech and market structure in financial services: Market developments and potential financial stability implications, in* https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/, *14 February, 2019 (ultima visita 27 marzo 2020).* In dottrina *cfr.* M.T. PARACAMPO, *Fintech – Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Seconda edizione riveduta e aggiornata, Vol. II, 2021; PONZIANI, *Imprese fintech e techfin: l'impatto dei big data sulla libera concorrenza*, in *I diversi settori del fintech. Problemi e prospettive*, a cura di CORAPI, R. LENER, Milano 2019, 33 ss; A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fintech, il paradigma Open banking e la minaccia delle big tech companies*, in *Mercato, concorrenza e regole*, 3/2018, pp. 441- 446; CIAN, SANDEI, *Diritto del Fintech, Wolters Kluwer* CEDAM, Milano, 2020; F. DI CIOMMO, M. RUBINO DE RITIS, G. CASSANO (a cura di), *Banche, intermediari e Fintech. I nuovi strumenti digitali in ambito finanziario*, 2020; E. MACCHIAVELLO, *FinTech. Problematiche e spunti per una regolazione ottimale*, in *Mercato Concorrenza Regole*, Fascicolo 3, dicembre 2019.

[19] Cfr. audizioni di Unicredit (8 marzo 2018), Intesa San Paolo (23 febbraio 2018), Generali (21 marzo 2018), Experian (28 novembre 2017), *CRIF (18* dicembre 2017), Allianz (17 novembre 2017), Vodafone (7 dicembre 2018), Wind-Tre (29 novembre 2018), Fastweb (7 dicembre 2018), TIM (7 dicembre 2018). In dottrina cfr. ex multis F. DI PORTO, G. GHEDINI, "I Access Your Data You Access Mine". Setting a Reciprocity Clause for the "Access to Account Rule" in the Payment Services Market in www.papers.ssrn.com, giugno 2019.

applicabile e le novità tecnologiche attualmente disponibili sul mercato dei servizi di pagamento.

4.1 Il nuovo quadro regolamentare della PSD2: l'introduzione di due nuovi servizi di pagamento e di nuovi operatori (i c.d. TPPs) tra protezione dei dati personali, responsabilità e concorrenza

4.1.1 Il nuovo mercato dei servizi di pagamento

Il nuovo quadro regolamentare per i servizi di pagamento creato dalla PSD2 ha voluto favorire l'ingresso sul mercato di nuovi operatori e, più in generale, la creazione di condizioni per lo sviluppo di un ecosistema più competitivo, introducendo il principio dell'accesso ai dati dei conti di pagamento da parte di operatori ("*Third-party providers*" o "TPPs") che, a tal fine, devono essere autorizzati dalle autorità nazionali competenti[20].

Si riconosce dunque l'esistenza di servizi di pagamento, che consentono a nuovi operatori di accedere ai conti di pagamento dei propri clienti detenuti presso un una banca o, più raramente, un altro intermediario come un istituto di pagamento o un istituto di moneta elettronica[21]. L'intermediario presso il quale è intrattenuto il conto è dunque obbligato a consentire tale accesso, qualora i conti della clientela siano consultabili *on-line*, secondo diverse modalità che verranno esaminate in seguito.

In linea generale, l'obiettivo della PSD2, rinvenibile nei numerosi *consideranda*, è stato quello di definire un contesto di fiducia, certezza e sicurezza in cui fosse neutrale la scelta della tecnologia sottostante i servizi offerti ai consumatori (c.d. principio di neutralità tecnologica); così da evitare di vanificare i benefici legati all'innovazione tecnologica in continua crescita.

Tuttavia, il legislatore europeo ha voluto fissare alcuni prerequisiti di carattere tecnico per garantire l'affidabilità e l'efficienza degli strumenti di pagamento elettronici, unitamente alla competitività e ad un adeguato livello di tutela del consumatore.

La tecnica legislativa prescelta definisce i principi generali, i diritti e gli obblighi che assistono la prestazione dei servizi, a livello di normativa primaria. Inoltre, per la prima volta nel settore dei pagamenti *retail*, il compito di emanare standard o linee guida sugli aspetti più tecnici viene dato all'EBA, in modo da rendere concretamente applicabili le disposizioni contenute nella PSD2.

Questa scelta regolamentare è altresì giustificata dal fatto che processi legislativi europei richiedono anni dalla pubblicazione della proposta da parte della Commissione europea per addivenire all'entrata in vigore del testo definitivo[22]: pertanto, essi non appaiono coerenti con la maggiore rapidità che

[20] In Italia, la Banca d'Italia è stata confermata autorità competente ai fini della PSD2, come già per la PSD1.

[21] A. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, F. MAIMERI, M. MANCINI (a cura di), in Quaderni di ricerca giuridica della Consulenza Legale, 5 dicembre 2019, p. 47-82.

[22] Per le direttive, tali tempi si dilatano ulteriormente in considerazione dei due anni normalmente previsti per il recepimento negli ordinamenti nazionali dei diversi Paesi membri.

caratterizza invece l'innovazione tecnologica[23].

Nell'intento del legislatore europeo, il rinvio all'EBA della predisposizione della normativa tecnica costituisce un impianto regolamentare più elastico, in grado di tenere il passo con la rapida evoluzione tecnologica in continuo cambiamento[24].

Inoltre, l'impostazione basata sul principio della neutralità tecnologica sopra citato, implica la possibilità che sul mercato possano convivere una pluralità di opzioni tecnologiche per l'offerta di uno specifico servizio o di singole componenti del servizio stesso.

Tale impostazione è l'unica in grado di innescare un processo che dovrebbe accrescere l'efficienza dei servizi di pagamento, consentendo la comparazione delle diverse offerte disponibili; si tratta di un mercato in cui sono presenti economie di rete che devono coniugare le diverse esigenze della filiera dei soggetti che partecipano alla domanda e all'offerta dei servizi. In particolare, la PSD2 ha consentito di riconoscere per la prima volta in Europa modelli di "*open banking*", fondati sulla condivisione di dati bancari tra i diversi operatori dell'ecosistema finanziario.

La PSD2 accelera, quindi, il passaggio al modello "*open banking*" aprendo per la prima volta i conti bancari all'accesso di nuovi operatori, con l'obiettivo di evitare rischi di frammentazione della componente più innovativa dei servizi e migliorare la competizione tra soggetti finanziari nuovi e tradizionali.

Vengono così introdotte e disciplinate due nuove tipologie di attori: *i)* i *Payment Initiation Service Providers* (PISP), che frapponendosi tra il pagatore ed il suo conto di pagamento *on-line*, avviando il pagamento a favore di un terzo beneficiario, consentono al pagatore di disporre un pagamento *on-line* mediante addebito diretto sul proprio conto corrente; e *ii)* gli *Account Information Service Providers* (AISP), che consentono a chi paga di ottenere, grazie ad una piattaforma unica, un'informativa completa sui propri conti di pagamento, anche se tenuti in diverse banche. Gli AISP, tuttavia, non potranno utilizzare i dati del cliente o effettuare l'accesso ai relativi conti di pagamento per scopi diversi da quelli previsti dal servizio[25].

---

[23] A titolo di esempio, la proposta di revisione della PSD1 da parte della Commissione risale al 2013, mentre l'entrata in vigore della PSD2 al gennaio 2016, il termine per il recepimento nazionale al gennaio 2018. In questi cinque anni si sono peraltro registrati, specialmente in un settore dinamico come quello dei pagamenti *retail*, cambiamenti rilevanti che hanno prodotto effetti sulla struttura del mercato tali da poter incidere sull'efficacia di alcune previsioni contenute nella PSD2.

[24] Sono ben 12 i mandati assegnati all'EBA dalla PSD2: dalla sicurezza ai rapporti tra autorità *home* e *host* nel caso di prestazione di servizi su base transfrontaliera, dagli obblighi di reporting degli incidenti di sicurezza alla raccolta dei dati sulle frodi con mezzi di pagamento.

[25] Il Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 (PSD2) per quanto riguarda le norme tecniche per l'autenticazione forte del cliente e gli standard aperti di comunicazione (nel seguito RTS), prevede che tutti i prestatori di servizi di pagamento che detengono conti accessibili on line (*Account Servicing Payment Service Providers* o ASPSP) predispongano, entro il 14 settembre 2019, un'interfaccia di accesso per consentire a terze parti (*Third Party Providers* o TPP) di svolgere la propria attività. Tale obbligo è volto a garantire un canale sicuro di autenticazione e comunicazione tra l'ASPSP e il TPP e può essere alternativamente soddisfatto attraverso: i) la realizzazione *ex novo* di un'interfaccia on line dedicata all'accesso dei TPP;

I nuovi due servizi disciplinati dalla PSD2, ovvero i servizi di disposizione di ordini di pagamenti (*Payment initiation services* – "PIS") e di accesso informativo ai conti (*Account information services*, "AIS"), presentano delle caratteristiche che in parte li distinguono dai tradizionali servizi di pagamento, non contemplano né la gestione di flussi finanziari né la detenzione di fondi degli utenti. Si è creato quindi un ampliamento della nozione di "servizio di pagamento", originariamente associata ad un trasferimento di fondi e alla gestione di un conto di pagamento.

La nuova direttiva ha anche semplificato il quadro regolamentare, evitando di rinviare ad una diversa normativa la disciplina applicabile ad operatori di uno stesso ecosistema e che offrono servizi appartenenti ad un medesimo settore; trattasi, infatti, di servizi che prevedono l'accesso a conti di pagamento *on-line* gestiti da un altro intermediario.

4.1.2 Profili di protezione dei dati personali tra GDPR e PSD2

Con riferimento ai profili di rischio legati alla sicurezza delle credenziali di accesso degli utenti ai propri conti e alla protezione dei dati personali, la PSD2 fissa un generico principio di accesso non oneroso solo per i dati volti a consentire lo sviluppo di due servizi essenziali e imprescindibili in ogni soluzione innovativa nel campo dei pagamenti. La PSD2 si considera dunque un "acceleratore dell'innovazione", obbligando le banche ad "aprirsi" (c.d. *open banking*) ed imponendo a queste ultime di effettuare investimenti in tecnologie, creando altresì le basi per lo sviluppo di nuovi modelli di *business* che consentano l'offerta di servizi innovativi[26].

Questo accesso gratuito *ex lege* è circoscritto sia nel perimetro (in quanto previsto solamente per i conti di pagamento), sia nelle finalità, che sono limitate per il *Payment initiation services providers* – PISP al disporre un ordine di pagamento, mentre per l*'Account information services providers* – AISP all'offerta di servizi informativi, consentendo all'utente "*di disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento*"[27].

Tali limitazioni dei TPPs sono dirette a compensare l'abbattimento delle barriere d'ingresso nella prestazione dei servizi di pagamento, con l'obiettivo di stimolare la concorrenza.

---

ii) l'adattamento di interfacce già disponibili ai clienti per accedere direttamente ai propri conti di pagamento on line. In materia di TPP cfr. V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, *op.cit*.

[26] Sul punto si veda KPMG, PSD2: *a game changer?*, ottobre 2018, secondo cui la direttiva pone nuove sfide per le banche in termini di *compliance* e ha l'obiettivo di aumentare la concorrenza nel settore, con conseguente minaccia per gli operatori tradizionali, ma con nuove ed interessanti opportunità di business.

[27] Il considerando 28 prevede che "*gli sviluppi tecnologici degli ultimi anni hanno portato anche alla nascita di una serie di servizi accessori, ad esempio servizi di informazione sui conti. Tali servizi forniscono all'utente di servizi di pagamento informazioni online aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce online del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento. Anche tali servizi dovrebbero essere trattati nella presente direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo status di prestatore di servizi di informazione sui conti*".

Infatti, tali limitazioni tutelano anche gli operatori tradizionali presso cui è incardinato il conto, visti gli investimenti che questi ultimi devono sostenere per preservare le infrastrutture tecnologiche utilizzate e per garantire la sicurezza di tutte le informazioni raccolte. A tal proposito, l'art. 66.3, lett. f), della PSD2 vieta al PISP di chiedere all'utilizzatore qualsiasi dato che non sia necessario per fornire il nuovo servizio di pagamento, senza l'utilizzo di una carta di credito; tuttavia, non è vietato per il PISP ottenere ogni altra informazione sull'utilizzatore, dato che tali maggiori informazioni sono ottenute offrendo il servizio e sono fornite solo al beneficiario previa suo consenso esplicito. Pertanto, i TPPs possono usare o negoziare solo quei dati utili per svolgere il servizio di pagamento per il quale sono stati autorizzati, e non possono modificare le caratteristiche della transazione (e.g. somma da pagare, il beneficiario o altre condizioni). In particolare, essi possono usare e negoziare i dati del conto di pagamento per accrescere il servizio e migliorare la sua efficienza, aumentando il benessere del consumatore.

Questo diritto dei nuovi operatori al libero accesso ai dati dei conti di pagamento è anche conosciuto come "*XS2A rule*" ed è contenuto all'interno dell'art. 36.1 della PSD2[28]; pertanto, l'introduzione della *XS2A rule* nella PSD2 ha altresì risolto un problema di *privacy*, in quanto i dati del conto di pagamento sono dati sensibili.

La banca presso cui è incardinato il conto di pagamento può negare l'accesso ai TPPs solo per ragioni giustificate e oggettivamente evidenti relative alla sicurezza (e.g. accesso fraudolento e non autorizzato al conto di pagamento).

La regolamentazione è stata quindi necessaria per affidare ai TPPs quelle informazioni che altrimenti non avrebbero avuto modo di ottenere a causa delle limitazioni della *privacy*.

C'è però chi potrebbe opinare che i detentori di un conto corrente già godono del diritto di accesso dell'interessato ai sensi dell'art. 15 GDPR e del diritto alla portabilità previsto all'art. 20 GDPR[29]; in particolare, quest'ultimo già consente ai clienti di fornire ai TPPs l'accesso dei loro dati del conto o di trasferirli da un operatore ad un altro. A tal proposito, occorre però ricordare che la PSD2 è entrata in vigore prima del GDPR; per risolvere un potenziale conflitto tra le due discipline, dottrina autorevole[30] ha proposto l'utilizzo del principio di specialità (*lex specialis derogat generali*), secondo il quale la *XS2A rule* della PSD2 prevarrebbe sul generico diritto alla portabilità dei dati previsto dal GDPR. Tuttavia, i dati che contiene una banca vanno ben oltre quelli del conto di pagamento (e.g. profilatura MiFID del cliente, informazioni sulla meritevolezza del credito); infatti, per questi ultimi

[28] In particolare, l'art 36.1 della PSD2 prevede che: "Gli Stati membri assicurano che gli istituti di pagamento abbiano accesso ai servizi di conti di pagamento degli enti creditizi in modo obiettivo, non discriminatorio e proporzionato. Tale accesso deve essere sufficientemente ampio da consentire agli istituti di pagamento di fornire servizi di pagamento in modo efficiente e senza ostacoli".

[29] Per un'analisi completa di entrambi i diritti sopra menzionati si rinvia al § 1.3.3.

[30] F. DI PORTO, G. GHEDINI , *op. cit.*, p. 7.

si applicherà il GDPR.

Altro aspetto importante, come si è visto, è che l'esercizio del diritto dei TPPs al libero accesso è subordinato al preventivo consenso del titolare del conto.

La mancanza del consenso preventivo dell'utente al TPPs non può essere eccepita dall'intermediario presso cui è incardinato il conto di pagamento; tale disposizione è inoltre in linea con la filosofia sottesa alla PSD2, volta a favorire la concorrenza ed a semplificare i processi; infatti, se si fosse consentito all'intermediario di eccepire la mancanza del consenso, si sarebbero disincentivati gli utenti ad usufruire dei servizi offerti dai TPPs, dilatando peraltro i tempi che sarebbero diventati incompatibili con l'immediatezza che caratterizza i servizi digitali. In altre parole, si è voluto evitare che questo controllo dell'intermediario sul consenso preventivamente prestato al TPP, potesse creare discriminazioni verso quest'ultimo.

Manca tuttavia una specifica disciplina per la revoca del consenso all'utilizzo del TPP da parte dell'utente. Com'è noto, il consenso è sempre revocabile, anche ai sensi dell'art. 7.3 del GDPR che prevede che: *"L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*[31]"

Di norma la revoca andrebbe portata a conoscenza del soggetto cui è stato prestato il consenso, escludendo in teoria la possibilità per l'utente di revocare il consenso all'accesso ai conti presso l'intermediario su cui è incardinato il conto di pagamento.

La mancata chiarezza sulla disciplina applicabile alla revoca del consenso crea una situazione di incertezza giuridica con riferimento al caso concreto in cui la banca dovesse procedere a bloccarne l'accesso al conto, a seguito dell'eventuale ricezione della revoca del consenso dell'utente originariamente prestato al TPP[32].

La revoca del consenso all'utilizzo di un TPP da parte dell'utente è un aspetto particolarmente delicato in quanto i limiti all'esercizio della stessa devono essere fissati in modo da bilanciare due esigenze diverse e potenzialmente contrapposte: da una parte, c'è l'esigenza di stimolare la concorrenza e di abbattere le barriere all'entrata nel mercato per i TPPs; dall'altra parte, c'è quella di non abbassare il livello di tutele accordate all'utente, tra cui la tutela del diritto del consumatore di poter comunicare direttamente alla banca la sua sopravvenuta volontà di revocare il consenso a un

[31] In materia di revoca si rinvia all'analisi fatta nel § 1.3.2.

[32] Inoltre, tale impostazione sembrerebbe escludere la possibilità che l'utente possa creare presso la banca delle cc.dd. '*black lists*' di TPPs, ovvero degli elenchi in cui indica gli operatori che non vuole che accedano ai suoi conti di pagamento, circostanza questa ammessa in altri casi in cui il conto dell'utente è movimentato da un soggetto diverso dall'utente stesso o dal prestatore che gestisce il conto di pagamento (a titolo di esempio, nel caso di addebiti diretti).

determinato TPP.
Sembra pertanto auspicabile un intervento chiarificatore del legislatore europeo, o, in subordine, dell'EBA, per evitare che i singoli Stati membri possano adottare approcci differenti su un aspetto così delicato.
Ebbene, in assenza di specifiche previsioni nella PSD2 su questo aspetto, il legislatore nazionale, nel d.lgs. n. 218/2017 di recepimento della direttiva, ha previsto che la revoca del consenso di cui sopra possa essere ricevuta *anche* dalla banca che gestisce il conto di pagamento, in un'ottica tesa ad accrescere le tutele a favore dell'utente. A tal riguardo, la PSD2 ha purtroppo lasciato alcuni margini di incertezza che sono stati colmati, in maniera potenzialmente difforme, dalle leggi di trasposizione nazionale; sarà quindi centrale il compito dell'EBA nell'assicurare la massima uniformità possibile delle prassi di supervisione adottate dalle diverse autorità nazionali competenti.

4.1.3 L'ingresso dei TPPs nel mercato dei servizi di pagamento: profili di diritto della concorrenza

Le previsioni della PSD2, come abbiamo visto, hanno seguito l'evoluzione tecnologica che fa assumere al dato una valenza "commerciale", una sorta di '*commodity*'; inoltre, come si è visto, il confine di questa disponibilità è oggetto di ampio dibattito.
In base a quanto previsto nella PSD2, da una parte, il cliente può accedere ai propri dati senza costi per i TPPs, dall'altra, emerge un contesto operativo che spinge le banche ad adattare i propri modelli di *business*, valorizzando le informazioni di cui dispongono, al di là delle previsioni della PSD2.
Inoltre, i due nuovi servizi di pagamento disciplinati dalla PSD2 si appoggiano sui conti di pagamento gestiti dalle banche; l'accesso al conto diventa quindi necessario per assicurare l'offerta e lo sviluppo dei servizi di AIS e PIS, nonché di altri servizi a valore aggiunto. I conti di pagamento diventano una sorta di *essential facility*, un'infrastruttura funzionale allo sviluppo di un ecosistema aperto per i pagamenti *retail*. Tuttavia, le autorità antitrust sono restie dall'applicare l'*essential facility doctrine (*di seguito anche *EFD),* anche alla luce di due importanti differenze: *i)* il prezzo in quanto, come già visto sopra, la *XS2A rule* della PSD2 non contempla una compensazione per l'accesso ai dati del conto di pagamento; e *ii*) non è necessario un preventivo accordo tra le parti, dato che è sufficiente un consenso preventivo dell'utente al TPP, il quale può accedere liberamente ai dati del conto.
Tuttavia, il quadro può apparire meno chiaro di come si potrebbe pensare; infatti, come noto, la disciplina antitrust, caratterizzata da una regolamentazione di tipo orizzontale, non è di norma ostacolata dall'esistenza di regolamentazioni settoriali, di tipo verticale. Pertanto, da una parte, le autorità antitrust e le singole autorità competenti di vigilanza bancaria potrebbero prendere indirizzi difformi sull'applicazione concreta del diritto di accesso ai dati sui conti di pagamento; dall'altra

parte, sia la disciplina antitrust, sia la PSD2 hanno l'obiettivo di prevenire esiti conflittuali[33]. Tuttavia, il terreno dove possono crearsi divergenze è ad esempio quello della definizione di mercato rilevante. Secondo la PSD2 l'accesso sarebbe consentito solo ai dati dei conti di pagamento degli utenti. In particolare, solo per il PISP è richiesto che le banche forniscano tutte le informazioni riguardanti l'esecuzione della transazione[34], dato che per l'AISP mancherebbe una simile disposizione che obbliga le banche a farlo; tuttavia, lo stesso principio potrebbe risultare implicitamente nello scopo dell'AISP, il quale può accedere alle informazioni dei conti di pagamento designati e alle relative transazioni di pagamento associate[35]. In altri termini, l'AISP può accedere a più informazioni rispetto al PISP, in quanto può accedere non solo alle informazioni del conto di pagamento ma anche a quelle dei conti di pagamento associati[36]. Inoltre, sia AISP che PISP sono soggetti a requisiti prudenziali più leggeri rispetto alle banche e ciò incoraggia il loro sviluppo nel mercato interno dell'UE; però, per questo motivo, né AISP né PISP detengono fondi del pagatore.

I principali vantaggi per il PISP consistono nell'offrire servizi per poter gestire al meglio i depositi nei vari intermediari dove i conti sono incardinati.

Ebbene, nonostante la PSD2 lasci spesso, come in questo caso, spazio a interpretazioni, la definizione di mercati rilevanti è sufficientemente chiara e, pertanto, i TPPs possono in anticipo conoscere i dati ai quali hanno il diritto di accedere.

Alla luce invece della disciplina concorrenziale, diretta a favorire l'ingresso dei TPPs nel mercato, gli *enforcers* potrebbero dare una definizione più ampia o più ristretta di mercato rilevante; essi, ad esempio, potrebbero inserire oltre ai dati dei conti di pagamento anche quelli relativi al comportamento degli utenti sui *social network* o sui motori di ricerca. In altre parole, le autorità di concorrenza potrebbero ben considerare quei dati come complementari o sostituibili, oppure potrebbero considerarli come ausiliari, utili per fornire migliori servizi di pagamento; esse, teoricamente, potrebbero dunque considerare il conto di pagamento del singolo utente come un mercato rilevante, così da considerare le banche come dominanti, sanzionando un loro rifiuto a fornire i dati al TPPs come un abuso.

Tuttavia, nella pratica sembra essere diverso; infatti, sotto il profilo delle autorità antitrust, come già visto nel secondo capitolo, è assai difficile applicare l'*EFD* nei mercati digitali, per non parlare del gravoso onere di prova che ricadrebbe sulle autorità stesse[37].

L'*EFD* non è dunque lo *standard* di responsabilità dominante nei casi antitrust, e ciò è ancora più

[33] S. VEZZOSO, '*Fintech, access to data, and the role of competition policy'*, 2018, p. 32 (disponibile in: https://ssrn.com/abstract=3106594).
[34] Art. 66 §4 lett. b) PSD2.
[35] Art. 67 §2 lett. d) PSD2.
[36] Entrambi possono perciò accedere ai dati senza ricevere discriminazioni dalla banca.
[37] Sul punto, si rinvia al § 2.1.5.

vero in un'economia come quella digitale dove le informazioni sono liberamente accessibili a tutti.
Infatti, anche quando una risorsa è un'importante fonte di vantaggio competitivo, e costituisce quindi una barriera all'entrata, la normativa *antitrust* non impone necessariamente alle imprese di condividere tale risorsa con i propri concorrenti. In altri termini, anche nel caso in cui l'*essential facility* sia costituita da dati, un eventuale rifiuto a concedere a terzi l'accesso a tali dati ha una rilevanza antitrust, se e nella misura in cui è idoneo a ridurre la concorrenza in un mercato complementare/a valle.
Pertanto, ai fini dell'applicazione dell'art. 102 TFUE, assumerebbero particolare peso le finalità alla base di una richiesta di accesso ai dati detenuti da un'impresa dominante.
La definizione stessa quindi di mercato rilevante nell'economia digitale non è semplice da individuare e, come detto già nel secondo capitolo, occorre ripensarla.
Una soluzione potrebbe essere quella di essere più severi con i BigTech, lasciando invece alle piccole start-up la possibilità di innovarsi.
Infatti, dal punto di vista concorrenziale, i TPPs non vanno visti come un'unica categoria, ma occorre fare una distinzione al loro interno tra: le piccole Startup tecnologiche (e.g. Satispay e Moneyfarm) e le BigTech (detti anche OTT o GAFA), già consolidate nel mercato; le prime subiscono svantaggi concorrenziali non irrilevanti nei confronti delle banche (e.g. assenza di servizio clienti affidabile, un accesso limitato ai dati dei potenziali utenti, la mancanza di una *brand reputation* e un alto costo del capitale), mentre lo stesso non può dirsi per le BigTech.
Queste ultime, come visto nei capitoli precedenti, oltre ad avere importanti risorse finanziarie, hanno importanti strumenti tecnologici basati sui *Big Data analytics* e sull'*Artificial Intelligence,* con la capacità di estrarre informazioni utili da grandi volumi e varietà dei dati, controllando le preferenze negli acquisti e nelle vendite di consumatori e commercianti[38].
Sebbene infatti le due categorie si assomiglino per la forte spinta all'innovazione, le start-up innovative possono offrire i soli servizi di pagamento, mentre le BigTech offrono una pletora di servizi digitali personalizzati, tra cui anche i PIS e gli AIS[39]. Tale distinzione emerge altresì dai pochi provvedimenti antitrust finora emessi da autorità di concorrenza. In particolare, l'autorità antitrust svizzera (Comco) ha adottato due orientamenti diversi per due casi simili. Nel dicembre 2018 ha aperto un'istruttoria contro i più grandi istituti finanziari svizzeri (e.g. Credit Suisse, UBS) per un possibile accordo con un associato prestatore di servizi di pagamento, Twint, diretto a escludere

[38] OCSE (2016), *"Big data: bringing competition policy to the digital era - Background note by the Secretariat", https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf* , pag. 22.
[39] The EBA's global registry (https://eba.europa.eu/risk-analysis-and-data/register-of-payment-and-e- money-institutions-under-psd2), è ancora in fase di realizzazione (cfr. EBA, '*Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366* (PSD2)', 23.2.2017).

Apple Pay e Samsung Pay dal mercato svizzero dei pagamenti[40]. Invece, appena pochi mesi dopo, la stessa autorità svizzera, ha chiuso un'indagine contro Apple pay per abuso di posizione dominante a danno di Twint, denunciando il lancio automatico di Apple Pay nel mercato dei pagamenti digitali che ha interferito con i pagamenti effettuati nell'app di Twint, escluso dal mercato. In quest'ultimo caso, l'indagine fu chiusa dopo che Apple Pay si impegnò a risolvere i problemi tecnici[41]. Pertanto, sotto il profilo dell'autorità, sia le banche che le BigTech potrebbero essere nella posizione di falsare la concorrenza e danneggiare il benessere del consumatore.

Nella pratica però, l'ingresso delle BigTech nel mercato sta creando grandi riduzioni nel fatturato delle banche, che stanno altresì fronteggiando una perdita di controllo sui loro utenti[42]; ciò, a causa del ruolo di *gatekeeper*[43] ricoperto dalle BigTech, in qualità di imprese operanti in più settori e capaci di togliere fette di mercato anche a operatori tradizionali quali appunto le banche.

Pertanto, occorre che le autorità creditizie e di concorrenza valutino i diversi casi alla luce del principio di proporzionalità di cui all'art. 5.3 del TUE. Ciò significa, da una parte, applicare la disciplina antitrust, dall'altra, supportare l'innovazione dei servizi finanziari; a tal proposito, le autorità dovranno valutare caso per caso i TPPs (start-up innovative o BigTech che siano) tenendo in considerazione il loro *business model*, la loro dimensione, la loro significatività sistemica, la loro complessità e la loro operatività transfrontaliera (c.d. *cross-border*). Inoltre, tale proporzionalità va applicata sia all'ingresso nel mercato e in sede di prima autorizzazione, sia nella fase successiva di supervisione *on-going*.

Il *Financial Stability Board* – FSB ha affermato che se, da una parte, l'innovazione tecnologica può aumentare la concorrenza, dall'altra, l'accesso di nuovi partecipanti al mercato può non essere costante. In particolare, il FSB ha constatato come sebbene le istituzioni abbiano un più agevole accesso a risorse finanziarie, esse siano assai limitate con riferimento alle risorse tecnologiche in comparazione con le BigTech, le quali detengono un importante vantaggio competitivo.[44]

4.1.4 Profili di responsabilità e di autorizzazione dei TPPs

Come sopra menzionato, una delle ragioni che aveva condotto il legislatore europeo ad emanare la PSD2, era quella che questi servizi erano di fatto già prestati da operatori non autorizzati che, a seguito

[40] Cfr. Comco/Weko, (SW) 13.11.2018
[41] Cfr. Comco/Weko, (SW) 18.12.2018
[42] Così C. SCHENA, A. TANDA, C. ARLOTTA AND G. POTENZA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in Quaderni Fintech, 2018.
[43] Sulla definizione e il ruolo dei gatekeeper in Europa v. §2.1.3 e § 3.2. In dottrina con riferimento ai "*digital conglomerates*" cfr. M. BOURREAU, A. DE STREEL, *Digital Conglomerates and EU Competition Policy*, marzo 2019, p. 8-9 disponibile a: https://ssrn.com/abstract=3350512.
[44] FINANCIAL STABILITY BOARD, *Fintech and Market structure in financial services: Market developments and potential financial stability implications*, 14 febbraio 2019, p. 5.

del rilascio delle credenziali di sicurezza da parte degli utenti, accedevano ai conti di pagamento per mezzo dell'interfaccia utente messa a disposizione dagli operatori tradizionali. Questi ultimi, infatti, non avevano sempre contezza del fatto che ad accedere fosse effettivamente non il proprio cliente ma piuttosto un soggetto terzo; queste modalità operative, rientrano nel c.d. '*screen-scraping*[45]' – ancora oggi ammissibile, con alcune limitazioni, fino all'effettiva applicazione della relativa normativa secondaria EBA[46] – e pongono alcuni problemi di natura giuridica.

In primo luogo, nel rapporto tra la banca e il proprio cliente si verificava nella teoria una violazione, da parte del cliente, dell'obbligo contrattuale di non divulgare a terzi le proprie credenziali di sicurezza, che poteva – al ricorrere di determinate condizioni – limitare l'obbligo di rimborso della banca, in caso di reclamo da parte del cliente per operazioni non autorizzate. Inoltre, la difficoltà di individuare in modo chiaro i diversi operatori coinvolti a vario titolo nella prestazione del servizio e l'assenza di una regolamentazione, rendeva difficile allocare eventuali responsabilità, ed attivare i conseguenti rimedi restitutori o risarcitori, in caso di malfunzionamento del servizio.

Invece, con la PSD2, anche con il fine di assicurare il funzionamento del meccanismo di accesso sopra illustrato, si introduce finalmente una chiara indicazione dei nuovi soggetti coinvolti e dei servizi offerti, consentendo un corretto riparto di responsabilità tra tutti i prestatori coinvolti nell'offerta dei nuovi servizi, a tutela non solo dell'utente ma anche degli stessi operatori.

In altre parole, a seguito dell'approvazione della PSD2, si sta affermando nella comunità bancaria un ecosistema aperto in cui gli aspetti cooperativi e competitivi trovano un loro equilibrio, al fine di favorire l'affermarsi di servizi utili all'utente e con un'indicazione chiara delle responsabilità dei diversi soggetti coinvolti.

Con riferimento ai profili di responsabilità ipotizzabili, il rapporto contrattuale non è tra la banca e i TPPs, ma tra la banca e l'utente; a tal riguardo, sarebbe la banca a dover rispondere contrattualmente in caso di mancata, inesatta o tardiva esecuzione di un ordine di pagamento. Tuttavia, la PSD2 disciplina l'azione di rivalsa della banca nei confronti dei TPPs; infatti, per quanto riguarda la legge italiana, il nuovo art. 25-bis del d.lgs. 11/2010 disciplina che il TPP deve immediatamente, e senza la necessità di una costituzione in mora, restituire alla banca gli importi che essa abbia rimborsato al proprio cliente. Il TPP, a sua volta, per difendersi dall'azione di rivalsa della banca, ha il diritto di provare il contrario.

Lo stesso vale in caso di utilizzo non autorizzato di uno strumento di pagamento: l'art. 72.2 della PSD2 stabilisce infatti che il cliente ha diritto a farsi prontamente rimborsare dalla banca di

[45] Lo '*screen-scraping'è* il processo di raccolta dei dati di visualizzazione dello schermo da un'applicazione a un'altra, in modo che quest'ultima possa visualizzarla.

[46] Si tratta dei *regulatory technical standards –RTS* dell'EBA adottati con regolamento delegato (UE) 2018/389 della Commissione europea in tema di autenticazione forte del cliente e standard aperti di comunicazione comuni e sicuri.

radicamento del conto, la quale a sua volta può esercitare l'azione di rivalsa sul TPP, salvo che quest'ultimo non dia prova contraria.

Però se da una parte si potrebbe parlare di responsabilità contrattuale della banca nei confronti del cliente, lo stesso non può dirsi nei confronti del TPPs, sebbene la banca abbia l'obbligo di consentire al TPP l'accesso ai dati del conto, salvo che il rifiuto della banca dipenda da un giustificato motivo oggettivo.

In caso di rifiuto della banca, come si è visto nel precedente paragrafo, siamo piuttosto nell'ambito della disciplina di tutela della concorrenza. Tuttavia, dato che si è visto come sia difficoltoso applicare gli strumenti antitrust, si riflette sull'opportunità di applicare la disciplina a tutela del consumatore; in particolare, in caso di comportamento ostruzionistico o discriminatorio della banca nei confronti di un TPP, si potrebbe configurare ai danni di quest'ultimo un atto di concorrenza sleale ai sensi dell'art. 2598, n. 3, c.c., con il conseguente diritto al risarcimento ai sensi dell'art. 2600 c.c.

Inoltre, ai fini di politica del diritto, tale soluzione sembra anche coerente con le finalità pro-concorrenziali e di allargamento del mercato dei servizi di pagamento.

Tale regime di responsabilità non sarebbe però pensabile senza l'identificazione dei TPPs; infatti, l'obbligo di identificazione viene assolto, in base a quanto stabilito dagli standard tecnici dell'EBA, grazie all'utilizzo di certificati digitali rilasciati da parte di operatori qualificati: trattasi dei *Qualified Trust Service Providers* – QTSP, la cui disciplina è dettata dal Regolamento (UE) N. 910/2014 sull'identità digitale (c.d. Regolamento e-IDAS"), entrato in vigore a luglio del 2016.

I certificati devono altresì indicare il ruolo svolto dai TPPs nella prestazione del servizio (di PISP o di AISP). Inoltre, sebbene per le banche non sussista un obbligo di munirsi di un certificato digitale, a parere dell'EBA sarebbe preferibile che ciò avvenisse, al fine di assicurare la mutua identificazione degli operatori coinvolti nella prestazione dei servizi di pagamento[47].

Questi certificati possono essere di due tipi: QWAC e QSeal. Il primo assicura la confidenzialità, l'integrità e l'autenticità dei dati trasmessi attraverso il canale di comunicazione certificato, mentre il secondo garantisce che i dati provengano effettivamente dal mittente che ha apposto il sigillo, e che non siano stati alterati dal momento dell'apposizione dello stesso. Sarà, tuttavia, la banca a decidere di quale certificato debba dotarsi il TPP, essendo essa responsabile per la messa a disposizione dell'interfaccia di comunicazione e per la garanzia sulla sicurezza del canale di accesso ai conti[48].

Inoltre, l'aver ottenuto l'autorizzazione a prestare servizi di pagamento dalla propria autorità competente è un prerequisito essenziale per ottenere il rilascio di tali certificati. Potranno quindi prestare tali servizi in Italia: i) le banche che, una volta autorizzate all'esercizio dell'attività creditizia,

[47] *Cfr.* EBA, *Opinion on the use of eIDAS certificates under the RTS on SCA and CSC.*
[48] *Cfr. supra,* EBA, *Opinion cit.*

possono di *default* prestare tutti i servizi di pagamento (ivi compresi quindi i nuovi AIS e PIS); ii) gli Istituti di moneta elettronica – IMEL che, una volta autorizzati, sono anch'essi abilitati di *default* ad emettere moneta elettronica e ad offrire tutti i servizi di pagamento; e iii) gli istituti di pagamento – IP, purché specificamente autorizzati alla prestazione dei nuovi servizi in questione. Infatti, l'autorizzazione agli IP viene rilasciata per la prestazione di singoli servizi di pagamento, debitamente indicati nell'istanza presentata alla Banca d'Italia.

In altri termini, le certificazioni di cui sopra assumono particolare rilievo con riferimento all'autorizzazione di IP che prestino esclusivamente i servizi di AIS/PIS, dato che le banche e gli IMEL non necessitano di apposita autorizzazione per prestare tali servizi. Inoltre, il rilascio della licenza costituisce un procedimento amministrativo e dunque soggetto alle regole precisate nelle Istruzioni di vigilanza della Banca d'Italia; quest'ultima, inoltre, sia in fase autorizzatoria che nella fase successiva di supervisione *on-going,* deve verificare se i *benchmarks* e le metodologie di analisi utilizzati oggi per gli operatori tradizionali, siano adeguati ai principali profili di rischio dei nuovi intermediari[49].

L'utilizzo dei certificati qualificati si riferisce dunque ai soli prestatori di servizi di pagamento autorizzati all'offerta dei servizi di AIS/PIS. Tuttavia, un potenziale problema della disciplina appena delineata risiede nella disciplina relativa agli obblighi che, in base al regolamento e-IDAS si applicano al QTSP; quest'ultimo è dunque tenuto a verificare l'esistenza di tutti i requisiti richiesti al momento del rilascio del certificato ma, una volta emesso, non risulta chiaro se sia anche tenuto ad effettuare una periodica analisi della permanenza del possesso di tali requisiti.

A ragion di logica, in caso di revoca dell'autorizzazione anche i certificati dovrebbero essere revocati, al fine di evitare che operatori non più regolamentati possano accedere ai dati di pagamento degli utenti; non dovrebbero esserci dubbi neppure sul fatto che la responsabilità di chiedere la revoca del certificato debba ricadere in capo al TPP non più munito di licenza.

Per rafforzare questo meccanismo, occorrerebbe chiedersi se sia opportuno coinvolgere nel processo di revoca le autorità competenti a rilasciare (e revocare) la licenza; non sembra, tuttavia, percorribile l'ipotesi di far assumere un ruolo attivo all'autorità, contattando ad esempio il QTSP e chiedendo di ritirare i certificati emessi a nome del soggetto al quale la licenza è stata revocata. Questo perché l'autorità potrebbe non avere alcuna informazione circa quale QTSP, ubicato potenzialmente in un qualsiasi Paese dell'Unione, abbia in effetti rilasciato il singolo certificato al TPP in questione.

[49] Inoltre, i servizi di pagamento rientrano tra le attività ammesse al mutuo riconoscimento; potranno pertanto prestare tali servizi di pagamento in Italia, in virtù del cosiddetto 'passaporto europeo', anche intermediari a ciò autorizzati in altri Stati membri dell'UE e che intendano estendere la propria operatività su base transfrontaliera in altri Paesi appartenenti all'Unione. A seconda delle modalità organizzative prescelte, si configureranno casi di esercizio del diritto di stabilimento (qualora nel Paese ospitante venga costituita una succursale o si faccia stabilmente uso di una rete di agenti) ovvero di libera prestazione, con prerogative e poteri diversi attribuiti all'autorità competente del Paese ospitante.

Inoltre, l'autorità nazionale competente è tenuta a predisporre ed aggiornare di volta in volta un registro pubblico in cui si dà evidenza di tutti gli intermediari cui è stata concessa l'autorizzazione in questione, nonché della eventuale revoca della stessa. Tali informazioni vengono a loro volta inviate all'EBA, incaricata anch'essa dalla PSD2 di tenere un pubblico registro centralizzato, dove ci sono tutte le informazioni contenute nei singoli registri nazionali, trasmesse dalle autorità competenti.
Inoltre, effettuare un aggiornamento tempestivo dei registri nazionali e una comunicazione altrettanto celere al registro dell'EBA, appare essenziale per assicurare che i registri possano rappresentare fedelmente la situazione del mercato, garantendo altresì la rispondenza tra l'effettivo status dell'intermediario e quello risultante dalle informazioni in esso contenute. A tal proposito, le autorità saranno altresì chiamate a ricercare soluzioni tecnologiche che possano ridurre al minimo la distanza temporale tra la conclusione di un procedimento amministrativo (di autorizzazione o di revoca) e la pubblicazione della relativa informativa. È questo un elemento del dibattito in corso sull'impatto che le nuove tecnologie possono avere sulle stesse modalità di conduzione delle attività di vigilanza (c.d. *SupTech*).

4.2 Le ultime innovazioni tecnologiche legate al mercato dei pagamenti:

4.2.1 L'accesso ai conti tramite le *Application Programming Interfaces* (APIs)

Nel nuovo quadro regolamentare appena delineato, le banche hanno dunque l'obbligo di consentire l'accesso ai conti di pagamento da parte dei TPPs, con lo scopo di garantire il diritto dell'utente di utilizzare tali servizi.
Da una parte, la normativa primaria, non impone una specifica soluzione per assicurare tale accesso, anche in ossequio al principio di neutralità tecnologica sopra richiamato, e rinvia la scelta alle banche. Dall'altra parte, la normativa secondaria dell'EBA delinea due possibili modalità con cui i TPPs possono accedere, previo consenso dell'utente, ai conti di pagamento: a) tramite l'interfaccia-utente messa a disposizione del cliente dalla banca nell'ambiente di *home-banking*; o b) attraverso un'interfaccia dedicata e sviluppata a tale scopo. In quest'ultimo caso, si parla appunto di *Application Programming Interface – API*[50].
Inoltre, a prescindere della modalità prescelta, bisognerà attenersi ai già citati vincoli normativi posti all'accesso ai conti da parte dei TPPs, tra i quali: i) accesso solo ai dati di pagamento contenuti in conti precedentemente individuati dall'utente; ii) obbligo di identificazione del TPP al momento dell'accesso; iii) i TPPs non possono conservare i dati ed utilizzarli per finalità diverse da quelle

[50] Nella terminologia di sviluppo *software*, con il termine *Application Programming Interface* (API) si individua quell'insieme di regole di attivazione e uso di un modulo software unitamente all'ambiente operativo per la sua attivazione ed uso.

espressamente indicate dalla legge[51].

Questa impostazione si traduce nell'ordinamento con il concetto dell''*open source*', proprio dell'evoluzione tecnologica più recente. Le APIs, sotto il profilo tecnico, consentono lo scambio di dati disponibili all'interno di reti non appartenenti allo stesso dominio. L'utilizzo di tali interfacce aperte ha un costo contenuto rispetto alle tradizionali attività di *systems integration*, spingendo gli operatori bancari a un vero e proprio "salto" nelle strategie commerciali e distributive adottate.

La grande novità, che favorisce anche la concorrenza, è la trasparenza delle specifiche tecniche da utilizzare per accedere alle informazioni, che ogni impresa mette a disposizione anche in assenza di una relazione contrattuale con i soggetti che possano eventualmente utilizzarla. Sul piano tecnico, una API consente ad un'impresa di essere "scelta ed inclusa" in un processo produttivo, beneficiando così di un prodotto di terzi.

Il concetto di API riporta immediatamente al concetto di *FinTech*, che nella definizione del *Financial Stability Board* collega l'innovazione finanziaria con quella "*tecnologica, che può concretizzarsi in nuovi modelli di business, processi o prodotti, producendo un effetto determinante sui mercati finanziari, sulle istituzioni, o sull'offerta di servizi*[52]".

Occorre aver presente che la PSD2, in linea con l'obiettivo di rafforzare il mercato interno dei servizi di pagamento al dettaglio, impone che la soluzione eventualmente adottata per assicurare l'accesso ai conti di pagamento da parte dei TPPs, sia strutturata in modo da rispondere alle esigenze di tutti i prestatori di pagamento autorizzati nel mercato europeo. A conferma di ciò, troviamo alcune previsioni regolamentari della PSD2 o dell'EBA (e.g. le norme sul *wide usage* ovvero quelle già esaminate relative alla pubblicità delle soluzioni tecniche per l'interfaccia).

A tal proposito, il già citato Regolamento Delegato (UE) n. 2018/389 adottato dalla Commissione europea – contenente le norme tecniche di regolamentazione per definire gli standard aperti di comunicazione comuni e sicuri tra prestatori di servizi di pagamento – ha l'obiettivo di garantire un canale sicuro di autenticazione e comunicazione tra banche e TPPs.

Come anticipato in precedenza, in base a questo Regolamento, i prestatori che detengono i conti devono predisporre le interfacce di accesso per consentire ai TPPs di svolgere la propria attività. Diversamente, deve essere assicurato ai TPPs la possibilità di accedere ai conti di pagamento attraverso l'interfaccia messa a disposizione dei clienti nell'ambiente di *home-banking* (c.d. '*fall-*

[51] Ciò comporta, ad esempio, che in caso di accesso tramite interfaccia utente, quest'ultima dovrà comunque essere debitamente modificata, per garantire la *compliance* con i limiti citati.

[52] Cfr. la definizione di *FinTech data* dal *Financial Stability Board* (FSB): "*Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial*", da *Financial Stability Implications from FinTech*, giugno 2017.

back option')[53]. Il meccanismo delineato dall'EBA, su impulso del legislatore europeo, trovava fondamento nella preoccupazione che un malfunzionamento dell'API, in assenza di una soluzione di *back-up*, potesse costituire un ostacolo allo sviluppo dei servizi di TPPs e alla protezione degli utenti stessi.

Un obbligo *tout court* di definire un meccanismo di *fall-back* era però apparso subito eccessivamente oneroso per le banche, costringendole a investimenti ingenti per mettere a disposizione due diverse modalità di accesso ai conti (API e *fall-back*, quest'ultima da attivare in caso di malfunzionamenti della prima). Tuttavia, per compensare gli opposti interessi in gioco, è stata prevista la possibilità di ottenere dalla propria autorità nazionale competente (per l'Italia, la Banca d'Italia) un'esenzione dall'obbligo di predisporre la *fall-back option*[54] per quelle banche che rispettassero una serie di condizioni definite nella normativa predisposta dall'EBA.[55]

In sintesi, le condizioni tecniche sopra esaminate possono così riassumersi: i) definizione e pubblicazione dei contenuti tecnici dell'interfaccia che i TPPs possono riusare per sviluppare le proprie procedure; ii) attivazione dell'interfaccia operativa per l'accesso alle funzioni necessarie allo sviluppo dei servizi; iii) la messa a punto di procedure di autenticazione dei TPPs, basate su certificati digitali conformi al citato regolamento e-IDAS; iv) l'implementazione di misure di sicurezza a protezione dei dati e delle credenziali degli utenti; v) la possibilità per i TPPs di utilizzare delle procedure di autenticazione messe a disposizione dell'utente; vi) l'attivazione di processi di *change management* dell'interfaccia, consentendo ai TPPs di adeguarsi velocemente alle modifiche delle procedure di colloquio della banca con i propri clienti; vii) la messa a disposizione di ambienti *test* e di supporto alle attività dei TPPs; viii) la disponibilità di procedure di *contingency* in caso di malfunzionamento dell'interfaccia[56].

Ebbene, tali previsioni sono funzionali ad assicurare ai TPPs il diritto a prestare i propri servizi; a tal proposito, una riflessione che ha accomunato tutti gli operatori europei è stata quella volta all'individuazione dei possibili spazi di cooperazione, per ridurre i costi di investimento ed attivare

---

[53] L'articolo 33, comma 4, del Regolamento delegato (UE) n. 2018/389, prevede che "*Nell'ambito di un meccanismo di emergenza, i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, [i TPPs] sono autorizzati a utilizzare le interfacce messe a disposizione degli utenti dei servizi di pagamento per l'autenticazione e la comunicazione con il prestatore di servizi di pagamento di radicamento del conto [la banca], finché per l'interfaccia dedicata non viene ripristinato il livello di disponibilità e di prestazioni previsto dall'articolo 32 [ovvero lo stesso livello di disponibilità e di prestazione, anche in relazione all'assistenza, delle interfacce rese disponibili all'utente dei servizi di pagamento per accedere direttamente al suo conto di pagamento online*".

[54] Cfr. Banca D'Italia, Comunicazione al sistema, 24 dicembre 2018, "*PSD2 – accesso ai conti: istruzioni per il procedimento amministrativo di esenzione dall'obbligo di realizzare procedure di contingency ('fall-back solutions'*)".

[55] Le condizioni per l'esenzione specificate all'articolo 33, par. 6 del Regolamento delegato (UE) n. 2018/389, sono dettagliate negli Orientamenti dell'EBA, "*Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC*", pubblicate il 4 dicembre 2018.

[56] D. GAMMALDI e C. IACOMINI, *Mutamenti del mercato dopo la PSD2* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, F. MAIMERI, M. MANCINI (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019, 123-142, spec. 136.

le esternalità positive proprie di una economia di rete.

In una prima fase, anche sotto la spinta di lavori avviati nell'ambito dell'*European Retail Payments Board* – ERPB[57], c'era stata la ricerca di una convergenza su *standard* tecnici, soddisfacendo i requisiti fissati dal quadro regolamentare.

Nella seconda fase, sono state invece sviluppate diverse soluzioni applicative, ricercando soluzioni condivise ed usando un processo tipico del mondo dei pagamenti, in cui la definizione di soluzioni cooperative o infrastrutturali è essenziale per assicurare l'efficienza del sistema e lo sviluppo delle dinamiche competitive sui servizi.

La necessità di adeguare rapidamente le previsioni regolamentari ha infatti favorito la ricerca di opzioni tecnologiche dirette alla soddisfazione di una molteplicità di utenti; in particolare, nel mercato italiano, sono state presentate diverse soluzioni[58], estese ovviamente anche a soggetti non italiani.

Il rispetto dei tempi regolamentari da parte dei singoli operatori e le esigenze di programmazione delle attività di sviluppo di applicazioni, rappresentano una novità per la maggior parte degli intermediari e hanno stimolato il regolatore italiano a ricercare soluzioni organizzative atte a coniugare le diverse esigenze. A tal proposito, la Banca d'Italia utilizza sia la funzione di vigilanza sui singoli operatori, sia quella di sorveglianza sulle infrastrutture rilevanti per il sistema dei pagamenti[59].

L'adesione ad un'iniziativa di sistema consente dunque alle banche una meno onerosa dimostrazione, in un'ottica di vigilanza, della *compliance* di alcuni requisiti tecnici indicati ai fini del riconoscimento dell'esenzione dalla *fall-back option*; questo, in particolare, grazie ai controlli già effettuati dalla Banca d'Italia in relazione ai servizi offerti dall'iniziativa di sistema, fermo restando la responsabilità della singola banca per la singola soluzione prescelta, anche in linea con la disciplina applicabile

[57] L'ERPB è un organismo operativo dal 2014, presieduto dalla BCE e composto da esponenti sia del lato dell'offerta che del lato della domanda dei pagamenti *retail* in Europa che, attraverso il dialogo tra i diversi *stakeholders* e le istituzioni, si propone di promuovere lo sviluppo di un mercato integrato, innovativo e competitivo dei pagamenti in euro nell'UE.

[58] Queste sono: i) *CBI Globe*, messa a punto dal *Corporate Banking* Interbancario e riconducibile all'esperienza associativa propria del Consorzio; ii) la soluzione messa disponibile da Cedacri; iii) *Fabrick*, promossa dal Gruppo Sella e iv) *Open Banking*, offerta da SIA.

[59] Giova qui ricordare i poteri di cui all'art 146 TUB, il quale prevede che la Banca d'Italia esercita la sorveglianza sul sistema dei pagamenti avendo riguardo al suo regolare funzionamento, alla sua affidabilità ed efficienza nonché alla tutela degli utenti di servizi di pagamento. Per tali finalità, nei confronti dei soggetti che emettono o gestiscono strumenti di pagamento, prestano servizi di pagamento, gestiscono sistemi di scambio, di compensazione e di regolamento o gestiscono infrastrutture strumentali tecnologiche o di rete, può, tra le altre cose, richiedere la comunicazione, anche periodica, di dati, notizie, atti e documenti concernenti l'attività esercitata; emanare disposizioni di carattere generale aventi a oggetto il contenimento dei rischi, l'accesso dei prestatori di servizi di pagamento ai sistemi di scambio, di compensazione e di regolamento nonché alle infrastrutture strumentali tecnologiche o di rete; il funzionamento, le caratteristiche e le modalità di prestazione dei servizi offerti; gli assetti organizzativi e di controllo relativi alle attività svolte nel sistema dei pagamenti; disporre ispezioni, chiedere l'esibizione di documenti al fine di verificare il rispetto delle norme disciplinanti la corretta esecuzione dei servizi di pagamento, adottare provvedimenti specifici volti a far cessare le infrazioni accertate o a rimuoverne le cause.

all'*outsourcing*[60].

4.2.2 I Big Data e i pagamenti digitali: il c.d. *mobile payment*

Nella disamina dell'utilizzo dei Big Data, svolta nel corso del primo capitolo[61], si è visto come la suddivisione della spesa in *Big Data Analytics* tra i vari settori merceologici, indica come primo settore quello bancario e, al suo interno, una fetta importante è caratterizzata dai nuovi servizi di pagamento.

A tal proposito, le imprese *FinTech*, come quelle coinvolte nel c.d. *BankTech* (che offrono applicazioni e servizi bancari) e nel *RegTech*[62] (che offrono strumenti di regolazione e *compliance*), si basano sulla condivisione e sull'elaborazione di dati personali, utilizzando i dati immessi nel flusso telematico per acquisire una conoscenza approfondita dei clienti, anche attraverso la cronologia delle ricerche, le informazioni e le preferenze condivise sui *social media*, le abitudini di consumo e di spesa[63].

Alla luce della rivoluzione digitale che sta investendo, tra gli altri, anche il settore bancario e finanziario, ne discende la necessità di rivalutare il ruolo dei dati e delle relative forme di trattamento e di tutela, soprattutto in relazione alla diffusione di nuovi sistemi di raccolta, conservazione ed elaborazione dei dati personali per il tramite dei *Big data analytics*[64].

Pertanto, occorre analizzare approfonditamente le possibili implicazioni negative derivanti da un uso non corretto o non "governato" dei *Big data*; infatti, le criticità relative al settore *FinTech* sottendono questioni connesse non solo alla vigilanza prudenziale, ma anche alla *cybersecurity*, alla tutela dei consumatori/utenti e della riservatezza dei dati.

Inoltre, come si è già visto nei capitoli che precedono, il principio della sacralità del consenso è entrato in crisi, diventando ormai obsoleto rispetto alle scelte relative al trattamento dei dati personali in una realtà ormai nuova, quella digitale. Infatti, per essere utile, il consenso dovrebbe essere dato consapevolmente e da un soggetto sufficientemente informato; cosa che purtroppo non sempre sembra applicarsi alla realtà. In questo contesto, infatti, l'asimmetria informativa tra utenti ed operatori è diffusa e strutturale: il consumatore non solo non ha a disposizione tutte le informazioni di cui avrebbe bisogno per prendere una scelta informata, ma molti dei suoi comportamenti, per essere

[60] Per una disamina aggiornata in materia di *outsourcing* cfr. in dottrina S. CASAMASSIMA , M. NICOTRA, *L'outsourcing nei servizi bancari e finanziari, La disciplina dell'esternalizzazione alla luce dei recenti interventi regolamentari (Linee guida EBA febbraio 2019 ed aggiornamento Circolare 285 della Banca d'Italia*, Walters Kluwer, marzo 2021.
[61] Cfr. § 1.4.
[62] L. ENRIQUES, *Financial Supervision and RegTech: Four Roles and Four Challanges*, in *Revue Trimestrielle de Droit Financier* 53, 2017, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3087292.
[63] G. BIFERALI, *op.cit., ibidem.*
[64] A. ROSS, *Il nostro futuro*, Milano, 2016.

efficienti, presupporrebbero un grado di conoscenza tecnica che va molto al di là delle competenze diffuse tra la popolazione media[65].

Pertanto, la nuova realtà impone di individuare nuove forme di tutela, per la cui identificazione appare imprescindibile prendere le mosse, facendo uso del metodo induttivo, proprio dalla concreta determinazione dei singoli usi cui i dati si prestano nei rispettivi settori di riferimento[66].

Spesso, inoltre, i nuovi operatori riescono a sfruttare informazioni che i clienti forniscono loro gratuitamente e inconsapevolmente, ottenendo un valore di gran lunga superiore a quello dei servizi resi.

Il tema della profilazione della clientela, strettamente interconnesso alla tutela dei dati personali, è recentemente giunto all'attenzione del legislatore europeo, che è intervenuto sulla materia con il già menzionato GDPR[67], attuato in Italia con il d.lgs. n. 101/2018; in particolare, l'art. 22, comma 1, del GDPR stabilisce che: "*L'interessato ha il diritto 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*"[68].

Tale disposizione, sebbene evidenzi la volontà del legislatore europeo di limitare i rischi derivanti dall'utilizzo incontrollato dei *Big data analytics*, non appare del tutto adeguata a raggiungere lo scopo di tutela sostanziale degli interessati. Inoltre, come si vedrà in seguito, tale disposizione mal si concilierebbe con le implicazioni derivanti dall'uso dei dispositivi mobili nell'esecuzione di operazioni bancarie[69]. Il fenomeno dei *Big data* ha reso infatti obsoleta la tradizionale distinzione tra "dati personali" e "non", risultando così estremamente difficile stabilire *ex ante* cosa rappresenta un dato personale e cosa no tra tutte le informazioni raccolte su un individuo.

Diversi elementi mettono completamente in crisi i principi su cui si basa la disciplina europea e statunitense della tutela della riservatezza: *i)* il riutilizzo dei dati, anche personali, per fini differenti rispetto a quelli per cui sono stati raccolti; *ii)* l'integrazione delle banche dati e l'elaborazione dei dati contenuti al loro interno, che, di fatto, contribuiscono a rivelare informazioni personali; *iii)* la

---

[65] Sul tema della obsolescenza delle leggi e delle gravi distorsioni dalla stessa provocate si v. A. GAMBARO, *Ancora in tema di falsa luce agli occhi del pubblico*, in *Quadrimestre*, 1988, 301 ss.

[66] La questione era già stata esaminata, con mirabile lungimiranza, da A. GAMBARO, *Falsa luce agli occhi del pubblico (False light in the public eye)*, in *Rivista di diritto civile*, 1981, I, 84. Nell'affrontare il tema dei danni derivanti dalla divulgazione di informazioni false o "distorte", o comunque impropriamente utilizzate, Gambaro ha evidenziato, in particolare, come la "sinteticità e standardizzazione" tipiche del linguaggio informatico, inidonee a rappresentare adeguatamente la "complessità dei casi della vita", ben si prestino alla diffusione di informazioni poco accurate, in grado di gettare "falsa luce" sugli affari dell'interessato. L'osservazione si attaglia perfettamente ai *Big Data* e ai rischi connessi a un eccessivo affidamento riposto sul contenuto degli stessi, precipuamente nella valutazione del merito creditizio.

[67] Per un approfondimento sul GDPR in generale si veda §1.3.

[68] Si rinvia più specificamente al §1.3.4 con particolare riferimento al rapporto tra GDPR e Big Data.

[69] Sul punto si rinvia a A. MONTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss.; G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1252; F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in *Id., Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 37 ss.

tendenza a profilazioni e categorizzazioni.

Nel contesto dei *Big data analytics*, l'originaria definizione della *privacy* come "*right to be let alone*"[70] è mutata in quella di *privacy* come diritto di controllare l'uso che altri fanno delle informazioni che ci riguardano, o, altrimenti, come "*diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata*"[71]. Inoltre, come si è visto, le scelte di un individuo in ordine alla cessione di propri dati al fine di ottenere un servizio, si indirizzano a seconda del bilanciamento operato tra benefici, spesso immediati (es. l'accesso a un servizio), e costi (spesso incerti e non conosciuti).

Il *mobile payment* sta attraversando un periodo di grande diffusione, grazie anche ad un insieme di fattori, quali l'innovazione tecnologica in ambito bancario e l'evoluzione del quadro normativo europeo. L'ampia rete italiana di accettazione *contactless* (una delle più importanti a livello europeo) e l'uso ormai diffuso degli *smartphone* rendono l'Italia uno degli Stati con il potenziale più alto in termini di pagamenti da *mobile*.

Negli ultimi anni, il sistema europeo dei pagamenti è stato dunque interessato da un'evoluzione senza precedenti.

L'idea di fondo è che l'elemento di maggior valore della filiera produttiva sia costituto dai "dati"; pertanto, la capacità di leggerli in modo orizzontale diventa il vero valore aggiunto dell'economia digitale. Inoltre, come abbiamo visto con riferimento ai profili concorrenziali, il "sistema dei conti di pagamento" assurge al ruolo di infrastruttura essenziale *sui generis*, con rilevanti impatti sul sistema di relazioni tra gli operatori.

Dal punto di vista della tutela dei dati immessi nel sistema, la PSD2 stabilisce che le banche restituiscano la proprietà dei dati ai clienti i quali hanno libera scelta sul fornitore di servizi di pagamento, aprendo il mercato a nuovi concorrenti anche non finanziari.

Il *mobile payment* è un modello composito che ha al suo interno molteplici paradigmi[72]: **i) *Mobile Remote Payment*[73]** grazie al quale è consentito, anche da remoto, effettuare il pagamento di un bene o servizio attraverso uno *smartphone*; **ii) *Mobile Commerce*** grazie al quale si offre la possibilità di effettuare con il telefono cellulare molteplici attività connesse al processo di acquisto (selezione,

[70] S. WARREN e L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, v. 5, n. 5, 1980, p. 193.

[71] S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, p. 122.

[72] Secondo una ricerca dell'Osservatorio *Mobile Payment & Commerce* del Politecnico di Milano, il *Mobile Payment* in Italia vale 6,7 miliardi di euro con tassi di crescita del 60% rispetto all'anno precedente. A trainare la crescita dei pagamenti da mobile è soprattutto la componente *mobile remote commerce* che nel 2017 ha toccato quota 5,8 miliardi di euro. La componente dei pagamenti mobile in prossimità ha mosso invece i primi passi concreti negli ultimi anni grazie al lancio in Italia di Apple Pay e Samsung Pay, servizi di *proximity payment* che sfruttano la tecnologia NFC. Assieme ai pagamenti NFC si stanno sviluppando soluzioni alternative che sfruttano la geolicalizzazione e il *qr code*.

[73] Inoltre, questi servizi utilizzano la rete *wireless*, sia essa rete Gsm, Umts o altro, e sono fruiti tramite varie piattaforme di interazione: l'invio di un *sms*, la navigazione su siti mobile ottimizzati per il cellulare o applicazioni installate su telefono cellulare o sulla *Sim* (*Sim Toolkit Application*), la Chiamata a *Ivr* (risponditore automatico che guida l'utente nell'attivazione del servizio) e l'invio di USSD (*Unstructured Supplementary Service Data*)

acquisto, confronto di prezzi e prodotti, configurazione del prodotto ecc.), oltre al pagamento del prodotto/servizio, con un modello vicino a quello dell'*e-commerce* da pc; **iii) *Mobile Money Transfer*** grazie al quale si consente il trasferimento di denaro da persona a persona, senza la necessità di uno scambio di beni o servizi[74]; **iv) *Mobile Proximity Payment***[75] (cc.dd. pagamenti elettronici "di prossimità"), ossia pagamenti per cui è necessaria una vicinanza fisica tra l'acquirente ed il venditore del prodotto/servizio acquistato.

4.2.3 Modalità innovative di analisi dei dati nel *mobile payment*

La diffusione dei pagamenti elettronici si muove di pari passo con quella dei dispositivi mobili (*smartphone*, *tablet*, *mobile internet device* – MID), i quali possono collegarsi *wireless* alla rete internet, permettendo così di realizzare una delle moderne forme di cd. *mobile payments.*

È evidente, dunque, la stretta connessione tra la diffusione dei pagamenti in formato digitale, in particolare mediante la rete mobile, e i diversi usi dei *Big data* raccolti mediante i flussi telematici collegati ai pagamenti[76].

Grazie ai *Big Data* e alle nuove tecnologie, infatti, le banche possono: *i)* fare offerte personalizzate ai propri clienti in forza di una migliore profilazione e conoscenza delle loro esigenze, preferenze e abitudini di consumo; *ii)* individuare frodi per mezzo di *alert* sui sistemi di pagamento, come le carte di credito e debito e sulle apparecchiature *Atm*; *iii)* creare un miglior profilo di rischio di credito del proprio cliente, come vedremo meglio in seguito; *iv)* effettuare previsioni sui *trend* dei consumi; e *v)* ridurre le inefficienze e favorire l'interazione tra banca e cliente nella creazione di nuovi prodotti e servizi, quali il *crowdfunding* e il *peer to peer lending*.

Inoltre, il controllo sistematico dei dati relativi alle transazioni, congiuntamente all'azione di algoritmi atti a individuare comportamenti sospetti nelle operazioni di pagamento, nel prelevamento di contanti o nella negoziazione di titoli, potrebbero integrare i processi di *compliance* degli istituti di credito, riducendo altresì il rischio di riciclaggio e di altri atti illeciti.

Come si è visto, l'analisi dei Big Data parte dall'incrocio e valorizzazione non solo di dati interni strutturati, ma anche di dati non strutturati. Nei primi rientrano quelli provenienti *i)* dalle transazioni delle carte di pagamento; *ii*) dagli investimenti finanziari e immobiliari; *iii*) dall'anagrafica interna

[74]Si usa spesso per trasferimenti tra familiari (ad esempio genitori e figli) o rimesse di denaro da parte di immigrati ai propri congiunti nei paesi d'origine (in quest'ultimo caso si parla di *Mobile Remittance*), facendo uso sia la rete cellulare per trasferimenti a distanza (ad esempio tramite sms o applicazioni) sia di tecnologie di prossimità a corto raggio (ad esempio il *Bluetooth*)

[75] Nel *Mobile Proximity Payment* il cellulare imita un pagamento tramite carta, non appoggiandosi necessariamente alla rete cellulare (che può senz'altro aumentarne l'interattività), ma facendo anche uso di tecnologie *wireless* di comunicazione.

[76] Sull'utilizzo dei *Big Data* nel *mobile payment cfr.* R. *MENZELLA, Il ruolo dei big data e il mobile payment, in Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, F. MAIMERI, M. MANCINI (a cura di), in Quaderni di ricerca giuridica della Consulenza Legale, 5 dicembre 2019, p. 143-156.

della banca; *iv*) dall'elenco fidi e affidamenti attuali e storici; e *v)* da dati esterni tradizionalmente utilizzati dalle banche, come *Crif* ed *Experian*.

Con i Big Data è dunque possibile non solo personalizzare le campagne *marketing*, ma anche realizzare modelli di rischio e di investimento in ambito bancario. In particolare, sono stati altresì individuati cinque principali casi di analisi dei Big data adoperati in ambito bancario, con particolare riferimento al *mobile payment*:

1. *Sentiment Analytic:* che si pone l'obiettivo di comprendere, attraverso l'analisi dei commenti *on line* effettuata tramite algoritmi di *text analytics*, il *sentiment* degli utenti per prodotti e servizi. Trattasi di dati non strutturati e dinamici, oggetto di un flusso che si genera di continuo, utili anche per un controllo a lungo termine.
2. *Customer insight*: tale metodo si pone lo scopo di definire il profilo del cliente per elaborare campagne di *marketing* più incisive, vendite targettizzate e miglior *customer service* tramite reti neurali o *decision trees*. In tal modo, è possibile acquisire una visione completa del cliente tipo, ed arrivare a prevederne le scelte mediante lo studio delle abitudini e dei comportamenti. Il principale utilizzo dei dati acquisiti è per finalità di *marketing*: questo tipo di risorsa offre le informazioni demografiche essenziali e altri dati utili per creare messaggi pubblicitari personalizzati.
3. *Customer Segmentation*: che ha lo scopo di costituire *cluster* coerenti con la costruzione di programmi di *marketing* mirati. A tal proposito, permette di ottimizzare la strategia di prezzo e di costruire relazioni consolidate con i clienti.
4. *Next Best Offer:* che consente di incrementare le opportunità di vendita, facendo previsioni sui prossimi acquisti di un cliente ed aumentando la fedeltà della clientela e il *cross selling*. A tal riguardo, i dati dell'utente consentono di comprendere in che momento della vita si trova il cliente, ottimizzando altresì le tempistiche per eventuali campagne *marketing* da comunicargli.
5. *Channel Journey:* in un momento in cui esistono numerosi canali con cui un cliente può interagire, tale metodo può essere facilitato dall'utilizzo dei *Big Data*, che consentono di avere una visione olistica dell'intero processo e delle esperienze associate ai singoli canali.

In questo modo, si delinea una visione generale delle esperienze dell'utente bancario; infatti, il settore dei pagamenti "*consumer* e *retail*" è quello che si muove con maggiore rapidità in termini di innovazione, cogliendo al meglio e sfruttando le potenzialità offerte dai Big Data e dalle nuove tecnologie.

La crescita dei pagamenti digitali, soprattutto sul segmento *mobile*, è senza dubbio trainata dalla crescita dell'*e-commerce*, che ha agevolato ed incoraggiato lo sviluppo di nuove esperienze di

pagamento; tra gli utenti si sta infatti diffondendo la volontà di avere un'esperienza di pagamento ottimale, in termini di rapidità, efficienza ed accessibilità multi-canale.

Questo nuovo modo di concepire l'esperienza di pagamento è consentito dallo sviluppo e dalla diffusione delle nuove tecnologie tra cui: a) ***Mobile wallet***, ossia un borsellino digitale che, attraverso l'utilizzo di tecnologie descritte in seguito, permette di "fare le veci" del proprio portafoglio, rendendolo "virtuale"[77]; e b) **Tecnologia NFC e "tokenizzazione**", dove: i) la "*NFC-Near Field Comunication*" rappresenta la tecnologia più utilizzata per i pagamenti via *wallet* e che, attraverso lo sfruttamento di radio frequenze in banda 13,56 MHz, permette a un dispositivo mobile di trasferire i dati necessari al pagamento al POS che riceve il pagamento; mentre ii) i sistemi di "tokenizzazione" riguardano invece l'innovazione in materia di sicurezza (la c.d. *payment security)* che è una delle principali preoccupazioni di chi intende effettuare un pagamento. In particolare, tali sistemi consentono all'utente di trasformare i dettagli della propria carta o del proprio conto di pagamento in "*token*" temporanei, permettendo di pagare senza la necessità di condividere i propri dati col beneficiario.

Inoltre, tali nuove tecnologie sono, in diverso modo, applicate alle diverse declinazioni del *mobile payment* (i.e. *proximity payment*, *remote payment* e *P2P payment*).

4.2.4 L'utilizzo dei Big Data nel settore creditizio e questioni giuridiche in comune con il *mobile payment*: possibili soluzioni?

Le strategie di regolazione a tutela della clientela bancaria e finanziaria a livello europeo stanno attraversando una fase di notevoli trasformazioni; a tal riguardo, occorre stabilire una stretta interconnessione tra normativa a tutela della clientela e la sana e prudente gestione.

Pertanto, le questioni relative al comportamento tenuto dagli intermediari finanziari verso i propri clienti non sono più circoscritte solo alla protezione della clientela, ma rientrano in una prospettiva più ampia, in ottica prudenziale, con particolare riferimento alla stabilità finanziaria e all'integrità complessiva del sistema.

Infatti, la globalizzazione finanziaria e l'integrazione dei mercati hanno confermato che le condotte scorrette degli intermediari nei confronti dei propri clienti si riverberano non solo sul piano del rapporto negoziale tra cliente ed intermediario (*retail conduct failure*), ma possono altresì riguardare la fiducia nel mercato e, conseguentemente, minare la stabilità e l'integrità del sistema nel suo complesso (*market conduct failure*).

[77] Si tratta generalmente di un'*App* che consente di memorizzare i dati delle carte di credito o di debito, attraverso le quali effettuare i pagamenti. Inoltre, la sempre più crescente presenza di *smartphone* tra la popolazione ha agevolato la diffusione di questi "*mobile wallet*"

Inoltre, il complesso quadro normativo e regolamentare che attualmente disciplina i mercati finanziari è composto, da una parte, dal rapporto tra obiettivi di integrità ed efficienza del sistema bancario e finanziario, dall'altra parte, da istanze dirette a incrementare i livelli di protezione del pubblico dei risparmiatori e degli investitori.

Pertanto, il legislatore e le autorità di vigilanza stanno adottando, partendo dal paradigma della centralità della tutela della clientela nel sistema di regolazione e di vigilanza finanziaria, una prospettiva più ampia e "sistemica" nella scelta delle misure più adeguate ad assicurare una efficace protezione del consumatore.

Sebbene dunque la trasparenza e correttezza contrattuale rimanga un punto di partenza, emerge la necessità di introdurre regole ispirate alla interconnessione tra tutela della clientela e sana e prudente gestione, vista e considerata la già citata interdipendenza tra le questioni afferenti al comportamento tenuto dagli intermediari finanziari nei confronti dei propri clienti e gli obiettivi di stabilità finanziaria e di integrità complessiva del sistema.

Ebbene, in questi termini si spiega il crescente interesse per il processo di "produzione" e di "distribuzione" dei contratti bancari, finanziari ed assicurativi, allo scopo di pervenire ad una limitazione del c.d. *conduct risk*[78].

Ad esempio, nel mercato bancario/finanziario, il *rating* di credito e le offerte personalizzate sono due esempi del modo in cui la tecnologia dei *Big Data* potrebbe incrementare la competitività nel settore bancario.

Infatti, la valutazione del merito creditizio è uno dei servizi offerti dai gestori delle piattaforme digitali sulla base dei *Big Data,* usando un'ampia gamma di informazioni considerate idonee alla determinazione del *credit scoring*[79].

A tal proposito, una parte della dottrina[80] ritiene che il dovere di valutazione del merito creditizio sia

---

[78] A tal proposito, con lo scopo di rafforzare la tutela dei clienti e ridurre il c.d. *conduct risk*, il legislatore e i regolatori europei hanno integrato la tradizionale produzione normativa incentrata sulla trasparenza e correttezza contrattuale con regole e misure volte a disciplinare il processo di strutturazione del prodotto/servizio (*product design*) e la successiva definizione delle modalità distributive e di vendita (*product governance*). La *Product Oversight and Governance* – POG mira ad assicurare l'adeguatezza del prodotto bancario-finanziario-assicurativo rispetto alle caratteristiche e alle esigenze del target di clientela cui lo stesso è rivolto, mediante l'adozione, l'implementazione e la revisione da parte delle imprese di procedimenti diretti ad assicurare che gli interessi, gli obiettivi e le caratteristiche dei destinatari dei prodotti siano sempre tenuti in considerazione, così evitando, altresì, potenziali pregiudizi e minimizzando il rischio di conflitti d'interesse.

[79] BCE, *Guide to assessments of fintech credit institution license applications*, settembre 2017, 4.1, p. 9.

[80] A. MIRONE, *L'evoluzione della disciplina sulla trasparenza bancaria in tempo di crisi: istruzioni di vigilanza, credito al consumo, commissioni di massimo scoperto*, in *Banca borsa tit. cred.*, 2010, 1, p. 592-593; M. GORGONI, *Spigolature su luci (poche) e ombre (molte) della nuova disciplina dei contratti di credito ai consumatori*, in *Resp. civ. prev*., 2011, p. 765; M. DE POLI, *Gli obblighi gravanti sui «creditori» nella fase anteriore e posteriore alla stipulazione del contratto e le conseguenze della loro violazione*, in *La nuova disciplina europea del credito al consumo*, a cura di G. De Cristofaro, Torino, 2009, p. 70; S. PELLEGRINO, *Le disposizioni attuative in materia di credito al consumo*, in *Obbl. contr*., 2011, p. 298; G. BIFERALI, *Il credito ai consumatori*, in *Concorrenza, mercato e diritto dei consumatori*, diretto da G. Cassano, A. Catricalà, R. Clarizia, Milano, 2018, p. 1857. Sul punto vedi anche F. SARTORI, *Disciplina dell'impresa e statuto*

collegato all'obbligo di astenersi dall'assunzione di decisioni arbitrarie e immotivate, finalizzato a vietare al finanziatore di concedere credito in caso di scarsa capacità del consumatore di adempiere all'obbligo di restituzione della somma finanziata.

Infatti, seguendo tale interpretazione, l'obbligo di verifica della solvibilità del debitore sarebbe espressione del più generale principio del dovere di sana e prudente gestione sancito dall'art. 5, primo comma, del TUB[81] (Testo unico Bancario[82]).

In tale prospettiva, ad esempio, la valutazione del merito creditizio effettuata sulla base dei *Big data* sarebbe non solo legittima ma opportuna, facendo altresì un bilanciamento tra l'interesse degli utenti di evitare pregiudizi negativi sulla propria solvibilità, e l'interesse dei prestatori ad una valutazione prudenziale del merito creditizio.

Inoltre, l'uso dei *Big data* nella valutazione del merito creditizio suggerisce di distinguere, anche riguardo ad eventuali responsabilità, due diverse questioni: i) quella della legittimità delle modalità di utilizzo delle informazioni reperite; e ii) quella della legittimità delle ricerche e delle modalità di ricerca svolte per reperirle.

La prima si incentra sulla necessità di un utilizzo corretto, non pregiudizievole e non discriminatorio, nonché sull'esigenza di trasparenza riguardo alle modalità di tale utilizzazione. Il gestore della piattaforma dovrebbe dunque rispettare gli obblighi informativi, volti a garantire la conoscenza delle tecniche adottate per il reperimento dei dati e dei criteri, grazie alle quali tali dati vengono considerati rilevanti per la valutazione del merito di credito[83]. Ebbene, i costi derivanti dal rispetto di tali obblighi potrebbero essere compensati dai benefici che la trasparenza offre, in termini di fiducia degli utenti e affidabilità dei servizi, anche sul piano concorrenziale.

La seconda questione invece riguarda la consapevolezza che l'eventuale violazione di norme a tutela della *privacy* è compiuta, non solo dal gestore della piattaforma che usa le informazioni disponibili, ma anche dal soggetto che consente che queste ultime siano reperibili e che le utilizza come fonte ulteriore di ricavi tramite la rivendita.

Tra le criticità connesse all'uso dei *Big data* nel settore creditizio vi è altresì la discriminazione dei prezzi, già vista nei precedenti capitoli[84], derivante da offerte personalizzate proposte all'esito di un

---

contrattuale: il criterio della «sana e prudente gestione», in *Banca borsa tit. cred.*, 2017, I, 152; A. DOLMETTA, *Trasparenza dei prodotti bancari, Regole*, Bologna, 2013.

[81] In particolare, l'art. 5, primo comma, TUB recita: "*Le autorità creditizie esercitano i poteri di vigilanza a esse attribuiti dal presente decreto legislativo, avendo riguardo alla sana e prudente gestione dei soggetti vigilati, alla stabilità complessiva, all'efficienza e alla competitività del sistema finanziario nonché all'osservanza delle disposizioni in materia creditizia*".

[82] Il testo unico delle leggi in materia bancaria e creditizia (in acronimo TUB) è un testo unico della Repubblica Italiana, emanato con il d.lgs 1º settembre 1993, n. 385, ed in vigore dal 1º gennaio 1994.

[83] E. PROSPERETTI, *Algoritmi dei Big Data: temi regolamentari, responsabilità, concorrenza*, in *Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini, G. Olivieri, Milano, 2018.

[84] Cfr § 2.3 e § 3.4.

processo di profilazione degli utenti, effettuato sulla base ai loro gusti, bisogni e propensioni di spesa[85].

Infatti, come individuata dagli operatori tramite tecniche di *Big data analytics* e di *pricing algorithms*[86], la discriminazione di prezzo consente all'impresa di offrire lo stesso prodotto o servizio a prezzi differenti (c.d. discriminazione nel prezzo[87]), a seconda della disponibilità a pagare dei singoli consumatori (o prezzo di riserva).

Pertanto, la grande disponibilità di dati personali connessa all'avvento dei Big data sta rendendo sempre più evidente la possibilità per gli operatori *online* di attuare strategie di perfetta discriminazione di prezzo. Sia la dottrina[88] che le Autorità[89] hanno peraltro evidenziato una certa ambiguità negli effetti, al contempo positivi e negativi, prodotti dalle offerte personalizzate[90].

In conclusione, anche nel settore bancario/finanziario, la "rivoluzione digitale" impone di mettere in discussione i paradigmi giuridici che finora hanno guidato la disciplina dei diversi fenomeni connessi all'uso dei *Big data*; a tal proposito, si potrebbe proprio iniziare dal *mobile payment.*

In questo contesto, le autorità pubbliche sono state chiamate a svolgere un'analisi ponderata dei fenomeni in atto, al fine di identificare iniziative e interventi che salvaguardino l'interesse pubblico, garantendo in tal modo un adeguato equilibrio tra opportunità e rischi del processo innovativo[91].

È, peraltro, evidente che gli interventi delle autorità di vigilanza, in Italia come all'estero, non possono non considerare l'attuale cornice regolamentare e normativa, che ad oggi, sebbene in continua evoluzione, appare non del tutto adeguata a cogliere le problematiche poste in luce dal progressivo sviluppo di questo nuovo fenomeno.

Un approccio innovativo alla regolazione potrebbe, ad esempio, iniziare dal fondamentale principio di cooperazione, promuovendo un'interazione sinergica tra le istituzioni coinvolte, che consenta di

---

[85] Si veda M. MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, fasc.1, gennaio 2016, p. 95; F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, in Giur. comm., 2018, I, p. 1064.

[86] Per i profili di diritto antitrust cfr. § 2.3.

[87] A tal proposito, si evidenzia anche l'esistenza di alcune problematiche legate ai costi sostenuti dalle imprese per porre in essere la discriminazione di prezzo, dato che simili strategie necessitano di allocare risorse che altrimenti sarebbero destinate ad altre attività.

[88] Cfr. M. ARMSTRONG, *Price Discrimination*, in www.else.econ.ucl.ac.uk, 6 ss.; M. LIBERTINI, *Concorrenza*, in Enc. dir., Annali III, Milano, Giuffrè, 2010, 191 ss.; G. COLANGELO, *Big data, piattaforme digitali e antitrust*, in *Merc. conc. reg.*, 3/2016, pp. 429-430.

[89] Si vedano i seguenti Report: *Big data and differential pricing*, by *The Executive Office of the President of the US*, February 2015, disponibile su http://obamawhitehouse.archive.gov; UK Competition & Markets Authority Report (CMA38, June 2015), *The commercial use of consumer data*, in www.gov.uk; *Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights, Latest White House Report on Big Data*, 4th May 2016; US Federal Trade Commission Report (January 2016), *Big Data. A tool for Inclusion or Exclusion?*, in www.ftc.gov; Report congiunto Autorité de la Concurrence francese e Bundeskartellamt tedesco, *Competition Law and Data*, May 10, 2016, in www.autoritedelaconcurrence. fr/doc/reportcompetitionlawdatafinal.pdf.

[90] Per un approfondimento si rinvia a § 3.4.

[91] Notevoli sono i rischi connessi, tra l'altro, all'abusiva concessione del credito derivante da errore nell'algoritmo: sarebbe pertanto auspicabile la predisposizione di forme di controllo dei modelli di analisi utilizzati, nell'ambito del mandato delle autorità di vigilanza.

elaborare una visione comune.

I dati, perciò, devono essere considerati non più come semplici numeri ma come un *asset* fondamentale da tutti i punti di vista: non solo quello degli operatori e degli utenti, ma anche e soprattutto, quello del legislatore e delle autorità di settore coinvolte.

4.3 Conclusioni

Gli operatori tradizionali del mercato bancario non solo stanno sostenendo costi per lo sviluppo e la manutenzione delle reti e dei sistemi informativi, ma sono anche chiamate ad aprire a titolo gratuito i conti detenuti a potenziali concorrenti sul mercato.

La PSD2, per bilanciare queste due esigenze, come già menzionato, limita il diritto di accesso *ex lege*: a tal riguardo, l'utilizzo dei dati di pagamento per finalità diverse o a conti di natura diversa deve essere disciplinato da accordi contrattuali tra la banca e il TPP, sempre previo consenso dell'utente.

In altre parole, la novità sta nel fatto che le banche debbano farsi carico di un investimento per soddisfare un obbligo normativo[92]; quest'ultimo determina, inoltre, la creazione di un ecosistema aperto, modificando non solo la struttura del mercato dei pagamenti, ma anche il valore di previsione dei dati sui pagamenti, chiaramente emerso in recenti lavori[93].

In compenso, le banche possono ampliare l'offerta di servizi alla propria clientela, sia per quelli obbligatori per legge sia per quelli a valore aggiunto; le banche e gli IP, oltre ad offrire i servizi previsti dalla PSD2, si stanno preparando, tramite forme di collaborazione con la galassia delle imprese *Fintech*[94], ad offrire servizi il cui elemento necessario è costituito dai dati dei clienti.

Con riferimento alla relazione con la clientela, i *TPPs* hanno dalla loro una maggiore conoscenza delle tecnologie e della relativa *user experience*, mentre le banche godono della storica fiducia relazionale, che può favorire una più rapida accettazione di nuovi servizi da parte degli utenti.

Da una parte, vi è un forte interesse delle banche ad offrire "in proprio" i nuovi servizi di PI e AI,

[92] Secondo l'indagine di *ABI Lab, Scenario e trend del mercato ICT per il settore bancario del 2019*, ai primi posti delle priorità d'investimento ICT troviamo, sulla scia della PSD2, le iniziative che riguardano l'*Open Banking.* Seguono il potenziamento dei canali digitali, con attenzione ai servizi di *mobile banking* e all'identificazione da remoto del cliente, e il rafforzamento delle componenti di sicurezza.

[93] Recenti studi mostrano l'esistenza di una forte correlazione tra l'attività economica nel breve periodo e i dati di pagamento; tramite questi ultimi è possibile dunque anticipare le previsioni degli aggregati economici (es. reddito, consumi, investimenti) e misurare tempestivamente l'impatto sui comportamenti di consumatori e imprese di *shock* nelle aspettative, nell'incertezza economica, nella fiducia nella moneta. Cfr. V. APRIGLIANO, G. ARDIZZI, L. MONTEFORTE, *Using the payment system data to forecast the Italian GDP*, Banca d'Italia – Working Papers (Temi di discussione) 2017, n. 1098; V. APRIGLIANO, G. ARDIZZI , L. MONTEFORTE, *Using payment system data to forecast the economic activity*, in *International Journal of Central Banking* (forthcoming) 2019; G. ARDIZZI, S. EMILIOZZI, J. MARCUCCI, L. MONTEFORTE, *News and consumer card payments*, presentato al Workshop della Banca d'Italia *Harnessing Big Data & Machine Learning Technology for Central Banks*, 26-27.3.2018, e in pubblicazione in Banca D'Italia – *Working Papers* (Temi di discussione).

[94] Si veda al riguardo il *Rapporto Fintech Community* 2019, *The European House* – Ambrosetti, secondo il quale le Finsocietàech hanno il potenziale per incidere in modo sostanziale sulla struttura e sulle dinamiche dei mercati finanziari, rappresentando inoltre un'opportunità di collaborazione che le banche possono cogliere per avviare la trasformazione digitale.

adeguando le loro infrastrutture tecnologiche. Dall'altra parte, nascono rapporti collaborativi con le *Fintech* che, in taluni casi, sfociano in rapporti partecipativi, anche di maggioranza[95].

Al di là degli aspetti regolamentari, le nuove tecnologie riprendono un'impostazione secondo cui la relazione con il cliente potrebbe essere ad appannaggio di un *brand* non bancario; quest'ultimo, oltre a fornire servizi digitali, completerebbe la propria proposta commerciale con servizi finanziari ancillari alla propria offerta, ricorrendo altresì ad operatori finanziari.

Per le autorità si apre dunque un nuovo scenario. Esse sono chiamate a riflettere sul modello di regolamentazione e di controllo da applicare.

A tal proposito, gli effetti della nuova regolamentazione sul mercato dei servizi di pagamento potranno valutarsi solo nel medio periodo; tuttavia, le scelte del legislatore europeo hanno già incrementato il livello di concorrenza e gli *standard* di sicurezza dei pagamenti elettronici.

Con riferimento alla concorrenza, si può concludere che le BigTech hanno una maggiore competitività rispetto alle banche, anche in relazione alla maggiore abilità delle prime con gli algoritmi; pertanto, la *XS2A rule*, così come introdotta dalla PSD2, non fa altro che aumentare il vantaggio competitivo delle BigTech sulle banche, dato che le prime non hanno neanche particolari limiti prudenziali da dover rispettare.

A tal proposito, come suggerisce autorevole dottrina[96], si potrebbe immaginare una sorta di "clausola di reciprocità" secondo la quale: da una parte, le BigTech nel rispetto della *XS2A rule,* hanno il diritto di accedere ai dati dei conti di pagamento detenuti presso le banche; dall'altra parte, queste ultime, secondo il principio di proporzionalità di cui all'art. 5.3 del TUE, potrebbero accedere ai c.d. "*behavioural data*" detenuti dalle BigTech, sebbene con gli stessi limiti e finalità che le grandi piattaforme digitali hanno sui dati dei conti di pagamento, e previo sempre il consenso dell'utente.

Diverso sarebbe invece il caso per le *start-up* innovative (o *FinTech*) che, sebbene godano della XS2A *rule* come le BigTech, non hanno un vantaggio competitivo tale da poter scardinare il ruolo che le banche hanno sul mercato. Infine, nulla priverebbe il legislatore, una volta che il mercato diventi competitivo e maturo, di far scomparire la regola di reciprocità. In altri termini, le banche richiederebbero un *level playing field* che gli consenta di poter competere con le BigTech.

Inoltre, in un mercato tecnologico così strutturato e in continuo cambiamento, non si può prescindere da una stretta collaborazione, sia a livello nazionale che a livello europeo, tra le varie autorità operanti nei vari settori interessati. In particolare, in Italia, oltre alla Banca d'Italia, nella sua duplice veste di

[95] Nel rapporto dell'*European Financial Management& Marketing Association* (EFMA) di Maggio 2019, '*Building the bank of the future', si parla di 'Bank as a Platform': the bank maintains the privileged relationship it has with its customers and enriches its value proposition by using services from other players e di 'Bank as a Service': the bank offers its value-added services to other players with the aim of increasing the flows and amortizing its IT investments at the risk of losing the relationship with its customers.*

[96] F. DI PORTO, G. GHEDINI, *op. cit.,* p. 22 ss.

autorità di vigilanza sugli intermediari che prestano i servizi di pagamento e di *overseer* sul sistema dei pagamenti, viene altresì in rilievo l'Agenzia per l'Italia digitale (AgID), che ha l'incarico di riconoscere i QTSP, operatori necessari per assicurare l'avvio dello sviluppo dei servizi di accesso ai conti.

Vista la natura prevalentemente informativa dei servizi di AI/PI, sono altresì apparsi particolarmente rilevanti i profili legati alla protezione dei dati personali, tra cui rientrano i dati relativi ai pagamenti. La PSD2, entrando in vigore prima del GDPR, tenta di risolvere la questione legata al rapporto tra le due normative, richiamando la necessità di rispettare la normativa sulla *privacy* nel trattamento delle informazioni relative ai pagamenti.

Infine, possibili comportamenti lesivi della parità concorrenziale, oltre a violare la normativa sui pagamenti, potrebbero rilevare sotto profili antitrust; da ultimo, non occorre tralasciare i rapporti con le autorità preposte al controllo delle infrastrutture di telecomunicazioni (in Italia, l'AGCOM), tenuto conto che le *BigTech* sono soggetti rilevanti per l'offerta dei servizi di mobilità.

Sebbene questa non sia la sede opportuna per riprendere nel dettaglio le interazioni e le possibili sovrapposizioni tra le diverse discipline richiamate, le autorità sono oggi consapevoli del fatto che uno stesso comportamento potrebbe rilevare sotto diversi profili, rendendo astrattamente configurabile l'applicazione concorrente di diverse sanzioni, stabilite a tutela dei diversi interessi presidiati dalle richiamate normative di settore.

La stessa Commissione europea, nel suo *Fintech Action Plan*[97] sottolinea come le Autorità devono impegnarsi per comprendere a fondo le tendenze nel settore delle tecnologie finanziarie, rafforzando i contatti con il mercato al fine di accrescere le proprie conoscenze e competenze sulle innovazioni digitali.

In conclusione, il nuovo contesto tecnologico pone diverse problematiche, nelle quali i profili regolamentari e tecnici interagiscono; a tal riguardo, la vera novità della PSD2, dal punto di vista delle autorità di vigilanza, è dunque rappresentata dal fatto che la disciplina dei pagamenti al dettaglio presuppone ad oggi un presidio stretto anche dei profili più operativi e tecnici relativi al funzionamento del mercato.

[97] Commissione europea, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, marzo 2018.

Conclusioni generali

Il primo nella storia a parlar di cittadini "consumatori" fu John F. Kennedy nel 1962, per indicare che nella economia di mercato vi era una parte debole. Il concetto di consumatore nasce dunque collegato sia all'idea di concorrenza sia alle regole del mercato. In ambito comunitario, come si è potuto vedere, la Commissione sta costruendo ora il mercato unico digitale.

Partendo dalla libera circolazione dei dati si è quindi arrivati ad un concetto mercatista degli stessi e alla possibilità di commercializzarli "senza limiti".

Tutte considerazioni che portano ad escludere la possibilità di costruire un diritto di proprietà dell'interessato sui propri dati e dunque il trasferimento della loro proprietà all'impresa controparte.

Le istituzioni e le diverse autorità di settore sembrano aver preso consapevolezza del mutamento della realtà sociale a causa dell'implementazione delle nuove tecnologie, e sembrano andare nella direzione di una regolamentazione orizzontale che superi le attuali regolamentazioni verticali tuttora esistenti, prevedendo norme generali con applicazioni settoriali specifiche. In particolare, rispetto alla matrice regolamentare attuale, in cui discipline orizzontali (concorrenza, tutela dei dati personali e tutela dei consumatori) s'intrecciano con quelle verticali (comunicazioni, energia, banche, mercati finanziari, assicurazioni e così via), l'evoluzione prospettica dovrebbe far prevalere discipline regolamentari nuovamente orizzontali, applicabili a tutti i settori.

Tale nuovo sistema, consentirebbe di dare risposte a quegli operatori dei settori bancario-assicurativo, delle informazioni creditizie e delle telecomunicazioni – comunemente soggetti ad una regolamentazione particolarmente strutturata e stringente – i quali, come abbiamo visto ad esempio nel settore dei pagamenti, richiedono un *level playing field*, al fine di consentire alle imprese tradizionali di competere con gli *Over The Top – OTT (Amazon, Facebook, Google*), senza il vincolo di asimmetrie regolamentari.

L'avvento del *FinTech* e, con esso, di nuovi operatori che sulla innovazione tecnologica fanno leva per scardinare barriere all'ingresso e acquisire sempre maggiori fette di mercato, impone dunque un ripensamento delle tradizionali strategie di analisi bancaria e, più in generale, un cambiamento di prospettiva da parte di vigilati e vigilanti.

Da una parte, la varietà dei dati a disposizione dell'industria bancaria e le nuove tecniche di analisi degli stessi rappresentano un fondamentale strumento di sostegno alla crescita economica e al progresso. Dall'altra parte, queste innovazioni tecnologiche devono però essere correttamente guidate e irreggimentate nell'ambito di un quadro normativo e regolamentare che metta al centro: la piena tutela degli utenti, la minimizzazione dei rischi derivanti dalla pervasività dei flussi informativi e il bisogno che venga loro assicurato un *level playing field*, al fine di consentire alle banche e agli intermediari finanziari di competere con gli OTT.

Ebbene, un assetto regolamentare di tipo orizzontale eviterebbe altresì che regolazione e tecnologia corrano a velocità diverse: in modo lineare la prima e in modo esponenziale la seconda. La tecnologia, infatti, sta ricoprendo, più o meno, tutti i settori produttivi, e molti dei problemi normativi sembrano riversarsi trasversalmente in diversi mercati; ad ampliare ciò, è stata da ultimo la pandemia di Covid-19, la quale ha portato ad un ripensamento delle abitudini e della realtà sociale, così come avevamo imparato a conoscerla.

John Maynard Keynes diceva: *"When facts change, I change my mind. What do you do sir?"*

Dunque, con il mutamento della realtà dei mercati, grazie alle nuove scoperte tecnologiche, è necessario modificare l'impianto regolatorio; ad esempio, come si è potuto analizzare, i test di prezzo tipici della concorrenza sono poco utili se il prezzo che l'utente paga non è monetario. Peraltro, la concorrenza può non essere l'unica soluzione nel brevissimo periodo, se rischia di risolversi in un monopolio nel medio.

La trasparenza è senz'altro un elemento importante, ma è limitata se l'algoritmo si rende indipendente dal suo autore. E allora diventa rilevante il rischio che la tutela dei dati personali diventi strumento in mano alle grandi piattaforme digitali, i quali la invocano a loro protezione per giustificare il rifiuto di condividere i dati dei propri utenti.

Il progetto regolatorio internazionale, così come proposto, può reggere solo se poggia su tutte e tre le gambe della regolamentazione orizzontale analizzate presente elaborato: tutela dei consumatori, tutela della concorrenza e tutela dei dati personali. Diversamente, è difficile che questi ultimi due possano da soli sostenere il peso della rivoluzione digitale.

L'ordinamento, nella moderna società digitale, dovrebbe dunque andare verso una tutela trasversale di questo nuovo soggetto debole, il cittadino, abbandonando la normativa verticale che ha sempre contraddistinto la società.

Tale ragionamento ben si sposa anche con quanto esposto all'inizio dell'elaborato con riferimento al diritto che insegue la società.

Infatti, il giurista non può ignorare il momento economico, in quanto esso rappresenta un elemento importante della realtà sociale disciplinata dal diritto; peraltro, le attività regolate dalla norma giuridica sono in buona parte attività strettamente economiche, ossia di produzione, distribuzione e consumo di ricchezza.

Ora viviamo nella società c.d. digitale o dell'algoritmo, dove siamo tutti iperconnessi, ed è dunque necessario superare le rigidità e le zone d'ombra prodotte dalla regolamentazione verticale e settoriale. A tal fine, può essere vista positivamente la portata orizzontale delle norme contenute nel GDPR; quest'ultime, infatti, essendo suscettibili di rivestire anche una valenza pro-concorrenziale – si veda ad esempio il diritto alla portabilità dei dati – potrebbero porsi come un primo modello

normativo che tenta di arginare il problema delle normative settoriali e verticali.

In altri termini, l'economia digitale e l'innovazione ci chiedono un ripensamento della regolamentazione, dato che le nuove tecnologie sono ormai presenti trasversalmente e orizzontalmente in tutti i mercati.

Come si è visto nel secondo capitolo, qualcosa si sta muovendo a livello normativo non solo in Unione europea, ma anche negli Stati uniti ed in Cina.

La convergenza che ci si auspica però non è solo normativa ma anche istituzionale. Tale convergenza deve intervenire non solo tra autorità operanti nello stesso settore di paesi diversi (e.g. *Consumer Protection Cooperation Network* – CPC, *European Competition Network – ECN*, e *European Data Protection Board – EDPB*), ma anche tra autorità diverse dello stesso paese (e.g. *Indagine Conoscitiva sui Big Data* svolta tra Garante per la protezione dei dati personali, l'Autorità per le Garanzie nelle Comunicazioni e l'AGCM).

Si sente, dunque, la necessità di ideare e regolamentare sistemi di collaborazione delle autorità nei singoli procedimenti. Collaborazioni, però, che non si limitino alla redazione di pareri di un'autorità verso l'altra, ma che comportino una sinergia simile a quella creata dal GDPR nell'ambito della cooperazione tra autorità di controllo ex artt. 60 e ss. In tal senso, di volta in volta si potrà ipotizzare la presenza di un'autorità capofila, competente *ratione materiae*, e un'autorità interessata per gli altri profili coinvolti. Ad esempio, la prossima volta che l'AGCM dovrà valutare l'impatto concorrenziale di una concentrazione tra imprese operanti nel mercato dei servizi basati sui dati personali, ben potrebbe rivestire il ruolo di autorità capofila, mentre il Garante Privacy sarebbe l'autorità interessata con riferimento ai profili relativi alla protezione dei dati. Così come il Garante potrebbe essere l'autorità capofila su tematiche quali la portabilità dei dati, mentre l'AGCM e/o l'AGCOM potrebbero essere le autorità interessate per i profili di loro competenza.

Infine, uno sguardo attento andrà altresì volto verso la c.d. *Technology Litigation*, nel quale ambito si inserisce la nuova *class action,* introdotta a livello europeo dalla direttiva (UE) 2020/1828, in attesa di essere recepita dagli Stati membri. In particolare, in Italia, l'azione di classe disciplinata dalla legge 13/2019 non potrà che essere oggetto di una revisione, se non altro in relazione ai soggetti legittimati a esercitare l'azione e in relazione al sistema probatorio.

Chissà se quindi questo nuovo strumento a livello europeo possa incrementare l'effettiva cognizione delle potenzialità del *private enforcement* e il suo utilizzo da parte dei cittadini europei ed italiani.

Bibliografia

ACQUISTI A., TAYLOR C.R. e WAGMAN L., *The Economics of Privacy,* in *J. Ec. Lit., Vol 52, No. 2, 2016.*

ADRIAN EMCH/WENDY NG, WANG XIAOYE *Liber Amicorum - The Pioneer of Competition Law in China*, https://www.concurrences.com/en/all-books/wang-xiaoye-liber-amicorum.

AGCM, AGCOM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui Big Data,* 10 febbraio 2020.

ALPA G., *Dignità. Usi giurisprudenziali e confini concettuali*, in *Nuova giur. civ. comm.*, 1997, II, 415 ss.

ALPA G., *La "proprietà" dei dati personali*, ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p.11.

ALPA G., *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996, n. 675 e successive modifiche*, Formello, 1998.

APRIGLIANO V., ARDIZZI G., MONTEFORTE L., *Using the payment system data to forecast the Italian GDP*, Banca d'Italia – Working Papers (Temi di discussione) 2017, n. 1098.

ARDIZZI G., IMPENNA C., MASI P., *La teoria economica dei sistemi di pagamento*, in C. Tresoldi (a cura di), *Economia dei sistemi di pagamento*, Il Mulino, Bologna 2005, pp.81-132.

ARGENTATI A., *Le banche nel nuovo scenario competitivo. Fintech, il paradigma Open banking e la minaccia delle big tech companies*, in *Mercato, concorrenza e regole*, 3/2018, pp. 441-446.

ARMSTRONG M., *Price Discrimination*, in www.else.econ.ucl.ac.uk, 6 ss.

ARPETTI, *Economia della privacy: una rassegna della letteratura,* in *Riv. dir. media*, 2018, p. 2.

ASTONE F., *Il rapporto tra gestore e utente: questioni generali*, in *Aida*, 2011, 114.

ATTARDI G. - MARINO N. - SANTUS E., *Contact tracing, perché è così importante contro il covid (anche in Italia),* Agendadigitale.eu. 21 aprile 2020.

AULETTA, *Diritto alla riservatezza e "droit a l'oubli"*, in *L'informazione e i diritti della persona*, a cura di ALPA, BESSONE et al., Napoli, 1983, p.127.

AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978.

BAGNOLI V., *The big data relevant market (Il mercato rilevante dei "big data"),* in *Concorrenza e mercato,* 2016, pt. 1, pp. 73-94.

BALDASSARRE, alla voce *Iniziativa economica privata*, in *Enc. Dir.,* Milano, 1971, XXI, P. 582 ss.

BALDINI D, *Il difficile equilibrio tra consenso della persona interessata e legittimo interesse del titolare del trattamento: problemi e prospettive nei rapporti tra fonti interne e dell'Unione europea*

in tema di tutela dei dati personali, in *Osservatorio sulle fonti*, 3/2017.
BALLARANI, *Soggettività del minore e potestà genitoriale nella problematica del diritto alla riservatezza*, Torino, 2004.

BANCA D'ITALIA, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, MAIMERI F, MANCINI M (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019.

BARBAGALLO C., Capo del Dipartimento Vigilanza Bancaria e Finanziaria della Banca d'Italia, presso il Convegno Invernale 2019 – Associazione dei docenti di economia degli intermediari e dei mercati finanziari e finanza d'impresa: *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, Napoli, 8 febbraio 2019.

BARIATTI-SODANO, *Gli abusi di posizione dominante*, in Frignani-Bariatti (a cura di), *Disciplina della concorrenza nella UE*, in *Tratt. dir. comm. dir. pubbl. econ*. Galgano, Padova, Cedam, 2012, 318-321.

BENJAMIN S. M., *Algorithms and Speech*, in *University of Pennsylvania Law Review*, 2013, 161, 1445 ss.

BERTI DE MARINIS G., *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Diritto della banca e del mercato finanziario*, 4, 2018.

BIANCA C.M., F.D. BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007.

BIANCA C.M., *Il Contratto*, Giuffrè Francis Lefebvre, Milano. 2019.

BIANCA C.M., *Il diritto alla riservatezza*, in *Scritti in onore di A. De Cupis*, Milano, 2005.

BIANCA C.M., *Istituzioni di diritto privato*, Giuffrè, Milano 2016.

BIANCA M., *Il trattamento per scopi statistici o scientifici*, Titolo VI, Capo III, a cura di BIANCA C.M., BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007, p.1426-1441.

BIFERALI G., *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Diritto inf. e inform*., fasc. 3, giugno 2018, p. 487.

BIFERALI G., *Il credito ai consumatori*, in *Concorrenza, mercato e diritto dei consumatori*, diretto da G. Cassano, A. Catricalà, R. Clarizia, Milano, 2018, p. 1857.

BOBBIO N., *L'età dei diritti*, Torino, 1990.

BOGNI, *Big Data: diritti IP e problemi della privacy*, in *Dir. Industriale*, volume n. 2/2015.

BONTEMPI P., *Diritto bancario e finanziario*, *Giuffrè*, Milano, 2016.

BORGHI M., *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 2018, fasc. 2, pp. 223-245.

BOSCO, *Portabilità e rinegoziazione dei mutui*, in *Giur. merito*, 2010, 1, p. 265 ss.
BOURREAU M., DE STREEL A., *Digital Conglomerates and EU Competition Policy*, marzo 2019 disponibile a: https://ssrn.com/abstract=3350512.

BOYD D., CRAWFORD K., *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, in *Information Communication and Society*, 2015, 15, 662 ss.

BRAVO, *Il consenso e le altre condizioni di liceità, in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati*, diretto da FINOCCHIARO, Bologna, 2017, p. 101 ss.

BROGGIATO T., *La tutela del consumatore nel rinnovato contesto*, in *Fintech: diritti, concorrenza e regole*, a cura di G. Finocchiaro e V. Falce, Zanichelli, 2019.

BURRELL, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms* in *Big Data & Society*, 2016.

BUSIA G., LIGUORI L., POLLICINO O. (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016.

BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997.

BYGRAVE L.A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, 2002.

CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio del dir. civ. e comm.*, 2018, 1, p. 67 ss.

CALABRESI G., MELAMED A.D., *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85(6) Harvard Law Review*, 1972.

CALABRESI, *Il futuro del law and economics. Saggi per una rimeditazione ed un ricordo*, Milano, 2018.

CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

CALIFANO, *Privacy: Affermazione e pratica di un diritto fondamentale*, Napoli, 2016.

CALVO R., *Le omissioni ingannevoli 179*, Giovanni De Cristofaro (a cura di), *Le pratiche commerciali sleali tra imprese e consumatori. La direttiva 2005/29/Ce e il diritto italiano* (2007).

CALVO, *Le pratiche commerciali «ingannevoli»*, in De Cristofaro (a cura di), *Pratiche commerciali scorrette e codice del consumo*, Torino, Giappichelli, 2008, 223 ss.

CALZOLAIO E., *Il Regolamento europeo sulla protezione dei dati personali: spunti introduttivi e profili problematici*, in *Diritto Mercato Tecnologia*, num. Spec. 2017, 19 ss.

CALZOLARI L., *International and EU antitrust enforcement in the age of Big Data (UE e applicazione internazionale dell'"antitrust" nell'era dei "Big Data")*, in *Il Diritto del commercio internazionale*, 2017, fasc. 4, pp. 855-879.
CALZOLARI L., La collusione fra algoritmi nell'era dei big data: l'imputabilità delle imprese delle

intese 4.0. ai sensi dell'art. 101 TFUE, Media Laws n.3, 2018: 231-232.

CAPPAI M., *Profili evolutivi del "soggetto" e dell'"atto-contratto" nel diritto dei consumi*, in A.A. Vv, *Consumerism 2019. Dodicesimo rapporto annuale. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?* Consumer's Forum e Università degli studi Roma Tre, 2020, 10 ss., disponibile in *https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf*.

CARLI C., *Big (digital) è davvero bad?*, in *Mercato, concorrenza e regole*, 3/2018, pp. 397 - 418.

CARUSO M.A., Le pratiche commerciali aggressive, 2010.

CASAMASSIMA S., NICOTRA M., *L'outsourcing nei servizi bancari e finanziari, La disciplina dell'esternalizzazione alla luce dei recenti interventi regolamentari (Linee guida EBA febbraio 2019 ed aggiornamento Circolare 285 della Banca d'Italia)*, Walters Kluwer, marzo 2021.

CASCINELLI F. - PISTONI V. - ZANETTI G., *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in www.dirittobancario.it.

CASELLA, *Nullità parziale del contratto e inserzione automatica di clausole*, Milano, 1974.

CATAUDELLA, *La tutela civile della vita privata*, Milano, 1972.

CATERINA R., *Cyberspazio, social network e teoria generale del contratto*, Aida, 2011, 96.

CATERINA R., *Paternalismo e antipaternalismo*, in *Riv. dir. civ.*, 2005, 6, 771 ss.

CEOLIN, *La c.d. portabilità dei mutui e la cancellazione semplificata delle ipoteche nel decreto Bersani bis (d.l. 31 gennaio 2007, n.7)*, in *Nuove leggi civ*., 2008, 2-3, p. 259 ss.

CERI S., "*On the role of statistics in the era of big data: A computer science perspective*" *Statistics & Probability Letters*, 136, 68-72, 2018.

CERVONE E., *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. diritto dell'economia*, 2016, p. 41.

CHANG M.-H. (1991), *The Effects of Product Differentiation on Collusive Pricing*, *in «International Journal of Industrial Organization»*, 9, pp. 453-469.

CHIEPPA R., *Ruolo dell'AGCM nel private enforcement e possibili ambiti di cooperazione con il giudice civile*, RAFFAELLI E.A., *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019.

CIAN, SANDEI, *Diritto del Fintech*, Wolters Kluwer CEDAM, Milano, 2020.

CIANCI A.G., *Il diritto all'immagine*, Commento a Cass. 22 luglio 2015, n. 15630, in Aa. Vv., *Libertà di manifestazione del pensiero e diritti fondamentali*, a cura di M. Bianca, A. Gambino e R. Messinetti, Milano, Giuffrè, 2016, 111-116.

CILENTO A., *"New deal" per i consumatori: risultati all'altezza delle ambizioni?* in *Contratto e*

impresa, 2019, fasc. 3, pp. 1195-1216.

CLARIZIA P. E SCHNEIDER E., *Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19*, IRPA - Osservatorio sullo Stato digitale. 19 aprile 2020.

COHEN, *Examined Lives: Information Privacy and the Subject as Object*, in *Stanford Law Rev*., 2000, 52, p. 1373 ss.

COLANGELO G., *"Big data", piattaforme digitali e "antitrust" (Big data, digital platforms and antitrust),* in *Mercato concorrenza regole*, 2016, fasc. 3, pp. 425-460.

COLANGELO G., *Big data, piattaforme digitali e antitrust*, in *Merc. conc. reg*., 3/2016, pp. 429-430.

COLANGELO G., MAGGIOLINO M., *Big Data, data protection and antitrust in the wake of the "Bundeskartellamt" case against Facebook (Big Data, protezione dei dati e "antitrust" sulla scia del caso "Bundeskartellamt" contro Facebook)*, in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2017, fasc. 1, pp. 9.

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale,* in *federalismi.it*, 21 novembre 2018.

COLOMBO – PIGNATARO, *Raccolta e condivisione di Big data: quali effetti sulla collusione?, in Mercato, concorrenza e regole*, 2/2019,p. 315 ss.

COMANDÉ G., MALGIERI G. (a cura di), *Manuale per il trattamento dei dati personali*, Roma, 2018.

COSENTINO F., *Il paternalismo del legislatore nelle norme di limitazione dell'autonomia dei privati*, in *Quadrimestre*, 1993, 1, 119 ss.

COSTI R., *L'ordinamento bancario*, Il Mulino, 2012.

CUFFARO V., *Cancellare i dati personali. Dalla damnatio memoriae al diritto all'oblio*, in ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 219 ss.

CUFFARO V., *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa*, 2018, 3, 1098 ss.

CUFFARO, *A proposito del ruolo del consenso,* in *Trattamento dei dati personali e tutela della persona* a cura di CUFFARO, RICCIUTO e ZENO ZENCOVICH, Milano, 1999, 117 ss.

CUSTERS B., CALDERS T., SCHERMER B. et al., *Discrimination and Privacy in the Information Society*, Heidelberg, 2013.

D'IPPOLITO G., *Il principio di limitazione della finalità del trattamento tra "data protection" e antitrust. Il caso dell'uso secondario di "big data"" (The principle of purpose limitation between data protection and antitrust, regarding to the so called "secondary use of big data")* in *Il Diritto dell'informazione e dell'informatica*, 2018, fasc. 6, pp. 943-987.

D'ACQUISTO G., NALDI M., *Big Data e Privacy by design*, Torino, 2017.

D'AMICO e PAGLIANTINI, *Nullità per abuso e integrazione del contratto*, Torino, 2015.

D'ANGELO, *Contratto e operazione economica*, Torino, 1992.

D'IPPOLITO, *Evoluzione della disciplina consumeristica e rapporto con la normativa sulla protezione dei dati personali personali* in A.A. Vv, *Consumerism 2019. Dodicesimo rapporto annuale. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?* Consumer's Forum e Università degli studi Roma Tre, 2020, 70 ss., disponibile in *https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf.*

DALLE VEDOVE G., Le pratiche commerciali aggressive 117, Anna Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette* (2008).

DE FRANCESCHI A., LEHMANN M., *Data as Tradeable Commodity and New Measures for their Protection*, in *The Italian Law Journal*, 2015, 1, 51 ss.

DE FRANCESCHI V, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017.

DE FRANCESCHI, *Il pagamento mediante dati personali*, in *I dati personali nel diritto europeo* (a cura di CUFFARO, D'ORAZIO e RICCIUTO), Torino, 2019, p. 1329 ss.

DE GREGORIO e TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy Digitale*, TOSI (a cura di), *Giuffrè Francis Lefebvre*, 2019, pp. 447-484.

DE MEO R., *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. inf.*, 2013, III, 604.

DE POLI M., *Gli obblighi gravanti sui «creditori» nella fase anteriore e posteriore alla stipulazione del contratto e le conseguenze della loro violazione*, in *La nuova disciplina europea del credito al consumo*, a cura di G. De Cristofaro, Torino, 2009, p. 70

DELLI PONTI A., *Mercato unico digitale: la nuova normativa per la fornitura di servizi online dell'UE*, in https://www.ictsecuritymagazine.com, 10 ottobre 2019.

DELMASTRO E NICITA, *Big data: come stanno cambiando il nostro mondo*, il Mulino, 2019.

DI CIOMMO F., RUBINO DE RITIS M., CASSANO G. (a cura di), *Banche, intermediari e Fintech. I nuovi strumenti digitali in ambito finanziario*, 2020.

DI MAJO GIAQUINTO, *L'esecuzione del contratto*, Milano, 1967.

DI NELLA L., Le pratiche commerciali sleali aggressive 215, Giovanni De Cristofaro (a cura di), *Le pratiche commerciali sleali tra imprese e consumatori. La direttiva 2005/29/Ce e il diritto italiano* (2007).

DI PORTO F., GHEDINI G., "*I Access Your Data You Access Mine". Setting a Reciprocity Clause for the "Access to Account Rule" in the Payment Services Market* in *www*.papers.ssrn.com, giugno 2019.

DI PORTO F., *La regolazione degli obblighi informativi*, Napoli, Editoriale Scientifica, 2017.

DI PORTO F., *La rivoluzione "big data". Un'introduzione,* in *Concorrenza e mercato*, 2016, pt. 1, pp. 5-14.

DI PORTO F., MAGGIOLINO M., *Algorithmic Information Disclosure by Regulators and Competition Authorities* (March 31, 2019). *Global Jurist*, 2019, *Bocconi Legal Studies Research Paper No*. 3363169, SSRN: https://ssrn.com/abstract=3363169 or http://dx.doi.org/10.2139/ssrn.3363169.

DI PORTO, *Dalla convergenza digitale-energia l'evoluzione della specie: il consumatore «iper-connesso»,* in *Merc. conc. reg.*, 2016, 67.

DI RESTA F., *La nuova privacy europea,* Torino, 2018, RICCIO G.M., SCORZA G., BELLISARIO E. (a cura di), *GDPR e normativa privacy.* Commentario, Milano, 2018.

DOLMETTA A., *Trasparenza dei prodotti bancari, Regole,* Bologna, 2013.

DOLMETTA, *Questioni sulla surrogazione per volontà del debitore ex art. 8 Legge n. 40/2007 (c.d. "portabilità del mutuo"),* in *Banca, borsa, tit. cred*., 2008, 4, pt. 1, p. 395 ss.

DONINI E., *Collusion and Antitrust: The Dark Side of Pricing Algorithms,* in https://www.associazioneantitrustitaliana.it/wp-content/uploads/2020/10/Tesi-Elena-Donini.pdf.

DURANTE, *Rethinking human identity in the age of automatic computing. The philosophical idea of trace,* in *Law, Human Agency and Automatic Computing*, a cura di Aa Vv., p. 85.

ENRIQUES L., *Financial Supervision and RegTech: Four Roles and Four Challanges,* in *Revue Trimestrielle de Droit Financier* 53, 2017, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3087292.

EUROPEAN BANKING AUTORITY, *Report on Big Data and Advanced Analytics*, in https://eba.europa.eu/sites/default/documents/files/document_library//Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf, gennaio 2020 (data ultima visita: 28 marzo 2020), p. 42.

EUROPEAN COMMISSION, *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions: A European strategy for data*, in https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, Brussels, 19 febbraio 2019 (data di ultima visita: 28 marzo 2020).

FAGGIOLI G e CATALETA A., *Sentenza Schrems è una vittoria per la sovranità digitale degli europei: ecco perché,* disponibile su https://www.agendadigitale.eu/sicurezza/sentenza-schrems-e-una-vittoria-per-la-sovranita-digitale-degli-europei-ecco-perche/, 21 luglio 2020.

FAMILIARI S., *Il diritto alla portabilità dei dati: origine e prospettive per il futuro (The rights to data portability: origin and perspectives for the future),* in *Ciberspazio e diritto,* 2016, fasc. 3, pp. 403-434.

FARACE, *portabilità del mutuo e atto di surrogazione,* in *Rivista di diritto civile*, 2012, 6, pt. 2, p. 615 ss.

FARALLI C., *Il diritto alla privacy. Profili storico-filosofici*, in ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p.1 ss.

FATTORI P. TODINO M., *La disciplina della concorrenza in Italia 86* (2010).

FERRARA F., *Teoria del negozio illecito nel diritto civile italiano*, Milano, 1914.

FERRETTI, *Osservazioni sulle proposte di modifica contenute nel Libro Bianco intitolato: "Verso un controllo più efficace delle concentrazioni dell'UE*", in *Contr. impr. eur*., 2015, 381 ss.

FERRI G.B., *Diritto all'informazione e diritto all'*, in Riv. dir. civ. 1990, p. 801 ss.

FIA T., *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo notiziario giuridico*, 2019, fasc. 1, pp. 60-133.

FILIPPELLI M., *Il problema dell'oligopolio nel diritto antitrust europeo: evoluzione, prospettive e implicazioni sistematiche*, in *Riv. Società*, ISSN 0035-6018. - 63:2-3(2018), pp. 567-614.

FINANCIAL STABILITY BOARD, *FinTech and market structure in financial services: Market developments and potential financial stability implications, in* https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/, *14 February, 2019 (ultima visita 27 marzo 2020).*

FINOCCHIARO (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

FIORIGLIO G., *Freedom, Authority and Knowledge on Line: The Dictatorship of the Algorithm*, in *Revista Internacional de Pensamiento Politico*, 2015, 10, 395 ss.

FORGÓ N., HÄNOLD S., SCHÜTZE B., *The Principle of Purpose Limitation and Big Data*, in M. Corrales et al. (eds), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*, Singapore, 2017, 17.

FRIGENI, *Segnalazione presso le centrali rischi creditizie e tutela dell'interessato*, in *Banca borsa e Titoli di Credito*, 2013.

FUSARO, *La portabilità dei mutui nel Testo Unico Bancario*, in *Contratto e impresa*, 2011, 6, p. 1422 s.

G. AMATO, *Il potere e l'antitrust*, Il Mulino, 1998, 93.

GABRIELLI E.,(a cura di), Il diritto all'oblio, Napoli, 1999.

GALGANO, *Diritto privato*, 18° ed., Padova-Milano, 2019, p. 261.

GALGANO, *Effetti del contratto. Rappresentanza. Contratto per persona da nominare*, in *Comm. Scialoja-Branca*, a cura del medesimo Art. 1372-1405, 65.

GALGANO, *Trattato di diritto civile*, Padova, 2009, I, p. 334.

GAMBARO A., *Ancora in tema di falsa luce agli occhi del pubblico*, in *Quadrimestre*, 1988, 301 ss.

GAMBARO A., *Falsa luce agli occhi del pubblico (False light in the public eye),* in *Rivista di diritto civile,* 1981, I, 84.

GAMBUTO S., *Algorithms, big data and tacit collusion new challenges for competition law*, in RAFFAELLI E.A., *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019.

GAMMALDI D. e IACOMINI C., *Mutamenti del mercato dopo la PSD2* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale,* MAIMERI F, MANCINI M (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019, 123-142.

GARANTE DELLA PROTEZIONE DEI DATI PERSONALI, *Relazione 2018,* 7 maggio 2019.

GENTILE-LINCIANO-LUCARELLI-SOCCORSO, *Financial disclosure, risk perception and investment choices. Evidence from a consumer testing exercise*, in *Quad. fin. Consob*, 82/2015.

GIACOBBE G, *Diritto all'oblio* in *Atti del convegno di Urbino 17 maggio 1997*, a cura di GABRIELLI, Napoli, 1999, p.30 ss.

GIACOBBE G., *Il "diritto alla riservatezza" in Italia*, Firenze, 1974.

GIAMPIERI, *Il decreto sulle liberalizzazioni. La portabilità del mutuo, le intenzioni del legislatore e gli effetti (forse indesiderati) della norma*, in *Nuova giur. civ*., 2007, p. 467 ss.

GIANNACCARI A., *Facebook e l'abuso da sfruttamento al vaglio del Bundesgerichtshof,* in *Mercato concorrenza regole*, 2020, fasc. 2, pp. 403-409.

GIANNACCARI A., *Facebook, tra privacy e Antitrust: una storia (non solamente) americana,* in *Mercato, concorrenza e regole*, 2/2019, p. 273-292.

GIANNACCARI A., *La storia dei "Big Data", tra riflessioni teoriche e primi casi applicativi (The Big Data antitrust story: theoretical approaches and the first enforcement cases)*, in *Mercato concorrenza regole*, 2017, fasc. 2, pp. 307-332.

GIANNONE CODIGLIONE G., *Libertà di impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali ([Free enterprise, competition and net neutrality in the transnational market of personal data])*, in *Il Diritto dell'informazione e dell'informatica*, 2015, fasc. 4-5, pp. 271-304.

GIMIGLIANO G. e NAVA G., *L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari,* in *Smart cities e diritto dell'innovazione* a cura di G. Olivieri e V. Falce, Milano, 2016, p.190.

GIORDANO G., *Lo sviluppo dei servizi di pagamento* in *Diritto ed economia di banche e mercati finanziari* di VELLA F. et al., il Mulino, 2019, p. 98 ss.

GOBBATO S., *"Big data" e "tutele convergenti"* tra concorrenza, GDPR e Codice del consumo in Rivista di diritto dei media, 2019, fasc. 3, pp. 150. Sul punto cfr. anche RABAI B., *I "big data" nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali,* in *Amministrare,*

2017, fasc. 3, pp. 405-422.

GOODMAN e FLAXMAN, EU *Regulations on Algorithmic Decisionmaking and Right to Explanation*, in www.ora.ox.ac.uk.

GORGONI M., *Spigolature su luci (poche) e ombre (molte) della nuova disciplina dei contratti di credito ai consumatori*, in *Resp. civ. prev.*, 2011, p. 765.

GRECO P., *I diritti sui beni immateriali*, Utet Giuridica, 1948.

GREENLEAF G., '*A World Data Privacy Treaty? "Globali- sation" and "Modernisation" of Council of Europe Convention 108'* in David Lindsay et al. (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014), 136-137.

GRIECO P., *La violazione degli obblighi informativi nell'intermediazione finanziaria tra disciplina civilistica e regolamentare*, in *Resp. civ. prev.*, n. 4/2017, p. 1265-1284.

HARCOURT, *Against Prediction. Profiling, Polishing and punishing in an Actuarial Age*, Chicago-London, 2007.

HELFRICH M. E HERWEG F. (2016), *Fighting Collusion by Permitting Price Discrimination, in «Economics Letters»*, 145, pp. 148-151.

HEMNES, *The Ownership and Exploitation of Personal Identity in the New Media Age*, in *J. Marshall Rev. Intell. Prop. L.*, 2012, 12, p. 1 ss.

KAPLOW L., *On the Meaning of Horizontal Agreements in Competition Law*, in *California Law Review*, 2011, 683 ss.

LASICA, *Identity in the Age of Cloud Computing – The Next Generation Internet's Impact on business governance and social interaction*, Washington DC, 2009.

LASSERRE B., MUNDT A., *Competition law and Big Data: the enforcers' view (Diritto della concorrenza e "Big Data": il punto di vista degli esecutori)*, in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2017, *fasc.* 1, pp. 17.

LIBERTINI M. *Lezioni di diritto industriale*, Torre, Catania, II ed., 1990.

LIBERTINI M. *Sull'efficacia orizzontale in diritto privato delle norme sui diritti fondamentali dei trattati europei*, in *Persona e mercato* [rivista telematica], 2018, 212-219.

LIBERTINI M., *Clausola generale e disposizioni particolari nella disciplina delle pratiche commerciali scorrette*, in Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette*, Padova, Cedam, 2008, 27 ss.

LIBERTINI M., Concorrenza, in Enc. dir., Annali III, Milano, Giuffrè, 2010, 119 e 216 ss.

LIBERTINI M., *Concorrenza*, in Enc. dir., Annali III, Milano, Giuffrè, 2010, 191 ss.

LIBERTINI M., *La tutela della libertà di scelta del consumatore e i prodotti finanziari, in Mercati finanziari e protezione del consumatore*, a cura di M.Grillo, Brioschi, Milano, 2010, 21-46.

LIBERTINI M., Pratiche concordate e accordi nella disciplina della concorrenza (commento a C. St., 29 novembre 1996, n. 1792), 5 Giorn. dir. amm. 445 (1997).

LIBERTINI M., *Regolazione e concorrenza nei servizi di pagamento*, in *Diritto della banca e del mercato finanziario*, 2013, 1-28.

LIBERTINI M., *Tutela e promozione delle creazioni intellettuali e limiti funzionali della proprietà intellettuale*, in A.I.D.A. (Annali Italiani del Diritto d'Autore), 2014, 299-336.

LIBERTINI, *I fini sociali come limite eccezionale alla tutela della concorrenza: il caso Alitalia (nota a Corte Cost. 22 luglio 2010, n. 270)*, in *Giuri. Cost*, 2010, 4, p.3296 ss.

LILLÀ MONTAGNANI M., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza e regole*, 2/2019, pp. 293-314.

LINCIANO, *Errori cognitivi e instabilità delle preferenze nelle scelte di investimento. Le indicazioni di policy della finanza comportamentale*, in *Quad. fin. Consob*, n. 66/2010.

LIU Q. E SERFES K. (2004), *Quality Information and Oligopolistic Price Discrimination, in «Journal of Economics & Management Strategy»*, 13, pp. 671-702.

LLEWELLYN D. T., (2001), "*The new economics of banking*", SUERF Study 5, Amsterdam, ripreso in "*Group of Ten Report on consolidation in financial sector*", gennaio 2010.

LO SURDO C., *Accordo contrattuale e intesa ai sensi della normativa antitrust*, *I Contratti* 299 (2001).

LUCCHINI GUASTALLA E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr.*, 2018, p. 113 ss.

MACCHIAVELLO E., *FinTech. Problematiche e spunti per una regolazione ottimale*, in *Mercato Concorrenza Regole*, Fascicolo 3, dicembre 2019.

MAGGIOLINO M., *Big data e diritto Antitrust*, Egea, 2018.

MAGGIOLINO M., *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, 2016, 95 ss.

MAGGIOLINO M., *EU Trade Secrets Law and Algorithmic Transparency* (March 31, 2019). *Bocconi Legal Studies Research Paper No*. 3363178, SSRN: https://ssrn.com/abstract=3363178 or http://dx.doi.org/10.2139/ssrn.3363178.

MÄIHÄNIEMI B., *Competition Law and Big Data: Imposing Access to Information in Digital Markets*, Elgar Publishing, 2020.

MALGIERI e CUSTERS, *Pricing Privacy: The Right to Know the Value of Your Personal Data*, in *Computer Law & Security Review*, 2018, 34, p. 289 ss.

MANGINI V.– TONI A.M., *Manuale breve di diritto industriale*, Giappichelli, Torino, 2015.

MANTELERO A., *The future of data protection: Gold standard vs. global standard*, *Computer Law & Security Review*, disponibile *online* dal 9 November 2020, in www.sciencedirect.com.

MANTELERO A., VACIAGO G., *The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, in *Computer Law Rev Int'l*, 2013, 161 ss.

MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf*., 2012, 135 ss.

MANTELERO, *The future of consumer protection in the E.U. Re-thinking the "notice and consent" para- digm in the new era of predictive analytics*, in *Computer Law & Sec. Rev.*, 2014, 30, 647 ss.

MANYIKA J. et al., *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, maggio 2011.

MASPES, *Trasferimento ad altro operatore di telefonia mobile*, in *Corriere trib*., 2009, 39, p. 3163 ss.

MASTRORILLI A., *Algoritmo scellerato?*, in *Mercato concorrenza e regole*, 2/2019, pp. 343-352.

MAYER-SCHÖNBERGER V. –CUKIER K., *Big data*, Milano, 2013, pp. 237 ss.

MAZZAMUTO, *Il principio del consenso ed il problema della revoca, in Libera circolazione e protezione dei dati personali*, a cura di PANETTA, Milano, 1996, p. 994 ss.

MELI, *Diligenza professionale, consumatore medio e regola di de minimis nella prassi dell'AGCM e nella giurisprudenza amministrativa* in www.orizzontideldirittocommerciale.it.

MELI, *Le pratiche sleali ingannevoli*, in Genovese (a cura di), *I decreti legislativi sulle pratiche commerciali scorrette*, Padova, 2008, 87 ss. spec. 105.

MENZELLA R., *Il ruolo dei big data e il mobile payment*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, MAIMERI F, MANCINI M (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019.

MERIANI, *Digital platforms and spectrum of data protection in competition law analyses*, in ECLR, 2017, vol. 38, Issue 2, 93.

MERLINO P, *Antitrust and Data protection Law: a relationship in search of clear boundaries* in RAFFAELLI E.A., *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019.

MESSIMETTI e DI CIOMMO, *Diritti della personalità*, in *Diritto Civile*, a cura di MARTUCCELLI e PESCATORE, Milano, 2011, p. 599 ss.

MESSINETTI D., voce *Personalità (diritti della)*, in *Enc. dir.*, XXIII, Milano, 1983, 355-406.

MESSINETTI R. *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, pp. 167 ss 2019.

MESSINETTI R., *Circolazione dei dati e autonomia privata*, ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, pp. 137 ss 2019.

METAFORA V., *Il mito di Narciso e la giurisprudenza: a pro- posito del diritto sul proprio ritratto*, in *Riv. crit. dir. priv.*, 1990, 867 ss.

MEZZANOTTE, *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009.

MIRONE A., *L'evoluzione della disciplina sulla trasparenza bancaria in tempo di crisi: istruzioni di vigilanza, credito al consumo, commissioni di massimo scoperto, in Banca borsa tit. cred.*, 2010, 1, p. 592-593.

MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 262.

MONETI S., *Mobile payments: gli sviluppi del mercato e l'inquadramento normativo, in Analisi giuridica dell'economia*, 2015, 101.

MONTAGNANI M.L, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato, concorrenza e regole*, 2/2019, p. 293 ss.

MONTELEONE, *Il diritto alla portabilità dei dati. Tra diritti della persona e diritti del mercato*, in *LUISS Law Review*, 2017, p. 205.

MONTELERO A., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss.

MONTELLA P., *La Direttiva PSD 2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, 2018.

MORBIDELLI, alla voce *Iniziativa economica privata*, in *Enc. Giur*., XVII, Roma, 1989.

MORERA-F. VELLA (a cura di), *Finanza comportamentale. Investitori a razionalità limitata*, in AGE, 1/2012.

MORERA, *Legislatore razionale versus investitore irrazionale: quando chi tutela non conosce il tutelato*, in AGE, 1/2009, 78 ss.

MOROZZO DELLA ROCCA P., *Il principio di dignità della persona umana nella società globalizzata*, in *Dem. dir.*, 2004, 2, 195 ss.

MOSCIANESE J.- DI BENEDETTO F., *Privacy, portability and interoperability regarding data produced by the consumer. The role of competition law and market regulation*, in RAFFAELLI E.A., *Antitrust between EU Law and National Law/Antitrust tra diritto nazionale e dell'unione europea*, Bruylant ed., 2019.

MUCCIARONE, *Centrale dei rischi e esclusione degli enti collettivi dalle tutele del codice della privacy*, in *Banca borsa Titoli di Credito*, 2015.

MUCCIARONE, *La portabilità dei conti: prime note*, in *Banca, borsa, tit. cred*., 2016, p. 581 ss

MUSCOLO G., *Big data e Concorrenza. Quale rapporto?* in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, 173.

NANNA, *Eterointegrazione del contratto e potere correttivo del giudice*, Padova, 2010.

NATOLI R., *Il contratto "adeguato". La protezione del cliente nei servizi di credito, di investimento e di assicurazione*, Milano, 2012.

NAZZINI R., *Online Platforms and Antitrust: Where Do We Go From Here? (Piattaforme "online" e "antitrust": dove andiamo da qui?)* in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2018, fasc. 1, pp. 18.

NICITA A., Il mercato del dato profilato tra privacy, concorrenza e potere contrattuale nella prospettiva economica, in I dati personali nel diritto europeo, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1167.

NISTICÒ J., *La tutela collettiva*, in Catricalà A., Cazzato C.E., Fimmanò F. (a cura di), Diritto antitrust, Giuffrè, 2021.

NIVARRA L., *La proprietà intellettuale tra "mercato" e "non mercato"*, in *Riv. crit. dir. priv.*, 2004, 517-532.

OLIVIERI G., *Dal mercato delle cose al mercato delle idee Relazione al Convegno "Le parole del diritto commerciale"*, Macerata, 7 aprile 2017 in *Rivista delle società*, 2017, fasc. 4, pp. 815-824.

OREFICE MARIA, *I "big data". Regole e concorrenza (Big Data. Rules and Competition)* in *Politica del diritto*, 2016, *fasc. 4*, pp. 697-743.

ORESTANO A. *La circolazione dei dati personali*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, II, Milano, 2003. 119.

OSBORNE CLARKE, *E-commerce: in arrivo nuove norme UE per proteggere i consumatori*, in https://www.osborneclarke.com/it/insights/e-commerce-arrivo-nuove-norme-ue-per-proteggere-consumatori/, 27 febbraio 2020 (ultima visita: 29 marzo 2020).

OSTI - PARDOLESI, *L'Antitrust ai tempi di Facebook*, in *Mercato, concorrenza e regole*, 2/2019, p. 195- 218.

OSTI C., Antitrust e oligopolio. Concorrenza, cooperazione e concentrazione: problemi giuridico-economici e proposte di soluzione, 165 (1995).

OSTI C., *La tutela del consumatore tra concorrenza e pratiche commerciali scorrette*, in Catricalà-Gabrielli (a cura di) *I contratti nella concorrenza, Trattato dei contratti* Rescigno - Gabrielli, Torino, Utet, 2011, 425 ss.

OTTOLIA, Privacy e social networks: profili evolutivi della tutela dei dati personali, in AIDA, 2011, 360 ss.

PAGALLO U. et al., *What Is New with the Internet of Things in Privacy and Data Protection? Four*

Legal Challenges on Sharing and Control in IoT, in R. LEENES ET AL. (cur.), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017, 74-76.

PAGE WILLIAM H., *Objective and Subjective Theories of Concerted Action, 79 Antitrust Law Journal* 215 (2013).

PALAZZOLO, *La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (UE) n. 2016/679*, in *Contr. e impr.*, 2017, p. 613 ss.

PARACAMPO M.T., *Fintech – Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Vol. I, II ed., 2021.

PARISI, *Privacy e mercato digitale*, Pacini, Pisa, 2020, 113 ss.

PATTI S, *Comm. sub. Art. 23*, in *Protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196*, BIANCA C.M. e BUSNELLI, Padova, 2007, I, p.553s.

PEIFER, *Territorialità e portabilità dei servizi di contenuti "online",* in Aida, 2016, p. 230.

PELINO, *I diritti dell'interessato, in Il nuovo regolamento europeo: commentario alla nuova disciplina sulla protezione dei dati personali* a cura di BOLOGNINI, PELINO e BISTOLFI, Milano, 2016, p. 249.

PELLECCHIA E., *Tutela della privacy (l. 31 dicembre 1996, n. 675)*, in *Nuove leggi civ. comm.*, 1999, 2-3, 459-478.

PELLEGRINO S., *Le disposizioni attuative in materia di credito al consumo*, in *Obbl. contr*., 2011, p. 298.

PENNISI, *Considerazioni in merito alle pratiche commerciali ingannevoli*, in questa Rivista, 2012, I, 653 ss.

PERLINGERI C., *Profili civilistici dei* social networks, Napoli, 2014, 88.

PERLINGERI P., *La personalità umana nell'ordinamento giuridico*, Napoli, 1972.

PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. dir. civ*., 1990.

PERUGINI S., *La modernizzazione del diritto dei consumi tra public e private enforcement: nuove prospettive di riforma*, in A.A. Vv, *Consumerism 2019. Dodicesimo rapporto annuale. Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?* Consumer's Forum e Università degli studi Roma Tre, 2020, 15 ss., disponibile in *https://consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf*

PINTO, *Mobile Number Portabilità (MNP): tempi di attivazione, perdita del credito residuo e costo del servizio*, in *Il nuovo diritto*, 2007, 5-7, pt. 4, p. 412 ss.

PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ*., 2017, p. 399.

PITRUZZELLA G., *Big Data and antitrust enforcement ("Big Data" e attuazione della disciplina*

"antitrust"), in *Rivista Italiana di Antitrust / Italian Antitrust Review*, 2017, fasc. 1, pp. 10

PITRUZZELLA G., *Big Data and Antitrust Enforcement*, in *Rivista Italiana di Antitrust*, n.1/2017, p. 77-86.

PITRUZZELLA G., *Big data, competition and privacy: a look from the antitrust perspective ("Big Data", concorrenza e riservatezza: uno sguardo dalla prospettiva "antitrust")* in *Concorrenza e mercato*, 2016, pt. 1, pp. 15-27.

PITRUZZELLA, *L'applicazione delle regole di concorrenza nel mercato globale: istanze di tutela, sfide ed opportunità*, in Benacchio-Carpagnano (a cura di), *L'applicazione delle regole di concorrenza in Italia e nell'Unione Europea*, Napoli, 2015, 1 ss.

PIZZETTI F., *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in *Id., Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 37 ss.

PIZZETTI, *Il caso del diritto all'oblio*, Torino, 2013.

POLLICINO O., *Covid19/ Perché si possono restringere le libertà fondamentali*, in https://www.viasarfatti25.unibocconi.it/notizia.php?idArt=21654, 26 marzo 2020 (ultima visita: 5 aprile 2020).

PONZANELLI G., *La povertà dei «sosia» e la ricchezza delle «celebrità»: il «right of publicity» nell'esperienza italiana*, in *Dir. inf.*, 1988, 129 ss.

PONZIANI, *Imprese fintech e techfin: l'impatto dei big data sulla libera concorrenza*, in *I diversi settori del fintech. Problemi e prospettive*, a cura di CORAPI, LENER R., Milano 2019, 33 ss.

PORTA F., *Obiettivi e strumenti della PSD2*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, MAIMERI F, MANCINI M (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019.

POSNER R., *The right of Privacy*, in *Georgia Law Rev*., 1978

PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contr. e impr./Europa*, 2015, 1, p. 200.

PROFETA V., *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, MAIMERI F, MANCINI M (a cura di) in *Quaderni di ricerca giuridica della Consulenza Legale*, 5 dicembre 2019.

PROSPERETTI E., *Algoritmi dei Big Data: temi regolamentari, responsabilità, concorrenza, in Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini, G. Olivieri, Milano, 2018.

PROTO M., *Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale*, 2012.

PURTOVA N., *Property rights in personal data: Learning from the American discourse*, in *Computer & Law Sec. Rev.*, 2009, vol. 25, 507 ss.

RABAI B., *I "big data" nell'ecosistema digitale: tra libertà economiche e tutela dei diritti*

fondamentali, in *Amministrare*, 2017, fasc. 3, pp. 405-422.

RESCIGNO P., *Il diritto all'intimità della vita privata*, in *Studi in onore di F.Santoro Passarelli*, IV, Napoli, 1993, p. 119.

RESTA e ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. e proc. civ.*, 2018, p. 411 ss.

RESTA G., *Autonomia privata e diritti della personalità*, Napoli, 2005.

RESTA G., *La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei Diritti)*, in *Riv. dir. civ.*, 2002, 801-848.

RESTA, *I diritti della personalità*, in *Le persone fisiche e i diritti della personalità*, a cura di ALPA e RESTA, in *Trattato di diritto civile*, diretto da SACCO, Milano, 2006, p.361 ss.

RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, p. 299 ss.

REYNA e SCHMON, *Digital Content Directive. Key commendations for the trialogue negotiations*, Bruxelles, 2018.

RICCI, *I diritti dell'interessato, in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da Finocchiaro, Bologna, 2017, p. 220.

RICCI, *La "funzione sociale" del diritto al trattamento dei dati personali*, in *Contr. e impr*., 2017, 2, p. 584 ss.

RICCIUTO V, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019 pp. 95 ss.

RICHARDS N. M., KING J. H., *Three Paradoxes of Big Data*, in *Stanford Law Review Online*, 2013, 66, 41 ss.

RICOLFI M., *IoT and the ages of Antitrust ("IoT" e le età di "Antitrust")* in *Concorrenza e mercato*, 2017, pt. 1, pp. 215-232.

RISPOLI FARINA M., *Informazione e servizi di pagamento*, in *Analisi giuridica dell'economia*, I, 2015, p. 175 e ss.

RISPOLI FARINA M., *La direttiva PSD2: novità e continuità nella disciplina dei servizi di pagamento* in BRUNELLA RUSSO, (a cura di), *I servizi di pagamento nell'epoca della digitalizzazione*, Atti del Convegno in onore di Giuseppe Restuccia, Taormina 15-16 febbraio 2018, Cedam, 2019, p. 30 e ss.

ROBERT BALDWIN, MARTIN CAVE, MARTIN LODGE, *Understanding Regulation* (2012).

RODOTÀ S., *Conclusioni*, in *Trattamento dei dati e tutela della persona*, a cura di CUFFARO, RICCIUTO e ZENO ZENCOVICH, Milano, 1998, p. 308.

RODOTÀ S., *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013.

RODOTÀ S., *Intervista su privacy e libertà*, *Laterza*, 2005.

RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012.

RODOTÀ, *Le fonti di integrazione del contratto*, Milano, 1969.

RODOTÀ, *Tecnologie e diritti*, Bologna, 1995.

RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, 2004.

ROPPO V., *Giustizia contrattuale e libertà economiche: verso una revisione della teoria del contratto?* in *Riv. crit. dir. priv.*, 2007, 602.

ROSS A., *Il nostro futuro*, Milano, 2016.

ROSSI, *Social network e diritto antitrust*, in AIDA, 2011, 84 83.

ROTHMAN J., *The Inalienable Right of Publicity*, in *Georgetown Law J*., 2012, 101, p. 185.

ROTUNNO I., La gestione del flusso trasfrontaliero dei dati dopo la sentenza Schrems II disponibile su https://www.orrick.com/it-IT/Insights/2020/11/La-gestione-gel-flusso-trasfrontaliero-dei-dati-dopo-la-sentenza-Schrems-II, 13 novembre 2020

RUOTOLO G. M., *I dati non personali: l'emersione dei "big data" nel diritto dell'Unione europea (Non-personal Data: The Surfacing of Big Data in European Union Law)*, in *Studi sull'integrazione europea*, 2018, fasc. 1, pp. 97-116

SAMMARCO P., *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0,* in *Dir. inf.*, 2010, 639.

SAMUELSON P., *Privacy as Intellectual Property? Standford Law Review*, Vol 52, No. 5, pp. 1125-1173.

SARACINI, *Nullità e sostituzione di clausole contrattuali*, Milano, 1971.

SARTORI F., *Disciplina dell'impresa e statuto contrattuale: il criterio della «sana e prudente gestione»*, in *Banca borsa tit. cred.*, 2017, I, 152.

SAVORANI, *La notorietà della persona da interesse protetto giuridico a bene giuridico*, Padova, 2000.

SCALZINI S., *L'estrazione di dati e di testo per finalità commerciali dai contenuti degli utenti. Algoritmi, proprietà intellettuale e autonomia negoziale*
in *Analisi Giuridica dell'Economia*, 2019, fasc. 1, pp. 395-423;

SCHENA C., TANDA A., ARLOTTA C. AND POTENZA G., *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale,* in Quaderni Fintech, 2018.

SCHWARTZ, *Property, Privacy, and Personal Data*, in *Harvard Law Rev.*, 2004, 111, p. 2056 ss.

SCOGNAMIGLIO, *Le pratiche commerciali sleali: disciplina dell'atto o dell'attività?*, in C. RABITTI BEDOGNI – P. BARUCCI (a cura di), *20 anni di antitrust. L'evoluzione dell'Autorità garante della concorrenza e del mercato*, Torino, 2010, vol. II.

SIRENA P., *Trattamento per scopi storici, statistici o scientifici, Profili generali e trattamento per scopi storici*, Capo I e II, Titolo VII, a cura di BIANCA C.M., BUSNELLI, *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, CEDAM, Padova, 2007, p.1413-1424.

SOMAINI, *The right to data portability and user control: ambition and limitation*, in *Riv. dir. media*, 2018, p. 8.

SORO A., *L'universo dei dati e la libertà della persona*, in *Il discorso del presidente Antonello Soro*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (a cura di), 7 maggio 2019, p. 17.

STAKHEYEVA-TOKSOY, *Merger control in the Big Data world: To be or not to be Revisited?* in ECLR, 2017, vol. 38, Issue 6, 270.

STANZIONE G., *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1252

STIGLER, *An Introduction to Privacy in Economics and Politics, The Journal of Legal Studies, The Law of Privacy*, 1980, 9, 4, p. 623-644.

SWIRE P.P., *Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall*, 18 October 2007, p.4, available at www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf .

TENE O., POLONETSKY J., *Big Data for All: Privacy and User Control in the Age of Analytic's*, in *Northwestern Journal of Technology and Intellectual Property*, 2013, 11, 5, 239 ss.

TESTA, Sub art. 22 Cod. cons., in L.C. Ubertazzi, *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, 6 a ed., Padova, Cedam, 2016, 2686 ss

THOBANI S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, in *Memorie del Dipartimento di Giurisprudenza dell'Università di Torino*, Ledizioni LediPublishing, Milano, 9/2018.

THOBANI S., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, 2, 540 ss.

TINDALL, *Argus Rules: The Commercialization of Personal Information, J. of L. Tech & Policy*, 2003, 1, p. 183 ss.

TONI A.M., *Il Right of publicity nell'esperienza nordamericana*, in *Contr. impr.*, 1996, 82 ss.

TROTTA, CHRISTINA T., *The Google-Doubleclick Merger, the FTC, and the Future of Transactional Privacy Inquiries in the United States* (December 13, 2007). Available at SSRN: https://ssrn.com/abstract=1071823 or http://dx.doi.org/10.2139/ssrn.1071823.

TURILLI M., FLORIDI L., *The ethics of information transparency*, in *Ethics and Information Technology*, 2009, 11, 2, 105.

UBERTAZZI L.C., *Riservatezza informatica ed industria culturale*, in *I diritti d'autore e connessi. Scritti*, Milano, Giuffré, 2003, 136 ss. spec. 137.

VANINI S., *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218*, in *Le nuove leggi civili e commerciali*, 4, 2018, p. 866 e ss.

VANZETTI A.– DI CATALDO M., *Manuale di diritto industriale*, Giuffrè, Milano, 2012.

VARIAN H., *Economie di rete e Big Data*, Aspen Institute Italia (https://www.aspeninstitute.it/system/files/private_files/2018.../Aspenia80_Varian.pdf).

VELLA F. e BOSI G., *Diritto ed economia di banche e mercati finanziari*, il Mulino, Bologna, 2019, pp. 417 ss.

VESCIO DI MARTIRANO V. Si possono cedere i dati a pagamento da parte degli interessati? 25 luglio 2019, disponibile in https://www.key4biz.it/si-possono-cedere-i-dati-a-pagamento-da-parte-degli-interessati/266715/.

VESCIO DI MARTIRANO V., *Facebook e il valore dei dati. Cosa dice la sentenza del Tar del Lazio*, 2020 in https://www.key4biz.it/facebook-e-il-valore-dei-dati-cosa-dice-la-sentenza-del-tar-del-lazio/285228/.

VESCIO DI MARTIRANO V., *WhatsApp, la nuova privacy policy è fonte di equivoci*, 2021 in https://www.key4biz.it/whatsapp-la-nuova-privacy-policy-e-fonte-di-equivoci/338701/.

VESSIA F., *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, I, p. 1064.

VIRGA W., *Inadempimento di contratto e sanzioni private nei social network*, Aida, 2011, 232.

WALCHEK S., *The unbundling of finance*, *TechCrunch*, 2015.

WATCHER, MITTELSTADT e FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *Int'l Data Privacy Law*, 2017, p. 76ss.

WEBER, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, in *Concorrenza e Mercato*, 2016, 23, 59, p.67 ss.

WERDEN GREGORY J., Economic Evidence on the Existence of Collusion: Reconciling Antitrust Law with Oligopoly Theory, 72, Antitrust Law Journal, 719 (2004).

WILS W.P.J., *The Obligation for the Competition Author- ities of the* EU *Member States to Apply* EU *Antitrust Law and the Facebook Decision of the Bunde- skartellamt*, www.ssrn.com, luglio 2019.

WISH-BAILEY, Competition Law, Oxford, 2012, 539 ss.

ZARSKY T., *Incompatible: the GDPR in the age of big data,* in *Seton Hall Law Review*, 2017, 47, 1014 ss.

ZARSKY T., *Transparent predictions,* in *University of Illinois Law Review*, 2013, 4, 1507 ss.

ZECH H., *Data as a Tradeable Commodity*, in DE FRANCESCHI A. (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution,* Cambridge, 2016, 51 ss.

ZENO ZENCOVICH, *Sull'informazione come "bene" (e sul metodo del dibattito giuridico),* in *Riv. crit. dir. priv*., 1999, 485 ss.

ZENO-ZENCOVICH V., GIANNONE CODIGLIONE G., *Ten legal perspectives on the "big data revolution" (Dieci prospettive giuridiche sulla rivoluzione del "big data")* in Concorrenza e mercato, 2016, pt. 1, pp. 29 - 57.

ZENO-ZENCOVICH V., *Il codice dei dati personali. Temi e problemi*, con Francesco Cardarelli e Salvatore Sica, *collana Diritto dell'informatica*, Giuffrè, 2004.

ZENO-ZENCOVICH, *Internet e concorrenza*, in *Dir. inf*., 2010, 697 ss. spec. 704.

ZIMMERMAN, *Living Without Copyright in a Digital World*, in Albany Law Rev., 2007, 70, p. 1375 ss.

ZOPPINI A., *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati),* in *Riv. dir. civ.*, 2002, p. 851 ss.

ZORZI GALGANO N., *Le due anime del GDPR e la tutela del diritto alla privacy*, in ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 35 ss.