INTRODUZIONE

di *Carlo Colapietro* e *Andrea Simoncini*

Nell'introdurre un volume sul *Valore economico dei dati tra diritto pubblico e diritto privato* non si può dimenticare il contesto in cui sono state redatte queste pagine. Nella fase storica caratterizzata dalla pandemia di Covid-19, dai *lockdown* e dalle restrizioni, è emerso infatti con lapalissiana evidenza che le nuove tecnologie e l'innovazione guidata dai dati genereranno enormi benefici per la società. In questo periodo, infatti, i servizi basati sui dati e facilmente fruibili dai più hanno permesso ad un amplissimo numero di persone di mantenere i contatti con gli altri e di proseguire la proprie attività quotidiane, ma anche di vedersi garantiti diritti costituzionali come la salute, l'istruzione o il lavoro, che solo grazie a grandi piattaforme digitali private hanno continuato a potersi esercitare; si pensi ad esempi come il tracciamento dei contatti, la didattica a distanza o il cosiddetto *smart-working.* Per altro verso, va sottolineato che anche quando il motore produttivo dell'industria tradizionale ha dovuto rallentare e, finanche, fermarsi, l'economia basata sui dati ha continuato il suo ciclo vitale, permettendo di limitare le perdite e di mantenere punte di attività in determinati settori.

Come osservato dal filosofo Hartmut Rosa, la pandemia potrebbe in realtà rivelarsi una delle molte forme di «*decelerazione (acceleratoria) funzionale*» che hanno costellato la storia della modernità e che in ultima analisi hanno reso possibile il progresso tecnologico. In altre parole, lo shock determinato dalla crisi innescata dalla pandemia ha accelerato processi di cambiamento già in corso, rendendo "improvvisamente obsoleto" ciò che già era vecchio e "improvvisamente indispensabile" ciò che era considerato come nuovo.

Non si può, d'altronde, esimersi dal prendere atto che le dotazioni tecnologiche rappresentano ormai l'architettura essenziale di pressoché tutti i servizi di interesse generale. Oltre a quanto già accennato, anche la gestione delle telecomunicazioni, dell'energia, dei trasporti, dei sistemi giudiziari, degli apparati militari dipendono da servizi digitali privati offerti dalle multinazionali. E ancor più profonda è la dipendenza tecnologica del sistema economico, sia

nella dimensione produttiva, che nei servizi, tanto da aver suggerito la nota definizione di Shoshana Zuboff "capitalismo di sorveglianza".

L'evoluzione tecnologica non smette, peraltro, di profilare scenari nuovi. Si pensi al Metaverso, una vera e propria dimensione ulteriore della vita dove vivere le relazioni, lavorare, istruirsi e svolgere tante attività ad oggi impensabili con il solo supporto dei computer, dei tablet e degli smartphone. Questa "terra promessa", proposta dal CEO di Facebook nell'ottobre 2021, è un non-luogo nel quale non ci sono malattie (i virus saranno solo informatici), non c'è il duro condizionamento della realtà e soprattutto non c'è la dolorosa fatica di sopportare sé e i propri limiti.

Ebbene, il punto è proprio che non si tratta solo di uno scenario futuribile, più o meno distopico. È solo un passo – l'ultimo in ordine di tempo – di una trasformazione che si è avviata a partire dagli anni '90 e che sembra travolgere irresistibilmente i precedenti assetti sociali, economici ed istituzionali.

La diffusione impetuosa e pervasiva delle nuove tecnologie nel settore dell'informazione e delle comunicazioni sta facendo sì che tali sistemi tecnologici stiano diventando indispensabili per lo svolgimento delle attività quotidiane. Dalle funzioni più semplici, legate alle preferenze della singola persona, a quelle più complesse, riguardanti la gestione di interessi collettivi, fino al governo di intere popolazioni; un numero sempre maggiore di funzioni – pubbliche e private – è realizzato attraverso strumentazioni di natura tecnica.

In effetti, questa considerazione, in sé, potrebbe non essere sorprendente: l'evoluzione è nient'altro che il frutto di una costante relazione tra l'umano e la tecnologia. La caratteristica che rende, però, peculiare questo tempo riguarda, da un lato, il tipo di cultura tecnica impiegata – quella nata a seguito della cosiddetta rivoluzione cibernetica – cultura che implica intrinsecamente un riflesso sull'ordine politico; dall'altro, la trasversalità di questa strumentazione tecnologica che, producendo anche decisioni – e non solo mezzi per eseguire decisioni – può applicarsi a qualsiasi ambito della esistenza umana.

Tuttavia, in una società in cui è in costante aumento la quantità di dati generati dai singoli cittadini, la metodologia di raccolta e utilizzo di tali dati deve porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e ai principi sanciti dalle tradizioni costituzionali degli Stati e sempre più presenti anche in ambito europeo, in costanza dell'integrazione dell'Europa dei mercati con l'Europa dei diritti.

Come ricordato dalla stessa Commissione europea nel documento sulla strategia europea dei dati presentato nel febbraio 2020, l'obiettivo è quello di sfruttare i vantaggi di un migliore utilizzo dei dati, contribuendo ad un approccio globale all'economia digitale. Da questo punto di vista, l'Europa rappresenta, infatti, un vero e proprio modello di riferimento, grazie a un quadro

giuridico solido, che protegge i dati personali e i diritti fondamentali, garantisce la sicurezza e la cyber-sicurezza e tutela la concorrenza nel suo mercato interno, caratterizzato da imprese competitive di tutte le dimensioni e da una base industriale diversificata.

Se è vero che non si può prescindere dall'attualità, né tantomeno dal continuare a guardare verso il futuro, è però altrettanto vero che tale sguardo deve, in ogni caso, filtrare attraverso le lenti della centralità della persona umana e del rispetto della dignità e dei diritti dell'uomo, che sono la cifra caratterizzante la Costituzione repubblicana, nonché il fondamento della convivenza dei popoli dell'Europa unita. È tempo di ritornare a crescere e di rimettere in sesto un'economia martoriata da quasi due anni di crisi sanitaria, ma non è certo tempo di dimenticarsi dei diritti fondamentali.

La sfida dell'innovazione, della digitalizzazione, dell'economia *data driven* non può essere scissa dalla sfida per la tutela delle persone e la protezione dei dati personali, sancita all'art. 8 della Carta di Nizza e vegliata dalla normativa di cui al Regolamento UE 2016/679, c.d. GDPR.

Il rapporto tra diritto e nuove tecnologie non è, infatti, privo di ambiguità e va affrontato nella prospettiva del "nuovo costituzionalismo".

In primo luogo, infatti, occorre chiarire a quale diritto si faccia riferimento e se non sia forse il caso di ripensare ad esso in ragione dei progressi della tecnica. Si prendano in considerazione, ad esempio, le modalità di conclusione di un contratto attraverso un *click* sullo smartphone, sul pc o su un altro *device*, oppure mediante l'applicazione di un'impronta digitale.

In secondo luogo, è bene altresì domandarsi quali siano i diritti che vengono in rilievo in questo contesto e se l'incessante evoluzione tecnologica non sia in grado di creare di continuo sempre nuovi diritti. A questa domanda – che vede confrontarsi coloro che sostengono che nelle Carte esistenti già si tuteli ogni forma di libertà e coloro che optano per un'ulteriore positivizzazione – per il momento è difficile dare risposta. Inoltre, come ben noto alla dottrina costituzionalistica, la tutela di istanze inedite – sia a livello giurisprudenziale che a livello normativo – non è mai priva di costi, poiché le risorse non sono infinite. Di certo, le nuove tecnologie creano nuove pretese, con cui i giuristi di domani dovranno confrontarsi anche più di quanto non facciano quelli di oggi.

Ancora, occorre chiarire che cosa si intenda precisamente con il lemma "nuove tecnologie". Nell'accezione comune, al giorno d'oggi con tale locuzione si fa principalmente riferimento alle tecnologie digitali, che sono una *specie* di un più ampio *genus.* Si tratta di una sineddoche inevitabile perché, ormai diffuse in ogni settore, le tecnologie digitali hanno trasformato profondamente la società e l'economia. È la cosiddetta Quarta Rivoluzione, che sta esplicando i suoi effetti sia nel campo della scienza che in quello dell'industria.

Difatti, 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 e l'intelligenza artificiale rappresentano i fondamenti di quella che stiamo vivendo noi e che oggi è ancora nella sua fase iniziale. Non a caso, la rivista *The Economist* già nel 2017 aveva titolato: "la risorsa più preziosa del mondo non è più il petrolio, ma i dati".

L'ingresso nel XXI secolo ha inaugurato un periodo di capillare digitalizzazione dell'ambiente umano, portando all'accumulo di un quantitativo di dati di gran lunga superiore rispetto a quanto prodotto sino ad ora nella storia dell'umanità, tanto che i fenomeni del mondo circostante, specialmente quelli afferenti all'essere umano, sono suscettibili di essere ridotti ad informazioni, mediante rappresentazione attraverso una serie di dati, che comportano una misurazione in forma quantitativa dei fenomeni stessi e la possibilità di condurre analisi molto efficaci.

Questa capacità di trasporre in dati ogni aspetto della realtà è stata resa possibile grazie alla combinazione di molteplici fattori, primi tra tutti la diffusione di internet e la conseguente realizzazione del web 2.0, del web semantico e dell'*Internet of Things*, che ha determinato la crescente connessione in rete di oggetti e dispositivi. In questo contesto, si deve, peraltro, considerare l'incremento della potenza di calcolo di cui sono dotati i moderni strumenti tecnologici e la progressiva diminuzione dei costi richiesti per il loro sviluppo e la loro implementazione. Nonostante l'alto livello di tecnologia raggiunto, acquistare uno smartphone non è, al giorno d'oggi, una spesa così proibitiva, ma al contrario tali dispositivi sono largamente accessibili, pur garantendo funzionalità superiori e notevolmente più complesse rispetto ai computer prodotti sino a qualche anno addietro. Pertanto, va evidenziato come la penetrazione tecnologica si vada gradualmente diffondendo in ogni aspetto della vita quotidiana, consentendo a ciascun individuo di avere a disposizione molteplici *device* attraverso cui poter interagire con la realtà circostante. Ciò contribuisce al processo di datizzazione e alla produzione di un costante flusso di dati.

Riprendendo il parallelo con il petrolio delineato poc'anzi, è bene, però, sottolineare come, rispetto al combustibile fossile, i dati presentano una caratteristica che li rende ancor più preziosi. Essi, infatti, non rappresentano una ricchezza finita e consumabile, ma costituiscono una risorsa che può essere liberamente condivisa, trattata e riutilizzata molteplici volte, senza che l'utilizzo dell'uno pregiudichi l'impiego di altri.

Ebbene, ciò premesso, si deve, d'altronde, rilevare che i dati di per sé non forniscono informazioni, né sono in grado di produrre valore. Affinché ciò sia

possibile occorre che gli stessi vengano lavorati, trattati ed aggregati, allo stesso modo di come avviene per il petrolio grezzo il quale, prima di poter essere effettivamente utilizzato come carburante, deve essere sottoposto ad un processo di pulizia e raffinazione. Ecco, dunque, che assumono centrale importanza le modalità e gli strumenti attraverso cui i dati vengono elaborati, cosicché, nel contesto attuale, acquisisce significativo rilievo l'utilizzo dell'intelligenza artificiale.

Tali processi di elaborazione, infatti, possono portare a soluzioni innovative e ad un efficientamento dei tempi decisionali, tanto che nel settore privato si fa ampio ricorso a queste tecniche al fine di massimizzare il profitto, attraverso un'offerta di beni e servizi ai consumatori sempre più razionalizzata; eppure, anche nel settore pubblico v'è una tendenza a rivolgersi a questo tipo di strumenti per modernizzare l'azione amministrativa, sebbene ciò comporti la necessità di rispondere a nuove sfide.

L'unica certezza, in questo quadro complesso, è che le soluzioni normative vanno adottate a livello europeo. Non si può, infatti, prescindere da un mercato tanto grande e ricco quanto il mercato unico europeo. A tal riguardo, sarà interessante analizzare le nuove discipline del DSA (*Digital Services Act*) e del DMA (*Digital Markets Act*), relative alla regolazione dei servizi e del mercato unico digitale, al momento in fase di proposta da parte della Commissione europea, nonché quella del DGA (*Data Governance Act*) e del Regolamento sull'intelligenza artificiale (*AI Act*).

D'altra parte, si tenga presente che dimensione pubblica e dimensione privata sono oggi profondamente sfidate nella loro storica distinzione; nella pratica della società digitale queste dimensioni sono costantemente mescolate, soggetti privati assumono volontariamente funzioni tradizionalmente proprie dei pubblici poteri, mentre i soggetti pubblici sono spesso costretti a rivolgersi a privati (e non volontariamente li scelgono) per poter continuare ad assolvere le proprie funzioni.

Inoltre, l'automazione dei processi decisionali, da quelli più semplici (come cercare il tragitto più breve per raggiungere una località in auto), a quelli più complessi (prevedere se una persona che ha commesso un reato, lo ricommetterà), solleva gli esseri umani da un'attività estremamente complessa e faticosa: quella di riflettere, valutare e decidere; attività che, in certe situazioni, oltre ad essere impegnativa, può diventare anche rischiosa e potenzialmente, costosa, se nelle decisioni sono coinvolti profili di responsabilità.

La conclusione è che ci si trova dinanzi ad una nuova forma di potere, intendendo con questo termine la capacità, di natura pubblica o privata, di produrre unilateralmente effetti rilevanti nella sfera giuridica di un soggetto. Effetti che possono essere liberamente voluti o accettati dal soggetto stesso, op-

pure subìti; possono ampliare la sua sfera di libera autodeterminazione ovvero restringerla.

Si è visto come lo strumentario classico, del diritto pubblico così come del diritto privato, faccia fatica a fornire le risposte che urgono nell'era dell'intelligenza artificiale.

L'erompere dei poteri (tecnologici) privati impone oggi di porre il tema della tutela della concorrenza in una ottica del tutto nuova, non solo al servizio della efficienza economica, ma anche della tutela delle libertà fondamentali, come invocava Giorgio Lombardi oltre cinquanta anni fa nel suo *Potere privato e diritti fondamentali* (1970), e dell'eguaglianza, intesa non più soltanto come eguaglianza delle imprese sul mercato (ormai tutte sotto il giogo della dipendenza economica dalle grandi piattaforme), ma anche come parità delle armi tra utente e piattaforma, come realizzazione della «*aspirazione a non essere assoggettati all'altrui autorità di diritto come anche di fatto*», recuperando così anche un'altra delle prime lucide riflessioni sul tema del potere privato, quella di Cesare Massimo Bianca ne *Le autorità private* (1977).

È una esplorazione da avviare, nella quale il costituzionalismo riscopre, come osservato da Massimo Luciani, la propria missione, trasversale al diritto pubblico e al diritto privato (come suggerisce il taglio di questo volume), che è quella di «*catturare nuovamente quel potere che molti secoli addietro aveva saputo subordinare al diritto e funzionalizzare ai diritti*», rifuggendo «*i rischi di un costituzionalismo irenico che si limiti a celebrare i trionfi dei diritti fondamentali*» e tornando «*ad un costituzionalismo polemico che si misuri con il potere*», pubblico o privato che sia.

PARTE I
IL CASO ITALIANO E IL CASO TEDESCO

UNA "VALUTAZIONE D'IMPATTO" DELLA PRIVACY SULLE BIG TECH

Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato

di *Valentina Pagnanelli*

SOMMARIO: 1. Introduzione. – 2. AGCM contro Facebook. Una vicenda emblematica. – 3. Alcune riflessioni sulla sentenza del Consiglio di Stato. L'"equivoco" dei dati personali come beni *extra commercium* alla luce dell'*habeas data*. – 4. Piattaforme digitali e profilazione degli utenti: il valore economico del *targeting*. – 5. L'impatto privacy sulle Big Tech. – 6. Europa 2030: verso una gestione più consapevole dei dati personali? – 7. Cenni conclusivi.

1. *Introduzione*

La vicenda da cui questo contributo trae spunto ha visto contrapposte Facebook e l'Autorità Garante della Concorrenza e del Mercato e si è conclusa con la sentenza emessa dal Consiglio di Stato il 29 marzo 2021 [1]. Quest'ultima pone in luce una delle questioni più dibattute dell'Era della digitalizzazione e dei Social Network: il valore economico dei dati personali. Infatti, per quanto il tornaconto economico dei giganti della rete, e nello specifico di Facebook, nel gestire enormi quantità di dati personali dei miliardi di utenti collegati da ogni angolo del globo sia di tutta evidenza, ciò non toglie che il rapporto economico tra fornitore del servizio ed utente non abbia trovato una regolazione giuridica che faccia sintesi dei due profili più evidenti del trattamento dei dati

[1] Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631. Si vedano i commenti di: G. SCORZA, *Si può fare commercio di dati personali? Scorza: "Consiglio di Stato boccia ricorso Facebook, ecco le questioni aperte*", in *AgendaDigitale*, 30 marzo 2021; O. POLLICINO, G. SCORZA, *Facebook, i dati personali possono essere corrispettivo di un servizio? Lecito dubitarne*, in *AgendaDigitale*, 15 aprile 2021.

personali: il profilo che riguarda l'esplicazione della personalità dell'utente – *interessato* nella dicitura del GDPR[2] – e il profilo che attiene all'attività commerciale che le grandi piattaforme digitali svolgono attraverso lo sfruttamento degli stessi, avvantaggiandosi in modo esclusivo della monetizzazione del trattamento dei dati personali.

Né tale questione sembra esser stata risolta dalla Direttiva 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e servizi digitali[3]. La Direttiva, pur disciplinando «*qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo*[4]» compresi i casi 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*», non si spinge infatti fino a qualificare la cessione dei dati personali come controprestazione[5], lasciando indefiniti i contorni del dibattito.

Detto altrimenti, il grande tema che occupa accademici, autorità, corti e talvolta cittadini è come frenare quella che sembra una inarrestabile corsa delle grandi *data companies* verso il monopolio assoluto dell'informazione, della comunicazione, dei dati personali, della ricchezza che attraverso tali dati viene incessantemente prodotta, senza che gli utenti, principali fornitori della mate-

---

[2] Sebbene la protezione delle persone fisiche con riguardo al trattamento dei dati personali sia la prima finalità indicata nel Regolamento europeo 2016/679 (GDPR), la definizione di "*interessato*" è rinvenibile solo in via indiretta nella più ampia descrizione dedicata al dato personale. Cfr. GDPR, art. 4, n. 1.

[3] Direttiva UE 2019/770 del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Vd. C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 3/2019, p. 499 ss.; A. LANDI, *L'exchange commerce. La Direttiva 2019/770*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Milano, 2021, p. 139 ss.; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, 4/2020, p. 635 ss. e, in questo volume, il contributo di G. VERSACI.

[4] Direttiva 2019/770, art. 3, par. 1.

[5] Così aderendo a quanto auspicato dall'European Data Protection Supervisor già nel parere 4/2017 sulla proposta di Direttiva sulla fornitura di servizi digitali. Il Garante europeo aveva accolto con favore l'estensione delle tutele garantite ai consumatori anche ai casi in cui i servizi digitali vengono presentati come gratuiti, precisando però al contempo che i dati personali non possono mai essere equiparati a denaro con cui pagare un prezzo: «*Personal information is related to a fundamental right and cannot be considered as a commodity*». Cfr. European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, p. 7.

ria prima grazie a cui le grandi piattaforme operano – i dati – siano in alcun modo partecipi dei vantaggi di tali operazioni.

Sebbene le decisioni di Autorità Garante e Corti amministrative abbiano avuto ad oggetto, nel caso citato, la violazione da parte della piattaforma digitale Facebook di alcune regole del Codice del consumo, ad una lettura più attenta dei fatti non può sfuggire che il tema sullo sfondo della contrapposizione tra AGCM e Facebook sia proprio una più equa distribuzione del valore economico che è possibile trarre dai dati, nel momento in cui i grandi *gatekeeper* delle rete, sfruttando raffinati sistemi di intelligenza artificiale, riescono ad impiegare i dati personali raccolti o dedotti dagli utenti per produrre ricchezza.

Il riconoscimento della protezione dei dati personali come diritto fondamentale sembra ostare all'affermazione che i dati personali possano essere disponibili, utilizzabili come merce di scambio per ottenere prestazioni e servizi digitali. D'altra parte è proprio la dinamica di scambio tra servizi digitali e dati personali ad essere alla base del sistema attuale. In questo contesto, la tensione tra le due accezioni di dato personale (espressione di inalienabili diritti della personalità e/o *asset* nella piena disponibilità del proprietario) può aumentare il rischio che da una doppia tutela formale – quella legata alla tutela dei dati personali e quella consumeristica – possa derivare piuttosto un dimezzamento delle garanzie.

Questo scritto propone una lettura del tema appena delineato attraverso le lenti della disciplina europea ed italiana in materia di protezione dei dati personali, al fine di saggiare l'efficacia degli strumenti della *data protection* nel contenimento del potere delle Big Tech e dunque nella correzione delle dinamiche di mercato [6].

La sentenza n. 2631/2019 della sez. VI del Consiglio di Stato, che come anticipato segna la conclusione di una disputa tra Antitrust e Facebook, fornisce interessanti spunti di riflessione sul tema poc'anzi delineato.

2. *AGCM contro Facebook. Una vicenda emblematica*

Il 29 novembre 2018 l'Autorità Garante della Concorrenza e del Mercato ha emesso il provvedimento sanzionatorio n. 27432 [7] nei confronti di Face-

[6] Pitruzzella ha sottolineato come il GDPR racchiuda un vasto insieme di diritti capaci di limitare poteri pubblici e privati, correggendo le mere dinamiche del mercato. Cfr. G. PITRUZZELLA, *L'Europa del mercato e l'Europa dei diritti*, in *federalismi.it*, 20 marzo 2019.

[7] AGCM, Provvedimento 29 novembre 2018, n. 27432.

book Inc. e Facebook Ireland Ltd. per la violazione di alcune norme del Codice del consumo relative all'esercizio di pratiche commerciali scorrette ai danni dell'utente/consumatore.

Alle due sanzioni amministrative pecuniarie irrogate, ciascuna di cinque milioni di euro, si sommava l'obbligo per la piattaforma di pubblicare sulla *homepage* italiana del sito internet aziendale e sulla *app Facebook*, «*in posizione che consenta una immediata visibilità*[8]» una dichiarazione rettificativa. Tale dichiarazione, visibile per venti giorni, doveva sopperire alla carenza di informazioni fornite ai consumatori rispetto all'attività di raccolta dei loro dati che il Social network avrebbe sino a quel momento posto in essere celando un intento commerciale, ed enfatizzando invece, al contrario, la gratuità del servizio offerto[9].

Le pratiche scorrette che avevano portato alla irrogazione delle sanzioni possono essere così riassunte:

– la pratica a) – pratica ingannevole, in violazione degli artt. 20, 21 e 22 del Codice del consumo, si sarebbe realizzata in quanto il professionista non avrebbe informato adeguatamente e immediatamente l'utente, in fase di attivazione dell'account, dell'attività di raccolta e utilizzo, per finalità informative e/o commerciali, dei dati che egli stava cedendo, rendendolo edotto della sola gratuità della fruizione del servizio, così da indurlo ad assumere una decisione di natura commerciale (la registrazione a Facebook) che non avrebbe altrimenti preso;

– la pratica b) – pratica aggressiva, in violazione degli artt. 20, 24 e 25 del Codice del consumo, si sarebbe realizzata invece in ragione dell'indebito

[8] *Ibidem*.

[9] Questo il testo della dichiarazione rettificativa: «*Le società Facebook Inc. e Facebook Ireland Ltd. non hanno informato adeguatamente e immediatamente i consumatori, in fase di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti. In tal modo hanno indotto i consumatori a registrarsi sulla Piattaforma Facebook, enfatizzando anche la gratuità del servizio. Inoltre, hanno esercitato un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono, senza espresso e preventivo consenso, la trasmissione e l'uso da parte di Facebook e di terzi, per finalità commerciali, dei dati che li riguardano. L'indebito condizionamento deriva dalla preselezione da parte di Facebook delle opzioni sul consenso alla trasmissione dei propri dati da/a terzi, attraverso in particolare l'automatica attivazione della funzione "Piattaforma attiva", unitamente alla prospettazione, a seguito della disattivazione di tale Piattaforma, di rilevanti limitazioni di fruibilità del social network e dei siti web/app di terzi, più ampie e pervasive rispetto a quelle effettivamente applicate. Tali pratiche sono state valutate scorrette, ai sensi degli artt. 21, 22, 24 e 25 del Decreto Legislativo, n. 206/2005 (Codice del consumo). L'Autorità ha disposto la pubblicazione della presente dichiarazione rettificativa ai sensi dell'articolo 27, comma 8, del Codice del consumo. (provvedimento adottato nell'adunanza del 29 novembre 2018 e disponibile sul sito www.agcm.it)*».

condizionamento che Facebook avrebbe esercitato nei confronti dei consumatori registrati, che in cambio dell'utilizzo di FB, sarebbero stati costretti a consentire a FB e a terzi la raccolta e l'utilizzo, per finalità informative e/o commerciali, dei dati che li riguardavano (informazioni del proprio profilo FB, quelle derivanti dall'uso di FB e dalle proprie esperienze su siti e app di terzi), in modo inconsapevole e automatico, tramite un sistema di preselezione del consenso alla cessione e utilizzo dei dati, risultando indotti 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, conseguenti alla deselezione.

Avverso il provvedimento n. 27432/2018 di AGCM, Facebook Ireland ha proposto ricorso al TAR.

Il TAR Lazio, sez. I, con sentenza 10 gennaio 2020, n. 260[10] ha accolto parzialmente il ricorso di Facebook Ireland Ltd, confermando l'atto sanzionatorio dell'Antitrust nella parte in cui si riferisce alla pratica a) (pratica commerciale ingannevole) e annullando la parte relativa alla pratica b) (pratica commerciale aggressiva). Di conseguenza sono state confermate le sanzioni inflitte solamente in riferimento alla pratica a).

Nei confronti della sentenza del TAR si sono poi appellate al Consiglio di Stato, per opposti motivi, entrambe le parti in causa. Con la decisione n. 2631 del 29 marzo 2021 i giudici di Palazzo Spada, disposta la riunione dei due ricorsi in appello, hanno deciso di respingerli entrambi confermando la sentenza del TAR Lazio in via definitiva.

Tra i motivi di riforma della sentenza di primo grado proposti dalla piattaforma, la ricorrente lamentava il difetto assoluto del potere di sanzionare Facebook Inc. e Facebook Ireland Ltd. in capo all'Autorità antitrust, per mancanza di pratiche commerciali da vagliare «*attesa l'assenza di qualsiasi coinvolgimento di un corrispettivo patrimoniale*[11]» da parte dei consumatori[12]. Secondo la Big Tech, infatti, gli utenti non potrebbero mai cedere i

---

[10] Tra gli innumerevoli commenti si vedano: A.L. TARASCO, M. GIACCAGLIA, *Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo,* in *Dir. econ.*, 2/2020; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, p. 126 ss.; I.M. ALAGNA, N. CENTOFANTI, *La consumerizzaizone della privacy tra California Consumer Privacy Act e GDPR*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Milano, 2021, p. 129 ss.; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, 4/2020, p. 650 ss.; M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *federalismi.it*, 13 maggio 2020, p. 226 ss.

[11] Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631, par. 4, punto n. 1.

[12] Sempre in ragione dell'assenza di un interesse economico e di prassi commerciali, ricorre-

propri dati come corrispettivo di una prestazione, essendo la gestione dei dati personali un'attività a carattere non patrimoniale, ove non è coinvolto l'interesse economico del singolo utente. Pertanto, nel sostenere la assoluta inapplicabilità della disciplina consumeristica, Facebook afferma che l'unica normativa applicabile al caso di specie sarebbe quella relativa alla protezione dei dati personali [13].

Nella sua decisione il Consiglio di Stato ha evitato di pronunciarsi sulla qualificazione giuridica dei dati personali, soffermandosi invece in modo più esteso sul nodo della presunta inapplicabilità della disciplina a tutela del consumatore. Richiamando ampie parti della decisione del TAR, i giudici di Palazzo Spada hanno chiarito che le due discipline (privacy e consumeristica) sono complementari, ed hanno escluso che l'omessa informazione sullo sfruttamento dei dati dell'utente a fini commerciali sia una questione disciplinata esclusivamente dal GDPR. La disciplina recata dalla Direttiva 2005/29 sulle pratiche commerciali sleali e quella prevista nel Regolamento 2016/679 in materia di *data protection* possono infatti garantire – congiuntamente – una tutela multilivello dei diritti delle persone fisiche «*anche quando un diritto personalissimo sia sfruttato a fini commerciali* [14]», peraltro senza che si verifichi alcun effetto plurisanzionatorio [15].

Come poc'anzi anticipato, nella decisione n. 2631/2021 il Consiglio di Stato non si è pronunciato sulla qualificazione dei dati personali come beni *extra commercium*. Cionondimeno, tale argomentazione utilizzata dalla difesa di Facebook per contestare il provvedimento dell'Antitrust ci consentirà nelle prossime pagine di affrontare una questione cruciale nella discussione sulla natura giuridica del dato personale, e di sgomberare il campo da alcune ambiguità.

---

rebbe un difetto assoluto di attribuzione *ratione materiae* con riferimento all'Autorità garante della concorrenza e del mercato, in favore del Garante per la protezione dei dati personali, e più specificatamente dell'Autorità capofila irlandese. Cfr. *ivi*, punto n. 5.

[13] «*Né può immaginarsi possibile […] che gli utenti cedano i propri dati a FB quale corrispettivo per la fornitura del servizio né che la trasmissione di dati personali possa attenere ad una attività economicamente valutabile, se non invece e al più, ad un mero profilo di tutela di alcuni diritti fondamentali della persona di carattere non patrimoniale*». *Ivi*, punto n. 1).

[14] *Ivi*, par. 8.

[15] *Ivi*, par. 7. Come è stato evidenziato in dottrina, il consumatore-interessato potrebbe così vedere sommati i due gruppi di rimedi, senza che l'uno escluda l'altro. Cfr. G. VERSACI, *La contrattualizzazione*, cit., p. 205.

3. *Alcune riflessioni sulla sentenza del Consiglio di Stato. L'"equivoco" dei dati personali come beni* extra commercium *alla luce dell'*habeas data

Come è emerso dalla sintesi della controversia appena proposta, la difesa di Facebook rispetto alle accuse di violazione del Codice del consumo si è incentrata principalmente sulla non-applicabilità della normativa consumeristica alla condotta oggetto di sanzione da parte di AGCM, poiché nel caso di specie l'unica disciplina applicabile – anche in base ad un principio di specialità [16] – sarebbe stata quella in materia di protezione dei dati personali. Tale assunto si basa, negli atti di difesa, sulla qualificazione dei dati personali come beni *extra commercium*, attinenti alla sfera dei diritti fondamentali e quindi certamente non commerciabili. Da qui l'impossibilità di configurare l'attività posta in essere da Facebook come attività soggetta al Codice del consumo.

Senza poterci soffermare su questo tema, in questa sede pare comunque utile evidenziare che la difesa della piattaforma sembra muovere – sebbene in modo strumentale – da un equivoco di fondo.

Come già ricordato, Facebook sostiene che gli utenti non potrebbero mai cedere i propri dati come corrispettivo di una prestazione, poiché i dati personali non possono essere considerati merce, costituiscono un bene *extra commercium*, trattandosi di diritti fondamentali della persona: per questa ragione non possono essere venduti, scambiati o comunque ridotti a mero interesse economico [17]. Ma, ed è questo il punto, nella logica della normativa sulla *data protection*, i dati personali in quanto tali non vengono mai considerati oggetto di un diritto fondamentale. Piuttosto è la *protezione* dei dati personali a costituire un diritto. A partire dalla c.d. Direttiva madre n. 95/46, che com'è noto ha dotato la allora Comunità di un primo modello europeo di protezione dei dati personali, oggetto della regolazione è il trattamento dei dati personali.

[16] Ci si riferisce al passaggio in cui la difesa di Facebook afferma che per dare corretta applicazione alla Direttiva 2005/29 sulle pratiche commerciali sleali, in tema di obblighi di informazione si dovrebbe applicare la normativa europea e nazionale sulla privacy, in quanto è l'art. 3 della Direttiva a prevedere un principio di specialità per la disciplina di aspetti specifici delle pratiche commerciali; al passaggio in cui dall'applicazione dell'art. 288, comma 2, TFUE sull'obbligatorietà dei regolamenti e la prevalenza degli stessi rispetto ad altre norme interne contrastanti, si fa derivare la prevalenza del Regolamento privacy su qualsivoglia atto legislativo nazionale in tema di pratiche commerciali scorrette; infine alla asserita violazione del principio di specialità in materia sanzionatoria (cfr. par. 2, 3, 4 della sentenza in commento). Insomma, un principio rafforzato di specialità imporrebbe la sola applicazione della disciplina posta dal Regolamento 679/2016.

[17] Cfr. par. 4 della sentenza in commento.

Come ben ricostruito anche da Giovanni Buttarelli nel suo volume del 1997 su *Banche dati e tutela della riservatezza*, il legislatore europeo già allora fece una scelta esplicita per una impostazione della regolazione incentrata sul trattamento piuttosto che sui dati [18].

Il lungo percorso della protezione dei dati come diritto fondamentale ha visto poi una affermazione nell'Unione europea con il suo riconoscimento all'interno della Carta di Nizza, approvata nel 2000. Nel 2009 la Carta dei diritti fondamentali dell'Unione europea ha assunto lo stesso valore giuridico dei Trattati. Il primo paragrafo dell'art. 8 della Carta dei diritti dell'UE recita: "*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*" [19], mentre l'art. 16 del Trattato sul funzionamento dell'Unione proclama il diritto di ogni individuo alla protezione dei propri dati personali, attribuisce al Parlamento europeo e al Consiglio il potere di stabilire norme relative alla protezione delle persone fisiche in relazione al trattamento dei propri dati personali, e affida il controllo sul rispetto di tali norme ad autorità amministrative indipendenti [20]. Infine, anche nella dicitura prescelta per l'art. 1 del GDPR, il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Dunque non vi è ragione di affermare che i dati personali *in quanto tali* siano un diritto fondamentale, e che per questa ragione non possano essere oggetto di scambio economico [21]. Al contrario, l'ordinamento tutela il pieno diritto degli individui alla protezione riguardo al trattamento di tali dati, cioè alla autodeterminazione informativa. La consapevolezza di poter controllare il proprio patrimonio informativo, e con esso la propria identità personale, anche e soprattutto nel contesto della digitalizzazione e dello sviluppo delle tecnologie dell'informazione e della comunicazione, segna un passaggio fonda-

---

[18] G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria e internazionale*, Milano, 1997, p. 45 ss.

[19] Per un recentissimo commento all'art. 8 si veda M. BASSINI, O. POLLICINO, *Art. 8*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, p. 35 ss.

[20] Si veda F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

[21] A possedere le caratteristiche dei diritti fondamentali, tra cui l'inalienabilità e l'indisponibilità, sarà piuttosto il diritto alla protezione dei dati personali, che si realizza attraverso il rispetto dell'apparato di norme relativo al loro trattamento.

mentale. Da una concezione della privacy intesa solamente come difesa della riservatezza e protezione della propria sfera personale dalle intrusioni esterne, si è andati muovendo verso l'*habeas data*[22], un diritto dinamico di controllo e gestione del proprio patrimonio informativo.

Si potrebbe dire, sintetizzando, e richiamando la lucidissima riflessione di Rodotà, che il controllo del proprio patrimonio informativo, ovvero l'autodeterminazione informativa, quindi la possibilità di decidere sui propri dati, sia strumentale alla realizzazione di un intero ventaglio di diritti e libertà fondamentali[23]. Cosa ben diversa è affermare che un dato in quanto tale costituisca *in sé* un diritto fondamentale. Affermazione che vale a maggior ragione in questo momento storico in cui gli algoritmi di *machine-learning*, e più in generale i sempre più sofisticati sistemi di Intelligenza artificiale, sono in grado di produrre informazioni personali anche come risultato dell'elaborazione di dati non personali[24].

Il legislatore europeo ha dotato l'interessato di un ventaglio di strumenti che gli consentono di svolgere un controllo effettivo sui propri dati. Mi riferisco al sistema di norme costituito dagli artt. 15 e seguenti del Regolamento europeo 2016/679[25], che comprende tra gli altri il diritto di accesso, di rettifica, di cancellazione dei propri dati, il diritto di chiedere ed ottenere il trasferimento dei propri dati da un fornitore di servizi ad un altro[26], cui va aggiunta la possibilità di prestare il proprio consenso informato[27] al trattamento dei dati personali[28].

---

[22] Cfr. S. RODOTÀ, *Il mondo nella rete, Quali diritti, quali vincoli*, Roma-Bari, 2014.

[23] S. RODOTÀ, *Privacy, libertà, dignità*. Discorso conclusivo alla Conferenza internazionale sulla protezione dei dati, Wroclaw (PL), 14-16 settembre 2004.

[24] Sul punto cfr. V. PAGNANELLI, *Conservazione dei dati e sovranità digitale*, in *Riv. it. inf. e dir.*, 1/2021, p. 15 ss.

[25] Per un commento agli articoli citati si vedano, *ex plurimis*, G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, L. BOLOGNINI, E. PELINO, *Codice della disciplina privacy*, Milano, 2019; R. PANETTA, (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019.

[26] Una interessante lettura del diritto alla portabilità nel bilanciamento tra privacy e concorrenza è offerta in E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 222-223. Gli aa. sottolineano come l'art. 20 del GDPR potenzi il controllo dell'interessato sulla circolazione dei propri dati, intesi come *asset* per i servizi digitali.

[27] A norma dell'art. 4, n. 11, del Regolamento europeo 2016/679 il consenso è una manifestazione di volontà libera, specifica, informata e inequivocabile.

[28] Fabio Bravo ricorda come il consenso sia uno strumento fondamentale della autodeterminazione informativa, concorrendo a delineare l'identità personale dell'interessato e al contempo

Inoltre, specialmente nei rapporti tra utenti e piattaforme web, rileva certamente come strumento di *empowerment* dell'interessato il diritto alla limitazione [29], che come è stato notato in dottrina [30] appare idoneo ad espandere i poteri di controllo dell'interessato in un contesto di vertiginosi sviluppi tecnologici che rendono difficile tener traccia dei flussi dei dati. L'esercizio del diritto di limitazione riduce infatti le attività di trattamento consentite al titolare alla mera conservazione dei dati, bloccando tutto il resto delle operazioni astrattamente possibili ed in questo modo ristabilendo un equilibrio tra le posizioni di titolare ed interessato. Lo stesso dicasi per il diritto di opposizione, previsto dall'art. 21 del Regolamento 2016/679, che garantisce all'interessato la possibilità di opporsi in qualsiasi momento a trattamenti posti in essere per motivi di interesse pubblico o di esercizio di pubblici poteri o sulla base del legittimo interesse del titolare, compresi i trattamenti di profilazione [31]. Il diritto di autodeterminazione informativa dell'interessato è rafforzato e completato con il riconoscimento del diritto di revocare il consenso prestato, in qualunque momento e con la stessa facilità con cui è stato accordato [32].

Dunque a ben vedere, la disciplina del GDPR garantisce all'interessato la possibilità di disporre dei propri dati, attraverso lo strumento del consenso, e con l'esercizio di una lunga serie di diritti, e in ogni caso egli ha il diritto di essere informato in modo trasparente e chiaro rispetto ad ogni trattamento che riguardi i suoi dati personali.

Il Regolamento europeo n. 2016/679 pone delle regole per il corretto e trasparente trattamento, quali il rispetto dei principi fondamentali del trattamento medesimo (liceità, correttezza, trasparenza, minimizzazione, limitazione delle finalità), l'individuazione della base giuridica che lo legittimi, i già citati diritti/doveri di informazione. È su questi aspetti che si basa il vaglio sul rispetto della normativa privacy, e si tratta di adempimenti e regole che ben si

---

permettendo allo stesso di avere il controllo sulla circolazione dei propri dati, cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d. lgs. 10 agosto 2018 n. 101*, Torino, 2019, p. 133.

[29] Previsto dall'art. 18 del GDPR.

[30] Cfr. G. CRISTOFARI, *Il diritto alla limitazione del trattamento*, in R. PANETTA, (a cura di), *Circolazione e protezione dei dati personali*, cit., p. 215 ss.

[31] Per un commento si veda *ivi*, M. FRAIOLI, *Il diritto di opposizione e la revoca del consenso*, p. 239 ss.

[32] Regolamento europeo 2016/679, art. 7, par. 3. Peraltro, è stato notato come la facoltà di revocare il consenso mal si concili con una logica proprietaria, e quindi con la possibilità di disporre dei dati personali come moneta di scambio, in quanto proprio in ragione del diritto di revoca, una volta prestato il consenso, l'interessato-proprietario continua a mantenere il controllo sul trattamento dei dati. Cfr. G. VERSACI, *La contrattualizzazione*, cit., p. 93.

possono collocare in una tutela multilivello posta a garanzia dei diritti delle persone fisiche, come bene evidenziato nella sentenza del Consiglio di Stato. Non compaiono invece divieti espliciti relativi alla commercializzazione dei dati. Anzi, lo ribadiamo, il GDPR ha la doppia finalità di tutelare le persone fisiche riguardo al trattamento dei loro dati e di stabilire norme per la libera circolazione degli stessi. Appare dunque condivisibile la scelta del Consiglio di Stato di affrontare il tema della patrimonializzazione dei dati personali evitando di pronunciarsi sulla natura giuridica dei dati medesimi, ma concentrandosi piuttosto sull'analisi degli elementi fattuali a disposizione, vale a dire sull'attività di elaborazione delle informazioni degli utenti che viene sistematicamente svolta da Facebook, e che costituisce il suo principale business.

4. *Piattaforme digitali e profilazione degli utenti: il valore economico del* targeting

Il Collegio affronta la questione del valore economico dei dati personali, e della loro commerciabilità, offrendo una considerazione molto acuta: «*Orbene, se pure si volesse aderire alla tesi della odierna parte appellante secondo la quale il dato personale costituisce una* res extra commercium*, la patrimonializzazione del dato personale, che nel caso di specie avviene inconsapevolmente […] costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali*[33]».

In un passaggio di poco successivo il Consiglio di Stato individua esattamente il nocciolo della questione: «*nell'appena descritta accezione non viene in emersione la commercializzazione del dato personale da parte dell'interessato, ma lo sfruttamento del dato personale reso disponibile dall'interessato in favore di un terzo soggetto che lo utilizzerà a fini commerciali*[34]».

Il Consiglio di Stato precisa infatti che non sono i dati *in sé* ad avere valore, ma l'attività di profilazione che viene eseguita in seguito alla raccolta degli stessi, o ancora più precisamente la fornitura dei risultati di tali elaborazioni a terzi (i veri clienti delle piattaforme digitali) che le utilizzeranno per i loro fini commerciali.

Ed infatti, attraverso l'analisi algoritmica dei dati raccolti il Social network riesce a realizzare profili sempre più dettagliati degli utenti, per poter offrire un sempre migliore servizio ai propri clienti, cui vende spazi pubblicitari in

[33] Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631, par. 8.

[34] *Ibidem*.

cui l'incontro con il potenziale acquirente / elettore / seguace è efficientato ai massimi livelli [35].

Come un'autorevole dottrina ha illustrato in modo analitico e spietato, riferendosi alla attività di sorveglianza di Google, «*Non siamo più il soggetto e nemmeno, come ha invece affermato qualcuno, il prodotto delle vendite di Google. Siamo invece gli oggetti dai quali vengono estratte le materie prime, espropriate per le proprie fabbriche di previsioni. Il prodotto di Google sono le previsioni sui nostri comportamenti, che vengono vendute ai suoi reali clienti, e non a noi. Noi siamo i mezzi per lo scopo di qualcun altro* [36]». Si tratta dello sfruttamento del *surplus comportamentale* degli utenti. In questa fase i dati personali vengono monetizzati, poiché le elaborazioni effettuate dai *gatekeeper* vengono poi vendute ai migliori acquirenti.

Non è possibile qui svolgere considerazioni approfondite sul tema del riconoscimento agli utenti dei servizi online di un equo corrispettivo economico per il conferimento dei propri dati personali, effettuato durante l'utilizzo dei servizi medesimi. Sia pur brevemente, sia però consentito ricordare che una serie di limiti oggettivi fanno ritenere tale prospettiva di difficile realizzazione pratica. Prima fra tutti si pone la difficoltà di quantificare il valore economico dei dati di un singolo internauta [37]. Il valore di tali dati risulterebbe in ogni caso esiguo, posto che per le piattaforme digitali sono i dati personali dell'utenza complessivamente considerata ad avere rilevanza [38].

---

[35] Sul business model di Google e Facebook si veda il report di Amnesty International, *Surveillance Giants: how the business model of Google and Facebook threatens human rights*, pubblicato nel 2019. Si veda anche A.L. TARASCO, M. GIACCAGLIA, *Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo*, in *Dir. econ.*, 2/2020, pp. 282-283.

[36] S. ZUBOFF, *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, pp. 104-105.

[37] Si veda sul punto G. VERSACI, *La contrattualizzazione,* cit., p. 19.

[38] Cfr. *ivi*, p. 48-49. Nel parere 4/2017 il Garante europeo per la protezione dei dati personali si sofferma sulla difficoltà di individuare il valore economico che potrà derivare dal trattamento dei dati, con conseguenze anche nella possibilità di gestire i rapporti contrattuali: «*[…] it should be reminded that if personal data might be compared with money to some extent, they are obviously not identical. Giving his/her data does not deprive the individual from the possibility to give the same data again to another provider. Moreover, as said above, the individuals cannot evaluate the value that will be created with their data. The consequence for the providers is also different: when an obligation of restitution exists, such restitution is easy when a price was paid, while is more difficult when data were exchanged. There is indeed little possibility to evaluate the value of personal data, and therefore to "reimburse" the individual on the basis of the value of these data, or even to give him/her a compensation for the value gained by the supplier in the transaction*». Cfr. European Data Protection Supervisor, Opinion 4/2017, cit., p. 9.

Tornando ora al tema dello sfruttamento del *surplus comportamentale*, è utile ricordare che le attività di *targeting* degli utenti dei Social media ed i rischi ad esse connessi sono stati analizzati nelle Linee guida pubblicate dall'European Data Protection Board il 13 aprile 2021[39]. Anche il Comitato europeo ha evidenziato come l'aumentata capacità di svolgere attività di *targeting* possa causare un incremento dei rischi per i diritti e le libertà delle persone fisiche, e che le campagne di *targeting* sempre più avanzate possono avere conseguenze rilevanti sia dal punto di vista della protezione dati che da quello della disciplina della concorrenza[40]. I due piani sembrano essere inscindibilmente connessi nel mercato e nella società digitale.

Vi è da chiedersi dunque quali siano gli strumenti forniti dalla legislazione per poter riequilibrare le posizioni delle grandi piattaforme che beneficiano in via esclusiva di tutti i vantaggi recati dallo sfruttamento dei dati personali raccolti e degli utenti che sembrano completamente impotenti, oltre che catturati dall'effetto rete e dai *lock-in*. Sembrano due i versanti di azione sui quali la normativa in materia dei dati personali può avere un rilievo: da una parte l'imposizione di stringenti obblighi ai giganti della rete / titolari del trattamento dei dati, dall'altra il rafforzamento dei diritti e delle prerogative degli utenti / interessati. Nei prossimi paragrafi vaglieremo dunque le possibilità di riequilibrio delle parti attraverso l'applicazione delle regole di *data protection*.

5. *L'impatto privacy sulle Big Tech*

Gli artt. 12 e seguenti del Regolamento 2016/679 pongono in capo al titolare del trattamento precisi obblighi di informazione nei confronti degli interessati, tra cui compare la trasparenza.

Il considerando 39 del GDPR specifica che dovrebbero essere trasparenti le modalità con cui i dati personali sono raccolti, utilizzati, consultati o altrimenti trattati, in particolare per quanto attiene alle finalità del trattamento. Inoltre la stessa disposizione richiede che gli interessati siano sensibilizzati rispetto ai rischi del trattamento e alle modalità di esercizio dei loro diritti. A parere di chi scrive, il considerando 39 contiene, in estrema sintesi e chiarezza, tutti gli strumenti di cui la disciplina in materia di protezione dei dati personali è dotata per riequilibrare il mercato e limitare il potere delle piattaforme di-

[39] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users*, 13 aprile 2021.

[40] *Ivi*, p. 9.

gitali. Da una parte l'imposizione di obblighi di trasparenza rispetto ai trattamenti effettuati, dall'altra la cura della consapevolezza degli interessati rispetto a tali trattamenti, in modo che essi possano sempre esercitare il loro diritto alla autodeterminazione informativa.

Sul primo versante, ad una verifica del rispetto degli obblighi di trasparenza e informazione posti dal GDPR da parte di Facebook si può apprendere che l'informativa pubblicata sul sito internet contiene l'elencazione delle finalità perseguite con il trattamento, così come le basi giuridiche che lo rendono lecito. In alcuni casi si fa riferimento al rapporto contrattuale, in altre al consenso esplicito dell'utente. Viene anche esplicitato il meccanismo per cui le informazioni raccolte vengono elaborate e fornite ai clienti della piattaforma (cioè agli operatori economici interessati ad acquistare spazi pubblicitari).

Nelle condizioni d'uso [41] l'azienda chiarisce che «*Anziché richiedere all'utente un pagamento per l'utilizzo di Facebook o degli altri prodotti e servizi coperti dalle presenti Condizioni, Facebook riceve una remunerazione da parte di aziende e organizzazioni per mostrare agli utenti inserzioni relative ai loro prodotti e servizi. Utilizzando i Prodotti di Facebook, l'utente accetta che Facebook possa mostrargli inserzioni che Facebook ritiene pertinenti per l'utente e per i suoi interessi. Facebook usa i dati personali dell'utente per aiutare a determinare quali inserzioni mostrare all'utente*» [42].

Poco più avanti Facebook informa l'utente rispetto ai dati personali che vengono condivisi con gli Inserzionisti: «*Forniamo agli inserzionisti report sui tipi di persone che visualizzano i loro annunci e sulle prestazioni degli annunci. Non condividiamo tuttavia informazioni che consentono di identificarti (informazioni quali nome o indirizzo e-mail utilizzabili per contattarti o identificarti), salvo tua autorizzazione. Ad esempio, forniamo dati demografici generali e informazioni sugli interessi agli inserzionisti (ad es. un'inserzione è stata vista da una donna di età compresa fra 25 e 34 anni che vive a Madrid e a cui piace l'ingegneria software) per aiutarli a capire meglio il proprio pubblico. Inoltre confermiamo quali inserzioni di Facebook hanno portato a un acquisto o all'esecuzione di un'azione con un inserzionista*».

Nella sezione dell'informativa ove vengono elencate le basi giuridiche che rendono leciti i trattamenti, questi ultimi sono suddivisi tra quelli necessari a fornire i servizi contrattuali e quelli basati sul consenso. Vengono poi elencati i

---

[41] Consultabili al link https://www.facebook.com/legal/terms/update. Ultima consultazione effettuata il 15 novembre 2021.

[42] Versaci ricorda come lo scambio tra prestazioni di carattere patrimoniale e dati personali fosse consuetudine commerciale ben prima dell'erompere del mercato digitale. Cfr. G. VERSACI, *La contrattualizzazione,* cit., pp. 137-138.

trattamenti basati sul legittimo interesse del titolare che consistono nel «*Fornire report precisi e affidabili ai nostri inserzionisti, sviluppatori e partner per garantire prezzi e statistiche accurati sulle prestazioni e per dimostrare il valore che i nostri partner ottengono usando i Prodotti offerti dalle aziende di Facebook; aiutare gli inserzionisti, sviluppatori e altri partner a comprendere i clienti e migliorare le proprie aziende, convalidare i nostri modelli e valutare l'efficacia dei contenuti e della pubblicità online all'interno e all'esterno dei Prodotti offerti dalle aziende Facebook*[43]».

Questa sommaria ricognizione pare confermare che Facebook abbia adempiuto agli obblighi di informazione che il Regolamento 2016/679 pone in capo al titolare del trattamento: l'attività commerciale dell'azienda è illustrata nell'informativa sull'utilizzo dei dati personali, in termini piuttosto espliciti e senza mistificazioni. Il social network raccoglie dati, profila gli utenti e vende agli inserzionisti preziose informazioni che consentiranno loro di aumentare le vendite (o gli elettori, o i seguaci).

Da questo punto di vista pertanto il rispetto della disciplina privacy non sembra particolarmente oneroso per la piattaforma web, né utile a riequilibrare le posizioni in merito allo strapotere di sfruttamento economico dei dati personali.

A ben vedere, non sorprende che nella controversia tra AGCM e Facebook, emerga una chiara opzione di quest'ultima per l'applicazione della disciplina in materia di protezione dei dati personali, piuttosto che per quella consumeristica.

Al netto delle comprensibili strategie processuali, Facebook ha indicato una alternativa ben precisa alla asserita incompetenza dell'Autorità Antitrust, apportando vari elementi per suffragare la tesi di una competenza del Garante per la protezione dei dati personali. Più precisamente, facendo applicazione di diverse regole contenute nel GDPR, Facebook ha sostenuto che la competenza a giudicare dovesse essere quella dell'Autorità capofila[44], ovvero quella dello Stato membro dove il titolare ha sede. Nel caso di specie, l'Irlanda.

Questa ricostruzione lascia trasparire una qualche percezione della disciplina privacy come meno severa di quella consumeristica. Una sorta di opzione per l'applicazione della normativa a tutela dei diritti fondamentali, piuttosto che per la tutela del mercato. Ciò stupisce ancora meno alla luce della vicenda che ha visto Facebook come destinataria di una sanzione irrogata dal

---

[43] Cfr. https://www.facebook.com/about/privacy/legal_bases. Ultima consultazione effettuata il 15 novembre 2021.

[44] A norma dell'art. 56 del Regolamento 2016/679, che individua l'autorità di controllo competente nei casi di trattamenti transfrontalieri di dati personali, qualificando l'autorità dello Stato dove il titolare ha lo stabilimento principale delle proprie attività come "capofila".

Garante per la protezione dei dati personali a seguito di una richiesta di chiarimenti scaturita dal clamore per la vicenda *Cambridge Analytica*.

Con l'ordinanza ingiunzione del 14 giugno 2019[45] il Garante privacy ha condannato Facebook a pagare un milione di euro. Da un'indagine effettuata dall'Authority era emerso che una applicazione di terze parti, scaricata attraverso la funzione *Facebook login* da 57 utenti italiani, aveva avuto accesso a dati personali di 214.077 altri utenti, senza che questi avessero direttamente scaricato la *app*. Durante l'istruttoria il Garante ha appreso che i dati erano stati raccolti e condivisi in assenza di una informativa completa, comprensiva della elencazione di tutte le finalità del trattamento, e in assenza di valido consenso.

Ci si chiede quanto, a posteriori, e a distanza di oltre un anno dai fatti contestati, questo tipo di intervento sanzionatorio sia stato efficace e tutelante, e quanto effettivamente una sanzione da un milione di euro abbia impattato su Facebook. Il sistema delle sanzioni amministrative economiche comminate ai giganti del web sembra essere in buona misura inefficace, soprattutto quando interviene a posteriori[46].

Nel tentativo di individuare differenti modalità per incentivare le Big Tech a rispettare le regole, potrebbe essere di una qualche utilità un cambio di prospettiva e di strumenti. Ad esempio potrebbe rivelarsi proficua e probabilmente più impattante sui destinatari l'applicazione di una norma del Codice della privacy come novellato dal d.lgs. n. 101/2018, a cui forse non è stata data ancora sufficiente attenzione per la sua potenzialità nella realizzazione di una efficace tutela multilivello dei diritti anche dei consumatori, sulla base della normativa privacy.

Si tratta dell'art. *2-decies* che stabilisce che «*I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*[47]». Sebbene la violazione di tale norma non sia direttamente collegata ad una sanzione, il trattamento illecito, come è stato evidenziato in dottrina[48], sarebbe certamente riconducibile alla violazione dei prin-

---

[45] Garante per la protezione dei dati personali*, Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. – 14 giugno 2019*, docweb n. 9121486.

[46] Sulle norme europee antitrust che agiscono *ex post* e per questa ragione rischiano di non essere efficaci si veda S. QUINTARELLI, *Capitalismo immateriale*, Torino, 2019, pp. 52-53. L'a. riflette su come una sanzione pari al 2,3% del fatturato annuo di Google, comminata per abuso di posizione dominante, sia inefficace nel momento in cui Google abbia consolidato il controllo del 95% del mercato di interesse: «*È una multa notevole, ma difficilmente sanzionare ex post chi ha vinto può ritenersi un incentivo a comportarsi bene*».

[47] Pizzetti ne critica la formulazione poco chiara, cfr. F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Torino, 2021, p. 133 ss.

[48] L. BOLOGNINI, E. PELINO, *Codice della disciplina privacy*, cit., p. 89.

cipi stabiliti dall'art. 5 del GDPR, e dunque alle sanzioni previste dall'art. 83. Inoltre l'interessato potrebbe sempre esercitare il suo diritto alla limitazione del trattamento dei propri dati personali, ove essi siano trattati in violazione di legge [49].

A parere di chi scrive, attraverso l'inutilizzabilità dei dati si potrebbe andare a toccare gli interessi dei titolari del trattamento, specie quando si tratta di Big Tech, in modo significativo, e questa eventualità potrebbe incidere molto più che una sanzione pecuniaria, alla luce dell'incontestabile valore economico dei dati personali.

Svolta una indagine sull'adempimento degli obblighi di trasparenza da parte di una Big Tech, muoviamo ora verso la seconda prospettiva di intervento qui proposta, ovvero l'accrescimento del controllo effettivo degli utenti / interessati sui propri dati.

6. *Europa 2030: verso una gestione più consapevole dei dati personali?*

Ad avviso di chi scrive, di fronte alle innumerevoli e complesse attività di elaborazione dei dati personali degli utenti poste in essere dalle Big Tech, l'interessato / utente / proprietario dei dati personali dovrebbe vedere rafforzati gli strumenti a tutela dei propri diritti.

Di fronte a questa circostanza tornano certamente in rilievo le appena richiamate regole di informazione cui il social network deve sottostare e gli strumenti che il GDPR offre all'interessato per controllare i propri dati personali, primo fra tutti il consenso al trattamento dei dati personali ai fini di profilazione.

Com'è noto l'art. 22 del GDPR pone un divieto generale all'adozione di decisioni completamente automatizzate, compresa la profilazione, che producano effetti giuridici o impattino comunque in modo significativo nella sfera personale degli interessati [50]. È ormai sempre più evidente infatti come le deci-

---

[49] Lo prevede l'art. 18, par. 1, lett. b), GDPR.

[50] Per un commento all'art. 22 si veda F. LAGIOIA, G. SARTOR, A. SIMONCINI, *Art. 22*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, cit., p. 378 ss. Non possiamo in questa sede soffermarci sulle questioni relative ai principi applicabili alle decisioni basate su trattamenti interamente automatizzati e sulle discriminazioni algoritmiche. È noto che i principi di conoscibilità e di comprensibilità degli algoritmi, il principio di non esclusività della decisione algoritmica, infine il principio di non discriminazione algoritmica possano essere tratti dalla lettura degli artt. 13, 14 e 22 del GDPR, oltre che del considerando 71. Su questi aspetti si rinvia certamente a A. SIMONCINI, S. SUWEIS, *Il cambio*

sioni algoritmiche possano impattare seriamente sui diritti e le libertà delle persone fisiche, che attraverso l'osservazione dei loro comportamenti sono inserite a loro insaputa in *cluster* cui verranno applicate determinate condizioni commerciali piuttosto che altre, o cui verranno fornite informazioni – e pubblicità – mirate [51].

Al divieto di profilazione enunciato nel primo paragrafo dell'art. 22 del GDPR segue una serie di eccezioni che, corredate da misure appropriate per tutelare diritti, libertà e interessi legittimi degli interessati, rendono leciti i trattamenti altrimenti vietati. Tra di esse compare il consenso esplicito del *data subject*.

Vi è da chiedersi però quanto questo consenso risponda ai requisiti di legge e quanto sia tutelante per l'interessato. Nelle Linee guida del Gruppo di lavoro Articolo 29 sul consenso [52] viene posto l'accento sui requisiti per cui l'espressione di volontà possa dirsi realmente informata. In particolare si sottolinea il fatto che l'interessato debba essere messo in condizione di comprendere *a cosa* sta acconsentendo [53].

La capacità di comprendere i meccanismi sottesi ai servizi digitali è di primaria importanza. Infatti i cittadini informati possono scegliere cosa condividere e cosa no, ma ulteriormente possono difendersi dai meccanismi di cui essi stessi sono vittime una volta inseriti nei *cluster* [54], anche con condotte "reattive" [55].

---

di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, in *Riv. fil. dir.*, I, giugno 2019, p. 86 ss., e A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019, p. 63 ss.

[51] Sulla profilazione passiva sia consentito rinviare a V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *Osservatorio sulle fonti*, 2/2021: «*Sempre più si verifica una tipologia di discriminazione algoritmica che può essere definita come profilazione passiva, in cui ciò che viene profilato è un contesto, più che un singolo individuo. Dalla osservazione di quante più persone che si muovono all'interno dello stesso contesto, e dei loro comportamenti, sarà possibile desumere – prevedere – il comportamento di singoli individui non profilati personalmente ma ricondotti per mezzo di altre correlazioni a quel determinato cluster*». Le mie osservazioni si basano su G. D'ACQUISTO, *Nuovi tipi di profilazione, ecco i rischi privacy: servono tutele più ampie*, in *AgendaDigitale*, 19 aprile 2019.

[52] Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del Regolamento (UE) 2016/679*, WP259 rev.01.

[53] *Ivi*, p. 15.

[54] Una maggiore consapevolezza potrebbe consentire di coordinare singole istanze per organizzare non solo forme di tutela ma vere e proprie modalità di gestione delle basi di dati collettive. Tale gestione, che in futuro potrebbe essere coordinata dai privati, certamente oggi potrebbe già avvenire per mano delle Pubbliche Amministrazioni, detentrici di enormi basi di dati appartenenti ai cittadini. «*Each of us is a producer of a commodity (personal data) which can present economic significance only if it is joined with other data. The larger the size of the data-base,*

Ma vi è una questione a monte, che emerge nonostante il GDPR preveda un "sistema a supporto dell'autodeterminazione informativa". Invero potrebbe verificarsi l'eventualità che l'interessato non sia in grado di comprendere le informazioni che gli vengono fornite dal titolare del trattamento, e che lo stesso non sia consapevole delle possibilità di utilizzo degli strumenti di controllo sui propri dati che gli sono garantiti dal Regolamento 2016/679. L'autorizzazione responsabile all'utilizzo dei propri dati presuppone infatti una consapevolezza sull'uso degli stessi, manifestata con piena cognizione [56].

L'alfabetizzazione digitale è un passaggio obbligato di consapevolezza, ed una realtà caratterizzata da elementi di novità assoluta rispetto al passato esige che ai cittadini siano garantiti gli strumenti per leggere e affrontare i rischi e le opportunità ad essa connessi.

Indubbiamente il tema del *digital divide*, ovvero l'impossibilità per parte della cittadinanza di godere dei vantaggi legati alla digitalizzazione e al progresso tecnologico, è dirimente. I principali documenti programmatici della Commissione europea contengono riferimenti all'obiettivo del superamento del divario digitale. È possibile individuare il tema dell'alfabetizzazione informatica e dell'incremento delle competenze digitali anche nel progetto che delinea una *Strategia europea dei dati* [57] ed il futuro digitale dell'Unione europea: in quella comunicazione la Commissione aveva sottolineato come la possibilità di utilizzo dei servizi digitali da parte dei cittadini fosse una priorità assoluta, in quanto presupposto di un reale significativo sviluppo dello spazio europeo dei dati [58]. Nella comunicazione *Plasmare il futuro digitale dell'Europa* si sotto-

---

generally, the greater its value. But each of us can extract from our own data – which hypothetically we control – very little use». Cfr. V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the "Big Data Revolution"*, in *Conc. e merc.*, vol. 23/2016, num. Spec. *Big Data e Concorrenza*, p. 33. Sui database come *assets* si veda *ivi*, p. 38 ss.

[55] Ne parla D. LYON in *La cultura della sorveglianza*, Roma, 2020, p. 55: «*Tra le pratiche della sorveglianza vediamo attività reattive, legate all'essere sorvegliati, e anche pratiche proattive di coinvolgimento nei confronti della sorveglianza. Alcuni esempi di pratiche reattive sono l'installazione di una forma di protezione crittografata dall'attenzione sgradita di agenzie per la sicurezza nazionale o corporation di marketing, oppure la decisione di indossare indumenti – cappelli, cappucci, maschere, talvolta chiamati "glamouflage" – che limitano la possibilità di essere riconosciuti dalle videocamere nei luoghi pubblici, o ancora quella di evitare l'uso delle carte fedeltà*».

[56] Cfr. A. FONZI, *Il principio di autodeterminazione dell'utente al cospetto delle nuove tecnologie*, in *dirittifondamentali.it*, 3/2021, 20 dicembre 2021, p. 578. L'a. riflette sull'importanza della consapevolezza dell'utente, affinché esso possa acconsentire con cognizione alle attività di monitoraggio delle proprie preferenze attraverso i c.d. *cookies*.

[57] Sulla Strategia europea dei dati si rimanda al contributo di A. MORETTI, in questo volume.

[58] «*Il funzionamento dello spazio europeo dei dati dipenderà dalla capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione, come pure nelle competenze digita-*

linea come le competenze digitali siano necessarie non solo nel mercato del lavoro, ma per garantire la partecipazione alla vita della società [59].

La Bussola per il futuro digitale dell'Europa per il 2030 (*Digital Compass*), lanciata dalla Commissione europea con la Comunicazione del 9 marzo 2021 [60], contiene una lunga ed articolata sezione riguardante gli obiettivi di incremento delle competenze digitali all'interno dell'Unione. Si fa riferimento all'alfabetizzazione di base dei cittadini europei, in particolare di quella larga parte di essi cui mancano le conoscenze di base, ma anche ai lavoratori specializzati di cui l'economia dei dati ha bisogno. Viene inoltre pianificata la creazione di Centri di ricerca avanzati, in cui gli studiosi potranno contribuire all'avanzamento delle conoscenze del più alto livello, in campo teorico ed applicativo [61].

Il *Digital Compass* prevede una integrazione dell'indice DESI [62] con nuovi indicatori [63], in modo che esso possa costituire la cartina tornasole dell'avan-

li, ed esempio l'alfabetizzazione ai dati (data literacy)», Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "*Una strategia europea per i dati*", COM(2020)66 final, 6.

[59] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "*Plasmare il futuro dell'Europa*", COM(2020)67 del 19 febbraio 2020, p. 6.

[60] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "*Bussola per il digitale 2030: il modello europeo per il decennio digitale*", COM(2021) 118 final.

[61] «*Nel mondo del futuro […] dovremo fare affidamento su cittadini digitalmente autonomi, responsabili e competenti […]. Le competenze digitali di base per tutti i cittadini e l'opportunità di acquisire nuove competenze digitali specialistiche per la forza lavoro sono un prerequisito per partecipare attivamente al decennio digitale […].* E ancora la Commissione precisa come *"Competenze digitali ad ampio raggio dovrebbero inoltre servire a costruire una società che possa fidarsi dei prodotti digitali e dei servizi online, capace di individuare casi di disinformazione e tentativi di frode, di proteggersi da attacchi informatici, dalle truffe e dalle frodi online e in cui i bambini possano imparare a comprendere e a districarsi tra la miriade di informazioni a cui sono esposti online*», cfr. ivi, p. 4-5.

[62] Lo strumento attraverso il quale la Commissione europea valuta annualmente i progressi digitali di ciascuno Stato membro rispetto ai principali ambiti della società e della economia digitale, consente di individuare le aree su cui è necessario agire più velocemente. Ad esempio, nel 2020 l'Italia si colloca al ventesimo posto della classifica DESI su 27 Stati membri. Il dettaglio dei vari settori oggetto di indagine restituisce risultati ancora meno positivi per quanto attiene al c.d. capitale umano. In questo ambito, infatti, l'Italia si colloca al venticinquesimo posto, con percentuali ben al di sotto della media degli altri Stati europei per quanto attiene alle competenze digitali dei propri cittadini. Meno di un italiano su due possiede le competenze digitali di base, meno di uno su quattro quelle avanzate. Solo il 42% delle persone di età compresa tra i 16 e i 74 anni possiede perlomeno competenze digitali di base (la media europea è del 56%) e solo il 22% dispone di competenze digitali superiori a quelle di base (31% nell'UE). Cfr. *Report Italia*, p. 6.

[63] Tra le integrazioni compaiono un indice collegato all'applicazione dell'ICT per il miglioramento della sostenibilità ambientale, e il resoconto sulla percentuale di imprese che offrono

zamento digitale degli Stati membri e al contempo possa guidare Stati e Unione verso gli obiettivi il cui raggiungimento appare più urgente.

Negli intendimenti dell'Unione europea il valore economico dei dati sembra dunque essere inscindibilmente legato allo sviluppo di una società digitale integrata, competente, capace di trarre ricchezza da essi.

7. *Cenni conclusivi*

La vicenda da cui questo elaborato ha preso le mosse, e la sentenza del Consiglio di Stato che l'ha definita, offrono numerosissimi spunti di analisi e riflessione. Questo contributo ne ha esplorato solo una minima parte, procedendo, come si è premesso, con le lenti della disciplina privacy, al fine di vagliare se vi fossero o meno, in tale apparato normativo, strumenti per contribuire al riequilibrio del mercato dei dati.

A questo punto dell'indagine, appare abbastanza evidente come talvolta gli strumenti di tutela e regolazione che dovrebbero in qualche modo imbrigliare il potere delle Big Tech mostrino i loro limiti. Il mercato digitale è sfuggente rispetto alla regolazione ed ai controlli e il volume economico degli introiti dei giganti del digitale rende quasi ogni sanzione poca cosa rispetto ai guadagni. Si potranno certamente ancora sperimentare nuove forme di regolazione, imponendo ai titolari del trattamento adempimenti, valutazioni di impatto, obblighi di informazione nei confronti degli interessati.

Forse però sarebbe utile, per ottenere risultati più soddisfacenti, sia dal punto di vista della tutela dei diritti fondamentali che dal punto di vista consumeristico, accrescere il potere del soggetto debole (l'interessato – consumatore) attraverso una maggiore consapevolezza rispetto a quanto avviene nel mondo digitale. Una felice espressione di Carlo Casonato esprime brillantemente il fallimento del consenso informato, sostituendolo con il "*consenso consapevolmente disinformato*" [64].

Il terreno è scivoloso, ma la questione appare oggi ineludibile, ove si voglia portare la riflessione oltre i rimandi allo scontro frontale e formale tra commerciabilità dei dati e tutela dei diritti della personalità. Appare infatti di poca

---

formazione in materia di ICT, cfr. https://digital-strategy.ec.europa.eu/en/policies/countries digitisation-performance.

[64] «*La categoria giuridica del consenso informato, insomma, è divenuta una mera finzione che, con il nostro consapevolmente disinformato accordo, ci espone quotidianamente ad essere profilati in ogni nostra dimensione e attività*», C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. eu.*, fascicolo speciale, maggio 2019, p. 107.

utilità il rafforzamento dei doveri di informazione e trasparenza che vengono posti in capo al titolare del trattamento / operatore commerciale, quando il destinatario non possieda gli strumenti per comprendere e discernere realmente, quali siano le armi a sua disposizione per autodeterminarsi[65]. L'attività di trattamento dei dati svolta per monetizzarne lo sfruttamento è molto complessa, e gli aspetti puramente tecnici e tecnologici della stessa la rendono spesso difficilmente accessibile anche per gli studiosi di lungo corso. Parrebbe dunque quantomeno ingenuo insistere esclusivamente sul rispetto degli obblighi da parte dei titolari. Questo perché, banalmente, come abbiamo visto, questi obblighi potrebbero essere, ed in alcuni casi sono, adempiuti correttamente[66].

Governare le Big Tech impone una alfabetizzazione digitale, in quanto la consapevolezza degli utenti rispetto all'utilizzo dei propri dati personali dovrà gradualmente prendere il posto dell'approccio paternalistico per cui le Autorità vigilano sull'operato delle grandi *gatekeepers* della rete[67]. Idealmente bisognerebbe forse rinunciare al termine "protezione dati", che contiene in sé il riferimento ad una minaccia costante, per ragionare in termini di scelta sui propri dati in una dimensione che comprenda sia lo sfruttamento economico che la tutela della propria personalità.

La disciplina del trattamento dei dati personali potrà allora davvero fungere da elemento di razionalizzazione e riequilibrio del mercato, intervenendo ove le leggi di settore faticano a contenere lo stra-potere delle piattaforme[68]. Nelle parole del presidente dell'Autorità Garante per la privacy Soro «*la protezione dati può rappresentare un requisito di tutela del consumatore e antitrust by design in quanto consente il governo dell'elemento fondativo dell'"economia a prezzo zero": il dato personale. Regolarne le condizioni di utilizzo, l'ambito di circolazione, le garanzie per l'identità che riflette, significa dunque armonizzare economia e persona, tecnologia e umanità, sicurezza e libertà*[69]».

---

[65] «*Se finora l'autodeterminazione è stata concepita nella prospettiva di esercizio di un diritto, con l'avvento delle nuove tecnologie l'autodeterminazione può essere intesa anche come consapevolezza dell'altrui "inganno" e, quindi, come conseguente capacità di resistere alle altrui pretese di governare la propria vita e di influire sulle proprie scelte*», A. FONZI, *op. cit.*, p. 585.

[66] Cfr. par. 4.

[67] In occasione del Convegno "*La via europea per l'Intelligenza artificiale*" tenutosi a Venezia presso l'Università Ca' Foscari il 25-26 novembre 2021 Andrea Simoncini ha ricordato come la consapevolezza sociale della necessità di una determinata regolazione sia fondamentale perché essa raggiunga il suo scopo. Ciò è gradualmente avvenuto, ad esempio, nel settore della tutela dell'ambiente.

[68] Sulla funzione di correzione del mercato dei diritti fondamentali ved. G. PITRUZZELLA, *L'Europa del mercato e l'Europa dei diritti*, cit., p. 10.

[69] Garante per la protezione dei dati personali, Relazione 2018, Discorso del Presidente Antonello Soro, *L'universo dei dati e la libertà della persona*.

Il Regolamento 2021/694, che istituisce il Programma Europa Digitale, stabilendo una dotazione finanziaria per il periodo 2021-2027, reca tra i cinque obiettivi specifici interconnessi lo sviluppo di competenze digitali avanzate[70]. Eloquente è il considerando 49, nel quale si legge che la trasformazione digitale dovrebbe consentire ai cittadini di accedere ai propri dati personali, usarli e gestirli in modo sicuro a livello transfrontaliero, indipendentemente dal luogo stesso in cui si trovano i cittadini stessi o i dati.

Se questi obiettivi saranno centrati, nell'Europa del 2030 il valore economico dei dati sarà sfruttato (anche) dai cittadini, dopo che avranno consolidato la capacità di gestire il proprio patrimonio informativo in modo autonomo, responsabile e competente[71].

[70] Regolamento UE 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240, art. 7 "*Obiettivo specifico 4 – Competenze digitali avanzate*".

[71] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "*Bussola per il digitale 2030: il modello europeo per il decennio digitale*", COM(2021) 118 final, p. 4.