RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0219 • articolo sottoposto a peer review • pubblicato in anteprima l'11 giu. 2025

Veronica Montozzi

Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza

Il valore economico e il conseguente rilievo assunto dai dati nell'ambito del mercato hanno determinato lo sviluppo di una nuova forma di capitalismo che comporta il rischio di realizzare un ordine economico che tende a comprimere i diritti fondamentali, creando nuove forme di disuguaglianza, e che rischia di alterare i meccanismi concorrenziali del mercato, con l'affermarsi del dominio dei c.d. poteri privati digitali. Partendo dall'analisi del fenomeno della monetizzazione dei dati, il contributo mira ad esaminare il recente approccio normativo dell'Unione europea che, nel fornire risposta alle sfide poste dallo sviluppo della *data driven economy*, tenta di delineare un modello di regolazione dei dati e delle nuove tecnologie che tenga in considerazione, da un lato, l'interesse economico relativo allo sviluppo di un mercato digitale europeo; dall'altro, quello di tutelare i diritti e le libertà fondamentali degli individui, adottando, sulla scia del nuovo movimento del costituzionalismo digitale, una serie di provvedimenti tramite i quali reinterpretare e riequilibrare il quadro dei poteri e delle libertà che vengono in rilievo. L'articolo riflette, dunque, sulle criticità derivanti dalla commistione delle diverse discipline che intervengono nelle vicende emergenti nell'ecosistema digitale, *in primis* la tutela della protezione dei dati e quella della concorrenza, analizzando le recenti pronunce giurisprudenziali che hanno tentato di individuare soluzioni per i casi concreti.

Protezione dei dati – Concorrenza – Monetizzazione dei dati – Poteri privati digitali – Costituzionalismo digitale

The new challenges of data regulation: analysis of a model starting from the intersection between personal data protection and competition

The economic value and the consequent importance assumed by data in the context of the market have led to the development of a new form of capitalism that involves the risk of creating an economic order that tends to compress fundamental rights, creating new forms of inequality, and which risks altering the competitive mechanisms of the market, with the affirmation of the domination of the so-called digital private powers. Starting from the analysis of the phenomenon of data monetization, the paper aims to examine the recent regulatory approach of the European Union which, in responding to the challenges posed by the development of the data-driven economy, attempts to outline a model of regulation of data and new technologies that takes into account, on the one hand, the economic interest related to the development of a European digital market; on the other hand, that of protecting the fundamental rights and freedoms of individuals, adopting, in the wake of the new movement of digital constitutionalism, a series of measures through which to reinterpret and rebalance the framework of powers and freedoms that come to the relief. The article reflects, therefore, on the critical issues deriving from the mixture of the different disciplines that intervene in the emerging events in the digital ecosystem, first and foremost the protection of personal data and of competition, analyzing the recent case law that have attempted to identify solutions for concrete cases.

Data protection – Competition – Data monetisation – Digital private powers – Digital constitutionalism

L'Autrice è dottoranda di ricerca in Discipline giuridiche pubblicistiche, curriculum Discipline pubblicistiche, internazionalistiche ed europee presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre

Sommario: 1. Circolazione dei dati, protezione dei dati e concorrenza: la sfida del nuovo costituzionalismo digitale. – 2. Profili problematici della c.d. monetizzazione dei dati personali. – 3. Il caso Facebook tra Italia e Germania. – 4. La decisione della Corte di giustizia: la necessaria cooperazione delle autorità amministrative indipendenti. – 5. Il Consiglio di Stato riafferma il principio leale collaborazione. – 6. Conclusioni.

1. Circolazione dei dati, protezione dei dati e concorrenza: la sfida del nuovo costituzionalismo digitale

La circolazione dei dati è la chiave di volta dell'economia digitale, settore chiave nella competizione economica globale. Già dal titolo del Regolamento UE 2016/679[1], infatti, si evince come, accanto alla tutela della protezione dei dati, una delle principali esigenze dell'Unione europea sia quella di promuovere la libera circolazione di essi in armonia con la tutela della persona, mediante regole che impediscano al fenomeno circolatorio di spingersi oltre il limite della dignità della persona[2], "nell'ottica di favorire un clima di fiducia per lo sviluppo di un'economia digitale nel mercato interno"[3]. Come preannunciato dal professore Thomas W. Malone nel 1987[4], nell'era dell'informazione, del digitale, delle nuove tecnologie, infatti la centralità assunta dai dati personali nella società, sempre più *data driven* e caratterizzata dalla crescente applicazione dell'IoT e dell'Intelligenza Artificiale, insieme alla loro attrazione entro una logica di consumo e di scambio[5], ha determinato il diffondersi, accanto all'economia tradizionale, della c.d. *data driven economy*, ossia un'economia basata sui dati e sulla loro attitudine ad incrementare le opportunità di business. Nei mercati "*data rich*", i dati hanno quindi assunto un rilevante valore economico[6], tanto da esser definiti il nuovo "petrolio"[7],

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
2. In senso critico Gentili 2022, in cui l'A. osserva che "a guardar bene non c'è un vero bilanciamento. C'è piuttosto una prioritaria legittimazione del mercato dei dati, con pochi, fiacchi e platonici limiti a protezione della persona".
3. Calisai 2019, p. 327 ss.
4. Cfr. Malone–Yates–Benjamin 1987, in cui Malone aveva previsto l'avvento dei "mercati elettronici".
5. "La presenza di IA è ormai una realtà acquisita ed in sviluppo esponenziale nel panorama industriale mondiale", Naldi 2018, p. 225-238. In questo scritto l'A. compie un'accurata analisi circa lo stato degli investimenti in IA, soprattutto da parte dei "cinque giganti del web", ossia Google, Apple, Facebook, Microsoft e Amazon.
6. Sul valore commerciale dei dati personali approfondiscono *ex multis*: Cremona–Laviola–Pagnanelli 2022; Battelli 2022, pp. 355-364; Resta 2019, pp. 127-153; Malgieri–Custers 2018; Midiri 2016, pp. 355-373.
7. Così *The world's most valuable resource is no longer oil, but data*, in "The economist", 6 maggio 2017; sul punto anche Colapietro 2021, p. 834: "Come il carbone e la macchina a vapore hanno rappresentato gli elementi essenziali della Prima rivoluzione industriale e il petrolio e il motore a scoppio quelli della Seconda rivoluzione industriale, i dati gli algoritmi e l'Intelligenza artificiale rappresentano i fondamenti di quella che stiamo vivendo noi e che oggi è ancora nella sua fase iniziale".

in quanto sempre più utilizzati nelle strategie imprenditoriali e rappresentando anche la fonte di un rilevante vantaggio competitivo[8]. Tuttavia, in tale contesto, caratterizzato da asimmetrie strutturali e funzionali[9], i dati vengono sfruttati per finalità commerciali, spesso a insaputa dello stesso utente, e l'enorme disponibilità delle informazioni – nonché la concentrazione delle stesse nelle mani di pochi – ha determinato l'erompere di nuovi poteri[10], i "poteri privati digitali"[11], che dettano le regole del gioco, sviluppando poteri sempre più simili ai poteri pubblici[12] e creando monopoli difficili da scardinare.

Questi sviluppi mettono in crisi le tradizionali forme di regolazione giuridica, dell'azione antitrust e della protezione dei dati personali[13], in quella che sembra delinearsi come una nuova forma di capitalismo – definito "capitalismo della sorveglianza"[14] – in cui cambiano, come detto, le regole del gioco e le dinamiche di domanda ed offerta funzionali ad assicurare la democrazia del mercato[15].

È innegabile infatti come nell'industria 4.0, caratterizzata dall'accumulo massivo di grandi quantità di informazioni personali da parte delle imprese, nonché, come vedremo, dalla continua ricerca di strategie per raccogliere dati, quali i *dark patterns*[16] o il c.d. *paywall*, si annidi il rischio di realizzare un ordine economico che tende a comprimere i diritti fondamentali associati all'autonomia individuale, creando nuove forme di disuguaglianza, e di alterare i meccanismi concorrenziali del mercato, rendendo necessario che l'attenzione venga spostata sulle tutele da accordarsi all'utente nell'ottica di rafforzarne la posizione quale soggetto debole nel contesto digitale e riequilibrare le asimmetrie di potere esistenti tra parti diverse del contratto[17].

È nell'ottica di implementare la tutela dei diritti che si pone il movimento del nuovo costituzionalismo digitale[18]: esso si prefigge l'obiettivo di introdurre strumenti che apprestino un'adeguata difesa dei diritti nel rapporto con i nuovi poteri, nella consapevolezza che le dimensioni assunte dal nuovo fenomeno digitale necessitano della massima attenzione da parte delle istituzioni politiche e regolatorie[19]. In questa direzione si sta

8. Cfr. Resta 2019, p. 127; v. anche Solinas 2021, p. 323: "Il rilievo da cui partire è che i dati personali sono ormai considerati una riserva economica a tutti gli effetti".
9. Di asimmetrie "strutturali e funzionali dei rapporti giuridici online" parla Cremona 2021, pp. 681-696; v. anche Simoncini 2019, pp. 63-89.
10. Espressione coniata da Predieri 1997.
11. Si rinvia a Simoncini–Cremona 2021, pp. 244-260.; Cfr. Pollicino 2019; Pollicino 2019-a; Mezzanotte 2018, pp. 507-530.
12. Klonick 2018; sul punto si v. anche Cremona 2021, p. 686, il quale spiega che "I nuovi sovrani […] i padroni degli algoritmi più intelligenti del mondo pervadono i mercati e avocano a sé sempre maggiori funzioni, anche tradizionalmente proprie dei pubblici poteri".
13. Midiri 2020.
14. Zuboff 2019.
15. Così osserva Sartoretti 2019.
16. Con tale termine si fa riferimento a tecniche che utilizzano la psicologia per convincere gli utenti a cedere i propri dati o a prestare il consenso al trattamento. Sul punto v. Mursia–Trovato 2021, pp.165-189.
17. Sul punto v. Iannuzzi 2024, p. 111, il quale evidenzia che "In un sistema senza intermediari il singolo si è mostrato spesso in balìa dei giganti della rete, per via dello sbilanciamento delle posizioni e della notevole asimmetria informativa"; v. anche Caggia 2019, p. 260.
18. Sul punto Cheli 2021, p. 955, prende atto che la rivoluzione industriale, messa in atto dalla digitalizzazione – più precisamente per effetto diretto "delle trasformazioni che la scienza e la tecnica hanno determinato e stanno determinando nella sfera fisica, psichica e relazionale della persona umana" – apre la strada ad una "nuova stagione del costituzionalismo" che denomina stagione del "costituzionalismo digitale". Secondo l'A. "questa nuova forma di costituzionalismo mira ad ampliare, a completare e a rafforzare gli strumenti del costituzionalismo tradizionale".
19. Cremona 2021, p. 689.

muovendo il legislatore europeo che, nel tentativo di attuare una più efficace ed efficiente definizione delle regole dei meccanismi propri di questa nuova forma di capitalismo[20], ha ritenuto opportuno recuperare la centralità delle fonti[21], optando per strumenti di *hard law*, sostanziatisi nei regolamenti recentemente approvati, quali il Digital Markets Act (DMA), il Digital Services Act (DSA), il Data Act (DA) e il Data Governance Act (DGA), insieme al Regolamento sull'IA. Tali provvedimenti si inseriscono nel più ampio progetto normativo dell'Unione europea di divenire il leader all'interno del mercato mondiale dei dati e delle tecnologie digitali, per il raggiungimento del quale un ruolo fondamentale è svolto dalla libera circolazione dei dati[22]. Pertanto, i nuovi Regolamenti mirano a definire, nel loro insieme e in combinato disposto col GDPR, un nuovo modello europeo di regolazione dei dati, tramite il quale il legislatore europeo, tenuta a mente la pluralità di interessi coinvolti, tenta di trovare un nuovo punto di equilibrio tra la tutela dei valori della persona e le esigenze di mercato, incentivando da un lato la circolazione dei dati, al fine di stimolare un mercato unico europeo, che prenda atto del valore economico dei dati, e dall'altro, aumentando il controllo pubblico sulle dinamiche emergenti nell'ecosistema digitale, in modo da realizzare una correzione del mercato in senso conforme non solo ai diritti fondamentali dell'individuo[23], ma anche alle esigenze degli imprenditori e delle PMI[24].

In tale quadro, volto a incardinare in schemi regolatori una realtà in costante e profondo mutamento, assumono un ruolo significativo le autorità amministrative indipendenti[25], le quali, in vista dei poteri di vigilanza e sanzionatori di cui sono investiti, sono chiamate a ricoprire un ruolo di crescente protagonismo nella difesa delle libertà e dei diritti di tutti gli attori coinvolti sia a livello europeo che nazionale[26]. Per tale motivo, i nuovi provvedimenti, prevedono infatti l'implementazione e l'integrazione del lavoro delle *authorities*, soprattutto nell'ambito delle dinamiche concorrenziali nei mercati digitali. Tuttavia, le novità introdotte dai nuovi regolamenti europei e il nuovo ruolo assunto dai dati presentano il rischio di sovrapposizioni delle funzioni attribuite a ciascuna autorità e alimentano, di fatto, la difficoltà di comprendere chi sia competente a risolvere le questioni emergenti nell'ecosistema digitale, rappresentando un serio problema specie per le imprese, che si ritrovano gravate di una serie di obblighi giuridici provenienti da fonti diverse, il cui inadempimento può attivare l'azione di autorità diverse, con conseguenze sanzionatorie di diverso genere.

20. Sartoretti 2019, p. 5.
21. V. anche Iannuzzi 2021, pp. 31-51, il quale individua quale nuova funzione del costituzionalismo, quella di "operare anche nella direzione di limite all'abnorme potere di soggetti privati che esercitano ormai sul web poteri paracostituzionali".
22. Parlamento europeo, *Risoluzione del Parlamento europeo su una strategia europea per i dati (2020/2217(INI))*, 25 marzo 2021.
23. *Ivi*, p.to 9, il Parlamento europeo "ritiene che l'Unione debba adoperarsi per una governance dei dati a livello dell'UE e per una società e un'economia dei dati antropocentriche, basate sui valori dell'Unione del rispetto della vita privata, della trasparenza e del rispetto dei diritti e delle libertà fondamentali, in cui i cittadini siano in grado di prendere decisioni informate in merito ai dati che generano o che li riguardano".
24. Cfr. Iannuzzi 2024, p. 108, il quale evidenzia che le piccole e medie imprese (PMI) "rappresentano la specificità europea nel mercato delle tecnologie e dell'informazione delle telecomunicazioni (ICT), e non solo, e che rischiano di rimanere schiacciate nella contesta globale, dal potere dei giganti della tecnologia (big tech)".
25. Sull'importanza dell'azione delle autorità amministrative indipendenti Cheli 2021, p. 956, scrive: "è certo che un ruolo rilevante potrà essere svolto da queste autorità, in ragione della loro nascita e della loro ragione di essere come soggetti 'bifronte' ancorati sia allo spazio nazionale che a quello europeo. […] Le autorità amministrative indipendenti […] sono anche soggetti che esercitano un potere qualitativamente diverso dai poteri tradizionali dello Stato, potere dove si combinano le tradizionali funzioni dello Stato al fine di offrire uno strumento rapido, flessibile e tecnicamente attrezzato per la difesa dei diritti nel rapporto con i nuovi poteri".
26. Cfr. Simoncini 2021, pp. 723-732; sul punto v. anche Calzolaio 2024, pp. 84-106.

Nei paragrafi che seguono, si cercherà di mostrare il dispiegarsi nella pratica di tale fenomeno, partendo da un approfondimento sul tema della c.d. monetizzazione dei dati personali, e le conseguenti criticità, e analizzando le vicende giurisprudenziali che ne sono derivate e che hanno dato piena dimostrazione degli effetti di questo intreccio di normative e di competenze delle autorità indipendenti.

2. Profili problematici della c.d. monetizzazione dei dati personali

Dall'analisi delle abitudini del mercato, si evince la circostanza che la raccolta di dati personali "è sempre più il motivo che anima l'impresa"[27]. La ragione per cui i dati personali hanno attirato l'attenzione delle imprese, venendo collocati alla base del loro modello di business, riguarda il fatto che i dati possono essere "trattati, analizzati, arricchiti e quindi riutilizzati al fine di trarne informazioni suscettibili di rilievo economico"[28], rendendo evidente come, tramite il loro trattamento, i dati vengano "patrimonializzati", traendone direttamente utilità economica o estraendone informazioni in seguito scambiabili sui mercati digitali[29].

Tra i vari *business models* sviluppatisi nella prassi del mercato[30], la fattispecie più comune nelle imprese, specie quelle che dispongono di *digital platforms*, è il modello c.d. *zero-price*[31]. Tale modello si basa sulla fornitura di servizi o contenuti digitali all'utente, che viene effettuata senza che quest'ultimo debba eseguire una controprestazione di natura pecuniaria. In cambio della fruizione di servizi/contenuti offerti, però, l'utente deve prestare il proprio consenso al trattamento dei propri dati personali per finalità che spaziano dalla necessità di eseguire la prestazione richiesta fino al soddisfacimento di interessi commerciali[32]. Così come configurata, in tale operazione i dati personali si pongono come corrispettivo per la fornitura di contenuti o servizi digitali[33]. Ciò ha condotto parte della dottrina a considerare la fornitura di dati personali alla stregua di una controprestazione, da cui si ricava l'equiparazione dei dati

27. Il tema è stato oggetto di un esame congiunto svolto dall'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali, nell'*Indagine conoscitiva sui big data*, 10 febbraio 2020.
28. D'Ippolito 2022, p. 58. Sul punto si veda anche Stazi–Corrado 2019, p. 471, dove si afferma che "la medesima dottrina ha rilevato come nell'ecosistema dell'economia digitale i dati personali siano tipicamente utilizzati proprio per finalità ulteriori, come la profilazione e la pubblicità mirata, costituendo in tal senso il 'corrispettivo' per l'accesso al servizio".
29. Zeno-Zencovich 2019, pp. 22-38. Sul punto la stessa AgCom, *Osservatorio sulle piattaforme online*, 27 dicembre 2019, p. 23, osserva che: "La disponibilità di grandi masse di dati individuali consente alle piattaforme di compiere un'accurata profilazione degli utenti, dalla quale dipende la possibilità per gli inserzionisti che si servono delle piattaforme di raggiungere target specifici di consumatori". Dall'analisi svolta dall'AgCom si ricava che per Facebook la pubblicità online, ottenuta mediante il trattamento dei dati forniti dagli utenti e la successiva vendita, genera il 99% dei ricavi, mentre per Google la raccolta pubblicitaria rappresenta ben l'85% degli introiti complessivi.
30. Ci si riferisce ai tre principali modelli di *business* incentrati sul trattamento dei dati, ossia: *zero-price, personal data economy, pay for privacy*. Per un approfondimento sul punto v. Elvy 2017, pp. 1369-1454. Si v. anche Ricciuto 2020, in cui l'A. evidenzia come lo schema dei modelli negoziali dei dati sia infatti aperto a diverse formulazioni.
31. Si tratta del modello di business che viene applicato principalmente da imprese quali Facebook, Google, Twitter come evidenziato da Competition and Markets Authority (CMA), *The commercial use of consumer data - Report on the CMA's call for information*, giugno 2015.
32. In senso critico si v. Strandburg 2013, pp. 96–99. L'A. ammonisce, infatti, l'utilizzo dell'etichetta *zero-price model* – definito anche *data-as-payment model* – dal momento che "Internet users do not know the 'prices' they are paying for products and services […] because they cannot reasonably estimate the marginal disutility that particular instances of data collection impose on them".
33. Ricciuto–Solinas 2021.

personali alla moneta e la massima che afferma che "se il servizio è gratuito vuol dire che la merce è l'utente", ossia la c.d. *Internet cost trap*[34].

Occorre, dunque, procedere ad un mutamento di prospettiva che giunga a valorizzare, nel necessario bilanciamento con i diritti fondamentali della persona, anche i profili di carattere patrimoniale del trattamento, propri dell'economia dei dati profilati[35], nella quale l'informazione relativa alla persona diventa essa stessa oggetto di scambio.

A lungo, infatti, il trattamento dei dati, quali elementi costitutivi della personalità dell'individuo, è stato associato ad un diritto alla privacy riconosciuto in un contesto più attento al riconoscimento dei diritti della persona che alla definizione di regole volte a disciplinare il nascente mercato dei dati – c.d. *Data Market* – all'interno del quale, invece, i dati si presentano quale principale risorsa economica di una società, come quella attuale, fondata sulle informazioni[36].

In ragione della stretta inerenza che vi è tra l'informazione e la persona, in grado di delinearne l'identità personale e influenzarne le condizioni di vita[37], la disciplina in materia di tutela dei dati personali è però sempre stata ancorata alla tutela della persona, ricomprendendo l'intervento normativo europeo nell'alveo della disciplina dei diritti fondamentali della persona[38]. Qualificando il diritto alla protezione dei dati personali come diritto fondamentale, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea, esso non potrebbe costituire oggetto di atti di disposizione e per questo non sarebbe immaginabile un'attività contrattuale avente a oggetto lo stesso[39]. Accanto alla indisponibilità, la situazione giuridica soggettiva coinvolta si caratterizza anche per la necessarietà, l'irrinunciabilità, l'intrasmissibilità e l'imprescrittibilità[40], attribuendo al titolare la possibilità di pretendere che i dati siano trattati da terzi solo nel rispetto delle regole stabilite dalla legge.

Tuttavia, la realtà fattuale si presenta in contrasto con la ricostruzione appena prospettata della situazione giuridica. È evidente, infatti, che la digitalizzazione ha invece dato vita ad un'economia digitale, nell'ambito della quale le imprese possono sfruttare l'enorme quantità di informazioni ricavabili dai dati per promuovere nuovi prodotti e servizi, dando vita alla c.d. *Data Driven Innovation*[41].

Il carattere pervasivo delle logiche del mercato ha messo, quindi, in dubbio l'utilizzabilità dei diritti della personalità mediante l'attribuzione di poteri di disposizione sugli stessi. È stato notato, infatti, che "la commercializzazione dei dati personali si distingue solo in parte dalla commercializzazione di altri diritti della personalità come, ad esempio, il diritto all'immagine"[42]. È ormai da

34. Ci si riferisce alla "trappola del dono", di cui discorre De Franceschi 2019, p. 1386.
35. Nicita 2019, p. 1164, il quale descrive il dato profilato come "un caso particolare di informazione che viene appropriata dalla piattaforma che lo profila, spesso attraverso scambi impliciti".
36. Battelli 2022; Ricciuto 2020, p. 642, per il quale, pur avendo la Dir. 95/46/CE creato le condizioni per la circolazione del dato personale al pari di altri beni e servizi nel contesto economico e sociale europeo, resta sullo sfondo la questione della regolazione della circolazione dei dati, quale elemento alla base dell'economia e della realtà sociale contemporanea.
37. D'Ippolito 2022.
38. Ricciuto 2020.
39. "Al pari degli altri attributi della persona […], non veniva concepita nessuna possibilità di vendita o redditività del dato personale" (Ricciuto 2018, p. 698).
40. Sulla categoria si rinvia a De Cupis 1982, p. 283.
41. Il concetto fa riferimento, in sostanza, alla capacità delle imprese e degli organismi pubblici di acquisire le informazioni derivanti dal trattamento dei dati e piegarle ai propri scopi, come prendere decisioni consapevoli o sviluppare servizi e prodotti migliori. L'OCSE, infatti, fornisce la definizione di *Data Driven Innovation* come la tendenza per cui "techniques and technologies for processing and analysing large volumes of data, which are commonly known as 'big data', are becoming an important resource that can lead to new knowledge, drive value creation, and foster new products, processes, and markets". (*Data-driven Innovation for Growth and Well-being: Interim Synthesis Report*, ottobre 2014, p. 4.).
42. De Franceschi 2019, p. 1381.

tempo, infatti, che nel panorama giuridico si sono fatte spazio fattispecie contrattuali aventi ad oggetto "beni personali", le quali sono state oggetto di un processo di tipizzazione sociale che è stato poi attratto nell'alveo degli interessi meritevoli di tutela per l'ordinamento giuridico *ex* art. 1322 c.c.[43] È da notare che la componente patrimoniale emerge anche in operazioni in cui si riscontra la gratuità per la mancanza di una controprestazione pecuniaria, ma che in realtà realizzano un vantaggio economico anche a fronte della cessione di un proprio bene personale.

Tale processo di mercificazione ha interessato – si ribadisce – pure i dati personali, imponendo al legislatore comunitario una "scelta precisa", consistente nel mantenere l'originaria impostazione delle normative nazionali e degli accordi internazionali, o di sostituirla con una disciplina che sancisca apertamente la mercificazione dei dati e regoli la circolazione di tale bene[44].

La questione del valore di scambio dei dati contro prodotti e servizi, in assenza di una disciplina specifica che si occupa della circolazione dei dati su "base contrattuale", ha reso necessaria una riflessione da cui sono scaturiti due principali orientamenti.

Un primo indirizzo nega la natura di bene economico ai dati personali, e pertanto, ravvisa, in ogni ipotesi di trattamento dei dati, la presenza di una responsabilità da fatto illecito resa inoperante dalla prestazione del consenso dell'avente diritto ovvero di un atto unilaterale di tipo autorizzatorio. Tale argomentazione si basa sull'impostazione volta a privilegiare il carattere non patrimoniale e indisponibile dei diritti della personalità, i quali, non essendo per definizione trasferibili a terzi, restano connessi al soggetto che ne è titolare. Il vantaggio di tale impostazione consiste nella salvaguardia delle prerogative riconosciute in capo al soggetto consenziente, lasciando così inalterato il principio di indisponibilità dei diritti della personalità[45].

Una diversa lettura del fenomeno ha condotto la dottrina a sostenere la necessità di "reinventare il capitalismo"[46], orientandosi ad affermare il valore commerciale assunto dagli attributi della personalità, in particolare dai dati personali, tale da renderli assimilabili ai beni in senso giuridico e quindi autonomamente suscettibili di essere oggetto di disposizione mediante strumento contrattuale[47]. Questa lettura è coerente con il valore economico assunto dai dati e trova riscontro non solo nelle strategie imprenditoriali, ma anche nelle considerazioni effettuate sul punto da parte del legislatore comunitario[48]. Tuttavia, è stato osservato come la circostanza che le informazioni abbiano assunto una valenza economica, non sia di per sé un "presupposto condizionante rispetto alle

43. Cfr. art. 1322, co 2 c.c.: "Le parti possono anche concludere contratti che non appartengono ai tipi aventi una disciplina particolare, purché siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico". Un esempio in questo senso è rappresentato dal contratto di sponsorizzazione sportiva, con il quale viene concesso l'utilizzo della propria immagine, verso il pagamento di un prezzo o altra prestazione non pecuniaria.

44. Simitis 1997, p. 575.

45. In favore dell'indisponibilità del diritto alla protezione dei dati personali si evidenzia la posizione del Garante europeo per la protezione dei dati personali, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts or the supply of digital content*, 14 marzo 2017, il quale afferma che i dati non possono essere considerati alla stregua di una merce. Sullo stesso punto, in dottrina, Mirabelli 1993, pp. 313-330, secondo cui il consenso va inquadrato nella generale categoria di consenso dell'avente diritto che elimina l'antigiuridicità del comportamento. In senso contrario alla ricostruzione del consenso come "scriminante" si esprime Sica 2001, p. 630: "La categoria del consenso legittimante, sotto forma dell'ipotesi codificata dall'art. 50 c.p., non è, pertanto, calzante del tutto, probabilmente perché è carente, nel caso che ci occupa, il *prius* della 'titolarità del diritto', nel senso conseguente della libera, totale disponibilità del bene 'riservatezza'".

46. Mayer-Schönberger–Ramge, 2018.

47. Così Resta–Zeno-Zencovich 2018, pp. 411-440; Stazi–Corrado 2019; Resta 2019; Resta 2010, p. 38.

48. Cfr. Proposta di direttiva del Parlamento europeo e del Consiglio, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, Bruxelles, 9 dicembre 2015, COM(2015) 634.

scelte di valorazione giuridica dei beni"[49]. A ciò si aggiunga la considerazione che i dati sono delle entità immateriali, e in quanto tali risulta pertanto difficile applicare ad essi il modello proprietario tradizionale, che si incentra sul bene quale cosa materiale, che può costituire oggetto di diritti e che circola mediante contratto[50].

In realtà, occorre notare che il Regolamento UE 2016/679 prende atto, quanto meno in parte, del processo di *commodification* che ha interessato i dati personali, ed infatti – come osservato nel precedente paragrafo – la principale esigenza cui è indirizzata la disciplina in esso contenuta riguarda la libera circolazione dei dati, rendendosi evidente, infatti, come lo stesso concetto di circolazione dei dati personali rimandi all'idea di negoziabilità degli stessi[51].

In continuità con il GDPR, il legislatore europeo ha successivamente emanato, il 20 maggio del 2019, la Direttiva 2019/770/UE relativa a determinati aspetti dei contrati di fornitura di contenuto digitale e di servizi digitali. Essa si caratterizza per un approccio "giusrealistico"[52], che non ignora l'evoluzione dei rapporti di mercato e il valore assunto dai dati nell'economia dell'informazione, riconoscendo espressamente, per la prima volta, il processo di patrimonializzazione dei dati personali, attraverso la tipizzazione della fattispecie negoziale contenuti/servizi digitali verso dati personali, largamente diffusa nelle pratiche dell'ambiente digitale[53]. Tale fattispecie consiste nella fornitura onerosa di contenuti o servizi digitali[54] a fronte o del pagamento di un prezzo o della fornitura da parte di un soggetto dei propri dati, i quali, alla stregua del prezzo, integrano una controprestazione che si pone in rapporto di corrispettività con quella ricevuta.

La direttiva in questione muove dalla constatazione che nei c.d. *multi-sided markets*[55] la logica della gratuità nasconde una razionalità economica, nel senso che molti servizi, apparentemente gratuiti, in realtà vengono adeguatamente remunerati attraverso il flusso di dati personali che perviene a seguito dell'attivazione del servizio[56]. Tutto ciò è stato ulteriormente ribadito nella dir. 2019/2161/UE 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.

Accogliendo una lettura c.d. *market oriented* del fenomeno, infatti, si è resa necessaria la previsione di una disciplina non divergente da quella

49. Resta 2019, il quale sottolinea che la scelta di stabilire se un'entità "sia un bene tecnicamente appropriabile e poi, secondariamente, se sia suscettibile di costituire oggetto di contratti" spetta in modo esclusivo all'ordinamento giuridico.
50. Stazi–Corrado 2019, p. 458.
51. Basunti 2020, p. 860 ss.
52. Resta 2019, p. 140.
53. Senigaglia 2020, p. 760 ss.
54. Cfr. considerando 19 della dir. 2019/770/UE, il quale ricomprende in tale categoria "programmi informatici, applicazioni, file video, file audio, file musicali, giochi digitali, libri elettronici o altre pubblicazioni elettroniche, nonché i servizi digitali che consentono la creazione, la trasformazione o l'archiviazione dei dati in formato digitale, nonché l'accesso a questi ultimi, fra cui i software come servizio quali la condivisione audio e video e altri tipi di *file hosting*, la videoscrittura o i giochi offerti nell'ambiente di *cloud computing* e nei media sociali".
55. I *multi-sided markets* si caratterizzano per il fatto di porre distinti gruppi di utenti in una situazione di interdipendenza reciproca. L'obiettivo della piattaforma che opera su due o più versanti è quello di attrarre più utenti su un versante, in modo tale che gli utenti sugli altri versanti si facciano carico dei costi necessari per interfacciarsi con il primo gruppo di utenti. Sul punto v. Commissione europea, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, 25 maggio 2016, COM (2016) 288.
56. Resta–Zeno-Zencovich 2018. Sul punto anche De Franceschi 2019, p. 1393. L'A. ritiene necessario un'evoluzione del concetto di "pagamento", al fine di ricomprendervi anche "l'esecuzione di una prestazione a carattere oneroso sotto forma del trasferimento e dell'autorizzazione al trattamento dei dati personali".

ordinaria, per quanto riguarda la tutela dei consumatori[57]. L'art. 3, par. 1 della Dir. 2019/770/UE, infatti, stabilisce l'applicabilità della direttiva sia ai contratti con cui un operatore economico fornisce, o si impegna a fornire, un bene o un servizio digitale dietro corrispettivo di un prezzo, sia ai contratti in cui "l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico"[58].

Il Garante europeo della protezione dei dati personali nel parere n. 4/2017 ha, però, puntualizzato che i diritti della personalità – nei quali rientra il diritto alla protezione dei dati personali – "non possono essere ridotti a semplici interessi dei consumatori", e che dunque i dati personali "non possono essere considerati una mera merce"[59]. Quest'indicazione è stata accolta dal legislatore europeo, il quale ha eliminato la parola "corrispettivo" dal testo finale della direttiva[60].

Da tali valutazioni è possibile cogliere il conflitto tra i due antitetici modelli di lettura del diritto alla protezione dei dati personali: da un lato, il modello improntato alla visione patrimonialistica, quale quello contenuto nella direttiva del 2019; dall'altro il modello costruito in chiave personalistica, delineato dal Garante, che rifiuta qualsiasi ricostruzione che possa concepire la fornitura di dati personali quale corrispettivo di prestazioni contrattuali. La presa di posizione del Garante si giustifica in ragione della specificità dei diritti della personalità, i quali nel momento in cui assumono valore economico devono essere necessariamente collocati su un piano diverso dagli altri beni, data la loro inerenza all'identità della persona[61]. Dal momento, quindi, che ogni forma di esplicazione della personalità individuale trova il limite della dignità umana, si rende necessario che il regime giuridico della circolazione dei beni personali, in particolare delle informazioni personali, tenga conto di tale assunto.

Non essendo, però, rintracciabile nella disciplina eurounitaria alcun divieto al fenomeno della commercializzazione dei dati personali – anzi, tale possibilità è ammessa e codificata[62] – occorre constatare, a discapito di quanto affermato dal Garante, che sia possibile concludere un contratto di fornitura di un servizio o contenuto digitale fornendo i propri dati personali a titolo di "controprestazione"[63], tenendo, però, presente che al fine di stabilire la legittimità del trattamento dei dati personali – forniti a titolo di "prezzo" – si deve trovare una difficile conciliazione tra quanto la normativa contenuta nella Dir. 2019/770/UE consente di disporre dei propri dati, e quanto il Reg. UE 2016/679 restringe e tutela tale possibilità[64].

57. Ricciuto 2020, p. 660.

58. D'altra parte, la Direttiva 2019/2161/UE, al considerando 31, evidenzia che "I contenuti e i servizi digitali sono spesso forniti online nell'ambito di contratti che non prevedono, da parte del consumatore, il pagamento di un prezzo, bensì la comunicazione di dati al professionista", e, assimilando tale fattispecie alla tradizionale ipotesi dello scambio tramite "moneta", auspica che sia assoggettata alle stesse norme.

59. EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts or the supply of digital content*, cit., nel quale il Garante "mette in guardia contro nuove disposizioni che introducono il concetto che le persone possono pagare con i propri dati, nello stesso modo in cui pagano in denaro".

60. La versione originaria della Proposta di direttiva presentata dalla Commissione conteneva una diversa formulazione dell'art. 3, par. 1, il quale qualificava espressamente la fornitura di dati personali come "controprestazione non pecuniaria" effettuata in cambio della fornitura di servizi o contenuti digitali. Inoltre, nel considerando 13 dava atto che "Nell'economia digitale, gli operatori del mercato tendono spesso e sempre più a considerare le informazioni sulle persone fisiche beni di valore comparabile al denaro. I contenuti digitali sono spesso forniti non a fronte di un corrispettivo in denaro ma di una controprestazione non pecuniaria, vale a dire consentendo l'accesso a dati personali o altri dati".

61. Senigaglia 2020.

62. Il riferimento qui è alla Direttiva 2019/770/UE.

63. D'Ippolito 2022, p. 55.

64. Battelli 2022, p. 5.

È discusso in dottrina se tali modelli negoziali possano effettivamente rappresentare un vantaggio per gli individui[65]. Questo dubbio è occasionato dal fatto che spesso gli utenti non sono a conoscenza né del reale valore dei loro dati né dello scambio che stanno ponendo in essere, soprattutto per quanto attiene alla fornitura "gratuita" di prodotti/servizi digitali.

Il nodo cruciale dello scambio diviene, dunque, il consenso dell'interessato, quale atto giuridicamente complesso, tramite il quale l'interessato esercita il proprio diritto all'autodeterminazione informativa[66]. Esso svolge una funzione conformativa dell'oggetto del contratto di fornitura di servizi e contenuti digitali contro dati personali, il quale consiste nel regolamento del rapporto interessato-titolare del trattamento, all'interno del quale il titolare acquisisce poteri di uso, godimento ed eventualmente ulteriore cessione dei dati dell'interessato. È, infatti, attraverso il consenso che l'interessato può delimitare le finalità, per il cui perseguimento viene concesso l'utilizzo delle informazioni personali.

Una recente novità, elaborata dalle imprese al fine di bilanciare la necessità di raccogliere e trattare i dati degli utenti e il rispetto dei diritti degli stessi, riguarda la tendenza alla remunerazione del consenso al trattamento dei dati personali, assunto come parte di uno scambio tra dati e servizi. Si tratta del fenomeno del c.d. "*cookie-or-pay wall*", o semplicemente "*paywall*", discusso dal Presidente dell'Autorità Garante per la protezione dei dati personali nella Relazione annuale sull'attività del 2022. Il *paywall* consiste in una modalità tramite cui l'utente è messo in condizione di accedere a determinati contenuti web, potendo scegliere tra le alternative del rilascio del consenso ai *cookie* o del pagamento di un prezzo. Si tratta quindi di un vero e proprio modello, definito "*consent or pay model*", che consentirebbe alle imprese di trattare dati, principalmente per finalità di marketing, rimettendo la scelta al singolo utente.

Utilizzato, per la prima volta, da alcune testate giornalistiche, il *cookie wall* è recentemente apparso nei servizi forniti dalla società Meta, all'interno dei quali veniva proposto agli utenti la possibilità di sottoscrivere un abbonamento per l'accesso ai servizi – in particolare Facebook ed Instagram – in alternativa al modello pubblicitario basato, invece, sul trattamento dei dati personali[67].

Il tema del *cookie wall* è stato oggetto di numerose osservazioni da parte delle Autorità garanti europee, le quali hanno assunto posizioni diverse dal 2019, adottando linee guida dal diverso tenore[68], tra cui rientrano anche quelle dettate dal Garante italiano per la protezione dei dati. Quest'ultimo, nelle linee guida aggiornate nel giugno 2021, ha affermato che non è escluso che lo scrolling o il *cookie wall* possano rappresentare delle procedure di acquisizione del consenso lecite, se queste consistono in una delle componenti di un più articolato processo, che consente al soggetto interessato di manifestare in modo inequivoco e consapevole il proprio consenso. In conformità con il principio dell'*accountability*, infatti, il titolare del trattamento può autonomamente individuare soluzioni adeguate e conformi alla disciplina sul trattamento dei dati al fine di ottenere il consenso al trattamento. Con particolare riguardo all'acquisizione del consenso online, tale condizione può tradursi nella possibilità per i titolari del trattamento di adottare delle modalità alternative ed equivalenti, tali da assicurare, in ogni caso, la non equivocabilità del consenso.

65. Mursia–Trovato 2021.

66. Per un approfondimento si v. Spatuzzi 2021, p. 373.

67. In sostanza, la proposta offrirebbe agli utenti la scelta di continuare ad accedere ai servizi "gratuitamente", con pubblicità personalizzate, o di pagare un costo di circa 9,99 euro al mese – che salirebbe a circa 12,99 euro al mese su dispositivi mobili – per versioni dei servizi senza pubblicità. Sul punto v. Agenda Digitale, *Pagare o farsi tracciare dalle big tech: il bivio che cambierà Internet*, 3 ottobre 2023.

68. In particolare, l'Autorità garante dei Paesi Bassi condanna l'approccio definito "*take it or leave it*" insito nel *cookie wall,* denunciandone l'illiceità. Al contrario, l'ICO (l'Autorità garante per la protezione dei dati britannica), sostenendo la necessità di un contemperamento del diritto alla protezione dei dati personali con altri diritti fondamentali, quali la libertà di iniziativa economica, ritiene che non sempre il *cookie wall* può essere considerato "*intrusive*". Infine, sia l'Autorità garante francese (CNIL) sia quella spagnola (AEPD), condividendo quanto affermato dall'Autorità olandese, esprimono un giudizio negativo sui *cookie wall*.

Tanto premesso, è possibile, inoltre, osservare come né la posizione del Garante né tantomeno le discipline contenute nel GDPR e nella Dir. 2019/770/UE porrebbero effettivi divieti o limitazioni all'utilizzo del *cookie wall*, fermo restando l'adozione di un sistema che consente al titolare del trattamento di rispettare quanto previsto sia con riguardo alle caratteristiche del consenso sia per quanto riguarda la corretta ed esaustiva informazione al consumatore.

Analizzando la tecnica di *wall* utilizzata, l'accesso al sito è subordinato alla scelta alternativa dell'utente di sottoscrivere un abbonamento o di prestare il consenso ai mezzi di tracciamento. In questo modo l'utente è immediatamente informato sulle modalità di visualizzazione e fruibilità del sito ed è posto nella posizione di scegliere, selezionando consapevolmente una delle due modalità alternative proposte. Il consenso può, quindi, dirsi: libero, in quanto l'interessato dispone di una scelta effettiva; informato, per la presenza della *cookie policy*, in cui si spiega l'identità del titolare, le finalità del trattamento, nonché le tipologie di dati trattati; specifico, in quanto è espresso per una determinata finalità. La soluzione dei *cookie wall*, dunque, consentirebbe di rispettare le caratteristiche del consenso richieste dalla normativa sulla protezione dei dati[69].

Tuttavia, sul tema è recentemente intervenuto il Comitato europeo per la protezione dei dati (EDPB) che ha escluso la validità di un consenso prestato per usufruire di un servizio fornito da una grande piattaforma digitale, come nel caso di specie Facebook, in alternativa al pagamento di un prezzo, notando che a fronte di una scelta binaria tra il consenso alla profilazione per finalità pubblicitarie e il pagamento di un abbonamento, il consenso non può dirsi realmente libero[70]. Al fine di garantire che l'utente effettui una scelta reale, infatti, il Comitato specifica che "i titolari dovrebbero prendere in considerazione anche l'offerta di un'ulteriore alternativa gratuita"[71]. In assenza di alternative gratuite che consentano all'utente di accedere allo stesso servizio, questo si troverebbe infatti a dover affrontare una conseguenza finanziaria, dovendo pagare un compenso per poter usufruire del servizio. Inoltre, le modalità con cui viene offerto il servizio e il corrispettivo non dovrebbero essere tali da inibire di fatto gli interessati-consumatori a compiere una scelta libera, spingendolo ad acconsentire. Pertanto, la tariffa non dovrebbe essere inappropriatamente alta e tenendo conto dell'essenzialità del servizio.

Pur tenendo a mente queste condizioni, non può farsi a meno di notare come lo stesso impianto del c.d. *paywall* rischia di arrecare un pregiudizio al più generale principio dell'uguaglianza, con una sostanziale contraddizione in termini. I servizi e contenuti online, e più in generale Internet, hanno avuto una rapida ed ampia diffusione, in quanto consentivano a chiunque di navigare in Internet ed accedere ai contenuti gratuitamente. Gli stessi social network offrivano la possibilità di creare un account senza la previsione di un corrispettivo monetario, permettendo la più ampia fruizione del servizio. Tuttavia, con l'installazione di *wall* da parte delle imprese, che obbligano così l'utente ad effettuare la scelta se fornire il consenso al trattamento dei dati o pagare il prezzo richiesto, vengono a differenziarsi gli utenti sulla base della loro condizione economica. Sebbene l'autorità danese abbia tentato di sopperire a tale questione, fissando il limite del "prezzo ragionevole", coloro i quali non dispongano di risorse sufficienti per pagare un compenso, seppur minimo, al fine di accedere ai servizi o contenuti, senza subire il trattamento dei propri dati, si trovano così costretti a "vendere" la propria privacy. In quest'ottica quindi per questa

69. V. Linee Guida dell'Agenzia danese per la protezione dei dati, *Brug af cookie walls*, 20 febbraio 2023, nelle quali sono indicati quattro criteri che formano la base da cui partire per la valutazione delle pratiche tramite cui un'azienda condiziona l'accesso ai suoi contenuti al consenso dei visitatori.

70. EDPB, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, 17 aprile 2024.

71. "Questa alternativa […] può essere una versione del servizio con una diversa forma di pubblicità che comporta il trattamento di meno (o nessun) dato personale, ad es. pubblicità contestuale o generale o basata su argomenti selezionati dall'interessato da un elenco di argomenti di interesse. Ciò è legato anche al principio di minimizzazione dei dati: i titolari del trattamento dovrebbero garantire che vengano trattati solo i dati personali necessari allo scopo di pubblicare tale pubblicità", *ivi*, p.to 74.

fetta di utenti, il consenso prestato al trattamento dei dati perde il requisito della libertà, non essendo prevista una valida alternativa per accedere al servizio. È inconferente anche l'argomento secondo cui gli utenti resterebbero liberi di non usufruire del servizio, in quanto, come nel caso dei servizi offerti dal gruppo Meta, si tratta di strumenti divenuti ormai imprescindibili per la partecipazione alla vita sociale[72].

3. Il caso Facebook tra Italia e Germania

Una volta resosi evidente che nell'economia digitale, in cui l'utente assume al contempo la qualifica di consumatore, a fronte del valore assunto dai dati, si creano problemi di sovrapposizione tra la disciplina in materia di protezione dei dati personali e quella derivante dalla tutela degli interessi dei consumatori e del mercato concorrenziale, si deve dar nota delle conseguenti ricadute in termini di sovrapponibilità delle competenze delle rispettive Autorità[73]. Il tema viene in luce nell'ambito delle "due saghe"[74] giurisdizionali, svoltesi parallelamente in Italia e in Germania, e scaturite dal confronto tra le Autorità garanti della concorrenza e del mercato nazionali, da un lato, e la società Facebook (nel frattempo divenuta Meta), dall'altro.

Come noto, la vicenda italiana si è conclusa con la sentenza 2631 emanata dalla sez. VI del Consiglio di Stato il 29 marzo 2021, mentre il caso tedesco è poi sfociato in una pronuncia di respiro europeo, vale a dire la sentenza del 4 luglio 2023 della Corte di giustizia dell'Unione europea, con la quale si è presentata l'occasione per abbozzare, a livello europeo, le linee di una cooperazione tra l'Autorità garante per la protezione dei dati personali e l'Autorità garante per la concorrenza e il mercato, seguite poi dal Consiglio di Stato che, in una vicenda successiva, ne ha ripreso, come vedremo, i passaggi salienti, cercando di ricomporre un sistema delle autorità indipendenti, incentrato sul dialogo e sulla cooperazione, con la sentenza n. 497 del 2024.

In breve, con la delibera 27438/2018 l'AGCM aveva irrogato a Facebook una sanzione di dieci milioni di euro per pratiche commerciali scorrette poste in essere a danno degli utenti[75]. Facebook, a sua volta, aveva impugnato queste decisioni, portando il caso prima al TAR Lazio e poi al Consiglio

72. BGH 23 giugno 2020 – KVR 69/19, § 58: "l'uso del forum a fini di reciproco scambio ed espressione di opinioni è di particolare importanza a causa dell'elevato numero di utenti e degli effetti di rete".

73. Moretti 2022, p. 98.

74. Di "saga teutonica" parlano Pardolesi–Van den Bergh–Weber 2020, p. 513. Cfr. anche Van den Bergh–Weber 2020, pp. 29-52. Sul tema v. anche Davola 2021; Midiri 2020.

75. Su segnalazione dell'Associazione Altroconsumo, l'AGCM aveva accertato con delibera n. 27432/2018 la natura illegittima di due pratiche, aventi ad oggetto lo scambio e l'utilizzo a fini commerciali dei dati degli utenti, messe in atto da Facebook. In particolare, la pratica a), consisteva in una "pratica ingannevole" posta in essere in violazione degli artt. 20, 21 e 22 del Codice del consumo, in virtù del fatto che il professionista, al momento della registrazione dell'utente alla piattaforma, non fornisse immediate e adeguate informazioni relative all'attività di raccolta e utilizzo dei dati che gli venivano ceduti, celando l'intento commerciale. Al contrario, l'iscrizione avveniva in presenza di un *claim*, contenuto nella pagina di iscrizione, che affermava: "Iscriviti. È gratis e lo sarà per sempre". In tal modo induceva l'utente ad assumere una decisione di natura commerciale che altrimenti non avrebbe preso, a parere dell'Autorità. La pratica b), invece, integrava l'ipotesi di "pratica aggressiva", in violazione degli artt. 20, 24 e 25 del Codice del consumo, in ragione del fatto che Facebook esercitava un indebito condizionamento nei confronti del consumatore, costringendolo a prestare il consenso a FB e a terzi al trattamento dei dati per finalità informative e/o commerciali, in cambio dell'utilizzo del servizio. Il consenso, secondo l'Autorità, veniva prestato in modo inconsapevole e automatico, attraverso un sistema di preselezione dello stesso, idoneo ad indurre a mantenere attivo il trasferimento e l'uso dei propri dati da e verso terzi operatori, per evitare di subire limitazioni nell'utilizzo del servizio, che conseguirebbero alla deselezione, residuando in capo al soggetto interessato la sola facoltà di *opt-out*. L'AGCM aveva, dunque, proceduto ad irrogare una sanzione dall'importo di dieci milioni di euro – cinque per la "pratica a)" e cinque per la "pratica b)" –, vietando contestualmente l'ulteriore diffusione della pratica ingannevole e disponendo la pubblicazione di una dichiarazione rettificativa sulla homepage del sito internet aziendale per l'Italia, sull'app Facebook e sulla pagina personale di ciascun utente italiano registrato.

di Stato, adducendo il difetto assoluto di attribuzione dell'AGCM, sia perché in realtà non si sarebbe trattato di pratiche commerciali, non essendovi stato il pagamento di un corrispettivo patrimoniale da parte degli utenti, sia perché la questione sarebbe stata, in realtà, da inquadrare nella materia "privacy" e sussunta nelle norme del Regolamento UE 2016/679, non in quello dei diritti dei consumatori[76].

La sez. I del TAR Lazio, tuttavia, pronunciandosi con le sentenze nn. 260/2020 e 261/2020, aveva accolto solo parzialmente il ricorso della società, annullando la sanzione relativa alla pratica b) – in virtù del fatto che non sono stati riscontrati i presupposti per qualificare in termini di aggressività la condotta – ma confermando la sanzione relativa alla pratica a), in quanto condivisibile il giudizio di ingannevolezza rinvenuto nel comportamento dell'azienda. Per quanto attiene il dibattito sulla natura dei dati personali e la conseguente competenza rispetto alla loro tutela, il Tribunale regionale era intervenuto affermando che, contrariamente a quanto sostenuta da Facebook, i dati personali costituissero "un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto"[77], ravvisando la necessità di prevedere accanto agli strumenti di tutela tipici del diritto alla protezione dei dati personali, anche delle garanzie del dato quale oggetto di scambi commerciali, riconoscendo gli obblighi di chiarezza, completezza e non ingannevolezza imposti agli operatori dal legislatore dalla disciplina posta a tutela del consumatore ed escludendo, altresì, la sovrapponibilità del piano della tutela della privacy e di quello della protezione del consumatore[78].

Contro la decisione del TAR Lazio entrambe le parti in causa hanno presentato ricorso al Consiglio di Stato, il quale, dopo aver proceduto alla riunione degli appelli, li ha respinti, confermando la sentenza del TAR[79].

Nella sentenza n. 2631/2021, la sez. VI del Consiglio di Stato si è confrontata con il problema della "non commercialità dei dati personali", da cui deriverebbe la non riconducibilità del loro trattamento al diritto consumeristico. Su questo punto Facebook ha incentrato la propria difesa, in quanto, sposando la tesi della natura di diritto fondamentale della protezione dei dati personali, ha sostenuto che la non patrimonialità di tali dati rende di fatto inapplicabile la disciplina in materia consumeristica alla tutela dei dati personali, cui è rivolta, in via esclusiva, la specifica normazione recata dal Regolamento eurounitario n. 679/2016. Di conseguenza, Facebook ha sostenuto che la competenza a giudicare nel caso di specie dovesse essere attribuita all'Autorità capofila[80], ovvero quella irlandese[81].

76. Nella memoria finale depositata in giudizio, la società Meta ha affermato, infatti, che l'Autorità antitrust agirebbe "sulla base di premesse erronee ed al di là delle proprie competenze nella misura in cui utilizza le norme a tutela del consumatore per analizzare le condotte che dovrebbero essere valutate sulla base della normativa sulla privacy e sul trattamento dei dati personali".

77. TAR Lazio, sez. I, 10 gennaio, 2020 n. 261, § 6.

78. *Ivi,* § 10: "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".

79. Ciò in quanto il Consiglio di Stato ha ritenuto, da una parte, non sussistente alcun elemento di travisamento o manifesta irrazionalità né per quanto attiene ai parametri normativi della scorrettezza delle pratiche commerciali sub a), né con riguardo alla proporzionalità delle sanzioni ingiunte dall'AGCM, e condividendo, dall'altra, le ragioni dei giudici di prime cure relativamente alla "non aggressività" della pratica commerciale sub b) operata da Facebook.

80. L'autorità di controllo capofila è disciplinata dall'art. 56 GDPR e consiste nell'autorità dello stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

81. Pagnanelli 2022, pp. 17-18, osserva che questa chiara opzione di disciplina presentata da Facebook potrebbe nascondere, in realtà, la percezione, per l'azienda, che la disciplina privacy sia "meno severa" rispetto a quella consumeristica.

Diversamente, il Collegio non è parso aderire all'idea del dato persona come *res extra commercium*, ma, pur evitando di assumere una posizione netta – come quella del TAR Lazio – sulla qualificazione giuridica dei dati personali, ha privilegiato una concezione di patrimonializzazione del dato secondo cui tale fenomeno "costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali". Pertanto, il Consiglio di Stato ha scisso il profilo privacy e quello antitrust, intendendo "i due "diritti" quali distinte categorie settoriali che sono disciplinate da normative speciali e quindi non sovrapponibili tra di loro", sottolineando che la pratica ingannevole risiede nello sfruttamento, inconsapevolmente per l'utente, dei dati offerti al momento dell'iscrizione. Proprio per questo, l'utente, che "si trasforma tecnicamente in 'consumatore' nel momento in cui rende disponibili i propri dati al fine di potere utilizzare gratuitamente i servizi offerti dalle società", resta erroneamente convinto che il conseguimento dei vantaggi collegati con l'accesso alla piattaforma sia gratuito. Così, secondo i giudici di Palazzo Spada, ritenere del tutto a sé stante il settore di tutela dei dati personali determinerebbe l'esclusione dell'applicabilità di ogni altra disciplina giuridica, che si tradurrebbe nella riduzione delle tutele garantite alle persone fisiche. I giudici considerano, invece, la disciplina in materia di pratiche commerciali sleali – Direttiva 2005/29 – e quella presente nel Regolamento 2016/679 tra loro complementari, contribuendo insieme a garantire una "tutela multilivello" che, anzi, incrementa "il livello di garanzia dei diritti delle persone fisiche" anche, e soprattutto, "quando un diritto personalissimo sia sfruttato a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore"[82].

4. La decisione della Corte di giustizia: la necessaria cooperazione delle autorità amministrative indipendenti

Come già osservato, nel frattempo, in Germania, si stava sviluppando una vicenda del tutto parallela[83].

Nel 2019, il Bundeskartellamt aveva sanzionato Facebook per abuso di posizione dominante, contestando la raccolta di dati senza esplicito consenso degli utenti da siti terzi. Ha ritenuto che questa pratica violasse il GDPR e il Bundesdatenschutzgesetz (BDSG), configurando un abuso di posizione dominante poiché gli utenti non avevano scelta se non accettare le condizioni imposte da Facebook[84].

In sede cautelare, l'Oberlandesgericht di Düsseldorf aveva bloccato la decisione, sollevando dubbi sulla mancanza di prova del pregiudizio alla concorrenza e sul nesso di causalità tra l'abuso di posizione dominante e la lesione del diritto degli utenti all'autodeterminazione, adducendoli come vizi della motivazione, sostenendo quindi che l'uso dei dati fosse legittimo, dato il consenso degli utenti, ed escludendo l'abuso di posizione dominante[85].

Tuttavia, il Bundesgerichtshof aveva, a sua volta, ribaltato la decisione del giudice di Düsseldorf, affermando che l'assenza di alternative per gli utenti costituisse un abuso di posizione dominante, indipendentemente dal consenso al trattamento dei dati, in quanto lesivo del diritto all'autodeterminazione informativa. I giudici di Karlsruhe ravvisavano "il maggior *vulnus* nell'elisione della possibilità di scelta"[86], da cui discende un pregiudizio del diritto del consumatore ad autodeterminarsi con conseguente abuso della posizione dominante dell'azienda. Secondo i giudici del Tribunale supremo, infatti, la decisione di Facebook di non mettere a disposizione opzioni tra cui scegliere nel momento in cui un utente decide di usufruire dei servizi di Facebook – decisione che comporta la mancata possibilità per gli utenti di scegliere di utilizzare Facebook senza condividere i propri dati

82. Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631, § 7.

83. Il caso viene trattato in Laviola 2022, p. 28 ss; Midiri 2021, pp. 111 ss.

84. L'Autorità aveva, infatti, ritenuto che i termini di servizio, apposti in violazione delle disposizioni del GDPR, fossero da considerare abusivi ai sensi del §19 (1) GWB. L'acronimo GWB sta per *Gesetz gegen Wettbewerbsbeschränkungen*, ossia la legge tedesca contro le restrizioni della concorrenza, modificata il 18 gennaio 2021. In particolare, la sezione 19, lett. a), del GWB disciplina l'abuso di posizione dominante.

85. OLG Düsseldorf NZKart 2019, 495 – Facebook.

86. Laviola 2022, p. 41.

conformemente alle modalità stabilite – determinava una lesione dell'autonomia decisionale con tanto di violazione del diritto costituzionalmente garantito all'autodeterminazione informativa[87]. Questa mancanza, secondo i giudici, non poteva essere colmata dalla possibilità che l'utente abbia a disposizione di rinunciare completamente all'utilizzo del social network, in quanto, al giorno d'oggi, esso è considerato uno strumento imprescindibile di partecipazione alla vita sociale[88].

Così, pressoché contemporaneamente, nel marzo 2021 – e per di più nel corso della stessa settimana –, le due "saghe" sono giunte a un punto di svolta decisivo.

Come si è visto, la sentenza del Consiglio di Stato del 29 marzo ha, infatti, posto l'ultima parola sul caso scaturito dalla sanzione dell'AGCM a Facebook, successivamente impugnata dinanzi al Tar Lazio. In un'udienza di solo cinque giorni prima, il 24 marzo, l'Oberlandesgericht di Düsseldorf aveva rinviato in via pregiudiziale alla Corte di giustizia dell'Unione europea la soluzione del caso tedesco[89].

Mentre si chiudeva la vicenda italiana, cominciava quella europea.

La principale questione su cui è stata interrogata la Corte di giustizia attiene al fatto se sia compatibile con gli artt. 51 e ss. GDPR che un'autorità diversa da quella preposta al controllo sulla liceità e correttezza dei trattamenti di dati personali – nel caso di specie l'Autorità garante della concorrenza e del mercato –, accerti, nell'ambito dell'esame di abuso di posizione dominante da parte di un'impresa ai sensi del diritto della concorrenza, che le condizioni contrattuali applicate da un operatore siano conformi al GDPR e, in caso di esito negativo, imponga di porre fine a tale violazione.

La Corte ha preliminarmente osservato che, ai sensi dell'art. 5 del Regolamento n. 1/2003, "le autorità nazionali garanti della concorrenza sono competenti ad adottare decisioni che constatino un abuso di posizione dominante da parte di un'impresa, ai sensi dell'art. 102 TFUE, il cui obiettivo consiste nell'istituire un regime atto a garantire che la concorrenza non sia falsata nel mercato interno, tenuto conto anche delle conseguenze di un tale abuso per i consumatori di tale mercato"[90]. Nell'ambito dell'adozione di una decisione di questo tipo è possibile, infatti, che un'autorità garante della concorrenza debba valutare, sulla base di tutte le circostanze del caso di specie, se il comportamento dell'impresa in posizione dominante abbia l'effetto di ostacolare, tramite il ricorso a mezzi diversi da quelli su cui si impernia la concorrenza normale tra prodotti o servizi, la conservazione del grado di concorrenza esistente sul mercato o lo sviluppo di detta concorrenza[91]. A tal fine, dunque, può risultare necessario che l'autorità garante della concorrenza dello Stato membro interessato esamini anche la conformità del comportamento dell'impresa a norme diverse da quelle rientranti nel diritto alla concorrenza, quali – per quel che rileva in questo scritto – le norme in materia di protezione dei dati personali previste dal GDPR.

Tuttavia, quando l'autorità nazionale garante della concorrenza ravvisi una violazione del GDPR, alla luce degli obiettivi perseguiti dalle norme delle diverse discipline, essa non si sostituisce alle autorità di controllo istituite da tale regolamento, ma la valutazione effettuata dall'autorità garante della

87. Come afferma il BGH 23 giugno 2020 § 102: "il diritto all'autodeterminazione informativa garantisce all'individuo la possibilità di esercitare un'influenza differenziata sul contesto e la maniera in cui i propri dati sono resi accessibili ai terzi e usati da loro"; e ha un impatto anche quando "s'interpretano le clausole generali del diritto civile, cui il § 19 Gwb può essere ricondotto".

88. BGH 23 giugno 2020 – KVR 69/19, cit., § 58 cit.

89. "La questione se Facebook stia abusando della sua posizione dominante come fornitore sul mercato tedesco dei social network perché raccoglie e usa i dati dei suoi utenti in violazione del GDPR non può essere decisa senza fare riferimento alla CGUE, essendo essa responsabile dell'interpretazione del diritto europeo" (OLG 24 marzo 2021).

90. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 46.

91. Come rilevato nelle conclusioni dell'Avvocato generale Rantos del 20 settembre 2022, causa C-252/21, *Meta Platforms Inc., già Facebook Inc., Meta Platforms Ireland Limited, già Facebook Ireland Ltd., Facebook Deutschland GmbH contro Bundeskartellamt*, par. 23. In tal senso, v. sentenza del 25 marzo 2021, *Deutsche Telekom/Commissione*, C-152/19 P, EU:C:2021:238, p.ti 41 e 42).

concorrenza in merito alla violazione del GDPR è limitata al solo scopo di constatare un abuso di posizione dominante e di imporre misure volte a far cessare tale abuso secondo le norme di diritto della concorrenza. È chiaro, quindi, che detta autorità non realizza alcuna invasione della sfera di competenza dell'autorità di protezione dei dati dal momento che – come rilevato dalla Corte[92] – non viene esercitato alcuno dei compiti di cui all'art. 57 GDPR, né si fa uso dei poteri riservati all'autorità di controllo in forza dell'art. 58 del medesimo regolamento.

La Corte tuttavia puntualizza che "nel caso in cui un'autorità nazionale garante della concorrenza ritenga necessario pronunciarsi, nell'ambito di una decisione relativa ad un abuso di posizione dominante, sulla conformità o sulla non conformità al GDPR di un trattamento di dati personali effettuato dall'impresa in questione, tale autorità e l'autorità di controllo interessata o, se del caso, l'autorità di controllo capofila competente ai sensi di tale regolamento devono cooperare tra loro al fine di garantire un'applicazione coerente di tale regolamento"[93]. Viene così richiamato il principio di leale cooperazione tra le autorità nazionali[94], al fine di garantire un'applicazione coerente del GDPR. Tale principio obbliga l'autorità garante della concorrenza, nel caso in cui ritenga necessario controllare il rispetto da parte di un'impresa delle disposizioni del regolamento, a concertarsi con l'autorità nazionale di controllo competente e, quindi, a verificare se tale comportamento – o un comportamento simile – sia già stato oggetto di una decisione da parte di tale autorità o, ancora, della Corte. Nell'ipotesi in cui l'autorità garante privacy competente si fosse già pronunciata, l'autorità garante della concorrenza non potrebbe discostarsi da tale pronuncia, restando, però, libera di trarre conclusioni utili per l'applicazione del diritto della concorrenza.

In forza, dunque, del principio di leale collaborazione, la Corte specifica che laddove un'autorità garante della concorrenza nutra dubbi sulla portata della decisione dell'autorità garante della privacy, laddove il comportamento di un'impresa sia, al contempo, oggetto di esame da parte di tali autorità privacy, nazionali o capofila, o laddove in assenza di un'indagine di dette autorità, l'autorità nazionale garante della concorrenza ritenga che un comportamento di un'impresa non sia conforme alle disposizioni del GDPR, quest'ultima "deve consultare l'autorità nazionale di controllo del regolamento e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione"[95].

In definitiva, dunque, la CGUE afferma la competenza di un'autorità garante della concorrenza di uno Stato membro a constatare che "le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare

92. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 48.

93. *Ivi*, p.to 52.

94. Cfr. art 4, par. 3, TUE il quale sancisce che "In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati". Secondo una giurisprudenza costante, infatti, l'obbligo degli Stati membri di assistersi reciprocamente, nell'adempimento dei compiti derivanti dai Trattati, di adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, nonché di astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione, include anche le loro autorità amministrative (v., in tal senso, sentenze del 7 novembre 2013, *UPC Nederland*, C518/11, EU:C:2013:709, p.to 59, nonché del 1° agosto 2022, *Sea Watch*, C-14/21 e C-15/21, EU:C:2022:604, p.to 156).

95. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 63. Nel caso di specie, risulta che, prima di giungere all'adozione della propria decisione, l'autorità federale garante della concorrenza abbia posto in essere una cooperazione con le autorità garanti della protezione dei dati tedesche (in particolare, il *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), commissario federale per la protezione dei dati e la libertà d'informazione, Germania, lo *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, il commissario per la protezione dei dati e la libertà d'informazione di Amburgo, competente riguardo a Facebook Deutschland, nonché la *Data Protection Commission* (DPC), ossia l'autorità per la protezione dei dati, Irlanda), senza ricevere obiezioni da parte di questi in merito al proprio intervento (cfr. p.ti 555 e 556 della sua decisione del 6 febbraio 2019).

l'esistenza di un tale abuso"[96], fermo restando però il rispetto dell'obbligo di leale cooperazione con le autorità di controllo.

Da un'analisi della sentenza, occorre tuttavia notare che se, da una parte, è stata ribadita la centralità del consenso dell'interessato, nel caso di trattamenti effettuati dal titolare di un social network online, dall'altra, la dirimente questione di fondo rimessa alla Corte, in merito alla possibilità che i dati personali abbiano o meno valore economico – su cui risulta essenziale un parere della Corte – è rimasta sostanzialmente senza risposta, non avendo i giudici preso una posizione netta in merito. La Corte, infatti, ha affermato la competenza dell'Autorità antitrust a sindacare il rispetto alle disposizioni del GDPR da parte di un operatore di un social network, riconoscendo che "i dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese dell'economia digitale" e che, pertanto, "escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione"[97]. Tuttavia, non ha ammesso una generale competenza dell'autorità garante della concorrenza, confermando così l'economicità dei dati, ma si è limitata a constatarne la competenza nella sola ipotesi di indagine di abuso di posizione dominante, vincolandola, inoltre, ad una cooperazione fattiva con le autorità garanti della protezione dei dati personali, di cui devono tenersi in considerazione qualsiasi decisione o indagine.

Pertanto, tale pronuncia, sebbene rappresenti un ulteriore passo in avanti nell'ottica di una stretta sinergia tra le attività svolte dalle diverse autorità amministrative indipendenti e di coordinamento tra le diverse normative al fine di costruire un *enforcement* armonizzato di regole volte alla costruzione del *Digital Single Market*, lascia sospesa la questione se i dati personali possano o meno essere considerati un bene economico, rimettendo la decisione ai singoli operatori nazionali.

5. Il Consiglio di Stato riafferma il principio leale collaborazione

Le conseguenze della posizione assunta dalla Corte di giustizia con la sentenza 4 luglio 2023 non hanno tardato a presentarsi. Il 15 gennaio 2024, a pochi mesi quindi dalla pubblicazione della sentenza della CGUE, il Consiglio di Stato ha emesso una nuova sentenza sulla questione[98], all'esito del procedimento del c.d. caso Telepass.

In breve, l'AGCM aveva irrogato alla società Telepass S.p.a. e Telepass Broker S.r.l. (d'ora in poi Telepass e Tb) una sanzione pecuniaria di due milioni di euro per pratiche commerciali scorrette in quanto nel comparto dell'*insuretech* fornivano informazioni ingannevoli e/o carenti sulla raccolta e trattamento dei dati degli utenti che richiedevano un preventivo assicurativo relativo a polizze RC auto tramite App Telepass e sulle modalità di preventivazione[99]. Infatti, le società Telepass e Tb e le Compagnie assicurative partner condividevano un *data base* dedicato per la gestione e l'acquisizione di dati assicurativi, separato rispetto alla piattaforma attraverso la quale la stessa Telepass gestiva i dati degli utenti titolari dei dispositivi per i servizi di pagamento in mobilità. Pertanto, nel corso dell'intera procedura digitale, il consumatore non era edotto circa la raccolta e l'utilizzo a fini commerciali dei suoi dati, che Telepass otteneva dalle

96. CGUE, sentenza 4 luglio 2023, C-252/21, p.to 62.

97. *Ivi*, p.to 51.

98. Consiglio di stato, sez. VI, 15 gennaio 2024, n. 497.

99. Su segnalazione dell'Associazione Nazionale Agenti Professionisti di Assicurazione (ANAPA), l'AGCM aveva accertato con delibera n. 28601/2021 l'illegittimità di due condotte poste in essere dalle due società del Gruppo Telepass, in violazione degli artt. 21 e 22, commi 1 e 2 del Codice del Consumo. In particolare, la condotta a), concerneva l'assenza di informativa ai clienti, che richiedevano il preventivo per la polizza RC auto tramite APP Telepass, circa la gestione, conservazione e trasferimento di dati dei clienti dalle compagnie assicurative alla stessa Telepass, la quale li sfruttava a fini commerciali. La condotta b) riguardava l'assenza di indicazione circa i criteri e parametri di riferimento e di selezione del preventivo RC auto proposto, enfatizzando piuttosto la particolare facilità e convenienza della proposta effettuata attraverso l'App.

compagnie assicurative in fase di preventivo, né tantomeno era a conoscenza dei criteri sulla cui base Telepass e Tb proponevano il preventivo RC auto definito "migliore", inducendo in tal modo i consumatori ad assumere decisioni di natura commerciale che altrimenti non avrebbero assunto, a parere dell'autorità.

Avverso tale provvedimento, le società Telepass e Tb hanno inizialmente proposto ricorso dinanzi al TAR Lazio, al fine di ottenere l'annullamento del suddetto provvedimento sanzionatorio, deducendo quale principale motivo di ricorso la violazione, da parte dell'AGCM, delle competenze e delle prerogative del Garante per la protezione dei dati personali, nonché la violazione dei principi di buon andamento dell'azione amministrativa e di leale collaborazione, in quanto era mancato, nel corso del procedimento conclusosi con il provvedimento sanzionatorio dell'AGCM, l'acquisizione del parere del Garante privacy, essendo indubbio che lo stesso fosse necessario nell'ambito dell'esame di un comportamento anticonsumeristico derivante da una condotta violativa delle norme poste a protezione del trattamento dei dati.

Con la sentenza n. 603/2023 il TAR Lazio ha respinto il ricorso[100], inducendo così le società a rivolgersi al Consiglio di Stato per chiedere la riforma della sentenza di primo grado e il conseguente annullamento del provvedimento adottato dall'Antitrust.

In giudizio si sono costituiti anche l'Autorità per le garanzie nelle comunicazioni, il cui parere era stato acquisito dall'Antitrust durante l'istruttoria ai sensi dell'art. 27, comma 6, del Codice del consumo, e il Garante privacy, quest'ultimo a difesa delle proprie prerogative[101].

Sotto il profilo della contaminazione normativa tra il settore consumeristico e quello della tutela dei dati personali ed in ragione dell'ingente rilevanza strategica che i dati hanno assunto nell'ambito dell'attività delle imprese, il Consiglio di Stato ha, in via preliminare, chiarito che "lo spettro amplissimo di ipotesi riconducibili all'attività di trattamento e dunque rilevanti in materia di dati personali delle persone fisiche e quindi ricadenti nella sfera di applicazione del GDPR, esclude, già da solo, che la sostenuta esistenza di compartimenti 'stagni', non permeabili tra loro, tra l'ambito di competenza e dei poteri di AGCM rispetto a quelli di altre Autorità, in particolare del Garante privacy, possa militare nel senso di escludere 'a priori' qualsiasi forma di collaborazione tra le due Autorità nel corso di una indagine che, seppure fondamentalmente indirizzata circa la compatibilità o meno con la disciplina consumeristica di condotte sviluppate da professionisti, abbia indubbiamente addentellati forti e robuste caratterizzazioni osmotiche con la tutela dei dati personali", potendosi sostenere "una funzionalizzazione tra i comportamenti contestati e la violazione, contemporanea, di discipline normative differenti perché riferite a settori specialistici e quindi la doverosità della cooperazione tra Autorità".

Al fine di giungere alla soluzione del nodo contenzioso principale, palesandosi un conflitto di competenze tra le due diverse Autorità

100. Il TAR infatti ha evidenziato che "il collegamento con l'informativa sulla privacy è solo incidentale e non è dirimente al fine di giudicare della legittimità dei comportamenti contestati. Nel caso di specie rileva l'omissione di informazioni essenziali per consentire ai consumatori il libero e consapevole esercizio delle proprie scelte negoziali, in quanto il piano attinente alla tutela della privacy e, di risulta, la corrispondente competenza del Garante per la protezione dei dati personali costituiscono aspetti del tutto autonomi". Secondo il tribunale, dunque, "non sussisteva alcun obbligo di interpellare il Garante, in quanto non si trattava di richiedere un parere obbligatorio nell'ambito di un settore regolato, ai sensi dell'art. 27, comma 1 bis del Codice del Consumo".

101. Cfr. Atto di costituzione del Garante Privacy, richiamato in sentenza, in cui l'Autorità ha, dapprima, ricordato che vi possono essere fattispecie alle quali si applicano più norme e beni giuridici la cui vigilanza è affidata a soggetti diversi, affermando però che è il principio – avente valore costituzionale – di leale collaborazione fra amministrazioni "ad imporre erga omnes la esigenza di risposte coordinate, soprattutto nei casi, non infrequenti, in cui la condotta possa attivare più apparati sanzionatori e dunque plurimi procedimenti di irrogazione". In riferimento al caso di specie, l'Autorità garante per la protezione dei dati personali ha rilevato come l'AGCM, sebbene abbia acquisito il parere dell'AgCOM e dell'IVASS, ha però omesso di richiedere il parere del Garante privacy, in una fattispecie che, rientrando nella previsione di cui all'art. 130 Codice privacy e attenendo alla libera circolazione dei dati, ricadeva sia in astratto che in concreto sotto la vigilanza del Garante.

indipendenti, i giudici di Palazzo Spada hanno ritenuto necessario fare richiamo alla recente sentenza della Corte di giustizia Ue 4 luglio 2023, superando le evidenti difformità[102] tra le fattispecie poste alla base delle due pronunce, in quanto in entrambe le ipotesi si riscontrano profili di "contiguità e prossimità tra l'indagine dell'Autorità Antitrust e il settore della tutela dei dati personali di competenza dell'autorità di controllo istituita nel paese di riferimento (nel caso il Garante privacy)"[103]. Nella sentenza 4 luglio 2023 era stato chiarito che, quando le autorità nazionali garanti della concorrenza si trovino, nell'esercizio delle loro competenze, ad esaminare la conformità di un comportamento di un'impresa alle disposizioni del GDPR, esse devono concertarsi e cooperare lealmente con le autorità di controllo competenti. Ne consegue che, qualora un'autorità nazionale garante della concorrenza ritenga che un comportamento di un'impresa non rispetti le disposizioni dettate in materia di protezione dei dati personali, l'autorità stessa deve consultare l'autorità di controllo competente in materia di privacy e chiederne la cooperazione, al fine di fugare i propri dubbi o valutare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione. Trovando i principi espressi dalla CGUE piena applicazione al caso in esame, a parere del Consiglio di Stato, si è reso evidente che il mancato coinvolgimento, nel corso dell'istruttoria svolta dall'AGCM, del Garante privacy si sia sostanziato in un vizio procedimentale che ha determinato nel provvedimento finale una patologia rilevante, tale da indurre il Consiglio di Stato ad accogliere il ricorso e ad annullare l'atto sanzionatorio emesso dalla stessa AGCM.

Occorre, a questo punto, evidenziare che la soluzione accolta nella sentenza analizzata in questo paragrafo è stata frutto dell'interpretazione estensiva che i giudici di Palazzo Spada hanno adottato dei principi riscontrati dalla sentenza 4 luglio 2023 CGUE. Come è stato osservato nel precedente paragrafo, quest'ultima non ha riconosciuto una generale e diffusa competenza dell'Antitrust a sindacare il rispetto delle regole in materia di dati personali nello svolgimento delle proprie indagini, ma essa è stata confermata solo nell'ipotesi di esame di abuso di posizione dominante da parte dell'Autorità, fermo restando l'obbligo di cooperazione con il Garante privacy. La sentenza in esame, invece, inserendosi nel solco tracciato dalla precedente sentenza del Consiglio di Stato (sent. n. 2631/2021), circa la commistione tra le due discipline, consumeristica e privacy, ha quindi rappresentato una importante svolta nel delineare i profili della collaborazione richiesta alle due Autorità, estendendo i contorni timidamente delineati dalla Corte di giustizia del principio di leale collaborazione.

6. Conclusioni

In conclusione, l'evoluzione tecnologica ed informatica ha determinato la sistematizzazione dell'attività imprenditoriale e la messa a disposizione di strumenti di circolazione di dati di ogni natura, rendendo la condivisione e l'utilizzo delle informazioni lo strumento necessario all'esercizio dell'attività economica e, più in generale, alla realizzazione di un mercato unico dei dati.

In questo contesto le sfide poste dal progresso tecnologico stanno esponendo il fondamentale diritto alla protezione dei dati personali e l'equilibrio del mercato a rischi nuovi, determinando di conseguenza il legislatore a sviluppare un sistema

102. Il caso concreto posto all'attenzione della Corte di giustizia riguardava, infatti, l'ipotesi di abuso di posizione dominante contestata dall'Autorità antitrust tedesca, la quale, nell'ambito del suo esame, aveva rilevato come la condotta posta in essere dalla società Meta Platforms Ireland violasse le disposizioni in materia di dati personali. È chiara, quindi, la difformità della vicenda tedesca rispetto alla vicenda odierna in cui l'indagine dell'Antitrust si è focalizzata su una condotta anticonsumeristica imputata all'impresa, sebbene entrambe le ipotesi riguardino la sovrapposizione tra la normativa a tutela dei dati personali e la disciplina consumeristica. È interessante anche notare che lo stesso Consiglio di Stato afferma che la vicenda sottopostagli, non attiene alla possibilità o meno, da parte delle società, di patrimonializzare i dati personali dei loro clienti, il che rende il c.d. caso Telepass ulteriormente diverso dal c.d. caso Facebook.

103. "Le deduzioni sviluppate e i principi espressi nella sentenza della Corte di giustizia UE 4 luglio 2023 si attagliano plasticamente al caso in esame e completano le osservazioni illustrate più sopra dal Collegio" (Consiglio di Stato, sez. VI, 15 gennaio 2024, n. 497, p.to 12).

in grado di reinterpretare e riequilibrare il quadro dei poteri e delle libertà che vengono in rilievo.

Tuttavia, la possibilità di governare i dati nel nuovo ecosistema digitale è resa difficile dalla mancanza di un quadro organico di riferimento. I casi analizzati nei precedenti paragrafi hanno infatti fatto luce sul problema di coordinamento tra le diverse normative, in particolare la tutela dei dati personali e la tutela della concorrenza, nonché sulla difficile commistione delle competenze delle rispettive Autorità di controllo. Tale quadro, già di per sé complesso, rischia di complicarsi ulteriormente alla luce dei numerosi provvedimenti adottati a livello europeo. DGA, DA letti di concerto con DMA, DSA, AI Act, NIS 2 e vari altri recenti interventi normativi, sebbene definiscano le regole per disciplinare e controllare il mercato digitale e imbrigliare il potere delle *big tech*, tenendo in considerazione la correlazione, ormai instauratasi tra concorrenza e privacy[104] e prevedendo, al fine di garantire l'equilibrio nel mercato, maggiore trasparenza nei rapporti tra i fornitori e utenti e il controllo da parte di autorità amministrative indipendenti, nascondono il rischio di un'insostenibile frammentazione in termini di sovrapposizioni istituzionali e conflitti tra le diverse autorità designate dagli Stati membri.

Un duplice esempio in tal senso è rappresentato dal Digital Governance Act (DGA) e dal Data Act (DA), i quali hanno come principale obiettivo quello di favorire la condivisione dei dati, nel rispetto del diritto europeo o nazionale in materia di protezione dei dati. Il DGA, che introduce un nuovo quadro normativo per regolare l'intermediazione dei dati e promuoverne pratiche di altruismo in tutta l'Unione europea, all'articolo 13, richiede agli Stati membri di designare una o più autorità competenti per gestire la procedura di notifica relativa ai servizi di intermediazione dei dati. Lo stesso schema viene riproposto nel Data Act che, ai sensi dell'art. 37, attribuisce agli Stati membri la facoltà di istituire nuove autorità o affidare i compiti a quelle esistenti. La flessibilità concessa agli Stati, sebbene presenti profili di ragionevolezza, nella realtà potrebbe creare una sovrapposizione di competenze, in quanto le autorità preesistenti, come chiarisce il DGA stesso all'art. 13, par. 3, mantengono i loro poteri, e il regolamento richiede che si instauri una forte cooperazione tra loro.

Fermo restando che, in un settore delicato come la gestione dei dati e la regolazione delle nuove tecnologie, in cui le interpretazioni normative possono divergere sensibilmente, la cooperazione tra enti con competenze diverse può risultare spesso problematica, occorre notare, tra tutti questi provvedimenti, l'assenza di una legge che definisca un quadro generale in materia di autorità amministrative indipendenti sia in Italia che in Europa. Sarebbe auspicabile, infatti, adottare una legge generale che razionalizzi in modo chiaro i processi e l'organizzazione delle funzioni delle varie autorità indipendenti, o che comunque raccordi le discipline che vengono in rilievo, introducendo eventuali criteri di prevalenza. In altre parole, sarebbero necessarie regole generali riguardanti l'organizzazione degli uffici, le competenze delle singole Autorità e il procedimento istruttorio, includendo anche procedure di coordinamento delle diverse discipline sulle questioni di interesse comune.

La proliferazione normativa e la mancanza di un reale raccordo tra i nuovi provvedimenti e la disciplina in materia di protezione dei dati personali[105] rischiano di tradire l'intento del legislatore europeo di incrementare la fiducia dei consumatori e valorizzare la competitività delle piccole e medie imprese europee. I primi, infatti, avranno difficoltà nell'identificare la normativa di riferimento e l'autorità a cui rivolgersi in caso di violazione dei loro diritti; le seconde invece si troveranno gravate da numerosi obblighi, incisivi quindi della loro libertà di iniziativa economica, il cui mancato rispetto potrà attivare i poteri sanzionatori e ispettivi di una pluralità di soggetti.

Dinnanzi a questo vuoto normativo e a fronte dell'importanza della pluralità di interessi coinvolti,

104. Si tenga presente l'osservazione di Pitruzzella 2019, secondo cui, nel contesto eurounitario, la tutela dei diritti e il buon funzionamento del mercato sono del tutto complementari.

105. Si nota, infatti, che il considerando 4 del DGA specifica che "In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o del diritto nazionale adottato conformemente a tale diritto dell'Unione, il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali dovrebbe prevalere", utilizzando quindi una forma condizionale senza specificare come realmente tale "prevalenza" si manifesta in concreto.

tra i quali la tutela della privacy, la tutela del consumatore e della concorrenza, fondamentale risulta l'intervento della giurisprudenza, prima europea e poi nazionale, nelle cui pronunce è stata di fatto dettata una regola risolutiva del caso concreto, prevedendo un obbligo di leale cooperazione tra le Autorità, sanzionabile con l'annullamento dei provvedimenti adottati.

In un quadro così problematico – in cui al valore personalistico dei dati attinente alla dignità e all'identità della persona viene ad aggiungersi anche un'ulteriore tipologia di valore, il valore economico, ossia il fatto che i dati possano considerarsi dei beni e circolare liberamente nel mercato, ed entrambi vanno tenuti in egual considerazione affinché le esigenze del mercato o della collettività non rischino di determinare un'ingiustificata compressione della libertà del singolo[106] – la giurisprudenza impone dunque una regolazione di tipo partecipativo[107], che coinvolga, oltre al controllo del Garante per la protezione dei dati personali, anche la vigilanza e l'intervento delle altre autorità indipendenti.

Sulla scia della giurisprudenza, specie quella europea, e alla luce delle criticità evidenziate, il 16 gennaio 2025, l'EDPB ha pertanto pubblicato una dichiarazione sull'interazione tra il diritto della concorrenza e la protezione dei dati[108], nella quale, dopo una parte introduttiva in cui spiega lo sviluppo dell'interazione tra le due discipline – chiarendo che, pur trattandosi di "*fields of law that pursue diffent objectives*", hanno dei potenziali punti in comune – suggerisce raccomandazioni volte a migliorare la cooperazione tra le diverse autorità di regolamentazione. All'interno del documento, infatti, l'EDPB ipotizza, fra tutti, la possibilità di una stipulazione tra le autorità di accordi di cooperazione – ad esempio accordi amministrativi, dichiarazioni comuni o protocolli d'intesa – nei quali stabilire i principi e le regole per la cooperazione, nonché una miglior comprensione del rapporto tra le discipline, e nell'ambito dei quali prevedere la formazione all'interno delle singole autorità, di gruppi di lavoro dedicati alla cooperazione e prodromici quindi a costituire un punto di contatto unico per gestire il coordinamento con le altre autorità di regolamentazione.

Tale documento costituisce infine un ulteriore tassello e ulteriore presupposto fondativo del sistema di regolazione dell'ecosistema digitale che, a fronte del repentino evolversi dell'economia digitale, il legislatore europeo sta tentando di delineare, tenendo a mente l'importanza che assume la promozione di sinergie tra le diverse autorità di controllo in modo tale da offrire un'efficace tutela ai diritti fondamentali che vengono in rilievo e creare quel "clima di fiducia" che consentirebbe di "mantenere l'Ue all'avanguardia dell'economia agile basata sui dati, rispettando e promuovendo nel contempo i valori fondamentali che costituiscono i capisaldi delle società europee"[109].

Riferimenti bibliografici

C. Basunti (2020), *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in "Contratto e impresa", 2020, n. 2

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

106. Laviola 2021, pp. 195-211.

107. EDPS, *Opinion 8/2016, on coherent enforcement of fundamental rights in the age of big data*, 23 settembre 2016, p. 10: "The synergies between the fields of law, which have been discussed intensively in the recent years, could propel closer cooperation between authorities, especially where there is neither guidance nor case law. It is not a question of 'instrumentalising' another area of law but rather of synchronising EU policies and enforcement activities, adding value where a supervisory authority lacks expertise or legal competence in analysing". L'esigenza di un coordinamento tra le due autorità è stata evidenziata anche in altre occasioni, v. *Antitrust, Privacy and Big Data*, discorso dell'EPDS, 3 febbraio 2015, Joint EDPS-ERA Workshop; *Competition Rebooted: enforcement and personal data in Digital Markets*, 24 settembre 2015, Brussels.

108. EDPB, *Position paper on Interplay between data protection and competition law*, 16 gennaio 2025.

109. Commissione europea, *Una strategia per i dati*, COM(2020) 66, 19 febbraio 2020, p. 2.

F. Caggia (2019), *Libertà ed espressione del consenso*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

F. Calisai (2019), *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

E. Cheli (2021), *Conclusioni*, in "Osservatorio sulle fonti", 2021, n. 2

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

E. Cremona (2021), *Le nuove tecnologie oltre la "grande dicotomia" tra pubblico e privato*, in "La rivista Gruppo di Pisa", 2021, Quaderno n. 3

E. Cremona, F. Laviola, V. Pagnanelli (a cura di) (2022), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, 2022

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

A. Davola (2021), *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in "Diritto di internet", 2021, n. 1

A. De Cupis (1982), *I diritti della personalità*, in "Trattato di diritto civile e commerciale", vol. IV, Giuffrè, 1982

A. De Franceschi (2019), *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

S. Elvy (2017), *Paying for privacy and the personal data economy*, in "Columbia Law Review", vol. 117, 2017, n. 6

A. Gentili (2022), *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in "Rivista trimestrale di diritto e procedura civile", 2022, n. 3

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei "data spaces": Data Governance Act e Data Act*, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209

K. Klonick (2018), *The new governors: the peoples, rules and processes governing online speech*, in "Harvard Law Review", vol. 131, 2018, n. 6

F. Laviola (2022), *Il diritto all'autodeterminazione informativa tra concorrenza e* data protection, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

F. Laviola (2021), *Diritti fondamentali ed efficienza economica nel mercato digitale: tra protezione dei dati personali e tutela della concorrenza*, in "La rivista Gruppo di Pisa", 2021, Quaderno n. 3

G. Malgieri, B. Custers (2018), *Pricing privacy – the right to know the value of your personal data*, in "Computer Law & Security Review", vol. 34, 2018, n. 2

T.W. Malone, J. Yates, R.I. Benjamin (1987), *Electronic markets and electronic hierarchies*, in "Communications of the ACM", vol. 30, 1987, n. 6

V. Mayer-Schönberger, T. Ramge (2018), *Reinventare il capitalismo nell'era dei Big Data*, Egea, 2018

F. Mezzanotte (2018), *I poteri privati nell'odierno "diritto dello sviluppo economico"*, in "Politica del diritto", 2018, n. 3

F. Midiri (2016), *La giuridificazione della protezione dei dati personali*, in L. Ferrara, D. Sorace, B. Marchetti, M. Renna (a cura di), "A 150 anni dall'unificazione amministrativa italiana. La giuridificazione", vol. iii, Firenze University Press, 2016

M. Midiri (2021), *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in "Il diritto dell'informazione e dell'informatica", 2021, n. 2

M. Midiri (2020), *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in "federalismi.it", 2020, n. 14

G. Mirabelli (1993), *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in "Il diritto dell'informazione e dell'informatica", 1993, n. 2

A. Moretti (2022), *Il valore dei dati nell'*European Data Strategy*: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

M. Mursia, C.A. Trovato (2021), *The commodification of our digital identity: limits on monetizing personal data in the European context*, in "MediaLaws", 2021, n. 2

M. Naldi (2018), *Prospettive economiche dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

A. Nicita (2019), *Il dato profilato nella prospettiva economica tra* privacy, propertization, secrecy, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

V. Pagnanelli (2022), *Una "valutazione d'impatto" della privacy sulle Big Tech*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

R. Pardolesi, R. Van den Bergh, F. Weber (2020), *Facebook e i peccati da "Konditionenmissbrauch"*, in "Mercato concorrenza regole", 2020, n. 3

G. Pitruzzella (2019), *L'Europa del mercato e l'Europa dei diritti*, in "federalismi.it", 2019, n. 6

O. Pollicino (2019), *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19

O. Pollicino (2019-a), *New Technology, Algorithms and the Rising of Private (Digital) Powers and new Challenges for Constitutional Law*, in "Eurac research", 11 July 2019

A. Predieri (1997), *L'erompere delle autorità amministrative indipendenti*, Passigli Editori, 1997

G. Resta (2019), *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra direttiva (UE) 2019/770 e il Regolamento UE 2016/679*, in "Annuario del Contratto 2018", 2019

G. Resta (a cura di) (2010), *Diritti esclusivi e nuovi beni immateriali,* UTET, 2010

G. Resta, V. Zeno-Zencovich (2018), *Volontà e consenso nella fruizione dei servizi in rete*, in "Rivista trimestrale di diritto e procedura civile", 2018, n. 2

V. Ricciuto (2020), *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in "Rivista di diritto civile", 2020, n. 3

V. Ricciuto (2018), *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in "Il diritto dell'informazione e dell'informatica", 2018, n. 4-5

V. Ricciuto, C. Solinas (2021), *Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in "Giustiziacivile.com", 2021, n. 5

C. Sartoretti (2019), *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in "federalismi.it", 2019, n. 13

R. Senigaglia (2020), *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in "Contratto e impresa", 2020, n. 2

S. Sica (2001), *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in "Rivista di diritto civile", 2001, n. 6

S. Simitis (1997), *Il contesto giuridico e politico della tutela della privacy*, in "Rivista critica di diritto privato", 1997, n. 4

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal–Rivista di BioDiritto", 2019, n. 1

A. Simoncini, E. Cremona (2021), *European Private Law Integration through Technology: the Constitutional Dimension*, in "Persona e mercato", 2021, n. 2

C. Solinas (2021), *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in "Giurisprudenza italiana", 2021, n. 2

A. Spatuzzi (2021), *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali*, in "Notariato", 2021, n. 4

A. Stazi, F. Corrado (2019), *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 2

K.J. Strandburg (2013), *Free Fall: The Online Market's Consumer Preference Disconnect*, University of Chicago Legal Forum, 2013

R. Van den Bergh, F. Weber (2020), *The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law?*, in "World Competition", vol. 44, 2020, n. 1

V. Zeno-Zencovich (2019), *Do "Data Markets" Exist?*, in "MediaLaws", 2019, n. 2

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019