DIMENSIONE GIURIDICA | LEGAL DIMENSION
Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

4

Il valore economico dei dati personali tra diritto pubblico e diritto privato

a cura di
Elia Cremona, Francesco Laviola, Valentina Pagnanelli

G. Giappichelli Editore

DIMENSIONE GIURIDICA | LEGAL DIMENSION

Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

4

Dimensione giuridica/Legal dimension *si pone in continuità ideale con i "Quaderni del dottorato fiorentino in scienze giuridiche" pubblicati tra il 2013 e il 2017 e vuole porre in evidenza come quanto avviato negli anni passati sia diventato ora un dato strutturale. È questo il caso anzitutto del processo di internazionalizzazione, che ha condotto a un'elaborazione scientifica che è bene sia accolta in una tipologia di pubblicazione capace di evidenziare, anche già nel nome, la rilevanza non puramente municipale del suo contenuto.*

Il percorso costruito attraverso gli anni ha permesso di gettare le basi anche dell'elemento di innovazione introdotto in questa nuova fase, ossia la valorizzazione del lavoro dei dottorandi e di chi si è recentemente formato nel dottorato fiorentino e sta costruendo il proprio percorso scientifico. Dimensione giuridica/Legal dimension *non vuole infatti proporsi come luogo dove i "giovani" sono semplicemente invitati a fornire contributi all'interno di iniziative ideate e dirette da altri, più avanti negli anni e nella carriera, ma intende accogliere principalmente ricerche proposte e coordinate in prima persona proprio da* early career scholars, *pur senza escludere a priori l'inclusione di scritti di studiosi affermati.*

Il valore economico dei dati personali tra diritto pubblico e diritto privato

a cura di

Elia Cremona, Francesco Laviola, Valentina Pagnanelli

IUSTITIAM COLIMUS

G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-2219-2
ISBN/EAN 978-88-921-6259-4 (ebook - pdf)

Volume pubblicato con il contributo del Miur per i progetti di eccellenza 2018-2022.

Stampa: Stampatre s.r.l. - Torino

INDICE

pag.

pag.

PARTE III

LA VIA EUROPEA ALLA REGOLAZIONE
DEL MERCATO DEI DATI TRA "PROTEZIONE" E "CIRCOLAZIONE"

IL VALORE DEI DATI NELL'*EUROPEAN DATA STRATEGY*:
SVILUPPO DELLA PERSONA, DINAMICHE DI MERCATO
E BENESSERE SOCIALE

di *Alessandro Moretti*

DATI E INTELLIGENZA ARTIFICIALE
ALL'INTERSEZIONE TRA MERCATO E DEMOCRAZIA

di *Giovanni De Gregorio* e *Federica Paolucci*

pag.

PARTE IV

DATI PERSONALI E CONTRATTO

pag.

PARTE V

AL DI LÀ DELLA "GRANDE DICOTOMIA" PUBBLICO-PRIVATO

SOLIDARIETÀ DIGITALE E CONDIVISIONE DEI DATI TRA PUBBLICO E PRIVATO

di *Matteo Giannelli*

BIG DATA, BIG TROUBLES: COME SI CONTROLLA IL POTERE DEI DATI?

di *Elia Cremona*

GLI AUTORI

Filippo BAGNI, *Assegnista di ricerca (2019-2020) in Diritto commerciale presso l'Università di Firenze*.

Carlo COLAPIETRO, *Professore ordinario di Diritto costituzionale presso l'Università Roma Tre*.

Elia CREMONA, *Dottorando in Diritto pubblico presso l'Università di Siena*.

Giovanni DE GREGORIO, *Ricercatore PostDoc presso il Centre for Socio-Legal Studies dell'Università di Oxford*.

Guido D'IPPOLITO, *Dottore di ricerca, funzionario presso il Garante per la protezione dei dati personali*.

Matteo GIANNELLI, *Assegnista di ricerca in Diritto costituzionale presso l'Università di Firenze*.

Francesco LAVIOLA, *Dottorando in Diritto pubblico presso l'Università Roma Tre*.

Alessandro MORETTI, *Dottore di ricerca in Diritto pubblico presso l'Università Roma Tre*.

Valentina PAGNANELLI, *Dottoranda in Scienze giuridiche (diritto pubblico) presso l'Università di Firenze*.

Federica PAOLUCCI, *Dottoranda in Diritto pubblico presso l'Università Commerciale "L. Bocconi" di Milano*.

Tommaso POLVANI, *Dottorando in Scienze giuridiche (discipline civilistiche) presso l'Università di Firenze*.

Andrea SIMONCINI, *Professore ordinario di Diritto costituzionale presso l'Università di Firenze*.

Giuseppe VERSACI, *Ricercatore in Diritto privato comparato presso l'Università di Siena*.

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.

IL DIRITTO ALL'AUTODETERMINAZIONE INFORMATIVA TRA CONCORRENZA E *DATA PROTECTION*

Riflessioni a margine della saga Facebook c. Bundeskartellamt *nella giurisprudenza delle corti tedesche e in attesa della Corte di Giustizia*

di *Francesco Laviola*

SOMMARIO: 1. Il contesto: il confronto globale tra Facebook e Autorità Antitrust. – 2. La condotta oggetto della sanzione del *Bundeskartellamt*. – 3. Cronologia della vicenda giudiziaria. – 4. La questione giuridica sottesa alla "saga" tedesca. – 5. Cittadino o utente? L'uomo dell'età informatica e il valore dei suoi dati.

1. *Il contesto: il confronto globale tra Facebook e Autorità Antitrust*

Nelle odierne società occidentali tutto dipende dall'*Information and Communication Technology* (ICT) e l'accesso a determinati servizi (ad esempio: la posta elettronica, i motori di ricerca, i social network) diventa abilitante per poter esercitare taluni diritti o, più semplicemente, vivere pienamente inseriti nella comunità sociale. In questo contesto, chi è in grado di introdurre le innovazioni tecnologiche capaci di condizionare il progresso, chi detiene le maggiori quantità di dati e, soprattutto, chi riveste il ruolo di *gatekeeper*[1] svi-

[1] Così anche M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Dir. informazione e informatica*, 12/2021, p. 111, il quale in nota chiarisce che così è definito «*chi controlla l'accesso a servizi online cruciali per raggiungere gli utenti. Per distribuire le loro app agli utenti di dispositivi iOS, gli sviluppatori debbono passare per App Store: App Store "controlla" l'accesso agli utenti iOS (Apple non ammette sui dispositivi iOS altri app store: ecco la barriera all'ingresso). Per avere un gatekeeper non è necessario che esso sia l'unico punto di accesso; basta che controlli l'accesso a una categoria di utenti sufficientemente ampia. Un esempio è Google: è difficile per le imprese competere senza il traffico di ricerca generato da Google. E così Amazon: l'accesso alla sua piattaforma è vitale per molti rivenditori*».

luppa un potere privato non dissimile per certi versi dal potere pubblico[2]. Non è forse questa la sede per un'approfondita disamina di tale problema in tutte le sue sfaccettature, ma la presente analisi si focalizzerà in particolar modo su una variazione di questo tema.

Benché spesso nel c.d. *cyberspazio* non si abbia a che fare con lo Stato e le sue leggi[3] – almeno secondo la concezione tipica del diritto pubblico –, ciò non significa che un individuo non goda di determinati diritti o non abbia, comunque, determinate esigenze da soddisfare. Ne consegue, quindi, un interrogativo rispetto alla possibilità far valere i propri diritti fondamentali anche nei confronti di soggetti privati che esercitino poteri tali da incidere sulla libertà e sulla dignità della persona.

La protezione della libertà-dignità dell'uomo e dei suoi diritti fondamentali da violazioni perpetrate da parte del potere pubblico è una delle caratteristiche dello Stato di diritto. Eppure, una delle maggiori criticità con cui bisogna confrontarsi nel contesto odierno risiede nel garantire una tutela di quegli stessi diritti anche nei confronti delle imprese private, specialmente, come ricordato dal *Bundesgerichtshof* della Repubblica Federale Tedesca nel corso della vicenda giudiziaria oggetto di questo saggio, allorquando esse «acquisiscono una posizione dominante e assumono il controllo delle condizioni quadro per la comunicazione pubblica». Sembrerebbe, dunque, doversi riconoscere che i diritti costituzionali siano delle prerogative da far valere non solo nei confronti del potere pubblico, ma anche del potere privato.

Del resto, le derive del c.d. "capitalismo di sorveglianza"[4] rischiano di met-

---

[2] A. IANNUZZI, *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*, 1/2021; E. CREMONA, *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in *Osservatorio sulle fonti*, 2/2021, p. 879 ss.; K. KLONICK, *The new governors: the peoples, rules and processes governing online speech*, in *Harvard Law Review*, 2018. Interessanti le considerazioni sui semi-Stati privati e, soprattutto, il parallelismo con le vicende della Compagnia delle Indie Orientali svolto da A. VENANZONI, *Ipotesi neofeudale. Libertà, proprietà e comunità nell'eclissi globale degli Stati nazionali*, Firenze, 2020, p. 201 ss.

[3] Cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 2/1999, p. 501.

[4] Secondo la definizione di S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* trad. it. P. Bassotti, Roma, 2019, secondo cui «*Il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti. Alcuni di questi dati vengono usati per migliorare prodotti o servizi, ma per il resto diviene un surplus comportamentale privato sottoposto a un processo di lavorazione noto come "intelligenza artificiale" per essere trasformato in prodotti predittivi in grado di vaticinare cosa faremo immediatamente, tra poco e tra molto tempo. Infine, questi prodotti predittivi vengono*

tere in crisi il pluricentenario binomio capitalismo-liberalismo [5], andandone a minare i capisaldi, e cioè la garanzia dei diritti dell'uomo e la libera concorrenza nel mercato. La necessità di rendersi capaci di raccogliere ingentissime quantità di dati, analizzarle ed estrarre ulteriori informazioni, in modo da rendere possibile l'orientamento, il riorientamento e il condizionamento delle scelte dell'utente (o del consumatore, ma anche dell'elettore e, più in generale della persona) comporta, infatti, da una parte, una sorta di naturale riduzione degli attori sul mercato, atteso che per operare in modo sempre più efficiente occorre controllare volumi di dati sempre più ingenti; dall'altra, produce un'inevitabile compressione della libertà degli individui, in quanto limitante della possibilità di determinarsi autonomamente, specialmente sotto il profilo dei dati e delle informazioni. In breve, v'è un rischio proprio per quel diritto all'autodeterminazione informativa sancito come diritto costituzionale dal *Bundesverfassungsgericht* [6] nel 1983, che rappresenta uno dei cardini del diritto alla privacy, inteso non più soltanto quale diritto «*ad essere lasciati in pace*» [7] – quindi all'esclusione degli altri e dello Stato dalla sfera intima della persona –, ma anche come diritto alla protezione dei dati personali. Ciò è, peraltro, positivamente disposto dall'art. 8 della Carta dei Diritti fondamentali dell'Unione europea e dal Regolamento UE 2016/679 (*General Data Protection Regulation*, c.d. GDPR) [8], rimarcando il definitivo passaggio dal concetto di riservatezza al

---

scambiati in un nuovo tipo di mercato per le previsioni comportamentali, che io chiamo mercato dei comportamenti futuri».

[5] Crisi rilevata da autori come Y.N. HARARI, *Homo Deus. Breve storia del futuro*, trad. it. M. Piani, Firenze, 2019, p. 373, sulla base del fatto che «*i liberali sono a favore del libero mercato e di elezioni democratiche poiché credono che ogni umano sia un individuo prezioso in un modo unico e irripetibile, e che le sue libere scelte rappresentino l'origine ultima dell'autorità. Nel XXI secolo tre sviluppi concreti potrebbero rendere obsoleta questa fede: 1. gli umani diventeranno sempre meno utili sia sotto il profilo economico che sotto quello militare, di conseguenza il sistema economico e politico cesserà di accordare loro così tanta importanza; 2. il sistema continuerà a considerare preziosi gli umani come collettività, ma non come singoli individui; 3. Il sistema continuerà a considerare preziosi alcuni singoli individui, ma questi costituiranno una nuova élite di superuomini potenziati, non la massa della popolazione. […] è difficile immaginare come la democrazia, il libero mercato e altre istituzioni liberali potranno sopravvivere a un colpo simile*». Vedi anche V. MAYER-SCHÖNBERGER, T. RAMGE, *Reinventare il capitalismo nell'era dei Big Data*, trad. it. G. Maugeri, Milano, 2018.

[6] Sulla quale vedi G. SARTOR, *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz"*, in *Inf. e dir.*, 3/1986, pp. 95-118.

[7] L'espressione "*right to be let alone*" venne coniata nel 1878 dal giudice Cooley e poi ripresa nel celebre saggio di Warren e Brandeis. Cfr. S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 4/1890; T. COOLEY, *Torts*, Chicago, 1888, p. 91.

[8] Sulla disciplina in materia di dati personali cfr., *ex multis*, L. CALIFANO, C. COLAPIETRO (a

controllo sui propri dati e sulle proprie informazioni personali, sul quale la dottrina aveva già da tempo avuto modo di esprimersi[9].

È proprio in questa luce che è 'forse' opportuno leggere il confronto muscolare in atto a livello mondiale tra Facebook e le Autorità Antitrust[10]. Accanto alla vicenda italiana di cui al capitolo precedente[11], in queste pagine si intende analizzare la parallela "saga"[12] in atto in Germania, benché diversa per tipo di violazione contestata dalle due autorità garanti per la concorrenza nazionali – pratiche commerciali scorrette in Italia e abuso di posizione dominante in Germania – e per la giurisdizione dinanzi alla quale pendono le im-

---

cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; C. KUNER, L. BYGRAVE, C. DOCKSEY, *The EU General Data Protection Regulation: A Commentary*, Oxford, 2020; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016; ID., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Torino, 2016; G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016; L. BOLOGNINI, E. PELLINO, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018. Cfr. da ultimo R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA, *Codice della Privacy e Data Protection*, Milano, 2021.

[9] S. RODOTÀ, *Repertorio di fine secolo*, Bari, 1999, pp. 207-210. Cfr. anche S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

[10] M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il reno)*, cit.; ID., *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *federalismi.it*, 14/2020; D. SRINIVASAN, *The Antitrust case against Facebook: a Monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy*, in *Berkeley Business Law Journal*, 2018, p. 40 ss. Peraltro, il problema riguarda anche altri giganti del Tech, cfr. L. KHAN, *Amazon's Antitrust Paradox*, in *The Yale Law Journal*, 2017, p. 712 ss.

[11] Si veda il contributo di V. PAGNANELLI in questo volume.

[12] Di "saga teutonica" parlano R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, in *Merc., conc., reg.*, 3/2020, p. 513. Cfr. anche R. VAN DEN BERGH, F. WEBER, *The German Facebook Saga: Abuse of Dominance or Abuse of Competition Law?,* in *World Competition*, 2021, pp. 29-52. Sul tema vedi A. DAVOLA, *"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; M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, cit. Sulla vicenda tedesca cfr. anche O. MÖRSDORF, *Im Bermudadreieck zwischen Datenschutz und Kartellrecht. Das Geschäftsmodell der digitalen Plattformökonomie auf dem Prüfstand*, in *ZIP*, 2020, p. 2259 ss.; T. SPERLICH, *Informationelle Selbstbestimmung zwischen Wettbewerbs und Datenschutzrecht. Eine Analyse und Beurteilung der Wechselwirkungen zwischen dem Wettbewerbs und Datenschutzrecht*, Berlin, 2021.

pugnazioni dei provvedimenti – amministrativa in Italia e civile in Germania –. Esse, infatti, rappresentano due parti di uno stesso tutto, ossia il tentativo di limitare il potere delle c.d. *Big Tech*, attraverso la garanzia del diritto alla concorrenza e del diritto alla protezione dei dati personali. In particolare, la questione verte sulla possibilità di ravvisare una violazione del diritto della concorrenza ove si rilevino violazioni del diritto alla protezione dei dati personali e, una volta verificata tale ipotesi, in che termini qualificare tale *vulnus*.

Come avrà modo di vedersi più diffusamente in seguito, la raccolta dati da parte di Facebook non avviene solo a partire dalle sue applicazioni web come Whatsapp o Instagram, ma anche da siti terzi attraverso *pixel* e *plug-in* (cioè i *like*), senza chiaramente chiedere esplicitamente il consenso degli utenti. Così, Facebook può creare «superprofili» degli utenti, combinando dati provenienti da tutti i tipi di fonti online (dati off-Facebook). Ebbene, queste condizioni generali del contratto sono state il bersaglio del *Bundeskartellamt* che le ha qualificate come violazione del GDPR e del *Bundesdatenschutzgesetz* (BDSG) [13], sanzionando la società americana.

2. *La condotta oggetto della sanzione del* Bundeskartellamt

Come noto, i servizi digitali sono apparentemente gratuiti: non viene, infatti, generalmente richiesto alcun corrispettivo in denaro per creare e utilizzare un indirizzo di posta elettronica, né per effettuare una ricerca su un motore di ricerca, né per potersi registrare e interagire sui social network [14]. Tuttavia, è evidente che una controprestazione in realtà ci sia ed essa consiste nella cessione dei dati [15] – che, come accennato in precedenza, costitui-

[13] Cfr. S. SIMITIS, G. HORNUNG, I. SPIECKER, *Datenschutzrecht. DSGVO mit BDSG. Großkommentar*, Baden-Baden, 2019.

[14] Sul punto, molto interessante, J. RIFKIN, *The zero marginal cost Society. The Internet of Things, the Collaborative Commons, and the eclipse of Capitalism*, New York, 2014.

[15] Cfr. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679 2019*, in *Annuario del contratto*, 2019; Sul punto vedi anche G. MALGIERI, B. CUSTERS, *Pricing Privacy: The Right to Know the Value of Your Personal Data*, in *Computer Law & Security Review*, 34, 2018, p. 289 ss.; H. ZECH, *Data as a Tradeable Commodity*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge-Antwerp-Portland, 2016.; A. METZGER, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, in *AcP*, 2016; A.A. WANDTKE, *Ökonomischer Wert von Persönlichen Daten. Diskussion des 'Warencharakters'von Daten aus persönlichkeits- und urheberrechtlicehr Sicht*, in *Multimedia und Recht*, 2017.

scono la "materia prima" utilizzata per condurre analisi e prendere decisioni rilevanti sul mercato.

In particolare, per quanto riguarda Facebook, gli utenti privati possono accedere sia tramite sito internet che tramite app mobile, previa registrazione mediante la creazione di un profilo. Gli utenti possono scegliere di inserire informazioni su loro stessi, a partire dai loro nomi reali fino ad arrivare a dettagli più intimi. Per ogni utente viene così creata una pagina, suddivisa in tre sezioni: "profilo", "trova amici" e "home", nella quale è possibile visualizzare notizie relative ad altri utenti privati e commerciali, ordinate sulla base di un algoritmo programmato per rispondere ai propri interessi. Vi sono, inoltre, altre funzionalità integrate come il servizio di messaggistica Facebook Messenger, ma anche forum di lavoro, organizzazione di eventi e altro. Oltre agli utenti privati, possono utilizzare Facebook anche imprese o associazioni, al fine di pubblicare contenuti ed espandere la propria rete sociale, creando delle pagine attraverso le quale interagire con gli utenti privati tramite iscrizioni o *like*.

Non viene richiesto un corrispettivo in denaro per la registrazione alla piattaforma, in quanto gli introiti di Facebook provengono dalla pubblicità *online* offerta agli editor e alle imprese, basata sui profili individuali degli utenti del social network, ai quali vengono presentati annunci per loro potenzialmente interessanti, secondo delle elaborazioni basate sul comportamento, sugli interessi e sulle loro condizioni di vita. Tale meccanismo viene definito come pubblicità targettizzata [16].

Col tempo, il gruppo Facebook ha acquisito anche altri servizi come Instagram e WhatsApp. Il primo, che si è notevolmente sviluppato nel corso degli ultimi anni, è un servizio per la condivisione di foto e brevi video clip che viene spesso definito come una "rete di foto" o un servizio di "*photo blogging*", anch'esso finanziato attraverso la pubblicità targettizzata. Il secondo offre, invece, un'applicazione di messaggistica istantanea, attraverso la quale gli utenti possono inviare o ricevere contenuti multimediali come messaggi di testo o vocali, foto, video, documenti, posizioni e altro.

---

[16] Si tenga, presente, inoltre, che il gruppo Facebook mette a diposizione anche dei *Facebook Business Tools*, cioè una selezione di strumenti e prodotti gratuiti per operatori di siti web, sviluppatori, inserzionisti e altre aziende da integrare nei propri siti web, applicazioni e offerte online tramite interfacce di programmazione (*Application Programming Interfaces*, API) predefinite da Facebook. La selezione comprende plugin sociali ("Mi piace" o "Condividi"), il login di Facebook e altri servizi di analisi (Facebook Analytics) implementati tramite "Facebook Pixel" o "*software development kit*" (SDK) per cellulari. Sulla pubblicità targettizzata vedi ampiamente G. D'IPPOLITO, P*rofilazione e pubblicità targettizzata online. Real-Time Bidding e behavioural advertising*, Napoli, 2021.

Per utilizzare il social network Facebook.com è necessario che l'utente presti il proprio consenso ai termini di servizio al fine di concludere il contratto. Tali termini prevendono, tra l'altro, che Facebook raccolga i dati personali degli utenti e dei loro dispositivi anche al di fuori delle proprie attività [17] – come specificato nell'informativa privacy – mediante i *Facebook Business Tools* integrati da inserzionisti, sviluppatori di app ed editori. Inoltre, Facebook elabora i dati degli utenti raccolti in altre società e prodotti del gruppo. La base giuridica del trattamento è la necessità di fornire il servizio e l'interesse legittimo della società.

Con riferimento al caso in parola, è bene evidenziare, conformemente all'istruttoria condotta dal *Bundeskartellamt* (l'Autorità Garante per la concorrenza tedesca) e durata circa tre anni, che nel 2018 la piattaforma Facebook.com contava in Germania una popolazione di 32 milioni di utenti mensili, di cui 23 milioni attivi giornalmente. Ai dati di tutte queste persone vanno aggiunti anche quelli raccolti dagli altri servizi del gruppo, i quali non solo aumentano questo già elevatissimo numero, ma permettono, fornendo ulteriori informazioni sui soggetti i cui dati sono già in possesso della società, di fornire profili ancora più dettagliati. Si tenga, altresì, presente che i termini di servizio proposti agli utenti sono delle condizioni *take it or leave it* e quindi non lasciano scelta ad essi, neanche per quanto riguarda la possibilità di combinare i dati della piattaforma Facebook.com con quelli di Instagram e WhatsApp.

L'accettazione di questa sorta di "pacchetto" che implica l'unione e l'elaborazione dei dati provenienti da Facebook, Instagram, WhatsApp e dai siti terzi è stato oggetto di attenzione da parte del Bundeskartellamt, che ha provveduto a contestare alla società l'utilizzo e la combinazione dei dati personali senza valido consenso dell'utente *ex* artt. 6 e 7, par. 4, GDPR.

3. *Cronologia della vicenda giudiziaria*

«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». Così si è espresso l'*Oberlandesgericht* di Düsseldorf durante l'udienza del 24 marzo 2021 – soltanto cinque giorni prima, cioè, della sentenza del Consiglio

[17] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit., p. 515.

di Stato, sez. VI, 29 marzo 2021, n. 2361 –, rinviando in via pregiudiziale la questione alla Corte di Giustizia dell'Unione europea. Dopo circa tre anni di serrato scontro legale tra il *Bundeskartellamt* e Facebook, la soluzione della controversia è stata, dunque, affidata ai Giudici di Lussemburgo. Considerato che sia la disciplina della concorrenza che quella della protezione dei dati personali discendono dal diritto europeo, rimettere *l'actio finium regundorum* alla CGUE piuttosto che ricorrere a soluzioni nazionali, appare non solo condivisibile, ma anche assai utile, in quanto una pronuncia sul tema può davvero rappresentare un fattore che favorisca l'uniformità delle risposte sanzionatorie delle Autorità antitrust di tutti gli Stati membri, nell'ambito di una questione di respiro globale.

Come anticipato, il giudizio in parola, ormai sospeso in attesa della decisione della Corte di Giustizia, era scaturito dall'impugnazione da parte di Facebook di una sanzione irrogata dal *Bundeskartellamt* il 6 febbraio 2019. A differenza del parallelo caso italiano affrontato nel capitolo precedente [18] – in cui le due sanzioni originariamente inflitte al colosso di Menlo Park dall'Autorità Garante della Concorrenza e del Mercato ammontavano a dieci milioni di euro – l'Autorità tedesca si era "limitata" a vietare alcuni dei termini contrattuali imposti da Facebook ai suoi utenti, rilevando un abuso di posizione dominante [19].

Tale divieto, però, risultava comunque pernicioso per il *business model* della società, la quale aveva, così, provveduto ad impugnare il provvedimento dinanzi al tribunale superiore (*Oberlandesgericht*) di Düsseldorf. Esaminata "in via cautelare" la questione, l'*Oberlandesgericht* aveva provveduto a bloccare l'esecutività della decisione del *Bundeskartellamt*, non condividendo la ricostruzione operata dall'autorità [20].

Il *Bundeskartellamt* aveva allora, a sua volta, impugnato la decisione dell'*Oberladesgericht* ricorrendo al *Bundesgerichsthof*, ossia la Suprema corte federale tedesca, e provocando il ribaltamento della decisione dei giudici di Düsseldorf con la "pronuncia pregiudiziale" del 23 giugno 2020. Nella sua decisione, infatti, il *Bundesgerichtshof* aveva mostrato di condividere la valutazione rispetto alla qualificazione in termini di abuso di posizione dominante della condotta di Facebook [21].

Così, all'udienza di merito, appunto il 24 marzo 2021, trovandosi di fronte alla scelta di conformarsi o meno a quanto deciso dal *Bundesgerichtshof*, l'*Ober-*

[18] Si veda il contributo di V. PAGNANELLI in questo volume.

[19] BKartA v. 6. 2. 2019 – B6-22/16 – Facebook.

[20] OLG Düsseldorf NZKart 2019, 495 – Facebook.

[21] BGH v. 23. 6. 2020 – KVR 69/19 – Facebook.

landesgericht di Düsseldorf ha preferito ricorrere alla Corte di Giustizia dell'Unione europea, affidandosi alla sua interpretazione del diritto eurounitario, piuttosto che prendere di nuovo autonomamente posizione.

4. *La questione giuridica sottesa alla "saga" tedesca*

Senza entrare nei dettagli tecnici del diritto della concorrenza tedesco, basti dire che, ai sensi del §18 del *Gesetz gegen Wettbewerbsbeschränkungen* (GWB) [22], Facebook rientra nella definizione di intermediario e, benché offra servizi gratuiti di social network, ciò non preclude in realtà l'esistenza di un mercato [23].

Dalla prospettiva che s'intende adottare in questo scritto, il punto focale è rappresentato dalla questione relativa all'esistenza o meno di un collegamento tra la violazione della normativa in materia di protezione dei dati personali e la disciplina antitrust.

Ebbene, il provvedimento adottato dal *Bundeskartellamt* contro Facebook ha risposto positivamente a questo interrogativo. Difatti, l'Autorità ha ritenuto che i termini di servizio, violando le disposizioni, del GDPR siano da considerare abusive ai sensi del §19 (1) GWB.

Tale decisione si è basata su alcuni precedenti giurisprudenziali del *Bundesgerichtshof*, quali i casi *VBL-Gegenwert* e *Pechtstein*, nell'ambito dei quali erano stati rilevati degli abusi di condizioni commerciali proprio sulla base del §19 (1) GWB [24]. Alla stregua di tali decisioni, questa disposizione deve essere

---

[22] Per i quali si rinvia a R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit., pp. 510-511, il quale ala nota 15 richiama gli sforzi compiuti per delineare una disciplina della concorrenza adatta ai mercati digitalizzati attraverso la *Neuntes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen*; vedi anche A. POMANA, M. SCHNEIDER, *Wettbewerbsrecht und Datenschutz: Facebook im Visier des Bundeskartellamts*, in «*BB*», 2018.

[23] Vedi *amplius* in A. DAVOLA, *"I vestiti nuovi dell'imperatore"*, cit., p. 63, il quale rileva come «*non sia valso a minare la valutazione del Bundeskartellamt il fatto che il servizio offerto da Facebook sia gratuito, posto che ai sensi della normativa tedesca (a seguito di un emendamento della GWB intervenuto nel 2016) non è necessario che una prestazione sia a pagamento per poterla qualificare nei termini di un servizio economico ai sensi dello scrutinio antitrust; una posizione di tal genere appare, del resto, anch'essa in linea con la lettura del fenomeno offerta dalle istituzioni europee*».

[24] Nelle decisioni prese nei casi *VBL-Gegenwert*, il BGH aveva considerato abusive condizioni contrattuali in violazione degli artt. 307 ss. del BGB; in particolare, allorquando l'applicazione di tali condizioni si riveli riflettersi in una manifestazione di potere di mercato o di po-

applicata nei casi in cui una parte contrattuale ricopre una posizione di potere tale da essere in grado di dettare i termini del contratto, abolendo di fatto l'autonomia contrattuale dell'altra parte, in un'ottica non soltanto privatistica, ma volta alla tutela dei diritti sanciti dalla Costituzione tedesca. Difatti, qualora una società sia in grado di incidere su tali diritti, secondo il *Bundesgerichtshof* è necessario che la legge intervenga al fine di proteggerli. Ciò, beninteso, operando un giusto bilanciamento.

Pertanto, il *Bundeskartellamt* ha ritenuto che, con riferimento all'adeguatezza delle condizioni concordate in una trattativa squilibrata, questi precedenti del Tribunale supremo federale possano valere per tutti i settori del diritto, inclusa la protezione dei dati personali. Invero, proprio al fine di garantire il diritto all'autodeterminazione informativa, la disciplina in materia di protezione dei dati personali garantisce il diritto all'individuo di decidere liberamente e senza coercizione sul trattamento dei propri dati.

Alla luce di ciò, è bene evidenziare come il *Bundeskartellamt* abbia esaminato con forte attenzione la relazione tra la disposizione di cui al §19 (1) GWB e i principi del GDPR. L'Autorità ha ritenuto, infatti, indispensabile vagliare il comportamento delle imprese in posizione dominante, secondo il diritto della concorrenza, anche sotto il profilo della correttezza delle procedure di trattamento dei dati personali, essendo il loro comportamento online assai rilevante.

Peraltro, il *Bundeskartellamt* ha sostenuto che le norme del GDPR non escludono, in realtà, che anche autorità di garanzia differenti dalle autorità nazionali di protezioni dei dati personali possano applicare il diritto sostanziale in materia di protezione dei dati. Per argomentare questo punto, l'Autorità ha evidenziato come la gran parte della giurisprudenza della Corte di Giustizia dell'Unione europea, utilizzata e citata dalle autorità di controllo e dall'European Data Protection Board (EDPB), sia composta da decisioni scaturire nell'ambito di procedimenti di diritto civile. Inoltre, sempre il *Bundeskartellamt* ha sottolineato la sua condotta volta a mantenere contatti regolari con le autorità di protezione dei dati tedesche, evidenziando, altresì, come la Conferenza delle autorità indipendenti per la protezione dei dati personali della Fe-

---

tere superiore della parte che utilizza tali condizioni. Cfr. BGH. *VBL-Gegenwert* I, 6 novembre 2013, KZR 58/11, *VBL-Gegenwert* II, 24 gennaio 2017, KZR 47/14. Nel caso BGH, *Pechstein/International Skating Union*, 7 giugno 2016, KZR 6/15, è stato affermato che il bilanciamento tra beni, entrambi dotati di protezione costituzionale, porta ad escludere l'abuso di posizione dominante alla stregua del § 19 GWB. Vedi R. PARDOLESI, *Clausole abusive nei contratti dei consumatori. E oltre?*, in *Foro it*., 2014, 11; ID., *Clausole abusive e «terzo contratto»*, in *Foro it.*, 2020, 1, p. 97. Cfr. anche M. MIDIRI, *Le piattaforme e il potere dei dati*, cit., pp. 123-124, in nota.

derazione e dei *Länder* (*Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*) aveva avuto modo di dichiarare che l'applicazione della legge sulla protezione dei dati non deve essere l'unica risposta alle violazioni dei requisiti di protezione dei dati, ma anche le leggi in materia di concorrenza e antitrust possono rappresentare una valida risposta. Inoltre, stando al provvedimento dell'Antitrust tedesco, perfino l'autorità di protezione dei dati personali irlandese era stata informata del procedimento, in quanto eventuale Autorità capofila ai sensi del GDPR.

Alla luce di quanto sopra, il *Bundeskartellamt* ha concluso che l'elaborazione dei dati effettuata da Facebook e dai Facebook Business Tools, anche attraverso la profilazione e il *device fingerprinting*, ha causato una violazione della normativa europea sulla privacy, in quanto mancante di un valido presupposto di liceità, ai sensi dell'art. 6 GDPR. Difatti, è stata ravvisata la mancanza di un consenso *ex* art. 6, par. 1, lett. a), GDPR per quei trattamenti di dati personali che non sono necessari al fine di adempiere il contratto, così come previsto dall'art. 6, par.1, lett. b). Non è stata ravvisata, d'altronde, la sussistenza di alcuna delle basi giuridiche previste dalle altre lettere di cui al par. 1 dell'art. 6 GDPR.

L'Autorità ha, quindi, qualificato questa violazione delle norme in materia di dati personali come una manifestazione del potere di mercato di Facebook. In particolare, gli argomenti mediante i quali è stata sostenuta la violazione sono stati, da una parte, la limitazione del diritto all'autodeterminazione informativa degli utenti[25] e, dall'altra, l'erezione di barriere all'ingresso del mercato tramite la combinazione di dati provenienti da servizi diversi.

---

[25] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit., p. 524 ss. che notano come: «*Il BKartA, forte del silenzio sul punto nelle sentenze del BGH cui fa riferimento, ha sostenuto che l'accertamento di un Konditionenmissbrauch non può passare per il solo tramite della clausola specifica contenuta nel § 19 (2) n. 2 GWB. Detta clausola postula la causalità della condotta (Verhaltenskausalität), vale a dire la valutazione di un mercato controfattuale caratterizzato da un assetto competitivo: si deve dimostrare, cioè, che la pratica contestata (prezzi elevati o condizioni contrattuali inadeguate) non si sarebbe verificata in un mercato apprezzabilmente concorrenziale. Al contrario, la clausola generale del § 19 (1) GWB, riferita agli abusi da esclusione, attenua il requisito della causalità. Per tale categoria, infatti, si suole ritenere sufficiente che il risultato della condotta illecita, perché vocazionalmente portata ad alterare il mercato, sia anticoncorrenziale, basta, dunque, una Ergebniskausalität (causalità normativa, sostanzialmente presupposta al verificarsi dell'illecito); mentre gli abusi da sfruttamento, proprio perché in genere non influenzano la struttura del mercato, richiedono, per conseguenza, uno scrutinio causale più serrato. Estendere la soglia di causalità attenuata a un abuso di sfruttamento quale il Konditionenmissbrauch è una novità. Ma è proprio quello che il BKartA ha fatto nel caso Facebook*»; cfr. anche A. DAVOLA, *"I vestiti nuovi dell'imperatore"*, cit., 68, il quale rileva che «*due elementi appaiono meritevoli di specifica considerazione: si pone, in primo luogo, la tematica del preteso collegamento tra la violazione del GDPR e danno (non*

Ciò avrebbe, secondo la ricostruzione del *Bundeskartellamt*, condotto ad un vantaggio concorrenziale rispetto alle altre imprese del settore, aumentando le barriere all'entrata nel mercato; fattore che, a sua volta, ha assicurato il potere di mercato di Facebook nei confronti dei clienti finali.

In forza di quanto fin ora esposto, il *Bundeskartellamt* ha vietato il trattamento dei dati da parte di Facebook *ex* § 19 (1) e § 32 GWB, ordinando la cessazione della condotta. In particolare, il bersaglio del divieto è stata la modalità di trattamento dei dati personali indicata nei termini di servizio e dettagliata nell'informativa privacy e nella *policy* sui *cookie*, specialmente per quanto attiene la raccolta dei dati relativi agli utenti e ad altri dispositivi da parte di altri servizi aziendali e da parte dei *Facebook Business Tools*, in quanto trattamenti effettuati senza consenso degli utenti; peraltro tali dati venivano combinati con i dati di Facebook per scopi legati al social network [26].

In breve, il ragionamento che ha condotto il *Bundeskartellamt* a inquadrare la condotta di Facebook come abuso di posizione dominante è stato orientato dalla considerazione che gli utenti non possono proteggere i propri dati personali dai trattamenti da più parti, dal momento che i termini e le condizioni in parola hanno una portata considerevole, atteso che il potere di mercato di Facebook si estende oltre il social network e i dati dei consumatori sono raccolti ogni volta che usano internet.

Il caso, pur non essendo del tutto analogo, ha, in realtà, delle assonanze sia con la "pratica a)" sanzionata dall'Autorità Garante della Concorrenza e del Mercato italiana quale pratica commerciale ingannevole, *ex* artt. 21 e 22 del d.lgs. n. 206/2005 – c.d. Codice del consumo –, poiché, stando a quanto rilevato, gli utenti venivano indotti a registrarsi sulla piattaforma senza adeguata

---

prettamente consumeristico, bensì squisitamente) concorrenziale. Un passo, questo, che, sebbene forzosamente imposto dalla volontà di attivare le tutele previste avverso l'abuso di posizione dominante, rischia di comportare una sostanziale liquefazione del rigore interpretativo del nesso di causalità: non a caso, si noti, la violazione delle regole previste dalla General Data Protection Regulation rappresenta (prima) uno degli aspetti oggetto di censura da parte della corte di appello, e (poi) viene gradualmente a perdere prominenza nel giudizio, pur pronunciato in favore del Bundeskartellamt, da parte della Corte Federale di Giustizia. In secondo luogo, è proprio l'origina – le utilizzo del Konditionenmissbrauch – ossia dell'illecito concorrenziale derivante dall'imposizione di condizioni contrattuali non eque – a costituire un profilo di interesse specifico: sebbene giovi osservare come tale soluzione appaia ben più affine all'ordinamento tedesco che non ad altre giurisdizioni. Una scelta, questa, che appare ancor più controversa laddove si consideri la difficoltà di sviluppare una soddisfacente ricostruzione del collegamento diretto tra struttura dei termini contrattuali e pregiudizio alla concorrenza».

[26] Nell'ordine di porre fine all'infrazione, a Facebook è stato ordinato di attuare le modifiche necessarie e di adattare di conseguenza le sue politiche sui dati e sui cookie entro un periodo di dodici mesi. Inoltre, a Facebook è stato dato un termine di quattro mesi per presentare una tabella di marcia per l'attuazione degli adeguamenti.

informazione, specialmente con riguardo alle finalità remunerative sottese alla fornitura del servizio, che, al contrario, veniva presentato come gratuito – ad esempio, attraverso il *claim "iscriviti, è gratis e lo sarà sempre"* –; sia con la "pratica b)", qualificata in termini di pratica commerciale aggressiva in violazione degli artt. 24 e 25 del Codice del consumo, dal momento che l'Antitrust contestava un indebito condizionamento sugli utenti esercitato in maniera inconsapevole e automatica, attraverso la trasmissione e l'uso dei propri dati da parte di Facebook e terze parti.

Eppure, il *Bundeskartellamt* ha, invece, qualificato la pratica messa in atto da Facebook come abuso di posizione dominante. Come ben rilevato in dottrina, tale ricostruzione comporta vari problemi, tra i quali quello attinente all'aspetto della prova del nesso di causalità tra la condotta di Facebook e il pregiudizio al mercato[27]. Il *Bundeskartellamt* ha, infatti, vietato la raccolta e l'aggregazione dei dati relativi agli utenti di Facebook mediante i servizi prestati da siti terzi sulla base del *Konditionenmissbrauch*, di cui al § 19 GWB[28], in quanto ha rilevato l'assenza di un consenso esplicito da parte degli interessati. In altre parole, ciò significa che, secondo la ricostruzione del *Bundeskartellamt*, l'abuso di sfruttamento nei confronti degli utenti è arrivato a cagionare l'esclusione dei concorrenti e, dunque, l'abuso di posizione dominante[29]. In questo contesto, viene peraltro in evidenza come le regole del GDPR vengano valutate alla stregua di un parametro normativo di liceità delle operazioni di raccolta ed elaborazione dei dati.

Orbene, Facebook ha impugnato la decisione dell'Antitrust dinanzi all'*Oberlandesgericht* di Düsseldorf. Come accennato in precedenza, nell'agosto 2019 l'*Oberlandesgericht* ha, quindi, concesso un provvedimento cautelare con il quale ha bloccato l'esecutività della decisione del *Bundeskartellamt*. Pur trattandosi di un procedimento sommario, la motivazione della decisione è stata molto dettagliata, tanto da far preconizzare un annullamento del provvedimento del *Bundeskartellamt* nel corso del procedimento principale.

I giudici di Düsseldorf hanno, infatti, sollevato dei dubbi rispetto alla prova del pregiudizio per la concorrenza e alla mancanza del nesso di causalità, adducendoli come vizi della motivazione del provvedimento.

Per quanto attiene al primo profilo, l'*Oberlandesgericht* ha constatato come il comportamento di Facebook non abbia provocato, in realtà, alcun danno

---

[27] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit.

[28] Non è questa la sede per soffermarsi sul punto. Per un'ampia disamina cfr. O. MÖRSDORF, *Im Bermudadreieck zwischen Datenschutz und Kartellrecht*, cit., p. 2265 ss.

[29] Per una ricostruzione completa cfr. A. DAVOLA, *"I vestiti nuovi dell'imperatore"*, cit., p. 62 ss.

alla concorrenza, poiché gli utenti non hanno subito alcuna perdita finanziaria. Pur ritenendo, quindi, sostanzialmente corretta la delimitazione del mercato operata attraverso l'applicazione del § 18 GWB, l'*Oberlandesgericht* ha, però, escluso che i termini di servizio considerati iniqui dal *Bundeskartellamt* potessero cagionare un abuso di posizione dominante, eccependo un difetto di indagine per mancanza di prova controfattuale.

Per di più, il § 19 (1) GWB è stato ritenuto inapplicabile, in quanto, secondo la ricostruzione del Tribunale, la presunta violazione del GDPR non avrebbe causato effetti anticoncorrenziali. È stata, così, rilevata una critica rispetto a quella che è stata considerata una "banalizzazione" del requisito di causalità al fine di individuare l'abuso [30]. Peraltro, dal momento che anche altre aziende stavano usando condizioni contrattuali simili, i termini di servizio "abusivi" non potevano considerarsi un risultato della posizione dominante sul mercato.

L'*Oberlandesgericht* ha, così, concluso di non poter qualificare come abuso di sfruttamento della posizione dominante la condotta di Facebook, anche tenendo conto che gli utenti avevano liberamente accettato i termini di servizio ed erano stati liberi di astenersi dall'utilizzare il social network del tutto. Perciò, nulla è stato aggiunto dai giudici di Düsseldorf per quanto riguarda i profili relativi alla possibile violazione della disciplina in materia di protezione dei dati, ritenendo tale profilo non rilevante nel caso in parola [31].

A questo punto, è stata la volta del *Bundeskartellamt* a procedere all'impugnazione – di nuovo in via cautelare – della decisione dell'*Oberlandesgericht* dinanzi al *Bundesgerichthof*, il quale con la "pronuncia pregiudiziale" del 23 giugno 2020, ha ribaltato la decisione dei giudici di Düsseldorf, ritenendo che le condizioni contrattuali per l'utilizzo di Facebook possono, in realtà, costi-

---

[30] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit.

[31] Con riferimento alle operazioni sui dati, i giudici di Düsseldorf hanno ritenuto che essi possono essere duplicati e utilizzati rispetto a diversi servizi, il consenso al loro impiego è regolarmente accordato dagli interessati, il fatto di condizionare la partecipazione al social network alla condivisione dei dati non basta a costituire un abuso o una perdita di controllo. Cfr. anche O. MÖRSDORF, *Im Bermudadreieck zwischen Datenschutz und Kartellrecht*, cit., pp. 2260-2261, il quale riporta che: «*Das Gericht begründete diese Entscheidung damit, dass das Bundeskartellamt das Vorliegen eines Marktbeherrschungsmissbrauchs gem. § 19 Abs. 1 GWB in kener seinen beiden Grundformen hinreichend dargetan habe. Zur Bejahung eines Ausbeutungsmissbrauchs fehle es am Nachweis, dass die datenschutzwidrigen Konditionen gerade auf der marktbeherrschenden Stellung von Facebook beruhten und bei ungestörtem Wettbewerb nicht durchsetzbar gewesen wären. Hinsichtlich eines Behinderungsmissbrauchs habe das Amt nicht konkret dargelegt, inwieweit der unter Verstoß gegen das Datenschutzrecht erlangte Zugriff auf Nutzerdaten Facebook einen weitergehenden Wettbewerbsvorteil auf dem von ihm beherrschten Markt für soziale Netzwerke verschafft habe*».

tuire un abuso di posizione dominante *ex* § 19 GWB. E questo, indipendentemente dalla loro conformità alla legislazione in materia di dati personali. Il supremo tribunale tedesco ha, infatti, ravvisato il maggior *vulnus* nell'elisione della possibilità di scelta – *fehlende Wahlmöglichkeit*[32] –. In pratica, la decisione di non mettere a disposizione delle opzioni tra cui scegliere nel momento in cui un utente decide di usufruire dei servizi di Facebook avrebbe comportato, secondo i giudici del Tribunale supremo, una lesione del diritto del consumatore ad autodeterminarsi con conseguente accertamento dell'abuso della posizione dominante dell'azienda.

È stato messo in luce, non senza ragione, come sia quanto meno bizzarro che una decisione cautelare d'urgenza sia stata resa con un provvedimento la cui motivazione raggiunge la lunghezza di circa cinquanta pagine e tocca tutti gli aspetti nel dettaglio[33]. E occorre, anche in questo caso, segnalare come il riferimento diretto al GDPR torni ai margini della vicenda rispetto a quanto avvenuto nella decisione del *Bundeskartellamt*[34].

Eppure, contrariamente a quanto sostenuto da parte della dottrina[35], es-

---

[32] O. MÖRSDORF, *Im Bermudadreieck zwischen Datenschutz und Kartellrecht*, cit., p. 2270: «*Der BGH hat einen solchen Verhaltensstandard, auch ohne unmittelbaren Rekurs auf die DSGVO, überzeugend aus dem verfassungsmäßig verbürgten Recht der Facebook-Nutzer auf informationelle Selbstbestimmung hergeleitet, welches auch die Möglichkeit der Kontrolle über die Preisgabe der eigenen Daten beinhaltet. Mit einer solchen Kontrollmöglichkeit ist es, angesichts der Bedeutung des Netzwerkzugangs für die Teilnahme der Nutzer am sozialen Leben, wiederum nicht vereinbar, dass Facebook seinen Nutzern einzig einen über ihre Bedürfnisse hinausgehenden, besonders datenintensiven Netzzuganganbietet. Größere Schwierigkeiten bereitet indes der Nachweis, dass mit dem beanstandeten Verhalten eine Behinderung von Wettbewerbern des marktbeherrschenden Unternehmens einhergeht. Nach Auffassung des BGH ergibt sich eine Behinderung der (potentiellen) Wettbewerber von Facebook auf dem von Facebook beherrschten Markt für soziale Netzwerke zum einen in Gestalt einer Verstärkung bestehender Lock-Effekte durch datenbasierte Leistungsoptimierung und zum anderen in Gestalt verbesserter Finanzierungsmöglichkeiten infolge der datenbasierten Möglichkeit zur Schaltung individualisierter Werbung. Im Hinblick auf den letztgenannten Umstand möchte der BGH zudem eine Beeinträchtigung des Marktes für Online-Werbung nicht ausschließen*».

[33] Come notato giustamente da R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit.

[34] Sul punto vedi O. MÖRSDORF, *Im Bermudadreieck zwischen Datenschutz und Kartellrecht*, cit., 2062: «*Anders als das Bundeskartellamt leitet der BGH diesen Befund nicht aus einer Unvereinbarkeit der Konditionen mit datenschutzrechtlichen Wertungen her. Anknüpfungspunkt für den Missbrauchsvorwur ist vielmehr die fehlende Wahlmöglichkeit der Nutzer hinsichtlich des Umfangs der von ihnen preiszugebenden Daten. Indem die Nutzer eine für sie unverzichtbare Leistung (die Nutzung des sozialen Netzwerks) nur zusammen mit einer weiteren unerwünschten Leistung (Bereitstellung eines personalisierten Erlebnisses) und hieran gekoppelter gesteigerter Datenpreisgabe erhielten, könnten sie nicht mehr frei über den Umfang der Preisgabe ihrer Daten entscheiden*».

[35] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, cit.

sendo il nocciolo delle argomentazioni svolte dal *Bundesgerichtshof* la lesione dell'autonomia decisionale mediante la violazione del diritto all'autodeterminazione informativa, in realtà viene pregiudicata la *ratio* stessa del diritto alla protezione dei dati personali per come qualificata nel contesto europeo. Negare, cioè, la possibilità di scelta per gli utenti di utilizzare Facebook senza condividere i propri dati conformemente alle modalità ivi previste, lede, secondo il *Bundesgerichtshof,* il diritto all'autodeterminazione informativa. Proprio questo risulta essere il punto cruciale: non si può valutare la rinuncia al servizio come possibile soluzione, in quanto, come rilevano giustamente i giudici di Karlsruhe, al giorno d'oggi le piattaforme hanno un ruolo abilitante rispetto alla partecipazione alla vita sociale.

La Suprema corte federale, nella sentenza in parola, ha sottolineato che non v'è un diritto generale dell'interessato a decidere come i propri dati verranno impiegati, quanto, piuttosto, una garanzia di poter «esercitare un'influenza differenziata sul contesto e la maniera in cui i propri dati sono resi accessibili ai terzi e usati da loro»; ciò considerato anche l'eventuale impatto rispetto all'interpretazione delle «clausole generali del diritto civile, cui il § 19 GWB può essere ricondotto».

Tuttavia, come anticipato, la pronuncia del *Bundesgerichtshof* non ha rappresentato in alcun modo la conclusione della "saga", avendo ad oggetto soltanto l'azione cautelare. Arrivati, infatti, all'udienza di merito, appunto il 24 marzo 2021, l'*Oberlandesgericht* di Düsseldorf si è trovato di fronte alla scelta se conformarsi o meno ai vari *obiter dicta* del *Bundesgerichtshof*.

Forse anche preso atto della divergenza di opinione che ha caratterizzato il provvedimento cautelare emesso dal *Bundesgerichtshof*, i giudici di Düsseldorf hanno optato per la strada del rinvio pregiudiziale alla Corte di Giustizia dell'Unione europea.

E così adesso saranno i giudici del Lussemburgo a dover stabilire se le violazioni della disciplina sulla protezione dei dati personali possano condurre o meno ad abusi di posizione dominante o ad altri effetti pregiudizievoli per la concorrenza.

E, verosimilmente, sarà il banco di prova definitivo per molte questioni. Sia per quanto riguarda l'integrazione della c.d. "Europa del mercato" con la c.d. "Europa dei diritti", sia – non ultimo – per quanto attiene al profilo della qualificazione dei dati personali come diritto o come bene commerciabile. Tale annosa questione potrebbe, infatti, trovare una soluzione pressoché definitiva ove intervenisse una pronuncia della Corte di Giustizia di un certo rilievo, posto che sia il diritto alla protezione dei dati personali sia il diritto della concorrenza fanno pienamente capo all'ordinamento eurounitario.

5. *Cittadino o utente? L'uomo dell'età informatica e il valore dei suoi dati*

Le informazioni circolano da quando gli uomini si sono dotati di mezzi per lasciare traccia di sé ai posteri e per comunicare con i propri simili. Soltanto negli ultimi tempi, però, nei Paesi più industrializzati si è sviluppata una società in cui sia il benessere individuale che quello sociale dipendono dalle ICT e non si può più fare a meno dei dati e delle informazioni per poter svolgere pressoché ogni attività[36]. Del resto, in questi ultimi anni, l'umanità ha creato più dati di quanti ne abbia prodotti complessivamente dai tempi dell'invenzione della scrittura e questo *trend* appare essere in crescita esponenziale[37].

Grazie a questa immensa quantità di dati e alle tecniche per elaborarli messe a disposizione dalla tecnologia, tutte le decisioni strategiche possono essere prese utilizzando modelli matematici basati su dati, e, in virtù di ciò, l'analisi dei *big data* guida oggi quasi ogni aspetto della società[38]. È qui che risiede la chiave del potere delle *Big Tech*: nell'enorme quantità di dati controllata. Come ricordato già nel maggio 2017 dal titolo di un articolo dell'*Economist*, *«la risorsa più preziosa del mondo non è più il petrolio, ma i dati»*[39].

Per quanto riguarda i dati non personali, non vi sono, in realtà, particolari questioni per quanto attiene il loro trattamento e la loro libera circolazione, una volta superato il problema della qualificazione del dato in termini di "dato

---

[36] Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. it. M. Durante, Milano, 2017, p. 7.

[37] Stando alla strategia europea per i dati, il volume globale dei dati trattati aumenterà, entro il 2025, del 530% (da 33 zettabyte nel 2018 a 175 zettabyte, una quantità equivalente a circa 36.000 anni di video in HD), per un valore economico dei dati trattati corrispondente a 829 miliardi di euro, in un business che arriverà ad impiegare circa 11 milioni di professionisti dei dati. Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Una strategia europea per i dati*, 19 febbraio 2020, reperibile in https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.

[38] V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013; Per quanto riguarda gli aspetti tecnici si rimanda a H.V. JAGADISH, J. GEHRKE, A. LABRINDIS, Y. PAPAKOSTANTINOU, J.M. PATEL, R. RAMAKRISHNAN, C. SHAHABI, *Big Data and Its Technical Challenges*, in *Comunications of the ACM*, 2014; per quanto attiene ai rischi vedi A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. informazione e informatica*, 2012; M. OOSTVEEN, *Indentifiability and the applicability of data protection to big data*, in *International Data Privacy Law*, 2016.

[39] *The world's most valuable resource is no longer oil, but data*, in *The Economist*, 6 maggio 2017; vedi anche *Data is giving rise to a new economy*, *ivi*.

personale" o meno, alla stregua dell'art. 4 GDPR[40]. Non è, infatti, sempre semplice determinare se un dato sia riconducibile ad una persona fisica o, comunque, se possa in qualche modo diventarlo incrociandolo con altri dati. Trattare dati personali, invece, comporta determinate garanzie e cautele, anche perché il diritto alla protezione dei dati personali è sancito positivamente dall'art. 8 della Carta di Nizza e confermato, tra l'altro, anche dall'art. 16 TFUE. Inoltre, come ben noto, vi è una specifica disciplina di tutela che deriva principalmente dal GDPR e dalle normative nazionali, attraverso cui è regolata la protezione e la libera circolazione dei dati personali.

Tutto ciò, in un contesto in cui gli utenti non ricevano una controprestazione patrimoniale per i dati che quotidianamente forniscono[41], trattandosi di servizi apparentemente gratuiti come la posta elettronica, i social o i motori di ricerca. Ma, come vuole un vecchio adagio: *«… se non lo paghi, il prodotto sei tu!»*. Ciò implica profili critici sia per quanto riguarda i diritti fondamentali delle persone – non ultimo, il diritto alla protezione dei dati personali[42] – che per quanto attiene il buon funzionamento dei meccanismi di mercato.

Come è stato rilevato in dottrina, la tutela dei diritti fondamentali e il perseguimento dell'efficienza economica del mercato non sono istanze necessariamente in contrasto tra loro[43]. Al contrario, esse risultano complementari, specialmente nel contesto eurounitario, nel quale *«l'integrazione positiva è divenuta un mezzo per realizzare un bilanciamento tra le libertà fondamentali del mercato e i diritti fondamentali, in modo da realizzare una correzione del mercato»*[44]. La tutela della libera concorrenza e la protezione del consumatore possono, infatti, essere funzionali anche alla protezione di altri diritti. Ciò risulta particolarmente evidente per quanto riguarda le garanzie in materia di dati personali nel mercato digitale.

---

[40] Per ulteriori approfondimenti si rimanda a Article 29 Working Party, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007, p. 12 ss.

[41] Cfr. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679 2019*, cit., p. 131; vedi anche M. NARCISO, *'Gratuitous' Digital Content Contracts in EU Consumer Law*, *Consumer Law*, in *EuCML*, 2017, p. 198 ss.

[42] C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Napoli, 2018.

[43] G. PITRUZZELLA, *Diritto costituzionale e diritto della concorrenza: c'è dell'altro oltre l'efficienza economica?,* in *Quad. cost.*, 3/2019.

[44] Così G. PITRUZZELLA, *L'Europa del mercato e l'Europa dei diritti*, in *federalismi.it*, 6/2019, p. 10; vedi anche V. KOSTA, *Fundamental Rights in EU Internal Market Legislation*, Oxford-Portland, 2018.

L'antico dualismo tra "concezione morale" dei dati personali, che ne esalta la correlazione con l'identità della persona e la sua dignità e libertà, e la concezione patrimoniale dei dati, alla stregua della quale essi possono essere considerati come dei beni e circolare liberamente nel mercato [45], può forse risolversi nella sintesi tra la disciplina a tutela del consumatore e quella in materia di protezione dei dati personali. Sebbene tale ricostruzione appaia *prima facie* contorta, essa trova, però, appigli non solo dal punto di vista teorico, ma, soprattutto, sul versante dell'applicazione pratica [46]. Proprio per questo, nel condurre una riflessione sul tema, non si può prescindere dall'analisi dei suesposti casi giurisprudenziali scaturenti dai provvedimenti emanati dalle Autorità antitrust tedesca e da quella italiana nei confronti di Facebook.

Come ricordato anche dal TAR Lazio, i dati personali possono costituire «*un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico*» e possono, quindi, assurgere «*alla funzione di "controprestazione"*» contrattuale. Per questo, è necessaria la coesistenza, accanto agli strumenti di tutela tipici del diritto alla protezione dei dati personali quale diritto fondamentale, di altre garanzie del dato quale possibile oggetto di compravendita. Stante questo fenomeno di "patrimonializzazione" dei dati in atto nei mercati digitali, il piano della tutela della privacy e quello della protezione del consumatore non sono tra loro in rapporto antinomico, bensì sono necessari l'uno all'altro per garantire una protezione piena alla sfera giuridica del cittadino-consumatore.

Ciò comporta l'integrazione di due problemi: il dilemma della democrazia liberale nel mercato [47] e la garanzia dei diritti fondamentali non solo da poteri pubblici, ma anche da poteri privati [48]. Tale integrazione è il risultato sia della particolare tendenza dell'attuale società globale a costruirsi per linee orizzontali [49], superando la dimensione territoriale in senso classico ed aprendosi a

---

[45] Sul dualismo tra concezione morale e concezione negoziale si veda G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2/2018; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, 4/2020; Sulla circolazione dei dati cfr. *amplius* R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in *federalismi.it*, 3/2019; G. DI LORENZO, *La circolazione dei dati personali tra tutela della persona e ordine giuridico del mercato*, in *federalismi.it*, 21/2019. Cfr. anche G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020.

[46] G. BUTTARELLI, *This is not an article on data protection and competition law*, in *Competition Policy International*, 2019.

[47] Approfonditamente G. AMATO, *Il potere e l'antitrust. Il dilemma della democrazia liberale nella storia del mercato*, Bologna, 1998.

[48] Si veda il contributo di E. CREMONA in questo volume.

[49] M.R. FERRARESE, *Le istituzioni della globalizzazione*, Bologna, 2000, p. 43.

nuovi spazi grazie alla pressoché illimitata capacità di connessione, sia del potere accumulato dagli intermediari digitali, proprio in virtù del fatto che essi controllano imponenti quantità di dati personali. In particolare, proprio Mark Zuckerberg, *leader* del gruppo che più di tutti rende possibili le connessioni, ha avuto modo di affermare che Facebook è sempre più simile a un governo, che a una società [50]. E ciò comporta effetti sia, dal punto di vista microscopico, nella vita di ogni persona che, dal punto di vista macroscopico, nei rapporti con i poteri pubblici.

Si paventa, infatti, l'affermazione di un nuovo modello sociale. Come nel Medioevo esisteva il *civis-fidelis*, suddito dell'imperatore e fedele religioso, così nel futuro si profila l'affermazione di un altro modello, vale a dire quello dell'utente-cittadino-lavoratore, per via della contestuale combinazione di vari piani attraverso i social network [51], soprattutto in costanza dell'integrazione progressiva delle piattaforme e delle proiezioni della vita reale nel "Metaverso". Per limitare gli effetti negativi di questa tendenza, è quindi necessario integrare i piani della tutela consumeristica e della protezione dei dati personali, ma anche quello delle garanzie del lavoratore.

In ogni caso, occorrerà seguire con grande interesse gli sviluppi futuri, dal momento che, per ora, la questione si inquadra in una prospettiva *de iure condendo*. Come anticipato, infatti, si attendono importanti novità dal punto di vista giurisprudenziale sulle vicende legate ai provvedimenti delle Autorità antitrust nazionali contro Facebook, a questo punto non solo da parte del Consiglio di Stato della Repubblica italiana e della giurisprudenza statale e federale tedesca, ma soprattutto da parte della Corte di Giustizia dell'Unione europea. Inoltre, bisognerà studiare con grande attenzione gli sviluppi normativi nell'ambito del processo di regolazione del mercato digitale e della circolazione dei dati in Rete da parte dell'Unione europea. Sono, infatti, tutt'ora pendenti importanti proposte regolatorie in queste materie, come il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA), nonché il *Data Governance Act* e il c.d. Regolamento *e-Privacy*, il quale andrà a completare la disciplina generale tracciata dal Regolamento UE 2016/679 (GDPR) [52].

---

[50] La dichiarazione è riportata anche K. KLONICK, *The new governors*, cit., p. 1599: «*In a lot of ways Facebook is more like a government than a traditional company. We have this large community of people, and more than other technology companies we're really setting policies*»

[51] Così L. GREENE, *Silicon States. The power and politics of Big Tech and what it means for our future*, Berkley, 2018, 43, secondo cui vengono contemporaneamente combinati gli elementi di «*consumer voting, personal governments documents all stored on Facebook, and people's résumés up for public scrutiny*».

[52] Sul punto cfr. G. DE MINICO, *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal*, 1/2021, p. 385, la quale nota come tali fonti, pur rappresentando le pietre d'an-

Si tratta non solo di una tutela multilivello dei diritti dei cittadini-consumatori[53], ma anche di una tutela in una prospettiva integrata tra dimensione pubblicistica e privatistica. È anche in virtù di questo che si sostanzia la necessità di esercitare talune forme di regolazione dell'autonomia privata, atteso che nell'attuale contesto tale limite rappresenta un elemento essenziale del controllo democratico sul potere; specialmente per quanto attiene al potere derivante dalle informazioni[54]. Pertanto, «*la "strategia giuridica integrata", che, nel combinare strumenti privatistici e pubblicistici, tecniche procedurali e sostanziali, controlli individuali e controlli collettivi, intende dare un contenuto sostanziale all'idea della protezione dei dati come diritto fondamentale, la quale – come ci ricorda l'art. 8 della Carta dei Diritti fondamentali UE – è un elemento che ormai connota una certa identità costituzionale europea*»[55].

Atteso, dunque, che non si può impedire la circolazione dei dati personali nella società e, soprattutto, nell'economia odierna, resta però il fatto che servono regole certe. C'è da chiedersi se l'integrazione delle tutele per il cittadino e per il consumatore (ormai cittadino-consumatore o cittadino-utente nell'ambiente digitale), comporterà delle forme di integrazione dei poteri delle *authorities* e se sia il caso di cominciare a ragionare su procedure istituzionali di cooperazione tra di esse.

---

golo di questa "architettura in fieri" implicano comunque delle forme di partecipazione da parte di soggetti privati, andando a caratterizzare un modello di co-regolazione secondo una distribuzione gerarchica dei poteri normativi tra pubblico e privato, argomentando: «*otherwise, something else is taking place, which carries only the name of co-regulation. In this respect, the three above mentioned acts present an old vice affecting the European legislation, namely not taking a well-defined and courageous position. In fact, the DSA and the Framework Resolution provided that, in principle, private codes of conduct would be ancillary to the European regulation in progress. This would imply, if translated into the typical language of the sources of law, that the codes of conduct are only lawful when they are secundum legem (where "legem" means the European regulation); while the codes prater legem should be considered unlawful*».

[53] Rispetto alla quale G. RESTA, *I dati personali oggetto del contratto*, cit., pp. 129-130 osserva che: «*Il settore della protezione dei dati personali è ormai quasi integralmente disciplinato dalle fonti di diritto europeo, primario e derivato. Perciò, per rispondere ai quesiti pocanzi formulati, è necessario adottare una prospettiva multilivello, integrando l'analisi del diritto interno con il diritto sovranazionale. In particolare, è necessario soffermare l'attenzione su due diversi testi, che, sia pure da differenti prospettive, si accostano al problema della "disposizione" dei dati personali. Il primo attiene, in senso ampio, al settore della contrattazione online e in particolare alla tutela dei diritti dei consumatori; il secondo alla protezione dei dati personali. Si allude, rispettivamente, alla Direttiva 2019/700/UE relativa alla fornitura di contenuti e servizi digitali, e al Regolamento 2016/679/UE sulla protezione dei dati personali*».

[54] Così S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 93; ID., *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

[55] G. RESTA, *I dati personali oggetto del contratto*, cit., p. 130.

Sul punto, un'analisi condotta dal *Bundesverband der Verbraucherzentralen und Verbraucherverbände* ha affermato che la concorrenza e la protezione dei dati personali sono «come Castore e Polluce»[56] e che la soluzione non può che essere un'integrazione e una cooperazione tra di esse. Un ampio studio, redatto in inglese pochi mesi prima, per conto della medesima associazione, finanziato peraltro dal *Bundesministerium der Justiz und für Verbraucherschutz*, aveva, altresì, evidenziato dettagliatamente le sinergie tra le due discipline, pur non ignorando come sussistano in realtà dei punti conflittuali[57].

In conclusione, la questione resta aperta, ma c'è da aspettarsi che in un futuro molto prossimo le innovazioni legislative e quelle giurisprudenziali condurranno ad una risposta. Si è, dunque, sull'orlo del cambiamento, in attesa di comprendere come verrà definita la dimensione giuridica della protezione del cittadino-consumatore nei decenni a venire. Frattanto, però, ci si può rappresentare con un certo grado di certezza che verrà ribadita la centralità del diritto all'autodeterminazione informativa, la quale continuerà ad essere il fulcro intorno al quale ruota il sistema di tutela della persona umana nel mondo delle macchine.

[56] *Wettbewerb und Datenschutz: wie Kastor und Pollux. Synergien zwischen Wettbewerb und Datenschutz sowie Lösungsansätze für eine integrative und kooperative Betrachtung beider Politikfelder*, Berlin, 2021 consultabile in *https://www.vzbv.de/sites/default/files/2021-11/21-11-22_vzbv_Synergien_Datenschutz_Wettbewerb_Zusammenfassung_DE.pdf.*

[57] Cfr. W. KERBER, L. SPECHT-RIEMENSCHNEIDER, *Synergies between data protection law and competition law*, Berlin, 2021, consultabile in https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf.

PARTE II

LO SFRUTTAMENTO ECONOMICO DEI DATI PERSONALI

MONETIZZAZIONE, PATRIMONIALIZZAZIONE E TRATTAMENTO DI DATI PERSONALI

di *Guido d'Ippolito*

1. *Introduzione*

Tra i temi giuridici più discussi e controversi che animano il dibattito inerente al diritto delle nuove tecnologie, quello della "commercializzazione" dei dati personali è probabilmente il più controverso oltre che trasversale in vari ambiti e settori [1].

Infatti, in una società sempre più digitale, *data driven* [2] e che guarda alle innumerevoli applicazioni aperte dell'*IoT* e dell'Intelligenza artificiale [3], la scelta

[1] Sul tema, in generale, si vedano: G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2, 2018, pp. 411-440; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. informazione e informatica*, 4-5, 2018, pp. 689-726 e ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 23-60; R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in *federalismi.it*, 21, 2019, pp. 1-23; S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – Riv. dir. media*, 3, 2019, pp. 131-147; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, 4, 2020, pp. 635-674.

[2] A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. informazione e informatica*, 2, 2019, pp. 443-487: «*La Data Driven Innovation consiste sostanzialmente nell'adozione di un approccio sistematico e metodologico capace di garantire la trasformazione dei dati in innovazione. Più specificamen-*

tra il ritenere lecito o meno lo scambio di dati personali contro beni o servizi produce effetti che vanno oltre la disciplina della *data protection* per estendersi a quella in materia di tutela del consumatore e, in generale, alla tutela della concorrenza e alla regolazione dei mercati nonché dei fenomeni e delle dinamiche tipiche della Rete e delle piattaforme c.d. Big Tech.

Si è sicuramente dinanzi un tema complesso e, come dimostra questo volume, analizzabile da più punti di vista.

Ciò premesso, una soluzione generale e onnicomprensiva al tema sembrerebbe improbabile nella misura in cui sotto l'etichetta della "commercializzazione dei dati" possono ascriversi una serie variegata di ipotesi che hanno in comune l'attribuzione di un rilievo economico del dato personale [4]. Sicché, in questa categoria possono rientrare non solo diversi modelli di business attuati

---

te, il concetto fa riferimento alla capacità delle imprese e degli organismi pubblici di utilizzare le informazioni derivanti dall'analisi dei dati al fine di prendere decisioni consapevoli o di sviluppare prodotti e servizi migliori, in grado di semplificare la vita quotidiana degli individui e delle organizzazioni. In tale prospettiva, l'attività di analisi dei dati diviene un fattore chiave dello sviluppo economico e sociale»; OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD publishing, Paris, 2015, https://doi.org/10.1787/9789264229358-en.

[3] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto*, 1, 2019, pp. 27; A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal - Rivista di BioDiritto*, 3, 2019, pp. 205-235; C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal - Rivista di BioDiritto*, 3, 2020, pp. 359-387; O. POLLICINO, *Getting the Future Right Artificial Intelligence and Fundamental Rights. A view from the European Union Agency for Fundamental Rights*, in *BioLaw Journal - Rivista di BioDiritto*, 1, 2021, pp. 7-11; G. D'ACQUISTO, *Intelligenza artificiale. Elementi*, Torino, 2021.

[4] V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017; L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; A. MANTELERO, *La privacy all'epoca dei big data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1181-1212. Sull'informazione quale "bene", anche in relazione alla "dematerializzazione" dei dati personali e le modalità e tempistiche di trattamento, si vedano: J. LITMAN, *Information Privacy/Information Property*, in *52 Stan. L. Rev*, 2000, p. 1283; S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 52 ss.; V. ZENO-ZENCOVICH, voce *Informazione (profili civilistici)*, in *Dig. disc. priv., sez. civ.*, IX, 1993, p. 420 ss.; R. PARDOLESI, C. MOTTI, *L'informazione come bene*, in G. DE NOVA (a cura di), *Dalle res alla new properties*, Milano, 1991, p. 37 ss.; G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 209 ss.; C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020. Il tema è stato inoltre analizzato dal Garante per la protezione dei dati personali, l'Autorità Garante della Concorrenza e del Mercato e l'Autorità per le Garanzie nelle comunicazioni nell'ambito dell'"Indagine conoscitiva congiunta sui big data" del 10 febbraio 2020, disponibile sui siti istituzioni delle tre autorità.

dalle piattaforme digitali ma anche diversi modelli di circolazione dei diritti, così come ognuna di queste fattispecie può integrare condotte rilevanti ai sensi della normativa in materia di protezione dei dati personali (dunque un trattamento di dati personali) come anche ai sensi della disciplina consumeristica (dunque un rapporto di consumo[5]).

In considerazione di ciò, tale lavoro cercherà di fornire una breve analisi dei fenomeni che rientrano nella macrocategoria della commercializzazione dei dati personali per confrontarli con il modello legale del "corretto trattamento" come delineato dal Regolamento UE 2016/679 (in seguito, anche, "Regolamento" o "GDPR") al fine di individuare se e quando è ammissibile tale particolare fenomeno circolatorio del dato. In altre parole, se e quando lo scambio di dati contro beni e servizi implica un trattamento di dati personali corretto, lecito.

Non mancheranno, infine, riferimenti alla disciplina consumeristica nella consapevolezza della trasversalità dei temi e, soprattutto, del fatto che l'oggetto della tutela non è una particolare categoria di soggetto (l'interessato del trattamento piuttosto che il consumatore[6] o l'utente che sia) bensì la figura unitaria del "cittadino" nel contesto digitale. Sicché, in questo lavoro si parlerà indifferentemente di "utente" per intendere la generale figura di "cittadino" o "persona" che agisce anche nel contesto digitale, lasciando le espressioni più tecniche di "consumatore" o "interessato del trattamento" per riferirsi specificatamente a tali figure. Dall'altro lato si parlerà genericamente di "fornitore di servizio digitale" riferendosi a quella figura professionale che può essere, allo stesso tempo, "professionista" e "titolare del trattamento".

A ciò consegue la necessità di un'applicazione congiunta delle normative coinvolte, la collaborazione tra le diverse autorità di settore ai fini di un'adeguata valutazione e regolazione dei fenomeni, nonché *de iure condendo*, l'abbandono di sistemi regolatori verticali (cc.dd. "*silos*") in luogo di normative orizzontali e trasversali[7].

---

[5] C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, cit., p. 669 ss.

[6] F. BASSAN, M. RABITTI, *I consumatori nella social economy, tra big data e fake news*, in *Astrid Rassegna*, 17, 2017.

[7] F. BASSAN, *Potere dell'algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Soveria Mannelli, 2019.

2. *Commercializzazione e disponibilità del diritto alla protezione dei dati personali*

Ammettere o meno la possibilità di scambiare dati personali (*rectius*, di consentire al trattamento dei propri dati personali) in cambio dell'accesso a beni e servizi digitali implica interrogarsi sulla disponibilità del diritto fondamentale alla protezione dei dati personali (art. 8 CEDU; art. 8 Carta dei Diritti fondamentali dell'UE; art. 16 TFUE) [8] e sulle conseguenti modalità di circolazione giuridica di tali beni immateriali [9], ossia l'informazione riferita a un determinato soggetto o gruppi di soggetti, oggi sempre più suscettibile di valutazione e sfruttamento economico [10].

L'orientamento tradizionale, sulla scorta del carattere di indisponibilità tipico dei diritti fondamentali [11], nonché sull'inerenza e stretto rapporto che vi è tra l'informazione e la persona, suscettibile di delinearne l'identità personale e influenzare o manipolarne le condizioni e possibilità di vita, conclude per l'indisponibilità anche del diritto alla protezione dei dati personali e, quindi, per l'impossibilità di commercializzare, monetizzare o in altro modo scambiare i dati personali come se fossero una moneta o altro bene suscettibile di valutazione economica.

Più recentemente si sta però diffondendo un orientamento più possibilista che, nel riconoscere l'appartenenza della protezione dei dati personali anche all'ambito negoziale e non solo a quello dei diritti della personalità [12], ammette la commercializzazione del dato personale sulla base di alcuni fattori.

---

[8] F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, che rinviene il diritto alla protezione dei dati personali tra i diritti fondamentali della persona previsti all'art. 2 della Costituzione; S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012; L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, p. 13 ss. e dello stesso Autore, *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014, p. 47 ss.; G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Scherms*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, p. 116.

[9] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 3, 2020, pp. 642-662.

[10] A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. informazione e informatica*, 2, 2019, pp. 443-487.

[11] L. FERRAJOLI, *Diritti fondamentali. Un dibattito teorico*, Roma-Bari, 2001, e ID., *Iura paria. I fondamenti della democrazia costituzionale*, Napoli, 2017, pp. 105-106.

[12] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali*, cit., p. 642.

Innanzitutto, indisponibilità del diritto fondamentale non significa che l'oggetto di tale diritto non sia suscettibile di scambio giuridico [13]. Al contrario, bisognerà verificare di volta in volta quale sia la corretta disciplina circolatoria di un determinato bene giuridico anche in considerazione del fatto che la pratica giurisprudenziale annovera ormai diversi esempi di «*atti in senso lato abdicativi di posizioni riconducibili alla categoria dei diritti fondamentali*» [14].

Si possono distinguere così diversi modelli circolatori dei diritti fondamentali in base al bene giuridico che ne è l'oggetto e che vanno dalla donazione di parti del corpo umano, per i quali è preclusa qualsiasi forma di circolazione di mercato (ossia di circolazione con finalità di lucro) ma è ammessa la disposizione gratuita con funzione solidaristica, alla cessione di attributi immateriali della persona suscettibili di sfruttamento economico, come i dati personali per i quali la disposizione è lecita purché nel rispetto della disciplina imperativa che presidia il settore, proprio a tutela dei valori della persona [15].

Alla tesi per cui indisponibilità del diritto non corrisponde necessariamente l'impossibilità di scambio dell'oggetto di tale diritto si associa, inoltre, il fatto che l'autonomia nelle scelte personali costituisce una componente essenziale del rispetto della dignità umana (artt. 3, comma 2, e 41, comma 2, Cost.; art. 1 della Carta dei Diritti fondamentali dell'UE) [16]. Elemento questo

---

[13] G. RESTA, *Contratto e diritti fondamentali,* in *Enc. dir.*, I, Milano, 2021, p. 298, per il quale: «*Decisiva è invece la constatazione per cui, anche a tenere saldo sul piano teorico l'assioma dell'indisponibilità, da ciò non può farsi discendere automaticamente la conseguenza dell'inoperatività del contratto quale specifico strumento di esercizio – non l'unico, ovviamente, ma uno dei vari strumenti che compongono il quadro dell'autonomia privata – dei diritti in oggetto. La distinzione di fondo tra la titolarità e l'esercizio di un determinato diritto soggettivo, ivi compresi i diritti che meritano la qualifica di fondamentali, gioca infatti un ruolo cruciale per spiegare il significato attuale del predicato dell'indisponibilità. Mentre l'assunto in discorso è direttamente riferibile al primo profilo ricordato, precludendo qualsiasi negozio dispositivo che abbia ad effetto un mutamento nella titolarità della situazione soggettiva, esso non è d'ostacolo al riconoscimento di altri atti d'autonomia, che senza provocare la perdita o il trasferimento del diritto, diano vita ad un rapporto giuridico, il quale non appaia, ad un apprezzamento nel merito, in contrasto con basilari scelte di valore dell'ordinamento*».

[14] Dalla limitazione volontaria della libertà di manifestazione del pensiero in ambito giornalistico o la rinuncia al diritto morale alla paternità dell'opera dell'ingegno, fino allo sfruttamento delle utilità economiche ottenibili dagli attributi corporei e incorporali della persona come il plasma o il materiale biologico umano, il nome e l'immagine di persone note e, ovviamente, i dati personali, sul tema si rinvia all'accurata analisi di G. RESTA, *Contratto e diritti fondamentali*, cit., p. 299.

[15] *Ivi*, p. 302.

[16] S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, p. 21 ss., e ID., *Antropologia dell'«homo dignus»*, ora in S. RODOTÀ, *Critica del diritto privato*, *Editoriali e saggi della Rivista Critica del Diritto Privato*, raccolti da G. Alpa e M. Marella, Napoli, 2017.

da cui deriva una libertà associata alla gestione e circolazione dei propri dati personali [17].

In secondo luogo, non si può non tener conto del fatto che il trattamento dei dati personali è un ambito ormai interamente regolamentato da una normativa di rango europeo diretta a conciliare la protezione della persona tramite il corretto trattamento dei suoi dati personali con l'esigenza di un'ampia e libera circolazione degli stessi nel mercato europeo (in particolare il Regolamento UE 2016/679) [18].

In terzo luogo, non solo in tale specifica normativa non è rintracciabile alcun divieto al fenomeno della commercializzazione dei dati personali ma, in altre normative, tale possibilità è ormai ammessa e codificata. Il riferimento è qui alla Direttiva 2019/770 [19], il cui art. 3, par. 1, espressamente consente di scambiare un contenuto o un servizio digitale in luogo della fornitura da parte del consumatore dei suoi dati personali. Tale disposizione è ulteriormente chiarita dal considerando 24 che parla, quale specifico modello commerciale, dei dati personali come strumento alternativo al pagamento in denaro [20].

Si è così concluso che l'attuale assetto giuridico non solo non vieta o anche solo "scoraggia" il fenomeno della commercializzazione o monetizzazione consapevole dei dati personali ma, specie in alcuni casi particolari come quelli regolati dalla Direttiva 2019/770, è oggetto di un peculiare regime basato sulla combinazione di un atto autorizzativo unilaterale e sempre revocabile, come il consenso [21], con un "*contratto conformato in chiave pubblicistica*" [22].

Sicché, se in generale, quanto meno a parere di chi scrive, è possibile concludere per l'ammissibilità della commercializzazione dei dati personali e, quindi, della disponibilità dell'oggetto del relativo diritto purché nel rispetto dei principi e della corretta applicazione degli istituti dettati dal Regolamento e dalle altre normative coinvolte, è nell'applicazione pratica e nell'esame dei

---

[17] R. MESSINETTI, *op. cit.*, pp. 1-23.

[18] C. COLAPIETRO, *Il nuovo quadro giuridico europeo sulla protezione dei dati personali e l'adeguamento della normativa nazionale*, in *Studi parlamentari e di politica costituzionale*, 2018, 201-202, pp. 7-25; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.; L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale. Convergenza tra regolazioni e tutele individuali nell'economia* data-driven, Milano, 2021.

[19] Direttiva UE 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

[20] A. DE FRANCESCHI, *Il "pagamento" mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1389.

[21] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., pp. 411-440.

[22] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 305.

differenti modelli di business adottati dal mercato che si rinvengono le maggiori difficoltà.

In altre parole, se è astrattamente configurabile la possibilità di attribuire valore economico ai dati personali al fine di un loro riutilizzo commerciale, nel concreto bisognerà poi verificare se tale possibilità è esercitata nel rispetto delle norme e del quadro giuridico posto a presidio del corretto trattamento dei dati personali. Infatti, solo il rispetto in concreto di tali norme permetterà di controbilanciare e attenuare i rischi connessi allo scambio, la dazione o al conseguente riutilizzo per finalità commerciali di attributi immateriali della personalità del soggetto a cui sono riferiti. La tutela dell'identità e, soprattutto, della dignità della persona nel contesto digitale passa dunque, non tanto dal divieto di ogni fenomeno circolatorio dei dati personali, operazione ormai difficilmente arrestabile nella pratica, quanto dal rigoroso rispetto delle norme che presidiano il settore e da un'accurata vigilanza del mercato da parte delle autorità preposte.

3. *Modelli di business: patrimonializzazione e monetizzazione dei dati personali*

Dall'esame delle prassi del mercato è possibile identificare diversi modelli di business incentrati sul trattamento e conseguente attribuzione di valore economico ai dati [23], cui può associarsi un diverso modello di circolazione dei diritti fondamentali in modo da desumerne disciplina, limiti e regole [24].

In primo luogo, dalle abitudini del mercato si evince la tendenza a passare da un sistema in cui il trattamento del dato personale costituisce un'attività accessoria ma necessaria a quella principale richiesta dall'utente, quale poteva essere la consegna di un pacco o l'erogazione di un servizio, a un sistema in cui il dato personale è sempre più la *ratio* che spinge a svolgere una certa attività. In altre parole, la fornitura del dato passa dall'essere un elemento strumentale all'esercizio di un'attività di business al motivo per cui questa è svol-

[23] Per una panoramica sui principali modelli di business adottati dalle piattaforme digitali si veda: M. MURSIA, C.A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in *MediaLaws - Riv. dir. media*, 2, 2021, pp. 165-189.

[24] Con riguardo alla possibilità e i limiti di disporre dei diritti fondamentali tramite lo strumento negoziale, si rinvia alle interessanti e limpide pagine di G. RESTA, *Contratto e diritti fondamentali*, cit. Per una rassegna sulle prospettate tesi di ricostruzione dei rapporti sinallagmatici tra le piattaforme digitali e gli utenti si veda G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 417 ss.

ta[25]. La raccolta di moli enormi di dati (*big data*) è sempre più il motivo che anima l'attività di impresa[26] che quindi dovrà ipotizzare e offrire un servizio che giustifichi la fornitura dei dati da parte dell'utente[27] configurando quello che è stato definito "mercato dell'attenzione"[28].

Il motivo per cui è il dato sono i dati l'oggetto dell'interesse delle imprese, nonché la base del loro modello di business, è che questi possono essere trattati, analizzati, arricchiti e quindi riutilizzati al fine di trarne informazioni suscettibili di rilievo economico. I dati vengono così "valorizzati" o "patrimonializzati" al fine di estrarne valore economico o informazioni scambiabili sui mercati digitali[29].

È dunque questa la prima fattispecie rilevante nell'ambito del fenomeno della commercializzazione dei dati personali, corrispondente al modello di business c.d. "*zero-price*"[30]. Si tratta di tutti quei servizi digitali che vengono offerti all'utente senza che lo stesso debba eseguire una controprestazione di natura pecuniaria. L'utente dovrà però consentire al trattamento dei propri dati personali per finalità che vanno dalla necessità di eseguire la prestazione richiesta ad interessi commerciali.

Nei modelli di business "*zero-price*" il valore economico per l'impresa deriva non tanto dalla raccolta in sé dei dati o della loro fornitura da parte dell'interessato, quanto dal successivo trattamento di aggregazione, profilazione, analisi e valorizzazione che l'impresa svolge, con propri algoritmi, sull'enorme numero di dati accumulati[31]. Quindi, per l'impresa il valore economico del

---

[25] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali*, cit., p. 652 ss., che invita ad analizzare il fenomeno circolatorio dei dati personali, con uno sguardo alla causa del contratto, attraverso la descrizione funzionale dell'operazione economica concreta realizzata.

[26] Il tema è stato oggetto d'esame da parte del Garante per la protezione dei dati personali, l'Autorità per le Garanzie nelle Comunicazioni e l'Autorità Garante della Concorrenza e del Mercato in un'indagine conoscitiva congiunta sul tema: *Indagine conoscitiva sui big data*, febbraio 2020, cit.

[27] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 416 ss.

[28] Y.N. HARARI, *21 lezioni per il XXI secolo*, Milano, 2018, p. 116.

[29] V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?*, in *Medialaw – Riv. dir. media*, 2, 2019.

[30] M. MURSIA, C.A. TROVATO, *op. cit.*, p. 169 ss.

[31] AgCom, *Osservatorio sulle piattaforme online*, dicembre 2019, p. 23: «*Nel caso dei servizi online gratuiti, si realizza di fatto uno scambio implicito tra gli utenti e la piattaforma, che si sostanzia nella cessione, da parte dei primi, dei propri dati a fronte, non già di un corrispettivo economico, ma appunto del servizio offerto gratuitamente dalla piattaforma. La disponibilità di grandi masse di dati individuali consente alla piattaforma di compiere un'accurata profilazione degli utenti, dalla quale dipende la possibilità per gli inserzionisti che si servono della piattaforma di raggiungere target specifici di consumatori*».

dato è indiretto nella misura in cui non si realizza al momento della fornitura del dato (*rectius*, del consenso dell'interessato al trattamento dei suoi dati) bensì in un secondo momento, in seguito ad un ulteriore trattamento di valorizzazione che, tramite sofisticati algoritmi, consente di estrarre valore economico dai dati creando categorie e profili degli interessati da reimpiegare, per esempio, nel settore della pubblicità online [32].

Questo modello è definito "*zero-price*" proprio perché l'utente accede a un bene o servizio senza il pagamento di alcuna somma di denaro, "gratuitamente". Ciò ha generalmente portato a ritenere che la controprestazione dell'utente consistesse proprio nella fornitura di dati personali [33] che assumono così il ruolo di corrispettivo [34] non monetario e integrando la nota massima per cui "se il servizio è gratuito vuol dire che la merce è l'utente" (c.d. "*Internet cost trap*") [35]. La dazione dei dati personali sarebbe quindi una componente implicita del prezzo pagato dagli utenti [36], una sorta di controprestazione e quindi un'equiparazione dei dati personali alla moneta [37].

Proprio in tale contesto si inserisce l'analisi svolta dall'Autorità Garante della Concorrenza e del Mercato che ha portato, nel 2018, a sanzionare Facebook per aver ingenerato nell'utente, tramite l'utilizzo della parola "gratuito" nei suoi *claim*, l'idea che l'accesso alla propria piattaforma *social* non comportasse alcuna "perdita economica" o comunque lo scambio di alcun valore da parte dell'utente [38]. Poiché invece l'AGCM accerta che l'utilizzo dei dati

---

[32] Con riferimento al trattamento dei dati personali per finalità di marketing online, agli algoritmi e ai vari sistemi di "*programmatic advertising*", sia consentito rinviare a G. D'IPPOLITO, *Profilazione e pubblicità targettizzata on line. Real-Time Bidding e behavioural advertising*, Napoli, 2021.

[33] A. METZGER, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *JIPITEC*, 8(2), 2017.

[34] Sul tema: OEDC, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers No. 220, 2013; G. MALGIERI, B. CUSTERS, *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017.

[35] Si fa riferimento a quella che è stata definita "trappola del dono". Sul tema: J. LANIER, *You Are Not a Gadget: a Manifesto*, Penguin, 2011; A. DE FRANCESCHI, *Il "pagamento" mediante dati personali*, cit., p. 1397.

[36] Organisation for Economic Co-operation and Development, *Quality considerations in digital zero-price markets. Background note by the Secretariat*, DAF/COMP(2018)14, 28 November 2018, p. 4.

[37] A. DE FRANCESCHI, *Il "pagamento" mediante dati personali*, cit., p. 1389

[38] AGCM, *Provvedimento del 29 novembre 2018. PS11112 – Uso dei dati degli utenti a fini commerciali: sanzioni per 10 milioni di euro a Facebook*: www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Face

degli utenti è essenziale per consentire alla piattaforma di remunerare la propria attività, ha ritenuto che l'utilizzo della parola "gratuito" integrasse una pratica commerciale scorretta perché idonea a trarre in inganno il consumatore che non verrebbe edotto del reale valore e utilizzo commerciale dei suoi dati e, quindi, dell'entità della prestazione richiestagli. Tale provvedimento è stato confermato sia dal TAR del Lazio, con la sentenza del 10 gennaio 2020, n. 260, che dal Consiglio di Stato, con la sentenza 29 marzo 2021, n. 2631[39].

Ciononostante, come si avrà modo di chiarire, non può essere sempre questa la corretta interpretazione di tali rapporti e, come è stato osservato: «*Una cosa è sostenere che i dati personali, nell'economia di un contratto, costituiscano il corrispettivo di un servizio e altra cosa è sostenere che pur in assenza di tale corrispettività, l'accesso ai dati personali – o, anche l'accesso ai dati personali – degli utenti sia il motivo o l'interesse economico che determina il fornitore del servizio a offrire gratuitamente il servizio senza effettivamente esigere un corrispettivo*»[40].

Pertanto, con riferimento al *genus* della commercializzazione dei dati personali, tale modello di business può essere considerato una sua *species* per la quale si può parlare di trattamento di "patrimonializzazione dei dati personali", per tale intendendosi tutte quelle attività volte ad estrarre valore e informazioni economicamente rilevanti da reimpiegare in altri mercati per fini remunerativi.

Un secondo modello di business rilevante è quello invece dello scambio diretto dei dati contro moneta. Anche conosciuto come "*personal data economy model*", esso si pone l'obiettivo di riconoscere agli utenti una parte o l'intero valore che le piattaforme attribuiscono ai dati personali attraverso processi di profilazione e *advertising* e, quindi, tramite la patrimonializzazione di cui sopra.

In questo caso, alla fornitura del dato da parte dell'utente segue la corresponsione di una somma di denaro[41]. Il valore del dato è quindi più o meno

book. L'AGCM ha così formulato la pratica commerciale scorretta ad oggetto: *«"Pratica a) pratica ingannevole" consisteva nelle violazione degli artt. 20, 21 e 22 del Codice del consumo, in quanto il professionista non informerebbe 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 cede, rendendolo edotto della sola gratuità della fruizione del servizio, così da indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (registrazione al social network e permanenza nel medesimo)*».

[39] G. SCORZA, *Facebook non è gratis?*, Commento a Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631, in *Dir. internet*, 3, 2021.

[40] *Ivi*, p. 356.

[41] M. MURSIA, C.A. TROVATO, *op. cit.*, p. 170 ss.

istantaneamente liquidato all'utente da parte dell'impresa sicché si può parlare di trattamento di "monetizzazione".

Sul mercato sono presenti diversi servizi che si pongono come obiettivo quello di retribuire o di rendere partecipe l'utente dei guadagni che le grandi piattaforme digitali ottengono tramite la valorizzazione e reimpiego dei dati in diversi settori. Sicché questi servizi si sostanziano nel retribuire direttamente l'interessato con una cifra corrispondente a una parte del valore ottenuto tramite la patrimonializzazione dei dati personali.

Ciononostante, anche questo modello di monetizzazione non sembrerebbe esattamente ricalcare lo schema dell'equiparazione tra dati personali e moneta. Ciò quanto meno stando allo schema descritto dall'art. 3, par. 1, della Direttiva 2019/770 che prevede che i dati siano utilizzati direttamente per accedere a beni e servizi, non anche per la remunerazione dell'utente.

Entrambi i modelli costituiscono comunque degli idealtipi che, seppur di agevole definizione in astratto, risultano nella pratica di non semplice distinzione laddove nella prassi le sfumature e le sovrapposizioni parziali tra più modelli costituiscono la norma.

4. *Trattamento di dati personali per finalità di "commercializzazione". La patrimonializzazione*

Al primo modello di business, quello c.d. "*zero-price*", si può associare un modello di «disposizione dei diritti sugli attributi costitutivi della personalità» definito dalla dottrina come "modello del consenso remunerato". Caratteristica di tale modello è quello di dotare sia l'atto dispositivo che il conseguente rapporto di una serie articolata di garanzie e salvaguardie disposte da una normativa *ad hoc*[42].

Nel caso della patrimonializzazione dei dati personali, tali garanzie sono dettate dal Regolamento e sono individuabili, per quanto riguarda l'atto dispositivo, nella corretta informazione, nelle particolari caratteristiche di effettività e validità del consenso, nella sua revocabilità[43] e negli altri presupposti per l'utilizzo dei fondamenti di liceità del trattamento, nonché, con riferimento al rapporto conseguente, nei diritti dell'interessato di cui agli artt. 15-22 del Regolamento e negli altri istituti da questo previsti. Come rileva-

[42] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 304 ss.

[43] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 435; R. MESSINETTI, *op. cit.*, p. 10 ss.

to [44] però, non ci si pone comunque al di fuori dello spazio di mercato perché non solo il Regolamento non vieta la patrimonializzazione ma la Direttiva 2019/770, in specifici casi, attribuisce particolare valore giuridico allo scambio di dati contro servizi.

Dunque, un fornitore di servizi digitali offre la propria attività a prezzo zero, senza richiedere il pagamento di una somma monetaria all'utente, perché confida di poter sfruttare il valore economico dei dati personali così ottenuti e di quelli ulteriori prodotti dall'interazione dell'utente con la sua piattaforma.

Dal punto di vista della protezione dei dati personali si integra quindi di un "trattamento" *ex* art. 4, n. 2), del Regolamento, la cui valutazione passa da un necessario chiarimento ontologico e dall'adeguato rispetto dei principi e delle norme del Regolamento.

Infatti, se può risultare agevole in astratto presumere che in assenza di un corrispettivo in denaro saranno i dati personali a fungere da risorsa e *asset* grazie al quale l'impresa può remunerare la sua attività, non è però sempre condivisibile, dal punto di vista della protezione dei dati personali, considerare i dati come una forma di pagamento, corrispettivo o controprestazione.

Bisognerà in via preliminare distinguere due ipotesi: da un lato il caso in cui i dati forniti dall'utente siano necessari affinché il fornitore del servizio possa eseguire lo stesso; dall'altro quello in cui tale fornitore richieda o un numero di dati personali superiore a quelli necessari per l'esecuzione della sua prestazione (*rectius*, richieda anche altre categorie di dati per finalità non necessarie, e quindi terze, alla fornitura del servizio richiesto dall'utente) oppure gli stessi dati necessari al servizio vengano trattati anche per raggiungere una finalità ulteriore rispetto a quella principale.

Nel primo caso non vi sarà alcuno spazio per fenomeni di patrimonializzazione o commercializzazione dei dati personali laddove si ricade nella fattispecie tradizionalmente prevista di trattamento di dati personali [45], in cui i dati sono necessari per eseguire il servizio, che risulterà lecito nella misura in cui saranno rispettate le norme in materia. Di tale eventualità, è significativo notare, tiene conto anche la Direttiva 2019/770 che correttamente esclude l'applicazione del-

---

[44] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 305.

[45] A tal riguardo, si veda la posizione espressa dallo European Data Protection Supervisor per il quale la cessione di dati personali come controprestazione al servizio digitale potrebbe non corrispondere ad un interesse economico e lucrativo del fornitore del servizio bensì essere necessario per il funzionamento del servizio offerto. Pertanto, l'automatica equiparazione tra la moneta e i dati renderebbe difficile, se non impossibile, identificare i casi in cui i dati vengono forniti perché necessari per la prestazione del servizio e quando siano controprestazione per la fornitura di servizi o contenuti digitali. EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017, p. 7 ss.

la stessa nel caso in cui: «*i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente Direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti*» (art. 3, par. 1) [46].

Con riferimento alle altre due ipotesi, invece, la possibilità di una patrimonializzazione dei dati forniti dagli utenti è sì astrattamente configurabile ma la sua liceità concreta non potrà che essere accertata previa valutazione caso per caso, ai sensi della disciplina contenuta nel Regolamento.

La liceità di questi fenomeni di patrimonializzazione dipenderà, anche qui, dal rispetto della normativa e, in particolare, dei principi di liceità, limitazione delle finalità e minimizzazione [47]. Sicché, per poter raccogliere e trattare dati ulteriori rispetto a quelli necessari per la fornitura del servizio richiesto dall'utente, il titolare del trattamento dovrà: innanzitutto darne idonea menzione nell'ambito dell'informativa all'interessato, insieme alle rispettive finalità (ossia la patrimonializzazione, la "valorizzazione" dei dati per trarne informazioni economicamente rilevanti), affinché questo sia edotto della presenza di trattamenti ulteriori che egli potrebbe non volere. Ciò sarà utile anche al fine di evitare pratiche commerciali scorrette sicché si può ritenere che la disciplina consumeristica e quella a tutela del dato personale abbiano un punto di contatto significativo sul tema della trasparenza.

Il titolare del trattamento dovrà poi individuare un'idonea base giuridica e, conseguentemente, applicare e rispettare gli istituti del Regolamento di volta in volta rilevanti. In altre parole, per richiedere ulteriori dati da sottoporre a un processo di patrimonializzazione, il titolare dovrà (almeno) essere trasparente e individuare un'idonea base giuridica che legittimi il trattamento in relazione alle finalità (tendenzialmente, è plausibile identificare tale base giuridica nella richiesta di un apposito consenso).

Caso più complesso ma affine al precedente è quello in cui il titolare utilizzi gli stessi dati necessari per il servizio anche per altri fini, in particolare per remunerare la propria attività. In questo caso, oltre al rispetto del principio di trasparenza e quello di liceità del trattamento, si associa il necessario rispetto del principio di limitazione delle finalità (art. 5, par. 1, lett. b), Reg.) [48]. Que-

---

[46] Si vedano anche i considerando 24, 25, 37 della Direttiva 2019/770.

[47] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 22, 2018.

[48] Sul tema, sia consentito rinviare a G. D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data*, in *Dir. informazione e informatica*, 2018, pp. 943-987.

st'ultimo dispone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con le finalità originarie. Ciò comporta che per usare gli stessi dati per finalità ulteriori e diverse rispetto a quella principale bisognerà dimostrare che le finalità secondarie siano comunque compatibili con quella principale.

Nel far ciò, l'art. 6, par. 4, del Regolamento annovera alcuni criteri di cui tener conto. Ossia, al fine di accertare che la finalità secondaria di patrimonializzazione sia compatibile con la finalità originaria per la quale l'interessato ha fornito i propri dati, il titolare dovrà tener conto di: ogni nesso tra le due finalità; del contesto e, in particolare, della relazione tra l'interessato e il titolare; della natura dei dati personali coinvolti, andando ad accertarsi se siano coinvolti categorie particolari di dati o dati relativi a condanne penali e a reati; delle possibili conseguenze sugli interessati; dell'esistenza di garanzie adeguate. Esemplificativamente, ciò vuol dire che il fornitore del servizio dovrà dimostrare, tra le varie cose, che l'ulteriore trattamento di patrimonializzazione non arrechi pregiudizio all'utente.

Qualora tale dimostrazione non fosse possibile, il titolare non avrà altra scelta che individuare una nuova base giuridica per legittimare l'ulteriore trattamento degli stessi dati già in suo possesso ma per una finalità altra. Si ricade così nel caso precedente in cui il titolare chiede dati ulteriori per finalità ulteriori.

Infine, l'ultima ipotesi di patrimonializzazione dei dati personali, tendenzialmente quella più diffusa nella prassi e alla quale fanno ricorso non solo le grandi piattaforme ma anche fornitori di servizi digitali di rilievo nazionale come i giornali e i siti di informazione[49], consiste nel condizionare la fornitura di un servizio richiesto dall'utente al consenso prestato dallo stesso al trattamento dei suoi dati (altri o le medesime categorie) per servizi a lui non necessari ma da cui il titolare può ottenere remunerazione, come nel caso dell'invio di newsletter per finalità di marketing.

È questo il fenomeno del c.d. "*tying*" o "*bundling*" esplicitamente previsto dall'art. 7, par. 4, del Regolamento. Tale articolo, ben lungi dal vietare tale possibilità, si limita a richiamare una particolare attenzione nell'esame di tale costruzione negoziale, in quanto la condizionalità sarà lecita solo se basata su un consenso "liberamente prestato". La norma introduce quindi una presunzione (relativa) di invalidità del consenso[50].

---

[49] G. SCORZA, *Facebook non è gratis?*, cit., p. 570 ss.

[50] Il considerando 43 del Regolamento afferma proprio che: «*Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contrat-*

Tale ipotesi è quindi ontologicamente diversa da quella in cui a fianco al servizio principale il fornitore offra altri servizi collegati ma autonomi che l'utente può liberamente accettare sulla base del consenso senza che un suo rifiuto pregiudichi la fornitura del servizio principale. In quest'ultimo caso non troverà applicazione l'art. 7, par. 4, del Regolamento laddove questo si riferisce solo al caso in cui la prestazione di un servizio sia condizionata, dunque subordinata e non oggetto di scelta da parte dell'utente, alla prestazione del consenso al trattamento di dati personali non necessari all'esecuzione del servizio richiesto [51].

In entrambi i casi potrebbero annidarsi forme di patrimonializzazione di dati personali (quindi di valorizzazione economica degli stessi) ma solo nel caso della condizionalità si pongono problemi di compatibilità con la disciplina in materia di protezione dei dati personali.

Il nodo della questione, tutt'ora irrisolto, si sposta quindi su quando tale consenso sia effettivamente libero [52]. Sono ravvisabili qui almeno due orientamenti.

Il primo deriva dall'interpretazione rigorosa che il Comitato europeo per la protezione dei dati (European Data Protection Board, EDPB) fa della norma citata, la cui portata applicativa viene ristretta a ipotesi non sempre facilmente realizzabili nella pratica. Per l'EDPB infatti: «*Se il consenso è un elemento non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio. […] In termini generali, qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in vari modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido*» [53].

L'EDPB, al fine di garantire che la finalità del trattamento non sia "mascherata" né accorpata all'esecuzione di un contratto o alla prestazione di un servizio, nonché per consentire all'interessato di mantenere sempre il controllo sui propri dati, ritiene lecita la condizionalità solo nel caso in cui il titolare offra all'interessato la scelta tra un servizio condizionato all'uso dei dati personali per finalità supplementari e lo stesso servizio, "equivalente", che però non richieda un siffatto consenso [54].

---

to, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione».

[51] Comitato europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, Versione 1.1, adottate il 4 maggio 2020, punto 32.

[52] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 426 ss.

[53] Comitato europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso*, cit., punti 13 e 14.

[54] EDPB, *Linee guida 5/2020 sul consenso*, cit., p. 10 ss., in particolare il punto 37 dove si

Questo orientamento restrittivo è seguito dalle autorità di settore. Per esempio il Garante italiano che, in un caso in cui una società aveva subordinato l'adesione del cliente al servizio (erogazione di vantaggi, sconti e partecipazione a concorsi a premi) all'acquisizione del consenso al trattamento dei dati che lo riguardano per finalità di marketing, ha ritenuto che così facendo si realizzasse una coazione della volontà dell'interessato che, in assenza di apposita informativa, viola gli artt. 7, par. 4 e 13, del Regolamento [55].

Il secondo orientamento è desumibile da una sentenza della Corte di Cassazione, la n. 17278/2018, la quale ritiene lecito, per il fornitore del servizio, non offrire lo stesso di fronte alla mancata accettazione dell'utente delle condizioni da questo imposte, purché a determinate condizioni [56]. Sicché ammette la possibilità di condizionare il contratto (ricezione di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro) alla prestazione del consenso al trattamento dei dati per altre finalità (l'invio di comunicazioni promozionali nonché di informazioni commerciali da parte di terzi) nel caso in cui il servizio principale sia "fungibile", nel senso che sia uno dei tanti servizi disponibili sul mercato a cui l'utente possa rinunciare senza gravoso sacrificio [57].

---

legge: «*Il titolare del trattamento potrebbe sostenere che la sua organizzazione offre all'interessato una scelta reale mettendolo in grado di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro. Finché esiste la possibilità che il contratto venga eseguito o che il servizio oggetto del contratto venga prestato dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti*».

[55] Garante per la protezione dei dati personali, *Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A.*, 15 gennaio 2020, doc. web n. 9256486, §3.4.

[56] Secondo la Cass. civ., sez. I, 25 luglio 2018, n. 17278, §2.7, infatti: «*nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito internet, il quale somministri un servizio fungibile cui l'utente possa rinunciare senza gravoso sacrificio, di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti*». La sentenza è commentata da S. THOBANI, *Operazioni di* tying *e libertà del consenso*, in *Giur. it.*, 2019, pp. 533-539. Si veda anche: F. RUGGERI, *Sulla nozione di consenso nella nuova disciplina privacy: alcune prime considerazioni*, in *giustiziacivile.com*, 21 marzo 2019.

[57] Cass. civ., sez. I, 25 luglio 2018, n. 17278, §2.5: «*Nulla, infatti, impedisce al gestore del sito – beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile –, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, me esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato*».

Se da un lato il primo orientamento sembra così rigoroso da ridurre drasticamente le possibilità di *tying* lecito di cui all'art. 7, par. 4, del Regolamento, dall'altro l'orientamento della Cassazione sembrerebbe invece troppo permissivo, anche in considerazione del fatto che si pone in netto contrasto con l'interpretazione dell'EDPB [58].

La soluzione sta probabilmente nel mezzo ma non potrà non passare da una più adeguata ed effettiva informazione all'utente della presenza e delle caratteristiche di tale condizionalità, nonché di una più adeguata valutazione degli stessi elementi "di apertura" previsti dall'EDPB, ossia la valutazione dell'operazione negoziale complessiva non solo in termini di libera scelta ma anche, appunto, di corretta informazione, di riconoscimento all'interessato della revoca e dei suoi diritti affinché mantenga un controllo sui propri dati, nonché dei possibili effetti pregiudizievoli sulla sua sfera giuridica [59].

Si tratta di una valutazione che ha punti di contatto con l'analisi in tema di pratiche commerciali, ingannevoli o aggressive, effettuate dall'AGCM che, pure, è intervenuta a dichiarare scorretta una pratica commerciale che imponeva, quale condizione obbligatoria per partecipare ad una promozione, il consenso all'utilizzo dei dati personali anche per finalità di marketing [60]. In questo caso la pratica è stata considerata aggressiva in quanto il consenso era richiesto dopo una lunga serie di passaggi che non lasciavano altra scelta all'utente se non quella di rispettare anche questa condizione [61].

---

[58] EDPB, *Linee guida 5/2020 sul consenso*, punto 38: «*Il Comitato ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste la possibilità di scegliere tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti*».

[59] EDPB, *Linee guida 5/2020 sul consenso*, cit., p. 10 ss.

[60] Sul punto si veda la violazione accertata dall'AGCM nei confronti di Samsung per aver questa posto in essere pratiche commerciali scorrette consistenti nell'aver promosso la vendita di propri prodotti con la promessa della attribuzione di ulteriori prodotti e/o rimborsi sul prezzo nel caso di loro acquisto: senza adeguata informazione (pratica A, sanzionata con 2.125.000 euro) e subordinandone l'operatività all'acquisizione del consenso all'utilizzo dei dati personali dei consumatori per finalità di marketing (pratica B, sanzionata con 975.000 euro). AGCM, *PS10207 – Promozioni scorrette, sanzioni a Samsung Electronics Italia per oltre tre milioni di euro*, 25 gennaio 2017.

[61] AGCM, *PS10207 – Promozioni scorrette, sanzioni a Samsung Electronics Italia per oltre tre milioni di euro*, 25 gennaio 2017, §V.3.3. L'AGCM ritiene lecita una pratica che, probabilmente, il Garante per la protezione dei dati personali avrebbe comunque considerato illecita sotto il profilo del mancato rispetto del principio di minimizzazione dei dati. Sicché la stessa viene sanzionata dall'AGCM per la sua aggressività. Ai punti 123-127 si legge, infatti: «*L'attività in ar-*

La fattispecie del *tying*, quale peculiare condizione a cui viene subordinata l'esecuzione del contratto, è quella dietro la quale è più probabile che si annidi un fenomeno di commercializzazione e patrimonializzazione dei dati personali, nonché, forse, quello che più si avvicina all'uso dei dati personali quale nuova *currency*, in quanto solo in questo caso l'utente non potrà accedere al servizio senza aver ceduto dati per finalità da lui non richieste, non necessari al servizio ma che soddisfano il solo interesse del titolare ad ottenere profitti. In ogni caso, tale trattamento sarà lecito o meno, ai sensi della lettera dell'art. 7, par. 4, del Regolamento, solo se il consenso sia libero ed effettivo, ma anche tale condizione, oltre che di difficile realizzazione pratica nonché oggetto di interpretazioni ancora aperte, non è accertabile in astratto ma solo dopo un'analisi caso per caso.

Dunque, l'applicazione del modello del consenso remunerato mira a presidiare i diritti, gli interessi e la dignità della persona, avvolgendo di garanzie sia l'atto dispositivo che il conseguente rapporto. Pertanto, il trattamento di patrimonializzazione dovrà essere portato all'attenzione dell'utente, fondarsi su un'idonea base giuridica e rispettare i principi in materia di corretto trattamento. Con riferimento alla base giuridica, questa coinciderà tendenzialmente col consenso di cui all'art. 6, par. 1, lett. a), del Regolamento, del quale dovrà rispettarne i requisiti previsti dai seguenti artt. 7 e 8.

Sarà quindi il consenso l'atto dispositivo che il Regolamento circonda di ulteriori tutele, così come la possibilità di esercitare i diritti di cui agli artt. 15-22 saranno una delle garanzie che il Regolamento prevede per il rapporto conseguente.

---

gomento, lecita di per sé, assume rilievo, nel caso di specie, allorché il Professionista procede all'acquisizione dei dati personali dei propri clienti, nell'ambito della procedura prevista per lo svolgimento delle attività promozionali, quando ormai il consumatore ha già proceduto all'acquisto del prodotto oggetto di promozione. […] Tale modalità di acquisizione dei dati personali appare, pertanto, suscettibile di integrare una pratica commerciale scorretta, ai sensi degli artt. 24 e 25 del Codice del consumo, in quanto il consumatore, dopo avere effettuato l'acquisto, non avrebbe potuto fare a meno di fornire il consenso al trattamento dei propri dati personali, anche per finalità diverse da quelle necessarie all'ottenimento del premio, pena il mancato riconoscimento del premio stesso. Tale circostanza configura un indebito condizionamento, tale da indurre il consumatore ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso». Con riferimento ad una pratica e analoga contestazione in ambito europeo, si veda la pronuncia del *Bundeskartellamnt* tedesco che, nel 2016 (BS-22/16), dopo aver accertato la posizione dominante di Facebook ha ritenuto abusive le modalità con cui il social network imponeva la prestazione del consenso al trattamento dei dati personali. Sul punto si veda: G. CREA, *Profili antitrust del consenso non libero al trattamento di dati personali*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale. Convergenza tra regolazioni e tutele individuali nell'economia* data-driven, Milano, 2021, p. 24 ss.

4.1. *La monetizzazione*

Muovendo al secondo modello di business rilevante, quello c.d. "*personal data economy model*", in cui si realizza il massimo livello di commercializzazione dei dati personali o di altri attributi immateriali della personalità in quanto gli stessi circolano sulla base del solo strumento negoziale [62], si può ad esso associare il modello di disposizione dei diritti fondamentali definito dalla dottrina quale «*modello del contratto conformato mediante strumenti privatistici*» [63]. Quest'ultimo, al fine di consentire una circolazione di tali beni nel rispetto dei diritti della persona, implica un processo di rilettura delle regole in maniera di contratti in modo da renderli coerenti coi principi costituzionali. Si cerca quindi di «*coniugare il rispetto della logica negoziale con la natura personale delle prestazioni coinvolte*» [64].

Dunque obiettivo del "modello del contratto conformato" è quello di individuare le regole e i presupposti in presenza del quale la disposizione negoziale di un diritto sia da ritenersi compatibile con i principi costituzionali.

Nel modello della "*personal data economy*", in presenza del quale si realizza una monetizzazione dei dati personali, l'accordo negoziale che intercorre tra il fornitore del servizio digitale e l'utente consiste proprio nella monetizzazione dei suoi dati personali. Ossia il fornitore del servizio digitale si impegna a remunerare l'utente in seguito alla ricezione dei dati o far partecipare lo stesso a parte dei ricavi generati dalla patrimonializzazione dei dati.

Rispetto al modello precedente, il presente nasconde qualche insidia in più perché più direttamente richiama le valutazioni che riguardano i limiti e, in generale, la possibilità di utilizzare lo strumento contrattuale a tal fine. Dal punto di vista della protezione dei dati personali, infatti, ferma restando la necessità che l'interessato sia sempre adeguatamente e sufficientemente informato sulle caratteristiche di tale attività, la stessa rinviene nel contratto il suo fondamento di liceità.

Infatti, l'art. 6 del Regolamento individua tra i fondamenti di liceità del trattamento, ossia quelle "basi giuridiche" che costituiscono il primo elemento imprescindibile per rendere lecito un trattamento di dati personali che altrimenti sarebbe vietato (art. 8.2 Carta dei Diritti fondamentali dell'UE), anche

---

[62] F.G. VITERBO, *Freedom of contract and the commercial value of personal data*, in *Contr. impr. Europa*, 2, 2016, pp. 606-607; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit.; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali*, cit., pp. 642-662.

[63] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 309 ss.

[64] *Ivi*, p. 309.

lo strumento contrattuale. In particolare, l'art. 6, par. 1, lett. b), del Regolamento considera lecito un trattamento di dati personali quando «*è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*»[65].

La monetizzazione dei dati personali potrebbe quindi rientrare in questo schema nella misura in cui la volontà e il conseguente accordo delle parti si sostanzia proprio nello scambio di dati contro moneta, sicché non è possibile non ritenere la fornitura di dati personali quale necessario per lo svolgimento del servizio o, anche, per l'esecuzione del contratto stesso.

Se questa ricostruzione è vera in astratto, nel caso concreto non sono mancate critiche incentrate proprio sull'impossibilità di disporre di diritti fondamentali tramite lo strumento negoziale.

A questa tesi, di cui già si è parlato in apertura, si affiancano quelle che si basano sull'interpretazione restrittiva che l'EDPB fa dell'art. 6, par. 1, lett. b), Reg. In tal senso si obietta che la norma in questione non contiene e non disciplina l'ipotesi in cui i dati siano l'oggetto del contratto, bensì quella in cui il trattamento del dato sia un elemento accessorio e strumentale, ancorché "necessario", per l'esecuzione del contratto richiesto dall'utente. In altre parole, tale norma non potrebbe comunque essere invocata per legittimare lo scambio diretto di dati contro moneta.

Allo stesso tempo, diverse associazioni a tutela dei diritti degli interessati denunciano che l'uso sempre più disinvolto che le grandi piattaforme del digitale fanno del contratto, qualificando come necessari per la sua esecuzione trattamenti che in realtà non lo sono e che dovrebbero basarsi su altri fondamenti, primo fra tutti il consenso, sta di fatto riducendo e minando le garanzie che il Regolamento europeo appresta agli utenti/interessati. Elementi utili per l'analisi giuridica di tali modelli di business possono sicuramente derivare dalla risoluzione di queste controversie, per le quali è attesa una pronuncia da parte della Corte di Giustizia UE[66].

Se tali preoccupazioni sono vere, le stesse possono allora essere riprese per "rafforzare" lo strumento negoziale a favore dell'utente quale soggetto debole del rapporto nel contesto digitale. È questo lo spirito del modello del "contratto conformato" che, al fine di consentire la circolazione di tali attributi del-

---

[65] Comitato europeo per la protezione dei dati personali, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del Regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, 8 ottobre 2019.

[66] Noyb, *OGH austriaco chiede alla CJEU se Facebook "mina" il GDPR dal 2018*, 20 luglio 2021: https://noyb.eu/it/breaking-ogh-austriaco-chiede-alla-cjeu-se-facebook-mina-il-gdpr-dal-2018.

la personalità nel pieno rispetto dei diritti fondamentali, impone di inglobare nel contratto alcuni elementi di tutela e garanzia per la persona [67].

Si sono così individuate le condizioni in presenza delle quali tale contratto è considerabile lecito, fermo restando che ciò che sarà alienabile non è la posizione giuridica soggettiva *tout court*, ossia la titolarità del diritto, ma una più circoscritta possibilità di sfruttamento di una sua attitudine [68].

Dunque, tra le condizioni che possono rendere lecita l'adesione a tale intesa contrattuale, sia la dottrina che esperti istituzionali, hanno individuato le seguenti. Innanzitutto l'oggetto del contratto deve essere determinato, espresso in modo puntuale e chiaramente identificativo delle prestazioni richieste o delle attività incidenti sulla persona [69]. La trasparenza e la corretta informazione, quale peculiare ambito di attenzione di diverse discipline tra cui quella consumeristica e quella di tutela del dato personale, riveste anche qui un ruolo importante. A tal fine, sia il Regolamento specifica quali elementi devono essere comunicati, come il contesto e le finalità del trattamento, sia la giurisprudenza amministrativa nel caso *AGCM c. Facebook* ha sottolineato l'importanza di una corretta e completa informazione [70].

Alla determinatezza dell'oggetto ben si associa il criterio di interpretazione restrittiva dell'atto di autonomia negoziale. Si può così recuperare l'orientamento interpretativo restrittivo dell'EDPB diretto a sindacare con rigore il requisito della necessità del trattamento per l'esecuzione del contratto e idoneo a eliminare dal campo tutte quelle situazioni in cui non può essere il contratto la base giuridica del trattamento [71]. A ciò la dottrina affianca il "criterio dell'uso prevedibile", in base al quale: «*anche in presenza di clausole a contenuto ampio e potenzialmente onnicomprensivo, il contratto non viene interpretato in senso letterale, ma in maniera tale da realizzare il trasferimento delle sole facoltà strumentali al perseguimento dello scopo cui esso era teleologicamente orientato*» [72].

---

[67] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 310 ss.

[68] *Ibidem*, p. 309 ss.: «*Tra questi baluardi non superabili può ritenersi fermo il principio, integrale all'ordine pubblico delle persone, dell'inalienabilità della posizione soggettiva sottostante, sicché, esemplificando, un contratto che trasferisca la titolarità del diritto all'immagine di una persona nota dovrà ritenersi nullo* ex *art. 1418 c.c., a differenza di un contratto volto alla costituzione di una licenza esclusiva di sfruttamento (alla quale peraltro potrebbe ben essere riconosciuta natura reale)*».

[69] *Ivi*, p. 310.

[70] TAR Lazio, sent. 10 gennaio 2020, n. 260 e Cons. Stato, sent. 29 marzo 2021, n. 2631. Oltre alla dottrina già richiamata si veda anche A. VIGORITO, *La "patrimonializzazione" dei dati personali a partire dalla recente controversia AGCM-Facebook*, in *giustiziacivile.com*, 4, 2020.

[71] EDPB, *Linea guida 2/2019 sul trattamento ai sensi dell'articolo 6, paragrafo 1, lettera b), del Regolamento*, cit.

[72] Per una disamina della giurisprudenza sul punto si rinvia a: G. RESTA, *Contratto e diritti fondamentali*, cit., p. 310

Tanto l'accurata determinazione dell'oggetto del contratto quanto la sua interpretazione restrittiva sono funzionali ad assicurare un altro requisito: il fatto che nessuna previsione contrattuale possa limitare o privare l'interessato dell'esercizio dei diritti a lui riconosciuti dal Regolamento[73]. Cosicché quest'ultimo resterà libero, in ogni momento, di chiedere la cancellazione dei propri dati o opporsi al trattamento[74]. Ancora, all'interessato dovrà sempre essere riconosciuto il diritto di recedere dal contratto per motivi legittimi[75].

Un ulteriore requisito può essere quello di non consentire il ricorso al contratto per fondare il trattamento dei dati dei minori per finalità di monetizzazione. Ciò in quanto per la disciplina civilistica il minore[76] non sembrerebbe disporre della capacità negoziale per stipulare contratti con effetti così invasivi sulla sua sfera giuridica. È probabilmente questo il motivo per cui il Regolamento richiede il consenso *ex* art. 8 per la fornitura di servizi ai minori. Allo stesso tempo dovrebbero essere esclusi dalla monetizzazione le categorie particolari di dati e dati relativi a condanne penali e reati di cui agli artt. 9 e 10 del Regolamento in quanto per tali dati il Regolamento non ammette lo strumento negoziale.

Altri requisiti prospettati sono quelli di redigere il contratto nella lingua dell'interessato, che lo stesso non sia suscettibile di modifica unilaterale, che non contenga clausole di cessione o comunicazione a terzi dei dati, che siano tenuti in particolare considerazione i principi di proporzionalità e minimizzazione o il fatto che l'eventuale beneficio economico riconosciuto dal titolare all'interessato non debba essere proporzionato alla "quantità" di dati personali o diritti di utilizzo oggetto del contratto per non spingere l'interessato a concedere sempre più dati[77].

---

[73] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 435: «Da quanto sin qui espresso si può concludere che, nella circolazione onerosa dei dati personali, il principio della forza di legge del contratto cede il passo all'esigenza di mantenere in capo al soggetto il potere di autodeterminarsi in relazione agli attributi della propria personalità».

[74] G. SCORZA, *Il dato personale: manifestazione della personalità vs forma di ricchezza,* al *Webinar Forniture di servizi digitali. Il pagamento con la prestazione dei dati personali?*, organizzato dall'Università "Tor Vergata" di Roma in collaborazione con "Gruppo24Ore", 9 giugno 2021. L'intervento è in corso di pubblicazione.

[75] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 310.

[76] Con riferimento alla generale tutela del minore, specie nel contesto digitale, si veda: E. BATTELLI (a cura di), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021. Si vedano anche: P. STANZIONE, G. SCIANCALEPORE, *Minori e diritti fondamentali*, Milano, 2006; D. DI SABATO, *Il contratto del minore tra incapacità di contrarre e capacità di consumare*, in *Riv. dir. impr.*, 1, 2011, pp. 75-87; P. STANZIONE, *I contratti del minore*, in *Europa dir. priv.*, 4, 2014, pp. 1237-1286.

[77] G. SCORZA, *Il dato personale: manifestazione della personalità vs forma di ricchezza*, cit.

Sicché, con riferimento al modello della "*personal data economy*", si può concludere che l'applicazione del modello di circolazione dei beni immateriali definito del "contratto conformato" consente di bilanciare gli interessi del mercato con quelli della persona come anche dei diritti fondamentali tanto degli utenti quanto dell'impresa. Infatti, individuando i criteri a rafforzamento dell'accordo negoziale, piuttosto che vietare del tutto la monetizzazione dei dati personali la si può regolamentare in modo da renderla compatibile con il quadro giuridico vigente e con i superiori diritti fondamentali.

Con le parole di Resta: «*"indisponibilità" non significa qui né sottrazione al mercato, né regolazione eteronoma del mercato medesimo in un'ottica di garanzia dei diritti fondamentali, ma più semplicemente preclusione di negozi con efficacia traslativa, assieme all'applicazione di una disciplina contrattuale preordinata ad assicurare un adeguato bilanciamento tra le ragioni dello scambio e le ragioni della persona*»[78].

5. *Conclusioni*

Sia per il primo che per il secondo modello di business si sono rinvenute le condizioni giuridiche in presenza delle quali la commercializzazione dei dati personali può considerarsi lecita sebbene si tratti di operazioni comunque non sempre agevoli da costruire sul piano pratico.

Sia per il caso della patrimonializzazione sia per quello della monetizzazione si sono rinvenute alcune modalità di trattamento dei dati personali che consentano al fornitore di dotarsi delle risorse economiche per sostenere la propria attività, nel primo caso, o che restituiscono all'utente tutto o parte del valore che si ottiene della valorizzazione dei suoi dati, nel secondo caso.

Riflessione a parte merita la possibilità di utilizzare i dati personali come moneta che, a rigore e salvo i casi particolari già esposti, non sembrerebbe rientrare né nel modello della patrimonializzazione né in quello della monetizzazione. Ciò anche in considerazione del fatto che, al di fuori di casi isolati riportati dalla cronaca, tale possibilità sembrerebbe ancora per lo più un fenomeno rimasto sulla carta, più precisamente tra le lettere dell'art. 3, par. 1, Direttiva 2019/770. Forse, sarà proprio questa disposizione ad aprire il mercato e innovare la normativa e non si esclude che in futuro vi possano essere servizi

[78] G. RESTA, *Contratto e diritti fondamentali*, cit., p. 311.

che, in modo lecito e trasparente e nel rispetto della normativa sopra evidenziata, consentano l'accesso a un servizio pagando in dati personali.

In conclusione, il generale fenomeno della commercializzazione dei dati personali, lungi dall'essere ammissibile o vietato *tout court*, si inserisce in un settore ormai pienamente disciplinato e che consente di individuare le condizioni in presenza delle quali può considerarsi lecito. Proprio in tale quadro normativo si possono rinvenire le misure a tutela della persona, del cittadino digitale, laddove l'applicazione corretta dei suoi istituti, almeno in astratto, consente di tutelare la dignità della persona all'interno di un'operazione tanto delicata quale appunto la commercializzazione dei suoi dati.

Tuttavia, poiché, come visto, l'analisi di tali modelli deve svolgersi in concreto, non vi sarà effettiva tutela della dignità e della corretta rappresentazione dell'identità delle persone senza una costante e intensa attività di controllo da parte delle autorità di settore. A questa è inoltre auspicabile che si affianchi una leale e fattiva collaborazione tanto tra le autorità in materia di protezione dei dati personali, nell'ambito del meccanismo di cooperazione disegnato dal Regolamento (c.d. *one-stop shop* o sistema della *lead authority*), quanto tra autorità preposte alla tutela di settori diversi.

In tal senso, la citata sanzione dell'AGCM a Facebook, per quanto importante per aver accesso i riflettori delle istituzioni su un tema tanto complesso, nonché utile per aumentare la trasparenza e l'adeguata informazione al consumatore, non sembrerebbe essere risolutiva in punto di diritto, non tenendo adeguatamente conto della normativa in materia di protezione dei dati personali[79]. A tal fine, probabilmente, l'analisi di mercato condotta dall'AGCM poteva essere impreziosita richiedendo il parere del Garante per la protezione dei dati personali in base a quanto previsto dall'art. 27, comma 1-*bis*, Codice del consumo (d.lgs. n. 206/2005).

Stesso dicasi per le successive sentenze del TAR e del Consiglio di Stato, anch'esse di enorme importanza per quanto riguarda l'analisi del fenomeno, ma non pienamente dirimenti sulla questione dell'ammissibilità o meno della commercializzazione.

Eppure, nella pronuncia dell'AGCM del 29 novembre 2018 era presente un aspetto di rilievo e di più effettiva tutela per il cittadino digitale che però non è stato valorizzato dalla giurisprudenza amministrativa. Si tratta della contestazione di tutte quelle condotte poste in essere da Facebook dirette a forzare il comportamento dell'utente in modo che questo acconsenta alla raccolta e allo scambio dei propri dati con soggetti terzi, qualificate quali pratiche com-

[79] G. SCORZA, *Facebook non è gratis?*, cit.

merciali scorrette perché aggressive [80]. Era probabilmente questa la tutela più utile e concreta disposta dall'Autorità nei confronti degli utenti [81]. Ciò non solo perché sopperiva alla mancanza di reale scelta dell'utente dinanzi le condizioni imposte dalle piattaforme per usufruire dei loro servizi, ma anche nella misura in cui andava a colpire condotte che la sola disciplina in materia di protezione dei dati personali avrebbe fatto fatica a censurare. Si pensi al già citato tema del *tying ex* art. 7, par. 4 del Regolamento e al complesso esame che le autorità di controllo sembrerebbero chiamate ad effettuare. Ben potrebbe l'autorità a tutela dei consumatori rinvenire delle ipotesi di pratiche commerciali aggressive in tutti quei casi in cui si forzi o si spinga l'utente a prestare un consenso per usufruire di un contratto per un servizio digitale. In altre parole, sanzionando tutte quelle tecniche per forzare o indurre il consenso dell'utente si può evitare lo sviamento e l'elusione delle norme del Regolamento tramite l'applicazione della disciplina consumeristica. Infatti, il rischio più grande al momento si annida nell'applicazione, anche minuziosa, di un plesso normativo ma strutturata in modo da porre in essere una forma di abuso del diritto.

Dunque, con riferimento a un tema tanto complesso quale la commercializzazione dei dati personali, che sia condotta o tramite patrimonializzazione/valorizzazione o tramite monetizzazione degli stessi, si può individuare un ideale riparto di competenze. Mentre l'analisi giuridica della legittimità di tali pratiche spetterà alla normativa in materia di protezione dei dati personali, come queste vengono implementate all'interno di rapporti di consumo spetterà invece alla disciplina consumeristica [82]. Punto di contatto tra tali normative è, chiaramente, il tema della trasparenza e della corretta informazione.

---

[80] AGCM, *Provvedimento del 29 novembre 2018. PS11112 – Uso dei dati degli utenti a fini commerciali: sanzioni per 10 milioni di euro a Facebook*. Questa pratica era così formulata: *«"Pratica b) pratica aggressiva" si riferiva alla violazione degli artt. 20, 24 e 25 del Codice del consumo, in quanto il professionista eserciterebbe un indebito condizionamento nei confronti dei consumatori registrati, i quali, in cambio dell'utilizzo di FB, verrebbero costretti a consentire a FB/terzi la raccolta e l'utilizzo, per finalità informative e/o commerciali, dei dati che li riguardano (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/a terzi operatori, per evitare di subire limitazioni nell'utilizzo del servizio, conseguenti alla deselezione)*».

[81] A. GAMBINO, *La circolazione dei dati personali, la configurabilità di un mercato e i diritti fondamentali*, al *Webinar Forniture di servizi digitali. Il pagamento con la prestazione dei dati personali?*, organizzato dall'Università "Tor Vergata" di Roma in collaborazione con "Gruppo24Ore", 9 giugno 2021. L'intervento è in corso di pubblicazione.

[82] S. THOBANI, *Il mercato dei dati personali*, cit., pp. 131-147.

Ciò posto, solo tramite un'accurata analisi sia in astratto sia in concreto del fenomeno della commercializzazione dei dati personali si riuscirà a bilanciare le esigenze del mercato con la tutela dei diritti fondamentali e gli interessi dei cittadini [83].

[83] G. D'ACQUISTO, F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *An. giur. econ*., 2019, p. 90, per i quali il GDPR non è solo una «*regolazione a tutela di un diritto fondamentale*», ma costituisce «*il baricentro intorno al quale costruire un'economia dei dati dell'Unione*».

IL CONSUMATORE "PREVEDIBILE": *BIG DATA* E INTELLIGENZA ARTIFICIALE NELLA EROGAZIONE DEI SERVIZI BANCARI

di *Filippo Bagni*

1. *Gli algoritmi nel mercato del credito*

1.1. *L'utilizzo della intelligenza artificiale per la profilazione del consumatore di servizi bancari*

L'elevata concorrenzialità del mercato bancario e gli accorgimenti richiesti dal regolatore europeo dopo la crisi del 2008 sulla gestione dei cosiddetti NPL (*non perfoming loans*[1]) hanno portato gli istituti bancari a guardare con sempre maggiore attenzione al c.d. *rating* bancario[2].

[1] Sulla definizione di crediti deteriorati si veda, tra gli altri, T. CRISAFULLI, *Crediti deteriorati: perché mettono in crisi il sistema bancario italiano*, disponibile all'indirizzo www.recuperolegale.it, 2018; C. BARBAGALLO, *Primo Congresso Nazionale FIRST CISL "La fiducia tra banche e Paese: NPL, un terreno da cui far ripartire il dialogo". I crediti deteriorati delle banche italiane: problematiche e tendenze recenti*, 2017. Per una analisi critica si veda anche A. PISANESCHI, *Verso una nuova ondata di Npe. La strategia europea e qualche dubbio*, in *Crisi d'impresa e insolvenza*, 2021, p. 1 ss.

[2] Per "*rating* bancario" si intende una istruttoria di affidamento che consta nello svolgimento di indagini per valutare la capacità di rimborso dell'impresa o persona fisica richiedente il credito. Per una indagine più approfondita si rinvia a R. RUOZI, *Economia della banca*, III ed., Milano, 2016.

È evidente come la previsione delle inadempienze dei consumatori di servizi bancari sia di fondamentale importanza per le banche (per selezionare i potenziali mutuatari, valutare i termini dei nuovi prestiti e gestire i rischi). Negli ultimi anni, grazie alla maggiore disponibilità di grandi *dataset* e di informazioni non strutturate, nel settore bancario ha assunto sempre maggiore rilievo la ricerca di modelli basati su algoritmi che applicano tecniche di *machine learning* (ML), capaci di realizzare modelli statistici in grado di elaborare velocemente risultati accurati su larga scala e limitare i rischi non (sempre) adeguatamente preventivati[3].

La "forza" di questi algoritmi infatti, com'è noto, non risiede tanto nella loro capacità di risolvere problemi, quanto nell'"imparare" da esperienze pregresse come risolverli, permettendo così alla banca di operare vere e proprie previsioni che poggiano su inferenze e connessioni di dati correlati[4].

Ad oggi, per una banca, la detenzione e corretta sistematizzazione in termini predittivi di un grande numero di dati riguardo i consumatori è sinonimo di riduzione di rischio e maggiore redditività. È evidente quindi il motivo per il quale la tecnologia finanziaria (Fintech) sta assumendo un ruolo sempre più incisivo nelle decisioni di prestito[5].

Il *credit scoring* automatizzato è ormai una realtà[6]. Le banche si affidano ai "punteggi di credito" (*credit scoring*) per prendere decisioni sui prestiti alle

---

[3] Si parla di banca "*data driven*", capace di governare e valorizzare il proprio patrimonio informativo e trarre beneficio da quello dei clienti, acquisendo vantaggi competitivi, ottimizzando i propri processi decisionali e il proprio modello operativo. Per una visione critica si veda anche F. CIAMPI, *Banche, per alzare la redditività servono nuovi modelli di rating*, disponibile all'indirizzo www.ilsole24ore.com, 2019.

[4] Sul tema si veda, tra gli altri, P. DOMINGOS, *L'algoritmo definitivo: la macchina che impara da sola e il futuro del nostro mondo*, Torino, 2016; J. KAPLAN, *Intelligenza artificiale: guida al futuro prossimo*, Roma, 2016.

[5] Ricerche recenti di Banca d'Italia sul tema (2019) rivelano che le banche italiane sono ancora in una fase iniziale nell'uso del *rating* automatizzato, basato per lo più su modelli di ML "semplici" o "di prima generazione" (es. *decision tree*). Negli ultimi anni abbiamo però assistito ad una crescita esponenziale dei finanziamenti degli istituti nazionali nel Fintech, con le banche più grandi che investono per lo più sulla realizzazione *in house* di progetti basati sull'IA, mentre le più piccole agiscono soprattutto in *outsourcing.* In particolare, l'indagine di Banca d'Italia rivela che nel periodo 2017-2020 gli investimenti *Fintech* nel sistema finanziario italiano si sono attestati attorno ai 624 milioni di euro, dei quali 233 spesi nel biennio 2017-2018 e 391 previsti in quello successivo. Di queste cifre oltre il 50% è usato per sviluppare *homebanking* e pagamenti online (PSD2) e il 16% nello sviluppo di tecniche fondate sui *big data*. Cfr. Banca d'Italia, *Indagine Fintech nel sistema finanziario italiano,* disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 2019.

[6] Il *credit scoring* è una procedura automatizzata eseguita al momento dell'istruttoria adottata dalle banche per valutare le richieste di finanziamento della clientela (in genere per la conces-

imprese e ai clienti persone fisiche, utilizzando come base dati, non solo le transazioni e le "storie" di pagamento dei clienti, ma anche fonti di dati aggiuntive (i c.d. "dati alternativi"), come l'attività sui social media, l'uso dello *smartphone*, l'attività dei messaggi di testo. Il tutto finalizzato al raggiungimento di una visione più accurata possibile del merito di credito del singolo cliente, tesa a migliorare l'efficienza e l'efficacia della decisione [7] e, secondo alcuni, a facilitare l'inclusione finanziaria [8].

1.2. *I benefici del* credit scoring *algoritmico*

La crisi finanziaria globale del 2008 ha messo in luce tutti i limiti dei sistemi di *rating* "tradizionali", soprattutto con riferimento alla loro lenta capacità di adattarsi ai cambiamenti economici e alla loro scarsa attitudine nel modellare complesse interazioni non lineari tra variabili economiche, finanziarie e creditizie [9].

I nuovi modelli di *rating* c.d. "algoritmici", fondati su tecniche di ML, differiscono da quelli tradizionali principalmente sotto tre profili: a) permettono agli intermediari di raccogliere e utilizzare una maggiore quantità di informazioni; b) utilizzano tecniche di apprendimento automatico tali da estrarre una informa-

---

sione del credito al consumo). Si basa su sistemi automatizzati che prevedono l'applicazione di metodi o modelli statistici per valutare il rischio creditizio e i cui risultati sono espressi in forma di giudizi sintetici (indicatori numerici o punteggi) associati all'interessato, diretti a fornire una rappresentazione, in termini predittivi o probabilistici, del suo profilo di rischio e affidabilità nei pagamenti. Per una definizione compiuta di "*credit scoring algoritmico*" si rinvia a L. AMMANNATI, G.L. GRECO, *Il credit scoring alla prova dell'intelligenza artificiale*, disponibile all'indirizzo www.associazioneadde.it. Per un approfondimento riguardo l'influenza dei *big data* sulla valutazione del merito creditizio del cliente si veda F. FERRETTI, *Consumer Access to Capital in the Age of FinTech and Big Data: the Limits of EU Law*, in *Maastricht Journal of European and Comparative Law*, 2018, 25, p. 476 ss.

[7] Cfr. C. BARBAGALLO, *FinTech: the role of the supervisory authority in a changing market. Speech by Carmelo Barbagallo Head of the Directorate General for Financial Supervision and Regulation Bank of Italy*, disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 8 febbraio 2019, p. 12 ss.

[8] Sui benefici dell'uso di fonti alternative in particolare per i consumatori a più basso reddito o con livelli inferiori di istruzione oppure residenti in aree a basso tasso di inclusione finanziaria si veda. S. AGARWAL, S. ALOK, P. GHOSH, S. GUPTA, *Financial Inclusion and Alternate Credit Scoring: Role of Big Data and Machine Learning in Fintech*, 2020, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507827.

[9] Cfr. M. MOSCATELLI, S. NARIZZANO, F. PARLAPIANO, G. VIGGIANO, *Banca d'Italia. Temi di discussione (Working Papers). Corporate default forecasting with machine learning,* disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 2019, p. 17 ss.

zione non lineare dalle variabili; c) stimano l'applicazione di molteplici modelli e utilizzano solo quello più accurato per eseguire compiti di predizione [10].

Recenti studi hanno confrontato i modelli statistici solitamente impiegati nella modellazione del rischio di credito con alcuni modelli di ML, evidenziando alcuni risultati rilevanti [11].

Anzitutto, quando i modelli hanno a disposizione un *set* di informazioni "limitato" (come, ad esempio, le informazioni finanziarie solitamente disponibili agli analisti creditizi esterni), la capacità dei modelli di ML di utilizzare anche informazioni "non tradizionali" permette loro di superare di gran lunga i modelli statistici in termini di precisione e capacità predittiva (capacità di stimare la PD, ossia la possibilità di *default* del singolo cliente).

In secondo luogo, in un "*esercizio di statica comparativa*" (*comparative statics exercise*), in cui il credito viene assegnato ai clienti (attuali) delle banche sulla base della loro probabilità di *default*, il passaggio a un sistema di *rating* fondato su tecniche di ML avrebbe un impatto positivo sull'ammontare del credito, senza aumentare le perdite di credito per i prestatori e, inoltre, porterebbe alla concessione di maggiori quantità di credito a tassi di *default* più bassi.

In terzo luogo, si è riscontrato che, non solo l'utilizzo di tecniche di ML applicate al *credit scoring* migliora notevolmente il potere predittivo delle valutazioni di default dei clienti, ma anche che le performance dei modelli IA/ML sono di gran lunga più efficienti nel caso vi sia uno shock esogeno dell'offerta aggregata di credito. Questo in quanto il modello basato sull'apprendimento

---

[10] Quest'ultima caratteristica, in particolare, dei modelli ML è particolarmente rilevante per le applicazioni del rischio di credito, al costo però di una minore trasparenza. Classico esempio di algoritmo utilizzato per il *credit scoring* è quello ad albero decisionale, in base al quale vi è un insieme di regole che partizionano ricorsivamente l'intero set di clienti in sottoinsiemi omogenei in base alle loro caratteristiche e alla variabile di risultato (*default*/non *default*). Le previsioni sono poi ottenute sotto forma di probabilità di un dato risultato in ogni sottoinsieme. Cfr. L. GAMBACORTA, Y. HUANG, H. QIU, J. WANG, *How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm*, in *Monetary and Economic Department*, December 2019, p. 4 ss. Per una indagine ulteriore si veda anche N. CULLERTON, *Behavioral credit scoring*, in *The George Town law journal*, vol. 101, 2013, p. 808 ss.; T. ALLOWAY, *Big data: credit where credit's due*, in *Financial Times*, February 2015, disponibile all'indirizzo www.ft.com/cms; A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria*, in F. CAPRIGLIONE (a cura di), *Studi di diritto dell'economia*, Torino, 2020.

[11] Cfr. M. MOSCATELLI, *Corporate default forecasting with machine learning*, cit., p. 8 ss. Sulla questione relativa alle migliori *performance* delle tecniche di ML applicate al *credit risk* in termini di capacità predittiva dell'evento *default* si veda anche C. CAPRARA, D. VERGARI, *Il ruolo del Machine Learning nel governo del credito: nuove tecniche a supporto delle decisioni*, in *Riv. banc.*, gennaio 2020, n. 1.

automatico dimostra una capacità maggiore di estrazione delle relazioni non lineari tra le variabili in caso di shock, migliorando così le performance predittive in termini di tasso di default dei clienti [12].

In definitiva, dalle ricerche emerge che l'utilizzo del *credit scoring* algoritmico rende, per così dire, "prevedibile" il consumatore di servizi bancari e consente di ridurre costi operativi e asimmetrie informative, migliorando il grado di personalizzazione dei servizi di finanziamento e le valutazioni in termini di merito creditizio del cliente.

2. *L'attuale (scarna) regolamentazione della tecnologia nel sistema bancario e i rischi connessi al* rating *automatizzato*

La tematica del *rating* bancario automatizzato sconta però dei limiti sotto più profili, anzitutto regolatori. L'elemento di redditività di una banca, infatti, è soggetto ad (almeno) tre variabili fondamentali: da una parte, la tecnologia e il mercato; dall'altra, le regole [13].

La valutazione del merito creditizio del consumatore è stata fino al recente passato oggetto di scarsa attenzione da parte del regolatore.

Il legislatore nazionale si è per molti anni astenuto dal dettare criteri ordinatori puntuali sul tema, prevedendo esclusivamente alcune regole settoriali di ampio raggio, contenute per lo più nelle disposizioni del Testo Unico Bancario (d.lgs. n. 385/1993) (artt. 5 e 124-*bis*) e nel d.lgs. n. 72/2016 in tema di

---

[12] La ricerca in parola ha utilizzato dati reali di una società Fintech leader in Cina. Nel caso di specie la *People's Bank of China*, la Banca Centrale Cinese, aveva emesso una specifica bozza di linee guida per inasprire la regolamentazione sullo *shadow banking*. Questo cambiamento normativo aveva portato molti intermediari finanziari ad aumentare i loro requisiti di prestito, causando un deterioramento delle condizioni di credito per i mutuatari. Cfr. L. GAMBACORTA, *How do machine learning and non-traditional data affect credit scoring?,* cit., p. 4 ss. Di rilievo anche uno studio statunitense che ha verificato che l'analisi dei dati disseminati dai debitori sul web consente di ridurre i tassi di default e sono correlati con le informazioni rivenienti dalle centrali rischi tradizionali. Cfr. T. BERG, V. BURG, A. GOMBOVIĆ, M. PURI, *On the Rise of FinTechs - Credit Scoring Using Digital Footprints*, in *Michael J. Brennan Irish Finance Working Paper Series Research Paper*, n. 18-12, July 2019.

[13] Con particolare riferimento alla questione problematica delle regole a cui assoggettare le *Fintech banks* onde evitare il fenomeno del c.d. *shadow banking*, si veda S. ROSSI, *Associazione Bancaria Italiana. Inaugurazione del Corso di Alta formazione per gli Amministratori e gli Organi di controllo delle imprese bancarie. Fintech e Diritto – Fintech e Regole. Considerazioni conclusive del direttore generale della Banca d'Italia e Presidente dell'Ivass Salvatore Rossi*, disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 2018, p. 7 ss.

contratti di credito ai consumatori relativi ai beni immobili (artt. 120-*septies* e 120-*undecies*) [14].

Il regolatore europeo, da parte sua, ha certamente dedicato maggiore attenzione alla valutazione del merito creditizio del cliente da parte delle banche, seppur mantenendo una terminologia di ampio respiro ("*adeguato*", "*corretto*"), tale da lasciare sostanzialmente impregiudicata la discrezionalità degli intermediari in merito a quali dati utilizzare nell'attività di *rating* e con quali metodi processarli [15].

Allo stesso modo, le autorità di vigilanza del settore bancario (BCE [16] e Banca d'Italia) non si sono mai troppo interessate del "merito" della valutazione del consumatore, guardando più al *fine* (la sana e prudente gestione dell'ente, nella specifica accezione di corretta gestione del rischio di credito) piuttosto che al *mezzo* (la valutazione di merito creditizio), rifuggendo dal fornire indicazioni chiare su quali tipologie di dati e modelli di valutazione dovrebbero essere preferibilmente utilizzati nell'attività di *credit scoring*.

Diverso e di maggior rilievo il ruolo ritagliatosi invece dall'EBA (European Banking Authority [17]), la quale ha il merito di essere stata la prima autorità di vigilanza europea che, non solo ha analizzato nello specifico il tema della tipologia di dati da utilizzare per valutare il merito creditizio del cliente [18], ma che

---

[14] Per un approfondimento si veda F. MATTASOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, in *Dir. banca e merc. fin.*, 2, 2020, pp. 187-220.

[15] Tra le discipline di riferimento a livello europeo per la strutturazione dei modelli di ML di speciale importanza è il Regolamento UE n. 575/2013 in tema di *rating* bancario e profilazione della clientela. Trattasi in particolare di una normativa rivolta agli enti creditizi e alle imprese di investimento che, assieme alla Direttiva UE n. 36/2013, forma il quadro giuridico di disciplina dell'accesso all'attività, il quadro di vigilanza e quello delle norme prudenziali da perseguire. Il Regolamento in parola è stato introdotto allo scopo, da una parte, di prevenire e attenuare i rischi sistemici connessi all'attività di *rating* bancario (considerando 15 Regolamento UE n. 575/2013), dall'altra, di scoraggiare la speculazione finanziaria (considerando 32 Regolamento UE n. 575/2013). Dal punto di vista della disciplina della privacy, ovviamente, le indicazioni più efficaci, seppure di carattere generale, sono contenute nel GDPR del 2016, da legge in combinato disposto con le *Linee Guida sulla profilazione* emanate nel 2017 (poi emendate nel 2018 post GDPR) dal WP29.

[16] BCE, *Guide to assessments of Fintech institution licence applications*, marzo 2018, reperibile sul sito www.bankingsupervision.europa.eu.

[17] L'EBA è stata istituita nel 2010 (Regolamento UE n. 1093/2010) in risposta alla crisi economica del 2008, e, assieme alla ESAs (European Supervisory Authorities), la EIOPA (European Insurance and Occupational Pensions Authority) e all'ESMA (European Securities and Markets Authority), fa parte del Sistema europeo di vigilanza finanziaria (SEVIF). Per un approfondimento si rinvia al sito www.eba.europa.eu.

[18] *Consultation Paper sulle Draft Guidelines on loan origination ad monitoring* (EBA/CP/2019/04 del 19 giugno 2019), consultabile sul sito www.eba.europa.eu.

ha fornito osservazioni-chiave che dovrebbero accompagnare l'utilizzo del *credit scoring* algoritmico [19], nella convinzione di fondo che le banche possono e devono adottare metodi di profilazione performanti (anche per mezzo di analisi di dati sulla base di tecniche di IA/ML), purché "di qualità", conosciuti da chi li adotta e spiegabili a chi ne è oggetto.

Le fonti citate rappresentano certamente un importante punto di partenza per la disciplina del *credit scoring* automatizzato, ma non possono dirsi ancora sufficienti a garantire una tutela efficace al consumatore dei servizi finanziari. Una tutela della quale si avverte sempre più il bisogno, essendo ormai chiaro a tutti come i benefici connessi all'adozione di tecniche di ML applicate al *credit scoring* scontino un "prezzo" in termini di: pericolo di opacità, errori, pratiche discriminatorie ed esclusione dal credito [20].

2.1. *I riflessi sulla* accountability *delle singole banche*

Come delineato, lo "stato dell'arte" della regolamentazione tecnologica nel sistema bancario lascia ampio spazio alla discrezionalità delle singole banche. Gli istituti di credito (quantomeno quelli di maggiori dimensioni) si stanno attrezzando di conseguenza, investendo cifre importanti nel settore Fintech. La tendenza è quella di utilizzare i sistemi innovativi digitali non solo, per così dire, "passivamente" (per meri scopi di *compliance*), ma anche "attivamente", analizzando il quadro normativo per sviluppare capacità competitive ed aumentare l'efficienza dell'infrastruttura organizzativa.

In questi termini, le banche sembrano aver ben compreso che la necessità di rafforzare l'*accountability* dell'algoritmo ha come fine prioritario quello di accrescere la fiducia dei consumatori nella correttezza delle decisioni. Ovviamente, un simile percorso presuppone che gli istituti di credito che si avvalgono di meccanismi di *machine learning* per profilare i consumatori di servizi bancari adottino procedure che consentano di conoscere le fonti di produzione dei dati, i modi di raccolta e i metodi di elaborazione degli stessi, nonché la previsione di procedure interne di controllo della qualità dei risultati e delle decisioni [21].

---

[19] I concetti anticipati nel *Consultation Paper* del 2019 sono stati infatti poi dall'EBA sviluppati nel 2020, dapprima, in un atto non normativo (*Report on big data and advanced analytics*, EBA/REP/2020/01) e, successivamente, in un vero e proprio atto normativo, seppur non vincolante (*Orientamenti in materia di concessione e monitoraggio dei prestiti*, EBA/GL/2020/06).

[20] Per una analisi approfondita sui rischi connessi si veda F. MATTASOGLIO, *Algoritmi e regolazione. Circa i limiti del principio di neutralità tecnologica*, in *Riv. reg. mer.*, 2, 2018, pp. 226-251.

[21] Per approfondimento si veda L. AMMANNATI, G.L. GRECO, *Il credit scoring alla prova dell'intelligenza artificiale*, cit., p. 5 ss.

Nel contesto attuale, qualora una banca decidesse di sperimentare un nuovo modello di *rating* automatizzato teso a valutare l'affidabilità dei consumatori, nel farlo dovrebbe, da una parte, in termini di *legal compliance*, tenere in debita considerazione le fonti (europee e nazionali) succitate, e, dall'altra, in termini di *accountability*, dedicare particolare attenzione nella selezione della base dati da utilizzare per il processo di *credit scoring*, nonché nella corretta individuazione della lista di indicatori/criteri da applicare al *data set* (es. andamentali interni, *status* e operatività del cliente, stile di vita, analisi delle transazioni e degli elementi reddituali).

In particolare, i principi/regole fondamentali a cui prestare particolare attenzione al momento della strutturazione dell'algoritmo possono considerarsi i seguenti: a) il principio di minimizzazione, pertinenza e non eccedenza, il quale richiede un utilizzo di dati (pertinenti) limitato a quanto effettivamente necessario per conseguire lo scopo prefissato; b) la sicurezza dei dati, garantendo l'accessibilità ai soli soggetti autorizzati al trattamento; c) l'esclusione dei dati c.d. "particolari", in quanto potenzialmente utilizzabili con fine o effetto discriminatorio; d) la garanzia di rettifica dei dati erronei; e) l'esecuzione di *stress test* periodici degli algoritmi tesi ad assicurare il trattamento funzionale dei dati e l'assenza di effetti discriminatori, anche alla luce della possibile aggregazione degli stessi.

Ciò detto, per quanto un processo *compliant* di strutturazione di un modello di *rating* automatizzato possa apparire lineare in astratto, in concreto esso incontra una serie di elementi critici rilevanti, primo fra tutti il fatto che l'algoritmo, seppur progettato e strutturato secondo dati criteri, evolve e si ottimizza in modo autonomo (*machine learning*), anche con modalità tecniche ed esiti non del tutto preventivabili *a priori*.

Si pensi poi alla difficoltà intrinseca di tradurre in concreti processi operativi una selezione dei dati che possa dirsi conforme al principio di minimizzazione e pertinenza. In senso lato, infatti, qualsiasi dato può, in misura maggiore o minore, fornire informazioni utili a definire una abitudine di comportamento e, per questa via, l'affidabilità e probabilità di *default* del cliente.

Senza dimenticare, infine, l'ormai annosa problematica connessa al fenomeno dei c.d. dati "aggregati" [22], ossia l'intrinseca difficoltà di evitare che, nonostante una corretta selezione (a monte) dei dati da utilizzare e dei criteri da applicare, l'algoritmo poi nell'ottimizzarsi (a valle) crei correlazioni di dati foriere di esiti illegittimi quali, ad esempio, effetti discriminatori [23].

---

[22] Per un approfondimento sul tema si rinvia a A. SIMONCINI, S. SUEWIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. fil. dir.*, 2019, pp. 87-106.

[23] Sui possibili effetti discriminatori delle tecniche algoritmiche si veda A. SIMONCINI, *L'al-*

Quanto evidenziato rende ancor più evidente la necessità di un intervento regolatore chiaro e dedicato al tema della tecnologia applicata al sistema bancario. I principi generali attualmente previsti (proporzionalità, integrità del mercato, neutralità tecnologica [24]) non bastano più. Il problema delle regole a cui assoggettare tali operatori è diventato cruciale e non può essere lasciato (solo) alla "sensibilità" o all'*accountability* delle singole banche [25].

3. *La Proposta di* Artificial Intelligence Act *della Commissione europea: una nuova prospettiva (anche) in termini concorrenziali*

Il quesito da porsi rispetto a questo tipo di tecnologie applicate al sistema di *rating* bancario evidentemente non è come arginarle (giacché non sarebbe comunque possibile, né auspicabile), bensì come definire un quadro etico-giuridico sostenibile all'interno del quale possano operare.

L'innovazione tecnologica è destinata a divenire l'elemento cardine della futura valutazione del merito creditizio. Per questo motivo l'ordinamento deve seriamente interrogarsi e dare indicazioni sul "tipo" di dato da utilizzare per il *rating* bancario automatizzato, promuovendo l'introduzione di apposite regole settoriali e specifici principi riferiti espressamente alle tecniche algoritmiche che vadano ad integrare le normative esistenti [26].

---

goritmo incostituzionale: intelligenza artificiale e il futuro delle libertà, in *BioLaw Journal - Rivista di BioDiritto*, 2019, pp. 63-89; con riferimento al settore bancario si veda, tra gli altri: C. HAVARD, *"On the take": The Black Box of Credit scoring and mortgage discrimination*, in *Public Interest Law Journal*, 2011, vol. 20, p. 241 ss.; Federal Trade Commission, *Big Data: a tool for inclusion or exclusion*, FTC, January 2016, consultabile sul sito www.ftc.gov. Sul tema, poi, è di particolare interesse il contributo di M. FOURCADE, K. HEALY, *Classification situations: Life-chances in the neoliberal era*, in *Accounting*, *Organizations and Society*, 2013, p. 559 ss., nel quale gli Autori analizzano i rischi e l'impatto di un sistema automatizzato di valutazione del merito creditizio sulle popolazioni meno abbienti, mettendo in luce come gli algoritmi possano acuire le differenze sociali e la distinzione tra classi.

[24] Per una analisi compiuta del concetto di "neutralità tecnologica" si rinvia a: F. PANETTA, *Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo*, Audizione del direttore generale della Banca d'Italia, disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 5 dicembre 2017; F. MATTASOGLIO, *Algoritmi e regolazione*, cit., p. 230 ss.

[25] Cfr. S. ROSSI, *Banca d'Italia. 29a Conferenza (EC)2 su Big Data Econometrics with Applications". Apertura dei lavori del Direttore Generale della Banca d'Italia e Presidente dell'IVASS Salvatore Rossi*, Roma, disponibile all'indirizzo www.bancaditalia.it/pubblicazioni, 13 dicembre 2018, p. 1 ss.

[26] Si pensi, a titolo esemplificativo, al principio di "comprensibilità" dell'algoritmo, secondo

Il settore bancario negli ultimi tempi ha infatti attraversato una vera e propria "rivoluzione": da una parte, l'ingresso di nuovi soggetti (*Fintech banks*) ha determinato la rottura di vecchi "monopoli"; dall'altra, la recente riforma delle banche popolari [27] ha favorito le aggregazioni determinando la progressiva riduzione dei protagonisti sulla scena. Stiamo lentamente (ma neanche troppo) assistendo al tramonto di quello che è stato definito un sistema "banco-centrico", con la profilazione di un mercato bancario più competitivo, ampio e fluido, dove accanto agli intermediari tradizionali si registra l'ingresso di nuovi attori e prestatori di servizi capaci di intercettare con la loro offerta una parte di clientela un tempo di esclusiva competenza delle banche che potremmo definire "tradizionali" [28].

L'innovazione tecnologica e la relativa circolazione dei dati sta determinando per le banche tradizionali la progressiva perdita del "vantaggio" del rapporto diretto con il cliente, laddove piuttosto il rapporto banca-cliente si sta strutturando sempre più sull'acquisizione ed elaborazione di informazioni, ormai raccoglibili "da remoto" per mezzo di piattaforme bancarie *on line*.

A ben vedere, quindi, i primi soggetti a trarre vantaggio dall'ingresso di una normativa *ad hoc* tesa a disciplinare l'utilizzo della tecnologia nell'attività di *rating* sarebbero gli stessi intermediari bancari tradizionali. È evidente, infatti, che se il futuro della redditività nel sistema bancario è lo sfruttamento dei *big data*, le banche si trovano in copioso svantaggio rispetto ai grandi detentori di dati (c.d. GAFAM: Google, Apple, Facebook, Amazon, Microsoft), i quali, peraltro, hanno già cominciato a fornire i primi servizi finanziari (ad esempio con riferimento al mercato del *payment*, con prodotti usati già da milioni di utenti [29]).

---

il quale ogni volta che un modello di IA/ML va ad impattare su diritti e libertà fondamentali del cittadino, deve operare un divieto assoluto di *black box* su quello specifico algoritmo. Cfr. A. SIMONCINI, *L'algoritmo incostituzionale*, cit., p. 63 ss. Sul tema si veda anche, tra gli altri, C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. eu.*, numero speciale, 2019, pp. 101-130.

[27] D.l. n. 3/2015, convertito dalla legge n. 33/2015, con il quale si è imposto la trasformazione della capogruppo in società per azioni.

[28] Per una analisi dettagliata della trasformazione in atto nel sistema bancario si veda: A. ARGENTATI, *Le banche nel nuovo scenario competitivo. FinTech, il paradigma Open banking e la minaccia delle big tech companies*, in *il Mulino rivisteweb*, 3, 2018; G. PITRUZZELLA, *FinTech e i nuovi scenari competitivi nel settore bancario-finanziario-assicurativo*, in *www.bancaria.it*, 6, 2018.

[29] Il riferimento è alla Direttiva c.d. PSD2 che, con l'obiettivo di incrementare la competizione nel settore dei pagamenti in Europa, ha aperto alla condivisione dei dati del cliente tra i diversi attori dell'ecosistema bancario, obbligando le banche a darvi accesso (previa autorizzazione del cliente) e spezzando così il monopolio da esse tradizionalmente detenuto. Facebook

Sotto questo profilo, quindi, gli istituti tradizionali hanno tutto l'interesse a distinguersi dai GAFAM utilizzando sul mercato un "prodotto" algoritmico applicato al *rating* virtuoso e *compliant* con le normative che verranno, dimostrandosi così agli occhi del cliente istituti attenti alle esigenze del consumatore. Su questa linea di pensiero, *pro futuro*, si potrebbe quasi immaginare la previsione di algoritmi "d.o.c.g. – di origine controllata", quali veri e propri prodotti di "qualità" tali da costituire elemento distintivo sul mercato bancario in termini concorrenziali.

A titolo conclusivo, non si può non fare riferimento alla Proposta di Regolamento della Commissione europea (c.d. *Artificial Intelligence Act*, AIA) del 21 aprile 2021, la quale rappresenta il primo vero tentativo compiuto di regolazione in termini generali dell'IA [30].

Nella proposta la Commissione europea ha espressamente indicato tra i sistemi di IA "ad alto rischio" quelli utilizzati per valutare l'affidabilità creditizia delle persone fisiche, in quanto dirimenti in termini di accesso e godimento a servizi privati essenziali e/o servizi e benefici pubblici (considerando n. 37; All. III, par. 5, lett. b).

Primo dato da sottolineare è il fatto che nella Proposta la Commissione abbia deciso di perseguire a livello di regolamentazione il c.d. "*risk-based approach*", di classico utilizzo nei casi in cui un sistema tecnologico non è soggetto né a divieto assoluto né a liceità assoluta. Trattasi di un metodo di regolamentazione favorevolmente orientato al mercato, flessibile e adattabile ai cambiamenti tecnologici e al rapido sviluppo che caratterizzano la tecnologia [31].

Si è quindi deciso di considerare gli algoritmi applicati al *rating* bancario (delle persone fisiche) quali strumenti non vietati *ex se*, bensì utilizzabili a pat-

---

ha ottenuto nel 2017 una licenza in Irlanda che consente l'emissione di moneta elettronica e la prestazione di servizi di pagamento; lo stesso ha fatto Amazon in Lussemburgo a dicembre 2018; Google ha ottenuto la licenza di moneta elettronica in Lituania a inizio 2019. Cfr. A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fintech*, cit.

[30] *Proposal for a Regulation of the European Parliament and of the Council – Laying down harmonised rules on Artificial Intelligence and amending certain union legislative acts*, Brussels, 21 aprile 2021, 2021/0106 (COD), consultabile sul sito www.ec.europa.eu. Per una analisi diffusa della Proposta si rinvia a C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di Intelligenza Artificiale*, in *Biolaw Journal*, 3/2021.

[31] La Commissione, consapevole dell'estrema mutevolezza delle applicazioni di IA, introduce due meccanismi di flessibilità del quadro normativo: in primo luogo, la Proposta AIA si completa di alcuni allegati (fondamentali, per esempio, per individuare la categoria dei dispositivi ad alto rischio) modificabili anche al di fuori del procedimento legislativo ordinario; in secondo luogo, si prevede un obbligo generale di revisione del Regolamento a cinque anni dalla sua entrata in vigore e, successivamente, con cadenza quinquennale.

to che rispettino determinate condizioni; ciò a riprova del fatto che l'utilizzo di tecniche di IA/ML in materia di *credit scoring* è considerato un dato ormai assodato, ma allo stesso tempo un elemento "pericoloso", per il quale si ritengono necessari schemi organizzativi interni ed esterni volti a ridurre o ad annullare i rischi.

Se il testo venisse confermato, dunque, le banche che utilizzano metodi di IA/ML per valutare l'affidabilità creditizia delle persone fisiche sarebbero obbligate (in via diretta ed immediata), affinché i sistemi ad alto rischio siano ammessi all'interno del mercato unico: da una parte, a garantire il rispetto di una serie di requisiti "minimi" in termini di "qualità" dei *set* di dati utilizzati (documentazione tecnica, conservazione, trasparenza, sorveglianza, robustezza, accuratezza e rappresentatività); dall'altra, a sottoporre ogni nuovo progetto di IA da immettere sul mercato (considerato ad alto rischio) ad una preventiva valutazione di conformità e a successive verifiche periodiche [32].

Una specifica regolamentazione in tema di IA è dunque prossima all'introduzione e il sistema bancario ne sarà protagonista. In attesa dei relativi sviluppi, è interessante rivelare come la stessa Commissione europea abbia ritenuto di dover affermare che, con l'introduzione di questa nuova regolamentazione, le banche si gioveranno dell'aumento della fiducia degli utenti, della maggiore certezza del diritto e dell'armonizzazione delle regole, con possibilità di accedere a mercati più grandi ed aumentare il numero dei propri clienti [33].

In questo senso c'è da attendersi che, nel prossimo futuro, la progettazione e lo sviluppo di algoritmi virtuosi e *compliant* con la regolamentazione in materia, orienterà l'evoluzione del *rating* bancario e, in termini generali, lo stesso mercato del credito.

---

[32] In particolare, l'art. 6 dell'AIA contiene una classificazione dei sistemi ad alto rischio (completata dagli allegati II e III) e prevede il necessario rispetto dei requisiti stabiliti nel capitolo II quale condizione per l'immissione in commercio: un procedimento di verifica della conformità; il rilascio di una dichiarazione di conformità (art. 48) e l'apposizione del marchio europeo (art. 49) che consente la circolazione nel mercato; la registrazione in una banca dati accessibile al pubblico posta sotto il controllo della Commissione (art. 60); la sottoposizione del sistema di IA ad alto rischio, una volta immesso nel mercato, ad una vigilanza post-market, volta a monitorare periodicamente il rispetto da parte dell'algoritmo delle condizioni stabilite dal Regolamento. Cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea*, cit., p. 11 ss.

[33] Commissione europea, *Nuove regole per l'intelligenza artificiale. Domande e risposte*, Bruxelles, 21 aprile 2021, consultabile sul sito www.ec.europa.eu. Sull'importanza dell'elemento della fiducia nel rapporto banca-cliente si veda anche: R.A. JARVINEN, *Consumer trust in banking relationships in Europe*, in *European journal of marketing*, 2014, p. 551 ss.; C. HALLIBURTON, A. POENARU, *The role of trust in consumer relationships*, ESCP Europe Business School, 2010.

Per le banche tradizionali, infatti, la prospettiva di una regolamentazione come quella delineata nella Proposta AIA può rivelarsi l'occasione di spostare nuovamente i termini della concorrenza sul mercato bancario a proprio favore (a discapito delle *Fintech banks*), puntando sulla valorizzazione, non di un prodotto bancario performante in termini predittivo-digitali "ad ogni costo", bensì di un servizio *compliant* e virtuoso, rispettoso delle esigenze e dei diritti del singolo consumatore.

PARTE III

LA VIA EUROPEA ALLA REGOLAZIONE DEL MERCATO DEI DATI TRA "PROTEZIONE" E "CIRCOLAZIONE"

IL VALORE DEI DATI NELL'*EUROPEAN DATA STRATEGY*: SVILUPPO DELLA PERSONA, DINAMICHE DI MERCATO E BENESSERE SOCIALE

di *Alessandro Moretti*

SOMMARIO: 1. Introduzione. – 2. L'*European Data Strategy*. – 3. Il valore personalistico ed economico dei dati. – 4. Il valore sociale dei dati. – 5. Osservazioni conclusive.

1. *Introduzione*

Negli ultimi anni ha avuto luogo un processo di profonda datizzazione [1] che ha investito il mondo digitale ed analogico, fino ad interessare direttamente l'individuo in ogni sua dimensione. Con l'ingresso nel XXI secolo si è assistito, infatti, ad una capillare raccolta d'informazioni dall'ambiente circostante e alla nascita del concetto di *big data* [2]. Contestualmente, si sono sviluppate nuove tecnologie per il trattamento dei dati così da consentire la realizzazione di più penetranti operazioni d'interconnessione e di analisi.

Il cambiamento intervenuto, dunque, non è stato unicamente di natura quantitativa, legato al volume e alla varietà dei dati raccolti, ma è stato altresì qualitativo, in ragione delle modalità innovative attraverso cui effettuare l'attività di elaborazione e, di conseguenza, mediante le quali estrarre valore dai dati [3].

---

[1] Al riguardo V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, p. 109.

[2] Sul concetto di *big data* si veda, *ex multis*, D. LANEY, *3-D data management: Controlling data volume, velocity and variety*, Application Delivery Strategies by META Group Inc, 6 febbraio 2001, reperibile in https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf; G. D'ACQUISTO, M. NALDI, *Big data e privacy by design*, Torino, 2017, p. 5 ss.; Garante per la protezione dei dati personali, AGCM, AGCOM, *Indagine conoscitiva sui Big Data*, 10 febbraio 2020.

[3] Così A. SORO, *Liberi e connessi*, Torino, 2016, p. 20. Occorre infatti osservare come il valo-

Proprio in virtù delle potenzialità sottese al loro utilizzo, i dati costituiscono oggigiorno una risorsa di fondamentale importanza a livello globale, tanto da venir spesso definiti come il nuovo petrolio digitale [4]. Per il loro tramite è possibile favorire la crescita dell'attività economico-imprenditoriale, così come l'attività di ricerca scientifica ed il progresso tecnologico. Basti pensare alla necessaria disponibilità di dati ai fini di un efficace sviluppo dei sistemi d'intelligenza artificiale [5].

Per tali ragioni, il rilievo politico-economico che ciascun continente può acquisire sul panorama internazionale passa anche attraverso la capacità di delineare un'efficace strategia per sfruttare al meglio le opportunità offerte dai dati, tanto in termini di sviluppo economico, quanto in termini di massimizzazione del benessere sociale.

2. *L'*European Data Strategy

Avendo consapevolezza dell'importanza che i dati acquisiscono nell'odierna società, l'Unione europea ha inteso tracciare un'apposita strategia diretta a promuovere e gestire il valore che può essere prodotto tramite i dati. La Commissione europea ha pertanto pubblicato, nel febbraio 2020, l'*European Data Strategy* o Strategia europea in materia di dati [6] con l'obiettivo sia di assi-

---

re dei dati non risiede unicamente nel loro mero possesso, ma si lega altresì alle modalità con cui gli stessi vengono lavorati, trattati ed aggregati. Al riguardo V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, cit., p. 139 ss.; A. MANTELERO, *The future of consumer data protection in the EU Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law & Security Review*, 2014, vol. 30, n. 6, p. 650.

[4] Si veda *The world's most valuable resource is no longer oil, but data*, in *The Economist*, 6 May 2017; J. SADOWSKI, *When data is capital: Datafication, accumulation, and extraction*, in *Big Data & Society*, 2019, vol. 6, n. 1.

[5] Sul punto, Commission Nationale Informatique & Libertes, *How can human keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*, December 2017, p. 18, evidenzia il rapporto d'interdipendenza che intercorre tra i dati e i sistemi d'intelligenza artificiale affermando che «*The algorithm without data is blind. Data without algorithms is dumb*». Non a caso, contestualmente all'*European Data Strategy*, la Commissione ha pubblicato il libro bianco in materia d'intelligenza artificiale, ove peraltro viene posta in evidenza la complementarietà tra lo sviluppo dei sistemi artificiali e la strategia sopra richiamata. Cfr. Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, COM(2020) 65 final, 19 febbraio 2020, p. 9.

[6] Cfr. Commissione europea, *Una strategia europea per i dati*, Bruxelles, COM(2020) 66 final, 19 febbraio 2020.

curare la disponibilità e la condivisione di quest'ultimi all'interno dell'Unione, sia di favorirne l'utilizzo. L'intento è quello di realizzare uno spazio unico europeo dei dati, facilitando così un accesso diffuso a dati di alta qualità per stimolare la crescita e creare valore[7].

Tale intervento della Commissione si aggiunge ad una serie di atti normativi già adottati in Europa – quali il *General Data Protection Regulation*, il Regolamento in materia di dati non personali e la Direttiva *Open Data*[8] – volti ad introdurre discipline specifiche per la tutela e l'utilizzo di determinate tipologie di dati. Tenuto conto della pressante esigenza di definire una direzione univoca e condivisa per la gestione del patrimonio informativo comunitario, l'*European Data Strategy* interviene dunque su di un contesto tecnologico-normativo complesso ed eterogeneo, fornendo una visione comune da seguire in ambito continentale.

Per far ciò, la strategia individua diversi punti di criticità su cui l'Unione è chiamata ad intervenire affinché possa esprimere appieno il proprio potenziale in termini di utilizzo dei dati[9].

Un primo punto di attenzione è individuato nell'effettiva disponibilità delle informazioni che non sempre risulta sufficiente per consentire la realizzazione di attività o progetti innovativi. Da un lato, rispetto allo scambio di dati tra il settore pubblico e le imprese (*Government to Business* – G2B), si rileva che all'interno degli Stati membri sussistono tuttora modalità eterogenee attraverso cui le Istituzioni rendono disponibili i propri *dataset*. Dall'altro lato, si riscontra una limitata condivisione d'informazioni dal settore privato a quello pubblico (*Business to Government* – B2G) o tra imprese (*Business to Business* – B2B), talvolta per l'assenza di idonei incentivi e, in altri casi, per mancanza di fiducia tra gli attori coinvolti[10].

La presenza di situazioni di squilibrio in termini di potere di mercato costituisce un ulteriore profilo indicato nell'*European Data Strategy* su cui occorre intervenire. Tali squilibri possono derivare da un'asimmetrica capacità di accesso ed utilizzo dei dati da parte di determinati soggetti che, in questo modo, sono

---

[7] Così European Data Protection Supervisor, *Opinion 3/2020, Opinion on the European strategy for data*, 16 June 2020, p. 4.

[8] Si fa riferimento al Regolamento UE 2016/679, al Regolamento UE 2018/1807 e alla Direttiva UE 2019/1024.

[9] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 7 ss.

[10] Per un'analisi approfondita delle limitazioni che incontra la condivisione dei dati dal settore privato a quello pubblico si veda European Commission, *Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the high-level expert group on business-to-government data sharing*, 2020, p. 31 ss.

in grado di acquisire e mantenere una posizione dominante all'interno di uno specifico settore [11]. Non solo. Anche ove i dati risultino agevolmente disponibili, la strategia europea rileva come l'Unione necessiti di assicurare agli stessi un maggior livello di qualità e interoperabilità, caratteristiche essenziali per favorire la condivisione e la combinazione di dati provenienti da fonti differenti.

Poiché il valore dei dati è strettamente connesso alle infrastrutture che ne consentono un utilizzo efficace, l'*European Data Strategy* sottolinea altresì l'importanza d'implementare strumenti tecnologici adeguati per la raccolta, l'elaborazione e la conservazione dei dati. Sul punto, vengono rilevate notevoli difficoltà con riguardo alla fornitura di servizi *cloud* da parte dell'Unione, sia sotto il profilo dell'offerta – stante la preminenza di fornitori extra-comunitari – sia in termini di domanda. Inoltre, fermi restando i recenti interventi normativi europei in materia di *cyber security* [12], viene posto l'accento sulla crescente attenzione che occorre dedicare alla sicurezza informatica. Ciò affinché si sia in grado di tutelare la disponibilità, l'integrità e – se del caso – la riservatezza dei dati, anche tenuto conto dei nuovi rischi e delle sfide introdotti dall'evoluzione tecnologica [13].

L'*European Data Strategy* si concentra poi sulle criticità che interessano più da vicino le persone. Si osserva, infatti, la sussistenza di limitati strumenti tecnici e normativi che favoriscano un agevole esercizio dei diritti da parte degli interessati, nonché un maggiore controllo sui propri dati [14]. Allo stesso tempo, viene ravvisata all'interno della popolazione una diffusa mancanza di conoscenze in materia di dati, sia in termini di competenze specialistiche, sia sotto il profilo dell'alfabetizzazione di base [15].

---

[11] Sul tema M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019, p. 67 ss.

[12] Cfr. Direttiva UE 2016/1148, ovvero la "Direttiva NIS" che risulta soggetta a proposte di revisione finalizzate ad elaborare una "Direttiva NIS 2.0"; Regolamento UE 2019/881, ovvero il "*Cybersecurity Act*". Più in generale sull'argomento R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *federalismi.it*, 2021, n. 21, p. 31 ss.

[13] Per una panoramica dei principali incidenti informatici recentemente verificatisi all'interno dell'Unione si veda European Union Agency for Cybersecurity, *Threat Landscape 2020 – Main Incidents*, October 2020. Con particolare riguardo al contesto italiano, CLUSIT, *Rapporto 2021 sulla sicurezza ICT in Italia*, 2021.

[14] La strategia europea sembra accogliere e recepire le istanze manifestate dalla società civile circa l'esigenza di assicurare agli interessati una maggiore capacità di autodeterminazione e controllo sui propri dati. Al riguardo, particolarmente significativa è la Dichiarazione dall'organizzazione no-profit MyData Global reperibile in https://mydata.org/declaration/.

[15] L'esigenza di raggiungere un maggior livello di alfabetizzazione e di competenze digitali rappresenta un obiettivo costantemente evidenziato da parte delle Istituzioni europee. Cfr.

Per superare le criticità sopra descritte, l'*European Data Strategy* individua dunque quattro macro ambiti ove concentrare i propri interventi migliorativi [16].

Il primo riguarda la formulazione di un quadro di *governance* intersettoriale per l'accesso e l'impiego dei dati. L'obiettivo è quello di delineare un sistema di regole che favorisca l'utilizzo del patrimonio informativo pubblico e privato, definendo le corrette modalità attraverso cui poter effettuare simili operazioni. È in tale contesto che si inserisce la proposta di *Data Governance Act* [17] quale primo atto normativo che, in attuazione della strategia europea, intende promuovere la disponibilità dei dati all'interno dell'Unione e potenziare i relativi meccanismi di condivisione [18].

La messa a punto d'infrastrutture tecnologiche abilitanti e di idonee competenze per la gestione dei dati costituiscono due ulteriori ambiti sui cui la strategia si sofferma. Vengono così previsti appositi programmi di finanziamento affinché in Europa siano sviluppati gli strumenti e le conoscenze necessarie per beneficiare appieno delle potenzialità economico-sociali connesse all'elaborazione dei dati. Da ultimo, la strategia prevede che vengano realizzati degli spazi comuni di dati in specifici settori considerati strategici per ragioni economiche e d'interesse generale [19]. Ciò allo scopo di favorirne un rapido sviluppo e poter rispondere efficacemente alle diverse esigenze che tendono a caratterizzare ciascun singolo contesto.

Le previsioni contenute nell'*European Data Strategy* consentono di rilevare come quest'ultima abbia alla base l'acquisita consapevolezza da parte dell'U-

---

Commissione europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, Bruxelles, COM(2021) 118 final, 9 marzo 2021, p. 4 ss.; European Parliament, *Rethinking education in the digital age*, EPRS-STOA, March 2020, pp. 18-19. L'alfabetizzazione digitale risulta un profilo d'intervento particolarmente urgente in Italia dal momento che – come rilevato in Commissione europea, *Indice di digitalizzazione dell'economia e della società (DESI) 2020. Italia*, 2020, p. 3 – quest'ultima si colloca al 25° posto in Europa per indice di digitalizzazione, registrando «livelli di competenze digitali di base e avanzate molto bassi».

[16] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 13 ss.

[17] Cfr. Commissione europea, *Proposta di Regolamento relativo alla governance dei dati (Atto sulla governance dei dati)*, Bruxelles, COM(2020) 767 final, 25 novembre 2020. Per un'analisi dei contenuti della proposta regolamentare si veda F. COLAPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *AISDUE*, 5 maggio 2021, vol. 3, n. 3, p. 58 ss., reperibile su https://www.aisdue.eu/.

[18] Giova segnalare che, assieme al *Data Governance Act*, la strategia europea prevede un ulteriore intervento legislativo destinato a comporre il quadro di *governance* intersettoriale per la gestione dei dati, ovvero il *Data Act*, la cui consultazione pubblica si è recentemente conclusa in data 3 settembre 2021. Cfr. https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act.

[19] I settori individuati come strategici sono indicati in Commissione europea, *Una strategia europea per i dati*, cit., p. 24 ss. e p. 29 ss.

nione che i dati racchiudano in sé diverse tipologie di valore. Viene colta, in particolare, l'importanza che questi assumono tanto per l'economia quanto per la società. Si afferma infatti che «*i dati sono la linfa vitale dello sviluppo economico*», riconoscendo poi, da un lato, come gli stessi rendano possibile «*un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici*» e, dall'altro lato, come i dati costituiscano altresì un elemento «*fondamentale per far fronte alle sfide sociali, climatiche e ambientali, contribuendo allo sviluppo di società più sane, più prospere e più sostenibili*»[20].

Al valore economico e sociale dei dati si affianca, tuttavia, un'ulteriore tipologia di valore che gli stessi presentano ove riconducibili ad un determinato individuo. Si fa riferimento al valore personalistico dei dati che, unitamente a quello economico e sociale, dev'essere tenuto in necessaria considerazione affinché le esigenze del mercato o della collettività non rischino di determinare un'ingiustificata compressione delle libertà del singolo.

La strategia europea sembra cogliere la triplice dimensione connessa al valore dei dati, mettendo in evidenza le opportunità sociali e di mercato derivanti dal loro utilizzo e, allo stesso tempo, inducendo a riflettere ed approfondire il possibile rapporto che intercorre tra il valore economico dei dati e quello personalistico.

3. *Il valore personalistico ed economico dei dati*

L'*European Data Strategy* individua tra i principali scopi quello di creare le condizioni necessarie per un'economia attrattiva basata sui dati. Ciò implica l'utilizzo di quest'ultimi per la realizzazione di nuovi servizi o prodotti e per assicurare agli stessi una maggiore personalizzazione ed efficacia.

Benché si interessi della gestione dei dati a prescindere dalla loro natura, occorre osservare come la strategia europea – per il perseguimento dei propri obiettivi – non può esimersi dall'occuparsi anche del valore che i dati personali acquisiscono all'interno del mercato digitale.

A ben vedere, il valore economico connesso all'elaborazione dei dati può risultare particolarmente profondo e per certi aspetti critico laddove quest'ultimi siano suscettibili di fornire informazioni riguardanti un individuo. Infatti, i dati personali racchiudono in sé differenti ruoli e funzioni, finendo per configurarsi allo stesso tempo quale risorsa economica e oggetto di un diritto fondamentale[21].

---

[20] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 3.

[21] Si veda S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, 1999, pp. 210-211; A. SORO,

È questo secondo aspetto ad aver conosciuto tradizionalmente maggior interesse in ambito europeo, orientando l'attenzione sul profilo personalistico e identitario connesso ai dati personali. Minor approfondimento, invece, è stato dedicato al valore economico-negoziale legato al loro trattamento, aspetto che tuttavia, nel tempo, è divenuto un elemento caratterizzante di molteplici modelli di *business* tipici della *data economy* [22].

In questo senso, non può che essere rilevato come i dati – anche di natura personale – abbiano di fatto assunto una propria valenza economica nel mercato digitale, tanto da acquisire rilievo all'interno dei rapporti negoziali tra i fornitori di beni o servizi e gli interessati [23]. Ciò è emerso in modo evidente con la Direttiva UE 2019/770 riguardante determinati aspetti dei contratti di fornitura di contenuti e servizi digitali, la quale, pur affermando che «*la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce*», riconosce altresì che «*La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato*» [24].

Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale, Milano, 2019, p. 43 ss. I dati personali costituiscono oggetto di un diritto fondamentale di radice nazionale e sovranazionale che, in ambito comunitario, trova riconoscimento all'art. 8 della Carta dei Diritti fondamentali dell'Unione europea, nonché all'art. 16 del Trattato sul funzionamento dell'Unione europea.

[22] La maggiore attenzione dedicata nel panorama europeo al profilo personalistico dei dati personali rispetto a quello negoziale è rilevata in V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. informazione e informatica*, 2018, fasc. 4, pp. 691-692.

[23] Così N. PURTOVA, *The illusion of personal data as no one's property*, in *Law, Innovation and technology*, 2015, vol. 7, n. 1, p. 87 ss.; G. MALGIERI, B. CUSTERS, *Pricing privacy – the right to know the value of your personal data*, in *Computer Law & Security Review*, 2018, vol. 34, n. 2, p. 292 ss. In particolare, possono essere individuate tre tipologie di modelli economici legati alla raccolta e al trattamento dei dati personali dell'interessato, ovvero: il *zero-price model*, il *personal data economy model* e il *paying for privacy model*. Al riguardo si veda S. ELVY, *Paying for privacy and the personal data economy*, in *Columbia Law Review*, 2017, vol. 117, n. 6, p. 1383 ss. e M. MURSIA, C.A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in *MediaLaws*, 2020, n. 2, pp. 169-170.

[24] Cfr. considerando 24 della Direttiva UE 2019/770. Giova rilevare che in fase di proposta l'art. 3, par. 1 della suddetta Direttiva faceva esplicito riferimento alla configurabilità di una «controprestazione non pecuniaria sotto forma di dati personali». Simile previsione è stata tuttavia oggetto di critiche da parte del Garante europeo della protezione dei dati, i cui rilievi hanno condotto ad una sensibile riformulazione – per lo meno di *drafting* legislativo – di talune disposizioni della Direttiva. Sul tema G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, in AA.VV, *Annuario del contratto 2018*, Torino, 2019, p. 130 ss.

Al riguardo, appaiono senz'altro condivisibili le criticità rilevate dal Garante europeo laddove si giungesse a ritenere i dati personali quali mera merce di scambio da utilizzare incondizionatamente per l'acquisto di beni e servizi [25]. E tuttavia, bisogna osservare come l'attribuzione di un valore economico a tali dati non comporta necessariamente che gli stessi risultino sottoposti ad un processo di "mercificazione". Il loro riconoscimento quale diritto fondamentale connesso all'identità e alla personalità dell'individuo, infatti, non ne determina di per sé l'esclusione da qualsivoglia dinamica negoziale.

D'altronde, i diritti legati alla personalità tendono a presentare caratteristiche e peculiarità differenti. In primo luogo si osserva come questi possano non avere valenza alcuna all'interno del mercato – si pensi all'onore – oppure, al contrario, siano suscettibili di acquisire rilevanza economica, come nel caso del nome o dell'immagine della persona. Inoltre, a seconda che vi sia una componente materiale o immateriale, i diritti della personalità possono trovare limiti più stringenti, così come avviene ad esempio per gli atti di disposizione su parti del proprio corpo [26].

I dati personali, dunque, ben potrebbero rientrare nell'ambito dei diritti della personalità privi di una componente materiale – risultando così soggetti a minori limitazioni – ed in grado di acquistare un certo rilevo negoziale. Quanto rilevato mostra come lo stretto legame che intercorre tra i dati personali e il valore personalistico non impedisca di attribuire a quest'ultimi anche un valore economico. Simile impostazione risulterebbe peraltro coerente alle previsioni contenute sia nel diritto primario che secondario dell'Unione europea.

Il riconoscimento della protezione dei dati personali quale diritto fondamentale all'art. 8 della Carta di Nizza, infatti, non esclude che tale tipologia di dati possa acquisire un rilievo economico. Mentre con riguardo al diritto all'integrità della persona la Carta pone il «*divieto di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro*» [27], rispetto ai dati personali non è

---

[25] L'inidoneità di considerare i dati personali come una merce o una controprestazione per l'ottenimento di un servizio è affermata in European Data Protection Supervisor, *Opinion 8/2016, Opinion on coherent enforcement of fundamental rights in the age of big data*, 23 September 2016, 7 e in European Data Protection Supervisor, *Opinion 4/2017, Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, cit., p. 6 ss.

[26] Sul punto G. RESTA, *The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives*, in *Tulane European and Civil Law Forum*, 2011, vol. 26, p. 48 ss.; M. MURSIA, C. A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context*, cit., pp. 178-179.

[27] Cfr. art. 3, par. 2, della Carta dei Diritti fondamentali dell'Unione europea.

individuato alcun espresso impedimento, essendo invece stabilito che, in presenza di un fondamento legittimo sancito dalla legge, gli stessi possono essere oggetto di trattamento da parte di terzi [28].

Lo stesso *General Data Protection Regulation*, poi, sembrerebbe accogliere al proprio interno una simile interpretazione. Già a partire dai considerando si afferma che la protezione dei dati personali non è da intendersi quale diritto assoluto, ma dev'essere contemperata con gli altri diritti fondamentali, ivi compresa la libertà d'impresa. Inoltre, unitamente alla tutela della persona, il Regolamento si pone l'obiettivo di assicurare la libera circolazione dei dati, anche al fine di favorire il progresso economico ed il rafforzamento del mercato interno [29]. Sono così individuabili determinate basi giuridiche – quali il consenso, la necessità di eseguire un contratto, l'interesse legittimo – e strumenti normativi – come il diritto alla portabilità – suscettibili di poter operare rispetto alla dimensione negoziale dei dati personali [30].

Ecco dunque che, se da una parte non è possibile considerare i dati al pari di una semplice merce di scambio, dall'altra parte risulta altrettanto difficoltoso ritenerli come una *res extra commercium*, ovvero del tutto estranei alle dinamiche di mercato. Sembrerebbe piuttosto configurabile una via intermedia che, tenendo fermo il valore personalistico connesso ai dati, riconosca altresì la possibilità di un loro utilizzo economico condizionato, nel rispetto dei limiti e secondo le modalità dettate dalla disciplina a protezione dei dati [31].

---

[28] Così G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, cit., pp. 140-141.

[29] Cfr. Cons. 2 e 4, nonché l'art. 1 del Regolamento UE 2016/679. In tal senso S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela* dell'utente, in *MediaLaws*, 2019, n. 3, pp. 146-147.

[30] Cfr. artt. 6, 7 e 20 del Regolamento UE 2016/679. Sul tema G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, 2020, fasc. 4, p. 656 ss.

[31] La possibilità di un utilizzo economico condizionato è dovuta, ad esempio, alla necessità di dover riconoscere all'interessato il diritto di revocare liberamente e in ogni momento il proprio consenso, nonché di dover impiegare i dati per le specifiche finalità su cui il soggetto è stato adeguatamente informato. Inoltre, potrebbero essere previste più stringenti condizioni di utilizzo economico – ove non anche veri e propri divieti – in ragione della natura particolarmente sensibile dei dati personali coinvolti. Al riguardo V. JANECEK, G. MALGIERI, *Commerce in Data and the Dynamically Limited Alienability Rule*, in *German Law Journal*, 2020, vol. 21, n. 5, p. 924; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, cit., p. 669. Per un maggiore bilanciamento degli interessi in gioco – tale da non far prevalere la logica proprietaria sul valore personalistico dei dati – sarebbe altresì ipotizzabile che l'interessato venga informato di quale sia il valore economico attribuito ai propri dati, oltre che al tornaconto che potrà avere un terzo tramite il loro utilizzo. In questo senso, gli obblighi d'informazione previsti nella normativa in materia di *data protection* potrebbero dilatarsi

Quest'ultima impostazione sembra poter essere individuata all'interno dell'*European Data Strategy.* Non a caso, ci si propone di creare i presupposti affinché tramite i dati sia possibile sviluppare nuovi prodotti e servizi e, allo stesso tempo, si riconosce apertamente che «*i cittadini daranno fiducia alle innovazioni tecnologiche basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati*»[32].

L'obiettivo perseguito dall'Unione attraverso la strategia europea è pertanto quello di far coesistere e conciliare il valore dei dati nelle sue diverse dimensioni, in modo tale da «*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*»[33]. Ciò suggerisce un approccio non di contrapposizione ma complementare tra il valore economico e personalistico dei dati, riconoscendo così come quest'ultimi possano racchiudere in sé le due tipologie di valore sopra richiamate, entrambe imprescindibili per un utilizzo sicuro ed efficace del patrimonio informativo europeo.

4. *Il valore sociale dei dati*

La condivisione e l'elaborazione dei dati rappresentano un elemento essenziale delle attuali dinamiche di mercato, affinché risulti possibile offrire beni e servizi competitivi nell'ambito dell'economia digitale[34]. Eppure, lungi dall'acquisire importanza rispetto al solo contesto economico, i dati costituiscono altresì una preziosa risorsa per favorire lo sviluppo della società.

Tale aspetto trova particolare attenzione all'interno dell'*European Data Strategy* ove si rileva come i dati possano divenire un fattore determinante a vantaggio della collettività, per raggiungere obiettivi d'interesse generale e per il perseguimento del bene comune[35]. La strategia europea mette dunque in

---

fino a ricomprendere, non soltanto aspetti relativi al profilo personalistico ed intimo dei dati, ma anche informazioni riguardanti il loro valore economico. Cfr. G. MALGIERI, B. CUSTERS, *Pricing privacy – the right to know the value of your personal data*, cit., p. 289 ss.

[32] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 1.

[33] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 2.

[34] Si veda V. MORABITO, *Big Data and Analytics*, Springer, 2015, p. 65 ss.; M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, cit., p. 49 ss.

[35] In questo senso Commissione europea, *Una strategia europea per i dati*, cit., p. 1, ove si af-

evidenza lo stretto rapporto che lega la condivisione dei dati ed il benessere sociale, ponendo l'accento sulle opportunità che possono derivare da tale relazione.

Le capacità e i modi attraverso cui impiegare i dati costituiscono senz'altro un aspetto centrale affinché da questi possa essere prodotto valore per la collettività. Tuttavia, ancor prima della modalità di utilizzo, risulta determinante che sia assicurata un'effettiva disponibilità dei dati. È soltanto attraverso l'analisi di un ingente quantitativo d'informazioni, infatti, che si è in grado d'intervenire su problematiche caratterizzate da un elevato grado di complessità, di migliorare i processi decisionali e i servizi pubblici, nonché di dare un deciso impulso a specifici settori d'interesse generale.

L'*European Data Strategy* individua proprio nell'accessibilità al patrimonio informativo uno dei profili critici su cui l'Unione è chiamata ad intervenire, rilevando altresì come numerose sono le problematiche che interessano in particolar modo la disponibilità dei dati a vantaggio del bene pubblico[36]. Con l'obiettivo di superare tale ostacolo, la strategia si concentra sull'implementazione dei necessari fattori abilitanti e sul rafforzamento dei meccanismi volti ad agevolare la circolazione dei dati.

In tal senso, viene posto in evidenza il contributo che ciascuno – dalle Istituzioni alle aziende, fino al singolo cittadino – può offrire attraverso la scelta di mettere a disposizione i propri dati cosicché tutti i componenti della collettività ne possano trarre beneficio.

Le Istituzioni rappresentano gli attori principali che operano per il perseguimento di finalità d'interesse generale e, allo stesso tempo, si configurano esse stesse come depositarie dei dati generati dal settore pubblico. In ragione di ciò, la strategia europea sottolinea l'importanza che abbia luogo un ricco scambio d'informazioni, non soltanto tra le medesime Istituzioni, ma anche verso le aziende e i cittadini[37].

---

ferma che «*l'Europa mira a sfruttare o vantaggi di un migliore utilizzo dei dati, compresi una maggiore produttività e mercati competitivi, ma anche miglioramenti in materia di salute e benessere, ambiente, amministrazione trasparente e servizi pubblici convenienti*».

[36] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 7.

[37] In R.M. GEORGE, *Data for the Public Good. Challenges and Barriers in the Context of Cities*, in J. LANE, V. STODDEN, S. BENDER, H. NISSENBAUM (a cura di), *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, New York, 2014, pp. 155-156 e 165 ss., si indica l'opportunità che i soggetti pubblici – a partire dalle singole città – beneficino quanto più possibile dei propri sforzi ed investimenti in termini di raccolta dei dati generati dal settore pubblico, andando oltre la veste di meri depositari ed operando sia quali diretti utilizzatori dei dati, sia attraverso la messa a disposizione del patrimonio informativo pubblico a vantaggio della collettività. Proprio in relazione a quest'ultimo aspetto, in Commissione europea, *Una strategia euro-*

Si fa dunque riferimento all'applicazione dei principi FAIR[38] ed al fenomeno degli *open data*, ovvero dati rilasciati in formato aperto, liberamente accessibili e utilizzabili da chiunque[39]. In ragione di tali caratteristiche gli *open data* rappresentano una risorsa che, oltre a favorire lo sviluppo di nuove forme di *business*, consente ai cittadini di operare un controllo diffuso sull'agire pubblico, fornendo allo stesso tempo la possibilità di migliorare i servizi e le iniziative finalizzate al bene comune, nonché di costruire un rapporto proattivo e collaborativo tra Stato, cittadini ed aziende[40].

La stessa Unione europea intende porsi come esempio virtuoso di riutilizzo e condivisione dei dati del settore pubblico per finalità d'interesse generale. Si propone così di ricorrere maggiormente al proprio patrimonio informativo per orientare i processi decisionali e le politiche interne. Inoltre, attraverso specifiche iniziative – quali ad esempio il portale *Open data* dell'UE e il *Cloud* europeo per la scienza aperta – l'Unione s'impegna affinché i dati pubblici prodotti e raccolti in ambito europeo possano essere liberamente accessibili[41].

Ciò posto, occorre osservare come, unitamente all'attività delle Istituzioni, anche il contributo dei soggetti privati può risultare determinante ai fini della messa a disposizione e dell'utilizzo dei dati per il bene comune.

Non di rado, le aziende presentano al proprio interno risorse tali da consentire processi di elaborazione particolarmente efficaci e capillari. Nel settore privato tendono infatti a concentrarsi, da un lato, figure professionali con elevate competenze in materia di dati e, dall'altro lato, strumenti tecnologici dotati di notevole capacità computazionale e di analisi, a cui spesso si aggiunge una disponibilità di dati di rilevante entità.

La sussistenza di tali fattori, unita alla crescente consapevolezza del valore sociale connesso ai dati, ha così condotto a sviluppare il concetto di *data phi-*

---

pea per i dati, cit., p. 8, si rileva che le informazioni detenute dalle Istituzioni costituiscono «*dati prodotti con denaro pubblico che dovrebbero pertanto essere utilizzati a beneficio della società*».

[38] L'acronimo FAIR descrive i principi di *Findability*, *Accessibility*, *Interoperability* e *Reusability*. Cfr. https://www.go-fair.org/fair-principles/.

[39] Cfr. considerando 16 della Direttiva UE 2019/1024.

[40] Si veda J. GURIN, *Open data now: the secret to hot startups, smart investing, savvy marketing, and fast innovation*, New York, 2014, 261, pp. 9 ss.; MCKINSEY GLOBAL INSTITUTE, *Open data: Unlocking innovation and performance with liquid information*, October 2013; B. COCCAGNA, G. ZICCARDI, *Open data, trasparenza elettronica e codice aperto*, in M. DURANTE, U. PAGALLO (a cura di), *Manuale di informatica giuridica e di diritto delle nuove tecnologie*, Torino, 2012, p. 403 ss.

[41] Così Commissione europea, *Una strategia europea per i dati*, cit., p. 17. Il portale *Open Data* dell'Unione europea e il *Cloud* europeo per la scienza aperta sono raggiungibili rispettivamente in https://data.europa.eu/en e in https://eosc-portal.eu/.

lantropy o filantropia dei dati. Un fenomeno che si sostanzia nella decisione da parte delle aziende di condividere con la comunità le proprie competenze, tecnologie e risorse in materia di dati per il perseguimento di attività finalizzate al benessere sociale [42].

Attraverso il coinvolgimento attivo di società private e la condivisione dei dati in loro possesso si può essere in grado d'intervenire con efficacia in situazioni emergenziali e di aiuto umanitario. Si ha così l'opportunità di realizzare un'adeguata preparazione e farsi trovare pronti prima che si concretizzino situazioni di crisi. Tramite un'attenta allocazione delle risorse disponibili e una ponderata pianificazione degli interventi da eseguire, risulta altresì possibile attuare una pronta risposta già durante il verificarsi dell'evento critico, nonché nella successiva fase post-emergenziale [43].

Non solo. La condivisione dei dati da parte del settore privato può risultare utile anche per assicurare una gestione efficiente di situazioni non necessariamente di crisi. È anzi in tale contesto che il patrimonio informativo privato può acquisire un più ampio valore sociale, non circoscritto alla risoluzione di singoli eventi specifici, ma diretto ad intervenire trasversalmente su settori d'impatto quotidiano per l'individuo [44].

Assieme al contributo offerto dai soggetti pubblici e dalle aziende, bisogna osservare come la volontà di condividere i propri dati per il bene comune può altresì collegarsi alla libertà decisionale di ciascun singolo cittadino.

---

[42] Sul tema Y. LEV-ARETZ, *Data Philantropy*, in *Hastings Law Journal*, 2019, vol. 70, p. 1491 ss.; M. TADDEO, *Data philanthropy and the design of the infraethics for information societies*, in *Philosophical Transactions of the Royal Society A*, 2016, vol. 374, n. 2083; N. KSHETRI, *The emerging role of Big Data in key development issues: Opportunities, challenges, and concerns*, in *Big Data & Society*, 2014, vol. 1, n. 2, p. 16; R. KIRKPATRICK, *A new type of philanthropy: donating data*, in *Harvard Business Review*, 21 March 2013, reperibile in https://hbr.org/2013/03/a-new-type-of-philanthropy-don.

[43] In questo senso A. ALEMANNO, *Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many*, in *European Journal of Risk Regulation*, 2018, vol. 9, n. 2, p. 183 ss.; QADIR *et al.*, *Crisis analytics: big data-driven crisis response*, in *Journal of International Humanitarian Action*, 2016, vol. 1, n. 12. Un esempio emblematico può essere individuato nella gestione del terremoto avvenuto in Nepal nel 2015, ove, assieme all'organizzazione non governativa Flowminder, è intervenuta la società Ncell, uno dei principali fornitori di servizi mobili presenti in Nepal. Sul punto Y. LEV-ARETZ, *Data Philantropy*, cit., p. 1493; Global Pulse, *The State of Mobile Data for Social Good Report*, June 2017, p. 7. Allo stesso tempo giova sottolineare che – qualora vi sia un trattamento di dati personali – anche per intervenire in situazioni emergenziali e di aiuto umanitario sarà necessario effettuare un necessario bilanciamento tra il valore sociale dei dati e quello personalistico ad essi connesso. Cfr. T. GAZI, *Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR*, in *Journal of International Humanitarian Action*, 2020, vol. 5, n. 9.

[44] Cfr. A. ALEMANNO, *Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many*, cit., p. 184.

Al riguardo, un intervento di particolare rilievo è stato realizzato attraverso una delle prime proposte regolamentari attuative dell'*European Data Strategy*, ossia il *Data Governance Act*. Nello specifico, la proposta regolamentare introduce il concetto di *data altruism*, che si sostanzia nella scelta volontaria di mettere a disposizione i propri dati per il perseguimento di scopi altruistici, senza che venga chiesto in cambio alcun corrispettivo [45].

Il *data altruism* trova alla propria base la volontà di fornire i dati perché possano essere impiegati per finalità d'interesse generale quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici e lo sviluppo della ricerca scientifica [46]. Affinché tale fenomeno venga favorito, è stabilita l'istituzione di apposite organizzazioni *no-profit* aventi il compito di gestire le informazioni condivise e, in particolare, di garantire che queste vengano effettivamente impiegate per le finalità d'interesse generale prescelte [47]. Inoltre, allo scopo di assicurare un meccanismo di condivisione uniforme all'interno dell'Unione, è stata prevista la predisposizione di un modello comune europeo di consenso per l'altruismo dei dati in modo tale che si sia tenuti ad agire secondo le stesse regole ed attraverso i medesimi strumenti [48].

---

[45] Le disposizioni riguardanti il *data altruism* o l'altruismo dei dati sono contenute nel Capo IV della proposta di *Data Governance Act*, che interviene per dare applicazione a quanto previsto in Commissione europea, *Una strategia europea per i dati*, cit., p. 15. Al riguardo, il Garante europeo ha tuttavia posto l'attenzione sulla necessità che il *data altruism* trovi applicazione nel rispetto del valore personalistico connesso ai dati e, conseguentemente, della disciplina sulla *data protection*. Il rischio che si vuole scongiurare è che l'altruismo dei dati – spesso associato al concetto di *data donation* o donazione dei dati – finisca per configurarsi in concreto come un atto di vera e propria alienazione attraverso cui il soggetto cede i propri dati perdendone il controllo. Cfr. European Data Protection Supervisor, *Opinion 3/2020, Opinion on the European strategy for data*, cit., p. 14. In European Data Protection Board, European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 March 2021, pp. 38-39, viene altresì rilevata l'opportunità che venga chiarito maggiormente il rapporto che intercorre tra il consenso previsto per l'altruismo dei dati e quello contenuto nella normativa sulla protezione dei dati.

[46] Così il considerando 35 della proposta di *Data Governance Act*.

[47] Cfr. artt. 15 ss. della proposta di *Data Governance Act*.

[48] Cfr. art. 22 della proposta di *Data Governance Act*. In European Data Protection Board, European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, cit., p. 45, si evidenza la necessità di uno stretto coinvolgimento delle autorità per la protezione dei dati in sede di predisposizione del modello di consenso per l'altruismo dei dati.

Riferendosi alle Istituzioni, alle aziende e ai cittadini, l'*European Data Strategy* individua i soggetti in grado di favorire attivamente la circolazione dei dati all'interno dell'Unione. E tuttavia, occorre rilevare come la scelta di condividere i dati può risultare strettamente legata al livello di sensibilizzazione che si ha dei potenziali benefici derivanti da tale decisione. Se un soggetto è cosciente dei vantaggi che i propri dati possono avere per la collettività, allora sarà certamente più disposto a metterli a disposizione. Per questo motivo, la strategia europea pone l'accento sull'alfabetizzazione ai dati [49], da intendersi non soltanto come sviluppo di specifiche competenze professionali, ma anche quale maggiore consapevolezza del valore sociale connesso alla condivisione dei dati per il bene comune. Una consapevolezza che si auspica venga acquisita in maniera trasversale, partendo dalle Istituzioni e dal settore privato, giungendo infine ai singoli individui.

La strategia europea tiene conto, inoltre, di come ciascun settore presenti caratteristiche proprie e possa rivestire una particolare rilevanza per i cittadini. È così prevista la realizzazione di spazi di dati settoriali in ambiti strategici [50], molti dei quali implicano di fatto la messa a disposizione d'informazioni a vantaggio della comunità. Basti pensare alla volontà di costituire uno spazio di dati sul *Green Deal*, destinato ad affrontare le sfide legate al cambiamento climatico e alla tutela dell'ambiente [51], così come gli spazi di dati sanitari, sulla mobilità, sull'energia o per la pubblica amministrazione.

Nel complesso, dunque, l'*European Data Strategy* riconosce appieno il valore sociale dei dati. Ne coglie infatti le diverse potenzialità e, una volta individuati i possibili profili di miglioramento, si adopera affinché venga assicurato un effettivo scambio ed utilizzo di dati per il bene comune [52].

---

[49] Sul concetto di *data literacy* si veda Commissione europea, *Una strategia europea per i dati*, cit., pp. 6 e 23-24.

[50] Si rimanda alla nota n. 19 contenuta nel par. 2.

[51] L'importanza della disponibilità dei dati per poter intervenire sulle sfide ambientali è stata rilevata anche in Commissione europea, *Il Green Deal europeo*, Bruxelles, COM(2019) 640 final, 11 dicembre 2019, p. 21. Fermo restando i potenziali vantaggi sociali derivanti dall'utilizzo dei dati per affrontare le sfide ambientali, in M.I. ESPINOZA, M. ARONCZYK, *Big data for climate action or climate action for big data?*, in *Big Data & Society*, 2021, vol. 8, n. 1, si evidenzia come tale attività possa talvolta nascondere una strategia da parte di certi soggetti privati per legittimare pratiche estrattive orientate al profitto aziendale.

[52] In European Data Protection Supervisor, *Opinion 3/2020, Opinion on the European strategy for data*, cit., p. 7, il Garante europeo accoglie con favore l'attenzione che la strategia europea dedica all'utilizzo dei dati per il bene comune, sottolineando inoltre come la stessa disciplina sulla *data protection* presuppone che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo». Cfr. considerando 4 del Regolamento UE 2016/679.

5. *Osservazioni conclusive*

I dati sono divenuti una risorsa di rilevante valore all'interno della *data economy* e per il benessere della collettività. Di ciò si è resa consapevole l'Unione europea che è intervenuta a delineare un'apposita strategia per la gestione e la valorizzazione del patrimonio informativo comunitario.

L'*European Data Strategy* intende così realizzare le condizioni necessarie sia per sviluppare una ricca economia fondata sui dati, sia per fornire una decisa spinta all'utilizzo di quest'ultimi per lo svolgimento di attività di pubblico interesse. Il tutto nel rispetto dei valori e dei diritti fondamentali europei e nella ferma «*convinzione che l'essere umano sia e debba rimanere l'elemento centrale*»[53].

L'obiettivo è di promuovere il valore dei dati nella sua plurima dimensione personalistica, economica e sociale, tracciando una direttrice che, nel contempo, sappia coordinare ed equilibrare vicendevolmente la tutela della persona, gli interessi del mercato e le esigenze della società nel suo complesso.

[53] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 5.

DATI E INTELLIGENZA ARTIFICIALE ALL'INTERSEZIONE TRA MERCATO E DEMOCRAZIA

di *Giovanni De Gregorio* e *Federica Paolucci*

1. *Introduzione*

I dati sono sempre più considerati una tra le principali risorse del presente, e del futuro. L'incremento nella raccolta, analisi, produzione e riproduzione di informazioni sta conducendo al consolidamento di una *data-driven economy* su di essi, ossia un sistema economico basato sull'utilizzo e la commercializzazione dei dati, attraverso, principalmente, tecnologie automatizzate, tra cui l'intelligenza artificiale. Proprio per tale ragione, l'Unione europea ha da tempo intrapreso una scelta di campo e di mercato con l'obiettivo di rendersi leader nel settore, sia dal punto di vista tecnico, sia da quello del design normativo di tali applicazioni [1]. Ed è proprio in questo contesto che si inseriscono la *Strategia europea per i dati* [2], pubblicata nel 2020, o l'adozione del Regolamento 2018/1807 sulla libera circolazione dei dati non personali [3], ritenuti tasselli necessari per la creazione di un'architettura del diritto che completi il quadro della

[1] Circa il percorso seguito dall'Unione europea nei confronti della protezione dei dati personali, si veda F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/67*, voll. I e II, Torino, 2016.

[2] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Una strategia europea per i dati*, Bruxelles, 19 febbraio 2020 COM(2020) 66 final.

[3] Regolamento UE 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, in *G.U.U.E.*, L 303/59-68.

protezione dei dati [4], già tratteggiato dal Regolamento sulla protezione dei dati personali [5].

Difatti, nell'impasse tra dati personali e non personali, il tema di discussione dovrebbe più che altro incentrarsi sul favorire quanto più possibile la circolazione dei dati, in un contesto che abbia ben chiara la necessità di non prescindere dai valori costituzionali. La costruzione di una società che sia in grado di cogliere tutti i benefici della quarta rivoluzione industriale [6] non sembra poter prescindere da una solida riflessione sul tipo di percorso che si vuol delineare per consentire uno sviluppo sia dal lato degli investitori sia dal lato degli utenti finali di sistemi tecnologici avanzati *affidabili*, come quelli di intelligenza artificiale: sistemi che invero fanno un largo uso sia di dati personali sia di dati non personali.

Questo pendolo tra esigenze di mercato e protezione dei diritti fondamentali rappresenta l'oscillazione dell'Unione europea sul tema. Sin dalla sua elezione [7], difatti, Ursula von der Leyen, ha sempre avuto ben presente come fosse prioritario delineare un percorso di sviluppo ed applicazione dell'IA che potesse essere, da un lato, rispondente alle esigenze della "società algoritmica" e, dall'altro, affidabile tanto sul piano dell'output decisionale, quanto su quello della raccolta dei dati in input.

Nella cornice di quello che è stato definito dalla letteratura contemporanea *surveillance capitalism* [8], è urgente definire gli spazi e i confini applicativi di una tecnologia che può far affacciare l'umanità su un nuovo mondo [9], ma che, allo stesso tempo, solleva degli interrogativi sul piano dell'etica e della tutela dei valori democratici [10]. Le sfide normative legate all'IA ricadono, dunque, all'in-

---

[4] M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Merc. conc. reg.*, 2019, 2.

[5] '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). Qui di seguito, GDPR.

[6] Sul punto, l'analisi di L. FLORIDI, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Milano, 2017.

[7] Si veda, ad esempio, Commissione europea, *A Union that strives for more: the first 100 days*, Press release, 6 marzo 2020, <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_403>.

[8] Si veda, sul punto, l'analisi di S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, 2019.

[9] «*Artificial intelligence will open new world for us. But these worlds also need rules*», con queste parole si è espressa Ursula von der Leyen, Presidente della Commissione europea, con un messaggio nel giorno della pubblicazione della *Proposta di Regolamento sull'Intelligenza artificiale*.

[10] S. DORIGO, E. LOMBARDI, E. LONGO, S. PIETROPAOLI, *The Phenomenon of the Algorithm*

terno di un quadro di algocrazia, o società algoritmica o datacrazia, termine con cui Danaher [11] intende «*un sistema in cui gli algoritmi sono utilizzati per raccogliere, collezionare e organizzare i dati su cui vengono tipicamente prese le decisioni e per assistere nel modo in cui quei dati vengono elaborati e comunicati attraverso il relativo sistema di governance*».

In questo contesto, dunque, il regime giuridico a tutela dei dati personali acquista centralità considerando il ruolo dei dati per l'evoluzione della società dell'informazione. Il design di un sistema di *governance* che tenga conto del valore dei dati e della disciplina loro dedicata può contribuire a favorire o ostacolare lo sviluppo delle tecnologie di intelligenza artificiale, e, più in generale, l'innovazione nel mercato interno. Pertanto, le norme che regolano il trattamento dei dati possono avere un forte impatto sulle basi tecnologiche dell'intelligenza artificiale. Rispetto al timore di un incontrollato sviluppo delle tecnologie algoritmiche, sarebbe sufficiente esaminare la tutela costituzionale riconosciuta ai dati personali in ambito europeo per dedurre, almeno apparentemente, un limite all'emergere di un'innovazione massiva ed incontrollata. A questo proposito, il GDPR, non a caso, ha dedicato i primi quattro considerando all'importanza della tutela della privacy e della protezione dei dati nel quadro dell'Unione. Tuttavia, il menzionato quadro di tutela dei dati personali non completa né esaurisce il quadro giuridico da applicare all'intelligenza artificiale, come, in particolare, è possibile constatare osservando la proposta di Regolamento sull'Intelligenza artificiale [12]. Il binomio protezione ed innovazione sembra scontrarsi con le caratteristiche dell'IA ed è proprio nella coordinazione efficiente tra questi due elementi che risiede la sfida più importante per l'UE. Nella quarta rivoluzione industriale è, dunque, prioritario capire dove tracciare una linea tra innovazione e rischio per la tutela dei diritti.

A partire, quindi, dalle problematiche ivi delineate riferite a questa che appare essere una fase cruciale per la politica dell'Unione nel campo dell'intelligenza artificiale, il presente lavoro si propone di esaminare la tensione presente nel regime giuridico europeo, in particolare rappresentato dal GDPR e dal Regolamento IA, tra l'esigenza di promuovere lo sviluppo delle tecnologie di intelligenza artificiale e la tutela dei valori costituzionali europei.

Pertanto, in questo contributo, si partirà inizialmente dai cardini della tutela

---

and its Impact on the EU Legal Systerm: An Attempt at a Multidisciplinary Approach, in *Legal Issues in the Digital Age*, 2020, 3, pp. 3-34.

[11] Citazione tratta da J. DANAHER, *The Threat of Algocracy: Reality, Resistance and Accommodation*, in *Philosophy & Technology*, 2016, 3, 29, pp. 245-68.

[12] Precisamente, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts*, Brussels, 21 aprile 2021 COM(2021).

costituzionale, per rintracciare poi i valori che definiscono la tutela della privacy e dei dati personali in Europa. In secondo luogo, si cercheranno nella disciplina della protezione dei dati spazi di adattabilità per la disciplina dell'intelligenza artificiale. Questa tensione verrà, nella terza parte, portata in evidenza dall'analisi comparata della bozza di Regolamento e del GDPR, attraverso cui si potranno scorgere le criticità del far convivere le due discipline, non solo sul piano della *policy*, ma soprattutto sul piano sostanziale, rinsaldando l'assunto tipicamente europeo secondo il quale non si può in alcun modo assoggettare la tutela diritti fondamentali alle spinte del mercato e dell'innovazione.

2. *Il consolidamento costituzionale della privacy e della tutela dei dati personali in Europa*

L'impatto del quadro giuridico europeo sull'intelligenza artificiale potrebbe essere analizzato direttamente guardando alle regole stabilite nel GDPR o della proposta di Regolamento sull'intelligenza artificiale. Tuttavia, lo sviluppo di tali sistemi è strettamente connesso alla cornice costituzionale di riferimento in materia di privacy e tutela dei dati personali [13]. Le norme sulla protezione dei dati, infatti, non sono solo il risultato di un'analisi normativa basata sul bilanciamento tra innovazione e rischi, ma anche di ragioni storiche e valori costituzionali.

La protezione dei dati nel quadro europeo costituisce un diritto individuale relativamente nuovo sviluppato in risposta all'ascesa della società dell'informazione guidata dalle nuove tecnologie automatizzate e, in particolare, da internet. In altre parole, se il diritto alla privacy è bastato a soddisfare gli interessi della tutela delle persone, nella società dell'informazione il trattamento diffuso dei dati personali, anche attraverso strumenti automatizzati, esso si è però limitato a tutelare la sola dimensione negativa del diritto in questione, come meglio si dirà a breve.

Sebbene alcuni Stati membri avessero introdotto una regolamentazione sulla protezione dei dati prima dell'avvento di internet, anticipando la Direttiva 95/46/CE ("Direttiva sulla protezione dei dati") [14] fino al 1995, la disciplina era

[13] Si veda a tal proposito J. RAUHOFER, C. BOWDEN, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, in *University of Edinburgh School of Law Research Paper*, 2013, 28.

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

stata già oggetto di analisi nell'ambito del Consiglio d'Europa, grazie all'interpretazione che la Corte di Strasburgo [15] ha fatto dell'art. 8, così come sancito dalla Convenzione Europea dei Diritti dell'uomo.

Difatti, la Direttiva sulla protezione dei dati è intervenuta solamente nel 1995, seppur prima dell'adozione della Carta di Nizza nel 2000 che ha riconosciuto la protezione dei dati come diritto fondamentale (sebbene non abbia esplicato alcun effetto vincolante fino all'entrata in vigore del Trattato di Lisbona nel 2009). Sarebbe sufficiente guardare ai considerando della Direttiva sulla protezione dei dati in quanto mettono ben in evidenza la natura funzionale (e non fondamentale) della protezione dei dati personali per il consolidamento e il corretto funzionamento del mercato unico e, di conseguenza, come strumento per garantire le libertà fondamentali dell'Unione [16].

In questo scenario fondato sul prevalere della dimensione economico-funzionale della protezione dei dati personali, il riconoscimento del carattere vincolante della Carta e il suo inserimento nel novero del diritto primario dell'UE hanno contribuito a codificare la dimensione costituzionale del diritto alla protezione dei dati nell'Unione. Difatti, gli artt. 7 e 8 della Carta, insieme all'art. 16 TFUE, costituiscono la base del rispetto della vita privata e familiare e della protezione dei dati personali.

Tali diritti fondamentali non sono assoluti ma possono essere limitati dalle autorità pubbliche solo secondo i criteri stabiliti dall'art. 52 basati sulla legalità, legittimità e proporzionalità. Tuttavia, la codificazione della protezione dei dati come diritto fondamentale non è sufficiente per comprendere il loro grado di protezione nel contesto europeo. Infatti, passando al campo della *law in action*, vale la pena osservare come la Corte di giustizia abbia svolto un ruolo fondamentale nel processo di costituzionalizzazione del diritto alla protezione dei dati.

Nonostante la mancanza di un'assiologia tra queste dimensioni, la giurisprudenza della Corte di giustizia in materia di protezione dei dati mostra come il rapporto tra libertà fondamentali e diritti nel mercato interno sia tutt'altro che equivalente. Basti pensare, ad esempio, alla pronuncia nel caso *Lindqvist* [17], dove per la prima volta la Corte venne chiamata a risolvere una controversia che vedeva contrapposti due diritti: la libertà d'espressione e la privacy. Già in

---

[15] Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, CEDU, (firmata a Roma il 4 novembre 1950).

[16] Un aspetto che merge a chiare lettere dalla Direttiva del 1995, ma anche dalla Direttiva 2000/31/EC relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") [2000] *G.U.* L 178/1.

[17] Decisione C-101/01 Bodil Lindqvist [2003] ECR I-12971.

questa fase la Corte si era impegnata a seguire un approccio di bilanciamento tra diritti che ne costituisce tutt'oggi la cifra stilistica, soprattutto nel riconoscere al diritto alla privacy una natura costituzionale. Dal primo riconoscimento della protezione dei dati come diritto fondamentale nel caso *Promusicae*[18], anche senza emanciparsi dal diritto alla tutela della vita privata, la Corte di giustizia ha rafforzato la tutela di tale diritto fondamentale: un aspetto ravvisabile nelle decisioni sulla privacy digitale nello scenario successivo all'entrata in vigore del Trattato di Lisbona, come è possibile osservare nelle decisioni *Digital Rights Ireland*[19], *Google Spain*[20] and *Schrems*[21].

Il percorso costituzionale della protezione dei dati personali ha compiuto un ulteriore passo con l'adozione del GDPR il cui primo obiettivo è quello di garantire il diritto alla protezione dei dati personali in quanto diritto fondamentale degli interessati. Nonostante l'elevato grado di salvaguardia di cui questi godono nel panorama comunitario, vale la pena evidenziare che questo diritto fondamentale non gode di una tutela assoluta ma «*deve essere considerato in relazione alla sua funzione nella società e bilanciato con altri diritti fondamentali, conformemente con il principio di proporzionalità*[22]». Infatti, il diritto alla privacy e il diritto alla protezione dei dati non sono diritti assoluti, quindi possono essere limitati per proteggere altri diritti costituzionali o per scopi legittimi secondo i test di proporzionalità sopra menzionati.

Tale contesto ha permesso di spostare l'attenzione da una dimensione "negativa" del diritto alla privacy, come nella connotazione statunitense, ad una dimensione "positiva" e dinamica, ossia come catalizzatore di diritti, o, per riprendere le parole di Rodotà, una *summa* dell'esercizio dei diritti nel mondo digitale[23]. Pertanto, tramite le spinte creative della Corte di Giustizia si arriva a delineare un concetto di privacy che va ben oltre «*il diritto ad essere lasciati soli*[24]», e che si incardina come predicato di una serie di valori predominanti

---

[18] Decisione C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU.*

[19] Decisione C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others.*

[20] Decisione C-131/12, *Google Spain SL and Google Inc v Agencia Española de Protectión de Datos (AEPD) and Mario Costeja Conzález.*

[21] Decisione C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.*

[22] GDPR, considerando 4.

[23] S. RODOTÀ, P. CONTI, *Intervista su privacy e libertà,* Roma, 2005.

[24] L. BRANDEIS, S. WARREN, *The right to privacy*, in *Harvard Law Review*, 1890, pp. 193-220.

che allargano i confini della protezione dei dati personali, anche oltre la giurisdizione dell'UE.

Nel quadro costituzionale europeo, il dilemma normativo tra innovazione e rischi non è solo fortemente influenzato dall'ampio ambito di protezione dei dati personali ma anche da altri interessi costituzionali. La raccolta discrezionale di dati personali va a minacciare la protezione di quel nucleo essenziale della persona umana, che, secondo la prospettiva comunitaria, risiede nella dignità dell'individuo. Non è, dunque, solo un problema di privacy ma anche di mosaico di diritti che contribuisce a creare un pilastro costituzionale nella società dell'informazione che pure metta al suo centro la valorizzazione del singolo e dei suoi diritti. Esempio paradigmatico è la rilevanza del principio della dignità umana nel costituzionalismo europeo, che può costituire, da un lato, un ostacolo al libero sviluppo delle nuove tecnologie nell'Unione ma, dall'altro, una salvaguardia dell'autonomia dei singoli contro le sfide derivanti dallo sviluppo incontrollato di nuove tecnologie di intelligenza artificiale. Secondo il Garante europeo della protezione dei dati, «*[The] respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics. [...] Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing*[25]». Ciò porta a ritenere che la protezione dei dati personali in Europa giocherebbe sempre più un ruolo critico contro i rischi di disumanizzazione nella società algoritmica.

Alla luce di queste considerazioni e ammesso che le tecnologie di intelligenza artificiale possano offrire nuove opportunità per il mercato interno, è necessario prendere in considerazione l'ampia protezione dei dati personali in Europa quando si affronta il potenziale percorso di queste tecnologie.

3. *GDPR e AI: le compatibilità tra i due sistemi*

La compatibilità tra l'architettura del GDPR e i sistemi di analisi di grandi quantità di dati non è da ricercarsi solamente nella problematicità della produzione di output non sempre trasparenti e prevedibili. Per valutare la compatibilità tra queste due discipline occorre rifarsi ai tracciati principi alla base del trattamento dei dati. Il GDPR, sin dalla prima enunciazione, rileva come cardinali i

[25] EDPS, Opinion 4/2015, *Towards a new digital ethics Data, dignity and technology*.

principi di liceità, correttezza e trasparenza del trattamento dei dati dell'interessato, introducendo un nuovo modello di trattamento dei dati personali basato sul *risk based approach* e il principio di *accountability*[26]. Secondo tale impianto, difatti, spetta al titolare del trattamento non solo assicurare il rispetto dei principi generali ma anche il provare di essersi conformato a quest'ultimi. Prendendo come riferimento il principio di trasparenza, il titolare del trattamento[27], è chiamato a mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente a quanto stabilito dal Regolamento[28]. Ne consegue che, considerata in particolare la complessità del fenomeno dei *big data*, il principio dell'*accountability* assume un rilievo fondamentale, in particolare ove la trasparenza non è sempre deducibile al cospetto di taluni procedimenti decisionali.

Come osservato, dunque, da Zarsky «*EU's strong position towards the protection of privacy rights is admirable, it is possible that the full implications the GDPR will have for the important big data practices, and their benefits, have not been fully and properly considered*[29]». Inoltre, alla luce delle considerazioni di talaltri commentatori[30], *big data* e AI sono degli strumenti che hanno modificato radicalmente le modalità di raccolta e perfezionamento degli output decisionali sicché è oggi possibile realizzare una "*datafication*" dell'intera esperienza umana[31].Tuttavia, se si guarda al testo del GDPR, manca totalmente un riferimento esplicito all'IA, sebbene il nesso tra sistemi automatizzati e raccolta dei dati sia non solo pacifico, ma anche scontato.

Tornando, ad esempio, al problema della trasparenza[32] che è una delle questioni maggiormente in discussione, i profili di maggior rischio emergono come

---

[26] Si veda in part. art. 5 (2) GDPR.

[27] Con riferimento al concetto della responsabilità, il GDPR adotta una definizione alquanto dinamica, di cui all'art. 5, comma 2.

[28] Sorreggono, in tal senso, altri due principi sanciti dal GDPR, ossia di quelli della privacy *by design* e *by default*, dei quali si dirà in seguito.

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

[30] Si veda V. MAYER, SCHÖNBERGER, K. CUKIER, *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*, London, 2013.

[31] L'intelligenza artificiale ha infatti bisogno di dati. Ed è su questo punto che spesso si creano delle incomprensioni: l'IA non utilizza solamente dati personali, ma anche dati non personali, ovverosia quei dati che non sono riconducibili a un'indentificata o identificabile persona fisica. Pertanto, vi è un forte collegamento logico tra le due discipline ma, per l'appunto, la materia della protezione dei dati personali non copre tutti gli aspetti relativi alle sfide poste da *big data* e IA.

[32] In tal senso, F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge MA, 2015; M. TURILLI, L. FLORIDI, *The ethics of information*

conseguenza della raccolta e del riutilizzo di dati personali attraverso l'impiego di algoritmi complessi i cui processi decisionali sono spesso opachi. Se, da un lato, attraverso queste tecnologie si può contare su una maggiore circolazione dei dati, dall'altro, resta, spesso, criptico come avviene il processo decisionale. Il dibattito sul nesso tra dati e IA si è, difatti, molto concentrato sul tema dell'*explainability* [33], vale a dire il diritto dell'individuo ad ottenere il disvelamento della *ratio* decisionale del sistema automatizzato a seguito di un'analisi effettuata sui propri dati (personali).

Invero, però, la menzionata necessità di assicurare un bilanciamento tra innovazione e protezione dei diritti, si trova al centro di un difficile meccanismo che prescinde dalla semplice conoscenza del processo decisionale. Piuttosto, ivi le categorie alla base della disciplina dei dati personali sono messe in crisi, sicché non è possibile spiegare preventivamente come i dati verranno trattatati in un modo che consenta al *data subject* di esprimere un consenso che risponda ai requisiti di correttezza e trasparenza. L'asimmetria informativa tra l'interessato e il *data controller* è di tutta evidenza, così come la crisi che il sistema di raccolta basato sul consenso, uno degli aspetti cruciali della disciplina del GDPR, vive con riferimento a sistemi quali IA e *big data*.

A dispetto di quanto è stato osservato da una pronuncia della Corte di Cassazione [34], nel contesto dei sistemi automatizzati, dato che vengono prodotti e lanciati sul mercato meccanismi sempre più in grado di influenzare l'individuo, la volontarietà della manifestazione del consenso, tra gli altri, è uno degli aspetti che mette maggiormente in crisi la connessione tra le esigenze dell'AI e la disciplina dei dati personali. Come evidenziato [35], vi è una tensione tra i principi tradizionali di protezione dei dati – quali, la limitazione delle finalità, la minimizzazione dei dati, il trattamento speciale dei "dati sensibili", la limitazione delle decisioni automatizzate [36] – e la possibilità di un pieno utilizzo dei sistemi di IA e di sfruttamento dei *big data*.

---

transparency, in *Ethics and Information Technology*, 2009, 11, 2, p. 105.

[33] Ad esempio, S. WACHTER, B. MITTLESTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7, p. 76 ss.

[34] Cass., sez. I, 25 maggio 2021, n. 14381, in cui, per specificare, la Corte si è pronunciata su un caso afferente alla previgente normativa in materia di privacy, come si è approfondito in O. POLLICINO, M. BASSINI G. DE GREGORIO, *Il Gdpr e la protezione dei dati nella società algoritmica: i nuovi sviluppi normativi e giuridici*, in *Agenda Digitale*, 10 settembre 2021.

[35] G. SARTOR, F. LAGIOIA, *Study: The impact of the General Data Protection Regulation on artificial intelligence*, in *Think tank Parlamento europeo*, 2020.

[36] In tal senso, la minimizzazione può richiedere, in alcuni contesti, di ridurre il collegamento tra individuo e dati disponibili, piuttosto che la quantità di tali dati, cioè può richiedere di ridurre,

Il GDPR ha cercato di fornire una soluzione a tali dispiegamenti massivi di raccolta dati attraverso diversi strumenti: uno su tutti, il c.d. '*right to explanation*', ossia il diritto di ricevere o accedere a informazioni significative sulle logiche, il significato e gli effetti previsti dei processi decisionali automatizzati [37]. Infine, l'art. 22 (1) introduce un meccanismo di contestazione, stabilendo il diritto a non essere soggetti a una decisione basata unicamente su un trattamento automatizzato, incluso il *profiling*.

Tuttavia, taluni aspetti della relazione tra dati personali e IA non sono stati del tutto assimilati per due ordini di motivi: l'IA possiede un ambito di applicazione ben più vasto, raccogliendo sia dati personali sia dati non personali; secondariamente, nei casi di utilizzo di sistemi automatizzati particolarmente complessi, come, ad esempio, il riconoscimento facciale, l'art. 22 (3) del GDPR non fornisce una protezione sufficiente, in quanto è ben frequente che il soggetto interessato non sia consapevole del tipo di trattamento cui è stato sottoposto [38]. Ovvero, ammesso che ne sia a conoscenza e ammesso che sia possibile una apertura trasparente della c.d. "scatola nera" [39], l'algoritmo può comunque essere di per sé discriminatorio [40]. Queste soluzioni, dunque, si sono rivelate non sufficientemente soddisfacenti e richiedono un'ulteriore e più attenta riflessione circa una regolazione che abbia ad oggetto l'IA e che, *a contrario*, non la tocchino solo per minima parte. L'aspetto che, sicuramente, preoccupa maggiormente è che le tecnologie algoritmiche non forniscono solo un "mezzo" per eseguire una decisione presa da un soggetto umano agente,

---

attraverso misure come la pseudonimizzazione, che agisce, per l'appunto, sulla facilità con cui i dati possono essere collegati agli individui.

[37] Come evidenziano numerosi studi, in particolare, S. WACHTER, B. MITTELSTADT L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, allo stato dell'arte l'art. 22 del GDPR non prevede un vero e proprio "right to explanation", essendo aspetto semplicemente richiamato dal considerando 71.

[38] Si fa riferimento, ad esempio, ai casi in cui tale tecnologia è utilizzata per scopi di pubblica sicurezza, situazione in cui la base giuridica del trattamento non è il consenso dell'individuo, ovvero al noto caso dell'app Clearview AI, azienda statunitense che è stata anche di recente oggetto di una pronuncia del Garante per la Privacy di Amburgo che l'ha sanzionata imponendo la cancellazione dei codici *hash*, ossia quei valori numerici che aveva associato alle foto dell'appellante, come anche riportato dalla organizzazione per i diritti digitali, NOYB in *How to Reclaim Your Face from Clearview AI*, *EDRi*, 10 febbraio 2021.

[39] Tema notoriamente affrontato da F. PASQUALE, *The Black Box Society. The Secret Algorithms that Control Money and Information*, cit.; ma anche, L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, vol. 16, 2017.

[40] A. SIMONCINI, S. SUWEIS, *Il Cambio di Paradigma nell'Intelligenza Artificiale e il suo impatto sul diritto costituzionale*, in *Riv. fil. dir.*, vol. 1, 2019.

ma, sempre più spesso, sono esse stesse ad assumere decisioni rilevanti per gli esseri umani e le loro libertà.

Un altro aspetto che emerge è la concreta possibilità di comprendere e disporre dei dati che il *data controller* potrebbe fornire in risposta alla richiesta del *data subject* di accedere ai propri dati. Poniamo il caso di una richiesta di accesso al proprio *device* di assistenza vocale. La risposta di Amazon consisterà in un elenco di date, orari e localizzazioni. Informazioni che per il *data subject* hanno un significato molto limitato, ma che molto dicono delle proprie abitudini, in termini di metadati, al *data controller*.

Il diritto, previsto dal GDPR all'art. 20, il c.d. *right to data portability,* si aggiunge al quadro di scetticismo che è stato prima evidenziato [41]. Il Regolamento, pur prevedendo in teoria tali possibilità, viene messo in crisi dall'implementazione pratica di talune sue disposizioni che hanno un impatto diretto su AI e *big data*. L'esercizio di tale diritto non è, difatti, semplice, non solo per un problema di carattere tecnico, ma soprattutto per una comprensione effettiva da parte dell'individuo di quell'elenco destrutturato dei propri *bits*, come taluni commentatori evidenziano [42]. Se, dunque, la possibilità di avere un accesso ai propri dati, comprenderli, e "trasportarli" da un *data controller* a un altro appaiono come delle soluzioni interessanti che possano mettere l'individuo al centro della catena di raccolta e analisi delle informazioni che lo riguardano, nella pratica incontrano ancora degli ostacoli tanto tecnici quanto normativi data la neutralità tecnologica del GDPR [43].

Pertanto, in un tale contesto, risultano ancora molteplici i nodi aperti nella relazione tra algoritmi, privacy e tutela dei dati personali. Come si è detto, le tensioni costituzionali che caratterizzano questi due ordini di sistemi si scontrano nettamente con i canoni di trasparenza e minimizzazione dei dati, i quali, a cascata, vanno ad inficiare l'esercizio di meccanismi di tutela da parte degli stessi individui.

Dunque, per via della vastità delle questioni giuridiche sollevate dall'avvento delle tecnologie algoritmiche e, soprattutto, a causa dell'ambito apparentemente limitato entro cui si muovono le tutele e le garanzie previste dalla disciplina in materia di protezione dati, enucleate dal GDPR, la Commissione europea ha pubblicato nel 2021 la proposta di Regolamento europeo sull'intelligenza arti-

---

[41] In tal senso, occorre citare le *Guidelines on the right to data portability*, del WP 29, adottate il 13 dicembre 2016.

[42] G. Noto La Diega, *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, 3, 2018.

[43] J. Wong, T. Henderson, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, in *International Data Privacy Law,* 2019, p. 9.

ficiale nel tentativo di fornire un sistema di *governance* che risponda a differenti esigenze: una su tutte, la costruzione del futuro digitale dell'Unione che possa rendere quest'ultima capofila nel delineare i tratti di un'interazione tra uomo e macchina rispettosa dei diritti fondamentali. Alle differenze e similitudini tra il GDPR e la recente proposta si dedicherà l'ultimo paragrafo, nell'ottica di andare ad individuare le tracce di quel bilanciamento funzionale tra interessi da preservare e sviluppo tecno-economico del mercato unico [44].

4. *GDPR e Regolamento AI*

Per evitare frizioni tra il sistema normativo e quello tecnologico, allo scopo di limitare, dunque, le incertezze anche degli operatori del mercato e favorire, di contro, l'innovazione e gli investimenti in questo campo, è necessario operare un design architettonico di regole che possano essere recepite dallo stesso sistema algoritmico sin dalla sua progettazione. Per tale ragione, l'Unione ha trasposto i propri intenti [45] in un Regolamento che ha come obiettivo il fornire un quadro armonizzato e dedicato all'intelligenza artificiale, fornendo persino una definizione di IA quale «*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato* [46] *alla proposta, per una determinata serie di obiettivi definiti dall'uomo di generare output quali contenuti, previsioni, raccomandazioni o decisioni* [47]».

Le prime similitudini con il GDPR sono state individuate nella stessa scelta dello strumento normativo, il Regolamento: una decisione che lascia trasparire l'intenzione di creare un quadro di *governance* non solo orientato al futuro dei

[44] Sul punto, anche il considerando n. 5 della Proposta, dove si legge che «*To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those rules, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence […]*».

[45] Nel febbraio 2020 la Commissione aveva già pubblicato il *White Paper on AI:* un testo che *in nuce* contiene aspetti che sono stati ripresi e approfonditi successivamente dalla proposta, ma che, per l'appunto, ha avuto un raggio di influenza e ricezione assai limitato e sicuramente non cogente trattandosi di uno strumento di *soft law.* Si veda Commissione europea, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, Bruxelles, 2020.

[46] Il riferimento è all'allegato I alla proposta, *Annex I to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, Bruxelles, 2021.

[47] Si veda l'art. 3, par. 1, lett. a), della proposta che introduce la definizione in esame di IA.

diritti e del mercato, ma, soprattutto, armonizzato in tutta Europa. Tale scelta normativa influenza di per sé ben poco la regolazione dell'IA, se non si provvede a costruire un sistema coordinato di governo delle diverse tipologie di fonti e applicazioni dell'IA e che la possa rendere compatibile con il sistema costituzionale europeo, la tutela dei diritti fondamentali, e, in particolare, la *rule of law*[48].

L'impianto progettato dalla Commissione parte, dunque, dalla necessità di delineare una nuova fiducia a due direzioni che riguardi al contempo persone fisiche e giuridiche[49]. Tali intenzioni sono contenute nell'approccio orientato al rischio: questo è per l'appunto l'elemento che maggiormente avvicina la disciplina di cui al GDPR e quella che dovrebbe applicarsi all'AI. La Commissione, difatti, ha tentato di replicare per l'intelligenza artificiale quel sistema già adottato con riferimento ai dati personali, ma con delle dovute differenze. La proposta enuclea quattro livelli di rischio ciascuno dei quali rimanda a determinati sistemi IA e alle relative applicazioni[50]. La *ratio* di questa divisione prevede una organizzazione circa gli usi consentiti e proibiti dell'intelligenza artificiale attraverso la creazione di una *climax* di rischio e la delineazione di un assetto di regole di *compliance* che sembra essere orientato ai valori europei, tra cui la tutela dei diritti fondamentali, come, del resto, suggerito dal considerando 15[51]. A tal proposito, seppur non estensivamente, non è un caso che la proposta menzioni l'impatto dei sistemi di IA sui diritti fondamentali di cui alla Carta fondamentale dei Diritti dell'Unione europea[52]. Tra questi: il diritto alla dignità uma-

---

[48] In questa direzione, anche il commento di A. SIMONCINI, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, *BioLaw Journal - Rivista di BioDiritto*, vol. 2, 2021.

[49] Come ha riconosciuto, difatti, Margarethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age and Competition, all'alba della pubblicazione del testo: «sull'IA, la fiducia è un *must*, non un *nice-to-have*. Con queste regole di riferimento, l'Unione Europa sta guidando lo sviluppo di nuove norme globali per assicurarsi che ci si possa fidare dell'IA», 'Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence', European Commission Press, 21 aprile 2021, «https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_1866».

[50] Il riferimento è ai Titoli II e III della Proposta. Un focus sulla divisione dei quattro livelli di rischio e l'approccio seguito dalla Commissione è stato fatto in O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *L'intelligenza artificiale made in Ue è davvero "umano-centrica"? I conflitti della proposta*, *Agenda Digitale,* 22 luglio 2021.

[51] Nel considerando 15 si dice, difatti, che «*aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child*».

[52] Carta dei Diritti fondamentali dell'Unione europea (2000/C 364/01), 'Carta di Nizza'.

na (art. 1), il rispetto della vita privata e la protezione dei dati personali (artt. 7 e 8), il principio di non-discriminazione (art. 21) e la parità tra donne e uomini (art. 23).

Anche dalle dichiarazioni istituzionali, emerge, dunque, l'interesse a creare una strada per quell'umanesimo digitale che intende porre al centro delle scelte di *governance* che hanno ad oggetto le tecnologie e, in particolar modo, i sistemi automatizzati, l'uomo. Accanto, dunque, all'approccio orientato al rischio, dovrebbe scorgersene un altro: quello "umano-centrico". Non sempre alle intenzioni corrisponde una sostanziale realizzazione e, purtroppo, dalla *littera legis* manca una vera e propria valorizzazione di questa scelta, nonostante le raccomandazioni dell'High Level Expert Group on AI[53]. Ad esempio, la parola "umano" si rintraccia, difatti, solamente una volta in tutto il testo. Tale assenza non solo rileva da un punto di vista semantico, ma questa mancata valorizzazione degli intenti di cui al considerando 15 testimonia il fatto che ancora manca una chiara messa a fuoco dell'impianto normativo. Il problema di fondo sembra essere, in altre parole, che la Commissione intende sposare il sistema del rischio per frenare l'espansione incontrollata del settore, senza però sforzarsi di rendere concreta la spinta costituzionalistica che viene promessa dal *framework* in cui si inserisce la proposta[54].

L'elenco di rischi e pericoli dell'AI resta appunto un elenco e non si spinge oltre, verso quella dinamicità e versatilità cui, invece, si è prestato sin da subito il GDPR. Come è emerso anche dalla *joint opinion* pubblicata dall'EDPB e dall'EDPS[55], urge che la Commissione adotti con maggiore chiarezza il concetto di "rischio per i diritti fondamentali" che fa da eco alla normativa sulla protezione dei dati personali, di modo tale da elevare le questioni tecniche a un rango costituzionale di bilanciamento tra interessi e diritti contrapposti.

All'interno poi delle applicazioni '*prohibited*' dell'AI si prova un senso di smarrimento nel leggere le numerose e lasche eccezioni previste dall'art. 5 ove la proposta reca un'ampia lista di casi in cui tali usi proibiti, vengono in realtà consentiti. Questa poca chiarezza è di tutta evidenza quando si guarda al problema delle tecnologie biometriche sicché la Commissione ha previsto come

---

[53] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[54] Si veda anche l'*explanatory memorandum* ove si dice che: «*the list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights*», p. 12.

[55] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021, https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf.

lecite le effettuazioni di identificazioni biometriche a distanza "in tempo reale", in spazi accessibili al pubblico [56] per ragioni di *law enforcement:* ossia, la ricerca mirata di un bambino scomparso; la prevenzione di una minaccia specifica, sostanziale e imminente alla vita o all'incolumità fisica delle persone fisiche o di un attacco terroristico; la localizzazione, l'identificazione o il perseguimento di un autore o di un sospetto di un reato grave. Tuttavia, queste linee di demarcazione non sembrano riprodurre lo schema di *accountability* del GDPR, atteggiandosi piuttosto come un soffitto di vetro, anziché costituire un sentiero capace di direzionare gli attori del mercato [57].

Il legame tra i due corpi di norme è, inoltre, evidente dal considerando 1 dove viene detto che lo scopo del Regolamento è di «*migliorare il funzionamento del mercato interno stabilendo un quadro giuridico uniforme, in particolare per lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale, conformemente ai valori dell'Unione*». Se si guarda, tuttavia, al testo della proposta europea sull'intelligenza artificiale, manca del tutto questo dinamismo, sostituito da un forte accentramento nelle mani della Commissione. Nella proposta manca il coinvolgimento delle voci del mercato, scelta che, probabilmente, risponde all'esigenza di non frammentare e settorializzare l'IA. Il rischio di converso è la riproduzione di un controllo invasivo e di un approccio verticale da parte della Commissione. Come è elevato il rischio che si verifichi uno scollamento sia di oggetto sia di tempistiche tra quelle che sono le esigenze di mercato e le abilità di manovra della Commissione, con la conseguenza di un ricorso alla *soft law*.

La scelta dell'approccio *top-down* tende ad elevare le soglie di rischio e che queste si traducano in una rigidità che non lasci margini di valutazione al *provider* su come adoperarsi nella pratica. Ciò che (almeno per ora) manca nella proposta è quella capacità del Regolamento di porre limiti ma aprire all'adattabilità: l'approccio *"by-design"* e *"by-default"* contenuto nel GDPR 58. Un vuoto che è stato notato anche nella richiamata opinione dell'EDPB e EDPS, dove si propone di modificare la procedura di valutazione della conformità di cui all'art. 43 della proposta, nel senso che una valutazione di conformità *ex ante* da parte di terzi deve essere generalmente effettuata per l'intelligenza artificiale ad alto rischio, anche se una valutazione di conformità da parte di terzi per il trattamento ad alto rischio dei dati personali non è un requisito esplicito del GDPR.

---

[56] Della nozione si dà una ricognizione al considerando 9 che pure esclude «*online spaces are not covered either, as they are not physical spaces*». Una scelta che lascia perplessi alla luce di quanto accaduto con la famigerata Clearview AI.

[57] Si veda, G. FINOCCHIARO, O. POLLICINO, *IA, dal GDPR maggiore garanzia dei diritti*, in *Italia Oggi*, 16 giugno 2021.

[58] Si veda S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, vol. 24, 2017.

Accanto, però, alle perplessità enucleate che hanno per lo più ad oggetto i mancati raccordi tra GDPR e proposta e che sembrano suggerire spazi di manovra per costruire una *compliance* dell'AI meno inscatolata ma più dinamica, un punto su tutti preoccupa, soprattutto alla luce di quelle che avrebbero dovuto essere le premesse del *corpus* normativo: la mancanza di meccanismi procedurali. Se lo scopo voleva essere di mettere al centro l'uomo, sembrano però mancare strumenti che possano consentire agli individui, vittime di decisioni automatizzate discriminatorie, o comunque errate, di ottenere un rimedio diretto al pregiudizio subito.

Non è sufficiente, difatti, come si è spesso rimarcato, fare riferimento alla disciplina dell'art. 22 del GDPR[59] che, seppur rappresenti il cuore della materia della protezione dei dati, non copre invece i vastissimi ambiti di applicazione dell'AI. Inoltre, l'art. 22, come l'annosa vicenda *Schrems*[60] ha messo in evidenza (*mutatis mutandis*), non rappresenta una garanzia assoluta, soprattutto quando tali trattamenti automatizzati sono svolti da operatori transatlantici. Una tale circostanza provoca tre conseguenze sostanziali: in primo luogo, si rischia di imporre degli obblighi eccessivi agli attori privati; in secondo luogo, senza una bussola, gli operatori – spesso provenienti da sistemi giuridici differenti in cui la privacy ha un valore diverso rispetto all'Europa – sono chiamati in prima persona ad effettuare un bilanciamento tra interessi, nel solco di quel che si era già accennato in merito alla privatizzazione dell'*enforcement* dei diritti fondamentali[61]; in terzo luogo e in maniera più vistosa, gli individui vengono lasciati senza una tutela procedurale sufficiente. Un'assenza che stupisce ancor di più se si leggono altre recenti iniziative normative dell'Unione europea che riguardano il digitale e che, invece, contengono dei meccanismi di *redress*, come nel caso della Direttiva *Omnibus*, lato persone fisiche, quanto nel c.d. Regolamento P2B, lato persone giuridiche[62]. In un contesto come quello digitale, ove gli attori privati sono già investiti di alcune forme di potere che non sono più di natura meramente economica[63],

---

[59] Non sembra, tuttavia, sufficiente il richiamo comparatistico ai rimedi offerti dal GDPR e ai diritti dell'interessato di richiedere un intervento in caso di contestazione delle decisioni automatizzate o trattamento avvenuto in violazione di legge.

[60] La "*diabolical persistence*" di cui O. POLLICINO, *Diabolical Persistence. Thoughts on the Schrems II Decision*, in *Verfassungsblog.de*, 25 luglio 2020.

[61] Nel merito M. BASSINI, *Fundamental Rights and Private Enforcement in the Digital Age*, in *European Law Journal*, vol. 25(2), 2019, 182-197.

[62] Rispettivamente la Direttiva UE 2019/161 (c.d. *Omnibus*) e il Regolamento UE 2019/1150 ("Regolamento P2B").

[63] Basti pensare al caso della moderazione dei contenuti, in cui le piattaforme prendano decisioni autonome nel disegnare le regole della moderazione, facendo rispettare queste norme che hanno come paradigma i propri interessi commerciali predicati dai loro "termini e condizioni".

occorre vigilare con attenzione sul deferimento di un'ampia gamma di attività decisionali agli algoritmi.

Il legame tra il GDPR e la nuova proposta di Regolamento europeo comunicano molto circa le tensioni tra mercato digitale e protezione dei diritti fondamentali, o, più in generale, tra mercato e democrazia. Come si è visto, i concetti sostanziali sono due. Il primo tema è la *compliance*, basata su un sistema di regole armonizzate, di monitoraggio e "buon governo". Di conseguenza, il secondo è il principio della fiducia. Da un lato, gli sviluppatori di IA devono poter contare su norme chiare e comprensibili per svolgere le loro attività all'interno del mercato dell'UE, rispettando un corpo di regole unificato per tutti gli Stati membri. Dall'altro lato, la proposta mira a tutelare i valori europei come limite allo sviluppo e utilizzo discrezionali delle tecnologie di IA.

Nonostante il terreno della *compliance* sia ancora molto forte rispetto a quello valoriale, e a dispetto delle dichiarazioni programmatiche che erano state fatte, la proposta sembra ancora non proporre un *legal design* che possa rappresentare un'alternativa, non solo per l'Europa, all'approccio da un lato autoritario, dall'altro liberistico alla tecnologia che guida lo scontro tra diverse espressioni della sovranità digitale.

5. *Conclusioni*

In questo *swing* tra mercato e democrazia, l'Unione europea sta tentando di conquistare un posto da capofila nel design delle architetture normative del futuro: ossia, nella costruzione di una cornice normativa che sia, da un lato, in grado di sostenere gli obbiettivi del mercato unico e, dall'altro, la tutela di valori europei, quali il principio della *rule of law*, la protezione dei diritti fondamentali, ma, soprattutto, la valorizzazione della dignità umana.

L'Europa sembra aver compiuto alcuni passi al fine di trovare un bilanciamento tra innovazione e tutela dei diritti. Favorendo, dunque, lo sviluppo di un tale modello, si potrebbe fondare una catena preziosa, capace di spingere verso un mercato del digitale che ricomprenda la scala valoriale dell'UE. In secondo luogo, come già si è notato con l'entrata in vigore del GDPR, in materia tecnologica, e non solo, l'Unione europea è un importante attore nel delicato equilibrio

---

Caso eclatante è la nota vicenda che sta riguardando Donald Trump e la "Supreme Court" di Facebook, l'Oversight Board. Per un'analisi sulle tematiche ivi accennate, si rimanda a K. KLONICK, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, in *Yale Law Journal*, vol. 129, 2020, pp. 2418-2499.

di potere [64] in grado di definire delle regole che hanno un impatto tangibile sulla vita quotidiana dei cittadini, proponendo un modello, dunque, del quale la privacy rappresenta il Primo Emendamento [65] e che ha la capacità di rendersi influente e cogente nella catena produttiva dei dati rendendo l'*humus* costituzionale europeo una parte fondamentale di quest'ultima.

La tutela costituzionale della privacy europea è, difatti, in grado di andare oltre questa sistematica e di diffondere un vero e proprio «*habeas corpus digitale*» [66] dei diritti sostanziali e procedurali, derivato dall'obbligo positivo degli Stati di garantire la protezione dei diritti umani. Una geometria vitruviana necessaria se si vuol costruire una quarta rivoluzione industriale che ponga l'uomo come misura di tutte le cose, pur favorendo, e non imbrigliando, il mercato di tali sistemi tecnologici, che, per primi, potranno giovarsi di un quadro normativo chiaro a definizione della governance dell'intelligenza artificiale. Una sfida che non ha solo un impatto sull'esercizio dei diritti *tout-court*, ma rappresenta, altresì, un'occasione per rendere l'Unione leader nel diffondere il proprio modello su scala globale.

---

[64] E. CAU, *La Yalta digitale*, in *Il Foglio Quotidiano,* 29 agosto 2020.

[65] B. PETKOVA, *Privacy as Europe's First Amendment,* in *European Law Journal*, vol. 25(2), 2019, 140-154.

[66] Di questo parlava Rodotà già nel 2001: «*proprio da qui nascono le nuove esigenze di tutela. Si invoca da tempo un habeas data, indispensabile sviluppo di quell'habeas corpus dal quale si è storicamente sviluppata la libertà personale. Questa è la prospettiva nella quale si colloca oggi la privacy, confermando quel che da anni diciamo e pratichiamo: la tutela dei dati è un diritto fondamentale della persona, una componente essenziale della nuova cittadinanza. Così ci siamo mossi anche prima che l'articolo 8 della Carta dei Diritti fondamentali dell'Unione europea attribuisse autonoma rilevanza alla tutela dei dati personali. Stiamo interpretando la legge appunto come un habeas data, non solo per respingere invasioni illegittime o indesiderate, ma anche per evitare di essere "costruiti" dagli altri*», discorso del Presidente del Garante per la protezione dei dati personali, 2001.

PARTE IV
DATI PERSONALI E CONTRATTO

IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI NEL DIALOGO TRA LE CORTI

di *Tommaso Polvani*

1. *La commercializzazione dei dati personali: una premessa*

Nella realtà dei traffici, la circolazione dei dati e delle informazioni relative alle persone fisiche ha acquisito un valore sempre crescente. I dati vengono sfruttati per comprendere ed esplicitare il sistema dei bisogni della clientela, così da poterlo ricostruire secondo logiche di marketing e di offerta più efficaci [1]. È oggi diffusa l'idea secondo cui all'economia tradizionale si sia affiancata

[1] V. CUFFARO, *Il diritto europeo sul trattamento dei dati*, in *Contr. impr*., 2018, 3, p. 1117; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ*., 3, 2020, pp. 645-647 e, ancora, a p. 659; C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in *Giur. it.*, 2021, p. 323: «*Il rilievo da cui partire è che i dati personali sono ormai considerati una riserva economica a tutti gli effetti*». A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 9: «*La progressiva crescita dei contratti che hanno ad oggetto la fornitura di beni o servizi basati sullo scambio e l'elaborazione di dati, ed in particolare di dati personali, ha fatto sì che i dati stessi siano in misura progressivamente crescente divenuti oggetto della prestazione*». Sul tema si vedano i rilievi di R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in N. ZORZI GALGANO, *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p.137 ss.; G. DI LORENZO, R. MESSINETTI, *Ordine giuridico ed evoluzione tecnologica, a proposito del recente libro su "i dati personali nel diritto europeo"*, in *Nomos*, 2020, S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano,

la c.d. *data driven economy*, un'economia, cioè, fondata sui dati e sulla loro attitudine ad incrementare le opportunità di business.

All'emersione di questa nuova economia si è accompagnata la creazione di operazioni contrattuali in cui un soggetto professionale fornisce servizi digitali senza richiedere in cambio un corrispettivo monetario, così da farli apparire gratuiti. Tuttavia, l'elemento caratterizzante queste fattispecie è dato dal fatto che il loro perfezionamento comporta «*una messa a disposizione da parte del consumatore di alcuni suoi dati personali, a vantaggio e per l'utilizzo a diversi fini da parte dell'operatore economico*»[2].

Da subito gli studiosi si sono interrogati sulla possibilità di qualificare i dati personali come corrispettivo, diverso dal denaro, per la fornitura di contenuti o servizi digitali[3].

Occorre allora chiarire se – e soprattutto a quali condizioni – sia ammesso o meno un mercato dei dati.

Si è evidenziato che la delicatezza di queste operazioni è costituita anche dal frequente difetto di informazione del consumatore[4] e dalla man-

---

2018; F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008; R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 2, p. 760 ss.; C. SOLINAS, *Circolazione dei dati personali, contratti di consumo e pratiche commerciali scorrette*, in *Giur. it.*, 2021, p. 320 ss.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.; A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Protezione e libera circolazione dei dati personali nel diritto europeo. Il Regolamento generale 2016/679 (e le Direttiva 2016/680 e 2016/681 sul trattamento dei dati in ambito penalistico)*, Torino, 2019, p. 1381 ss.; ID., *La circolazione dei dati personali tra privacy e contratto,* Napoli, 2017; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., p. 642 ss.

[2] 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.*, n. 3, 2019, p. 504.

[3] In senso analogo, V. RICCIUTO, C. SOLINAS, *Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in *giustiziacivile.com*, n. 5/2021, che si interrogano sulla «*possibilità di considerare i dati personali quale elemento di un'operazione economica e, dunque, in definitiva, di concepire la scelta del soggetto di consentire il trattamento dei propri dati personali anche come esercizio di libertà economica*».

[4] A. DE FRANCESCHI, *Vendita di beni con elementi digitali*, Napoli, 2020, p. 15: «*Non sempre gli utenti sono pienamente consapevoli del valore economico che assume il mettere a disposizione i dati*»; S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Riv. dir. media*, 2019, 3, pp. 131-147, p. 133; C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., p. 332. C. ANGIOLINI, *A proposito del caso Orange Romania deciso dalla corte di giustizia dell'Ue: il rapporto fra contratto e consenso al trattamento dei dati personali*, in *Nuove leggi civ. comm.*, 2021, 1, p. 253; I. GAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi com-*

canza di un valido consenso alla cessione del dato medesimo [5].

portamentali, in *Oss. dir. civ. comm.*, n. 1, 2018, p. 90; L. GATT, R. MONTANARI, I. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, n. 2, 2017, p. 363 ss.; M.C., GAETA, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi*, in *Dir. inf.*, I, 2018, p. 171 ss. Segnala come il tema della trasparenza sia la prospettiva emersa nell'ordinamento statunitense, M. GRAZIADEI, *Collusione transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. DI CIOMMO, O. TROIANO (a cura di), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, p. 367. Anche il Garante europeo per la protezione dei dati personali ha rilevato che le informazioni sulla cui base l'utente dà il consenso sono spesso vaghe e non consentono di comprendere realmente quale sarà l'uso dei dati fatto dal titolare del trattamento, GEPD, *Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy*, marzo 2014, p. 34.

[5] A conferma dell'importanza di una corretta informazione del consumatore, occorre menzionare l'obbligo di chiarezza previsto dall'art. 7, par. 2, GDPR, ai sensi del quale, nel caso in cui il consenso sia prestato all'interno di una dichiarazione scritta che riguardi anche altre questioni, la richiesta di consenso dovrà essere formulata «*in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*». Sul tema del consenso alla cessione dei dati personali cfr. S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583 ss.; ID., *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.* 1984, p. 732 ss.; G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, p. 324; A. SCALISI, *Il diritto alla riservatezza*, Milano, 2002, p. 1 ss.; S. PATTI, *Il consenso al trattamento dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583 ss.; G. OPPO, *Sul consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH, (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, pp. 123 ss.; V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, p. 204 ss.; G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 271 ss.; S. SICA, *Il consenso al trattamento dei dati personali*, in *Riv. dir. civ.*, 2001, II, pp. 621 ss.; ID., *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, p. 299 ss.; S. THOBANI, *Il consenso al trattamento dei dati personali come condizione per fruizione dei servizi online*, in C. PERLINGIERI, L. RUGGERI (a cura di), *Atti del convegno «Internet e diritto civile»*, Napoli, 2014, p. 459 ss.; ID., *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna**,** 2016, ID., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, 2, p. 513 ss.; V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. informazione e informatica*, 1993, p. 545 ss.; N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p. 137 ss.; S. PATTI, *Commento. Art. 23*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commento al D.Lgs. 30 giugno 2003, n. 196*, Padova, 1999, I, p. 553; S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, p. 993 ss.; V. CUFFARO, *A proposito del ruolo del consenso*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, cit., p. 117 ss.; V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 411 ss.; C. ANGIOLINI, *A proposito del caso orange romania deciso dalla Corte di Giustizia dell'Ue: il rapporto fra contratto e consenso al trattamento dei dati personali*, cit., p. 247 ss.

Nel presente scritto, quindi, dopo una ricostruzione storica degli orientamenti relativi alla disciplina posta a tutela dei dati personali, si esamineranno le principali disposizioni normative gravitanti attorno al tema della loro commercializzazione, anche alla luce degli indirizzi forniti dalla giurisprudenza. L'analisi non potrà prescindere da una doppia prospettiva: sarà necessario tenere presente la duplice natura delle informazioni personali, considerate ora come bene economico, ora come oggetto di un diritto fondamentale. Si tratta di un'ambivalenza presente nella stessa normativa in materia di protezione di dati personali, posta a presidio sia della libera circolazione dei dati, sia della tutela degli interessati.

Se sul tema della commercializzazione le recenti pronunce della giurisprudenza, sia nazionale che europea, hanno finalmente indicato la strada da seguire, sulla rilevanza da attribuire al consenso permane ancora una qualche incertezza. Mentre alcuni ritengono che l'*an* e il *quantum* del trattamento debbano dipendere soltanto dal consenso del singolo interessato [6], altri oppongono l'inidoneità di tale elemento a regolare la materia, sia per ragioni di carente consapevolezza del soggetto, sia per il carattere pubblico degli interessi tutelati, non suscettibili di una tutela meramente individuale [7].

2. *Commercializzazione di dati personali, corretta informazione e consenso*

Giova avviare l'analisi dal dato giurisprudenziale. Come si vedrà meglio nel prosieguo, il Consiglio di Stato, con la pronuncia del 29 marzo 2021, n. 2631 ha preso posizione sull'annoso dibattito relativo alla questione della patrimonializzazione e commercializzazione dei dati personali, disattendendo l'impostazione classica, secondo cui questo settore dell'ordinamento dovrebbe essere improntato unicamente a logiche di garanzia giuridica della sfera personale dell'indi-

[6] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 433-435; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 49.

[7] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente,* cit., p. 147; G. VETTORI, *Privacy: un primo bilancio*, in *Riv. dir. priv.*, 1998, n. 4, p. 675; R. CATERINA, *Cyberspazio, social network e teoria generale del contratto*, in *Aida*, 1, 2011, p. 96; S. SICA, G. GIANNONE CODIGLIONE, *I social network sites e il "labirinto" della responsabilità*, in *Giur. mer.*, 2012, p. 2714; S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in A. MANTELERO, D. POLETTI, *Regolare la tecnologia: il reg. UE 2016/679*, Pisa, 2018, p. 163; J.P. ALBRECHT, *Das neue EU-Datenschutzrecht- von der Richtlinie zur Verordnung*, in *Computer und Recht*, 2016, pp. 88, 91.

viduo e di tutela della libertà nell'autodeterminazione della persona[8]. Fin dal recepimento della Direttiva 46/1995, invero, malgrado alcune pionieristiche letture di segno opposto[9], la prospettiva teorica maggioritaria è consistita in una c.d. tutela *statica* del dato personale, la cui protezione avrebbe «dovuto trovare la sua esclusiva collocazione nell'ambito della tutela dei diritti della personalità[10], con la loro indisponibilità, imprescrittibilità ed assolutezza[11]».

---

[8] Ricostruiscono il dibattito, tra gli altri, V. CUFFARO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf*. 2018, p. 689 ss.; F. D. BUSNELLI, *Il trattamento dei dati personali nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. CUFFARO, V: RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, cit.; C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali,* in V. CUFFARO, V: RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, cit.; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv*., 1997, p. 583.

[9] S. RODOTÀ, *Conclusioni*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH, (a cura di), *Trattamento dei dati e tutela della persona*, cit., p. 308, il quale, a proposito della legge n. 675/1996 di recepimento della Direttiva, poneva interrogativi che hanno precorso i tempi e che risultano essere tuttora attuali e meritevoli di riflessione: «*Io credo che noi dobbiamo lavorare molto nella dimensione negoziale, non ho nessun dubbio. Negoziale vuol dire per esempio: il consenso può essere oneroso, può essere condizionato, può essere a termine? Io come risposta generale direi di sì, e perché no? Posso negoziare, e badate alcune forme improprie di negoziazione già ci sono*» […]. *Il problema capitale è quello dell'asservimento definitivo e naturalmente la legge offre molti spunti per dire che questo asservimento non è accettato. Il controllo non viene perduto, i motivi legittimi per i quali si può impedire la comunicazione di dati pur legittimamente raccolti, pertinenti o assentiti in tutto o in parte, dimostrano quindi che c'è una scelta dell'interessato che definisce l'area della protezione*».

[10] Sul tema dei diritti della personalità cfr. P. RESCIGNO, *Protezione dei dati e diritti della personalità*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona*, cit., p. 277; A. DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, diretto da Cicu-Messineo, 1959; P. VERCELLONE, *Diritti della personalità (voce), Novissimo Dig*., 1965, p. 1084; G. GIAMPICCOLO, *La tutela giuridica della persona umana e il diritto alla riservatezza*, in *Riv. dir. proc. civ*., 1958, p. 458 ss.; P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972; A. CATAUDELLA, *Riservatezza - diritto della* (voce), in *Enc. giur*., XXVII, 1989; P. RESCIGNO, *Personalità - diritto della* (voce), in *Enc. dir*., Milano, 1983, p. 355 ss.; D. MESSINETTI, *Personalità – diritti della* (voce), in *Enc. dir*., Milano, 1983, p. 355 ss.; G. B. FERRI, *Persona e formalismo giuridico: saggi di diritto civile*, Rimini, 1985; F. D. BUSNELLI, *Per una rilettura del diritto delle persone di cinquant'anni fa*, in AA.VV., *Scritti in onore di L. Mengoni*, I, Milano, 1995, p. 91 ss.; G. MARINI, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ*., 2006, p. 359 ss.; G. ALPA, M. BESSONE, L. BONESCHI, *Il diritto all'identità personale*, Padova, 1981. F. MACIOCE, *Tutela della persona e identità personale*, Padova, 1984; A. SCALISI, *Il valore della persona nel sistema e i nuovi diritti della personalità*, Milano, 1990, G. ALPA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983.

[11] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., p. 642.

Del resto, autorevoli studiosi avevano letto già nella Direttiva del 1995 un'apertura alla ricostruzione patrimonialistica del fenomeno [12]. Secondo questo orientamento a lungo minoritario, la disciplina comunitaria – tradita dalla legge di recepimento n. 675/1996, che rimaneva «*ancorata ad una (sola) lettura assolutistica della persona*» – prospettava, invece, l'ammissibilità di un trattamento fondato sul principio del *consenso,* da collocare nel contesto di una «*vicenda negoziale, con le conseguenti rispettive tutele* [13]».

È oggi evidente che il fenomeno del trattamento dei dati non possa essere ricostruito soltanto secondo la primigenia prospettiva del *right to be let alone* [14] e che anzi esso si sia sviluppato lungo un articolato percorso fino a giungere alla formulazione della privacy come «*diritto a mantenere il controllo sulle proprie informazioni* [15]». Peraltro, occorre precisare che il consenso di cui si

---

[12] S. RODOTÀ, *Conclusioni*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, (a cura di), *Trattamento dei dati e tutela della persona*, Milano 1998, p. 308.

[13] V. RICCIUTO, *La patrimonializzazione dei dati personali, contratto e mercato nella ricostruzione del fenomeno*, in *Dir. informazione e informatica*, 2018, n. 4-5, p. 694: «*la normativa italiana di recepimento (l. 675/1996) disattenderà quella prospettiva, rimanendo, in buona sostanza, ancorata ad una (sola) lettura assolutistica della persona, priva di riferimenti – contenuti invece nella Direttiva 46/95/ CEE – ad un fenomeno patrimoniale, di relatività delle situazioni giuridiche coinvolte, di rapporti giuridici riconducibili al diritto delle obbligazioni, e dunque di mercato nella sua accezione propria». […] «nel fenomeno si prospettavano, anche sulla base della disciplina comunitaria, due diverse situazioni soggettive, in termini di assolutezza e relatività, sul presupposto che i dati fossero trattati senza che il soggetto interessato partecipasse a quella operazione economica – e qui il richiamo è al principio del consenso al trattamento –, ovvero consapevolmente parte di una vicenda negoziale, con le conseguenti, rispettive tutele*».

[14] Questa nota formulazione risale al famoso saggio di S. D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, 4, 5, pp. 193-220.

[15] Sul tema, ancora attualissimi, i contributi di S. RODOTÀ, in particolare, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, pp. 588-589; ID., *Privacy e costruzione della sfera privata*, in *Pol. dir.*, 1991, n. 4, pp. 521-546; ID., *Tecnologie e diritti*, Bologna, 1995; G. VETTORI, *Privacy: un primo bilancio*, in *Riv. dir. priv.*, 1998, n. 4, p. 675, che parla di una «*necessità teleologica dei diritti. La possibilità di conoscere l'inizio di un trattamento, di opporsi, di chiedere la cancellazione, la modifica o l'integrazione, è un efficiente mezzo di tutela specifica che può impedire la violazione o la continuazione dell'attività lesiva*»; R. PARDOLESI*, Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in ID. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, p. 1 ss.; S. NIGER, *Le nuove dimensioni della privacy: dalla riservatezza alla protezione dei dati personali*, Padova, 2006; G. MARINI, *Diritto alla privacy*, *Commentario del codice civile*, diretto da E. Gabrielli, Torino, 2013, p. 209 ss. G. ALPA, *Privacy*, in G. ALPA (a cura di), *I precedenti. La formazione giurisprudenziale del diritto civile*, Torino, 2000, p. 259 ss.; G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, I, p. 115; E. ONDEI, *Esiste un diritto alla riservatezza*, in *Riv. dir. civ.*, 1955, p. 166; A. MUSATTI, *Appunti sul diritto alla riservatezza*, in *Foro it.*, 1954, IV, p. 184; ID., *Ancora sul diritto alla riservatezza*, in *Foro it.*, 1957, I, p. 1689 ss.; A. MANTELERO, *Il diritto alla riservatezza nella l. n. 675 del 1996: il nuovo che viene dal passato*, in *Riv. trim. dir. proc. civ.*, fasc. 3, 2000, p. 973.

discute, in realtà, non è relativo alla cessione, quanto piuttosto al trattamento dei dati per scopi diversi ed ulteriori rispetto a quelli necessari all'esecuzione del contratto [16]: chi riceve i dati personali potrà trarne profitto solo in quanto possa legittimamente disporne. La mera cessione non è particolarmente utile per colui che li riceve, in quanto una loro conseguente elaborazione da parte del destinatario sarebbe illecita in mancanza di un consenso al trattamento espresso in conformità con quanto stabilito dall'art. 6 del GDPR [17].

Nell'affrontare la questione tratteggiata, occorre tener presente che la disciplina europea – fedele alla sua matrice mercantile [18] – è volta a favorire la

---

[16] C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., 2021, p. 328: che evidenzia come la questione della corrispettività «*non opera nell'ipotesi in cui i dati personali forniti dal consumatore siano trattati esclusivamente ai fini di consentire la materiale esecuzione di una fornitura di contenuti o servizi digitali oppure per consentire l'assolvimento degli obblighi di legge gravanti sull'operatore e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti. È evidente, in tali casi, che la fornitura del dato non è, economicamente considerata, un'alternativa al denaro. Essa, infatti, in tali casi non si spiega quale "sacrificio" accettato dal consumatore al fine di accedere al servizio o ottenere il bene digitale, ma si giustifica quale condizione fattuale per poter eseguire materialmente un comportamento obbligatoriamente (già) dovuto in base ad un contratto o alla legge*»; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, n. 3, 2019, p. 506; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2, 16, pp. 531-532: «*l'utente acconsente al trattamento anche per scopi non necessari alla fornitura del servizio*».

[17] A. DE FRANCESCHI*, La circolazione dei dati personali tra privacy e contratto*, cit., pp. 78-79. Al riguardo, occorre chiarire che non potrà immaginarsi un diritto di proprietà sul dato, cfr. V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista,* in *www.medialaws.eu*, 2019, 5, pp. 33-34: «*Ma, poi, come possiamo qualificare la forma di appartenenza? "Proprietà", nel senso romanistico del termine, appare difficile per ragioni concettuali e comparatistiche. Da un lato sono ben note le impervietà teoriche quando si cerchi di applicare la disciplina della proprietà ed entità non materiali (ex multis, la "proprietà del credito") con tutte le aporie riguardanti il modo di acquisto, di godimento, di trasmissione ed i relativi rimedi*», risulta semmai «*più plausibile la prospettazione di una generica "titolarità" la quale attribuisce al soggetto una serie di diritti, facoltà e correlativi limiti e rimedi*»; C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., p. 325.

[18] R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione Europea*, Torino, 2020, p. 18, secondo cui la firma dei tre trattati (CECA, Euratom, CEE), «*prendeva le mosse un disegno unitario, volto principalmente, nella sua prima fase, a dar vita nel territorio dei sei stati fondatori a un mercato comune basato sulla libera circolazione delle persone, delle merci, dei servizi e dei capitali e caratterizzato da condizioni di concorrenza non falsate né da comportamenti degli attori economici, né dall'azione dei poteri pubblici*». Poi ancora gli Autori sottolineano come il processo di integrazione europea era «*costruito formalmente intorno alla prospettiva economico-commerciale del mercato comune*». In modo ancora più chiaro evidenziano, a p. 459, che «*La realizzazione di un mercato comune europeo ha rappresentato storicamente il primo e più qualificato obiettivo della CEE, al punto che per lungo tempo questa è stata spesso identificata, alternativamente, proprio*

circolazione dei dati personali [19]: il recente Regolamento n. 679/2016 all'art. 1, comma 3, sancisce il divieto di limitarne o vietarne la libera circolazione per motivi relativi alla protezione delle persone fisiche [20].

Al contempo, l'art. 3 [21] della Direttiva 770/2019 [22], pur essendo il frutto di

con tale espressione. Il mercato comune costituiva in effetti il risvolto per così dire economico del grande disegno di pacificazione tra gli Stati fondatori, in quanto puntava anche (ed allora, anzi, soprattutto) sull'apertura dei rispettivi mercati interni e sull'auspicata conseguente integrazione economica per rimuovere una delle principali cause storiche dei conflitti nel Continente e promuovere al tempo stesse le condizioni ed un clima di cooperazione piuttosto che di rivalità. […] Oggi, vuoi perché è stato in larga misura realizzato, vuoi per la connotazione non più meramente mercantilistica della costruzione europea e l'emergere quindi di nuovi obiettivi di più rilevante significato politico, il c.d. grande mercato non ha più quel rilievo preminente che ha avuto in passato» e comunque esso «*continua ad essere la prima delle Politiche dell'Unione disciplinato nella Parte Terza del TFUE*».; N. CATALANO, *Manuale di diritto delle comunità europee*, Milano, 1965, p. 8, secondo cui, oltre che per ragioni politiche, «*l'integrazione realizzata tra i sei Stati d'Europa è stata resa possibile dalla convergenza di interessi nel settore economico, dalla complementarità almeno parziale dell'economica degli Stati membri e dal comparabile grado di sviluppo economico raggiunto da ciascuno di essi*». G. VETTORI, *Contratti e rimedi*, Padova, 2017, p. 18, rileva che: «*la Comunità economica europea, […] nasce con l'obbiettivo di creare un Mercato Unico fra i paesi membri*»; G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, Bari, 2014, «*Obiettivo centrale del Trattato CE era in origine quello di realizzare un mercato comune, cioè un'area nella quale fosse assicurata la libertà di circolazione delle merci, eliminando i dazi doganali e le altre restrizioni al commercio tra gli Stati membri*».

[19] A. DE FRANCESCHI, *La vendita di beni con elementi digitali*, Napoli, 2020: «*proposito del legislatore europeo è promuovere la libera circolazione dei dati nel mercato interno, assicurando nel contempo la protezione dei dati personali, sorretta dai diritti di privacy nelle Costituzioni nazionali e nell'art. 8 della Carta dei Diritti fondamentali dell'Unione Europea*».

[20] Letteralmente l'art. 1, comma 3 recita: «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*».

[21] L'art. 3, comma 2, della Direttiva 770 recita, testualmente: «*La presente Direttiva si applica altresì al caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente Direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti*».

[22] A commento della Direttiva 770/2019 cfr. C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, n. 3, 2019, pp. 499-523; G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento*, in *Annuario del diritto dei contratti*, Torino, 2018, p. 127 ss.; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. informazione e informatica*, fasc. 3, 2020, p. 634 ss.; G. VERSACI, *Personal data and Contract law: challenges and concerns about the economic exploitation of the right to data protection*, in *European Rev. of contract law,* 2018, p. 376 ss.

un processo "tormentato" [23], ammette la circolazione dei dati, nella parte in cui prevede l'applicazione della Direttiva stessa al caso di una fornitura di contenuto o servizio digitale in cui il consumatore "*fornisce o si impegna a fornire*" dati personali all'operatore economico.

Alla luce delle considerazioni svolte appare, allora, che la protezione degli interessi fondamentali della persona non debba necessariamente essere perseguita mediante una non realistica «*depatrimonializzazione dei dati […] bensì attraverso un attento controllo dell'atto di autonomia finalizzato ad assicurare la salvaguardia dei valori incomprimibili della personalità* [24]».

Del resto, già l'art. 8 della Carta di Nizza, sancisce che i dati personali "*devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata*". Autorevole dottrina ha evidenziato che la commercializzazione dei dati non ha niente di illegittimo, «*purché però il consenso in oggetto rappresenti una effettiva espressione della autodeterminazione informativa*» [25]. Il riferimento contenuto nell'art. 8 della Carta deve intendersi pertanto come riferimento ad un «consenso informato», cioè «*all'accettazione del trattamento senza costrizione e con la consapevolezza dello stato delle cose* [26]». Ciò, discende peraltro dal c.d. principio della libertà del consenso, immanente a tutto il GDPR, in forza del quale una manifestazione di consenso che non si fondi su un livello minimo di consapevolezza dovrà considerarsi inefficace [27].

---

[23] L'originaria proposta di Direttiva prevedeva all'art. 3, una formulazione diversa che utilizzava le espressioni *contratto* e *controprestazione*: «*la presente Direttiva si applica ai contratti» di fornitura di contenuto digitale «in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato*». Tale definizione è stata poi riveduta e corretta nel testo definitivo, in seguito al parere del Garante europeo della protezione dei dati personali con cui l'Autorità europea criticava aspramente l'equiparazione dei dati personali ad una risorsa suscettibile di essere utilizzata alla stregua di controprestazione contrattuale.

[24] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., pp. 433-434.

[25] G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., pp. 432-433: «*Ci pare, in altri termini, che la monetizzazione dei dati personali non abbia in sé nulla di disdicevole né di giuridicamente sospetto, purché però il consenso in oggetto rappresenti una effettiva espressione della autodeterminazione informativa*». In senso analogo, A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., pp. 16-21.

[26] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 44.

[27] Si veda al riguardo, l'art. 7, par. 2, secondo periodo: «*Nessuna parte di una tale dichiarazione che costituisca una violazione del presente Regolamento è vincolante*». Si veda in senso analogo anche il considerando n. 32 GDPR.

3. *Il consenso al trattamento dei dati personali nel sistema multilivello*

Le prime riflessioni maturate intorno alla legge n. 675/1996 intendevano il consenso, non come elemento di una fattispecie negoziale, ma come un'esimente dell'illiceità del trattamento che il titolare dello stesso doveva ottenere dall'interessato per evitare i meccanismi sanzionatori previsti dalla legge. Si trattava, del resto, di un'impostazione coerente con la ricostruzione del fenomeno dei dati personali in termini di diritti assoluti e non di diritti relativi[28].

L'adesione ad una prospettiva di circolazione del dato fa mutare anche la qualificazione che viene fornita del consenso, che assurge a vero e proprio elemento della fattispecie negoziale.

La centralità del consenso al trattamento dei dati è confermata sia dal Reg. 679/2016 (GDPR), "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", sia dal citato art. 8, comma 2, della Carta di Nizza. Quest'ultima disposizione qualifica il consenso dell'interessato come una delle possibili basi idonee a giustificare il trattamento, mentre l'art. 4, n. 11, GDPR esplicita tale regola, individuandone i requisiti di liceità. Viene sancito che il consenso debba consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato. Al riguardo, è stato sottolineato che l'armonizzazione della disciplina sulla protezione dei dati, realizzata tramite il Regolamento, è stata perseguita mediante un significativo inasprimento dei presupposti richiesti per la manifestazione del consenso. Ne è dimostrazione la previsione, già menzionata, dell'art. 7, par. 2, che sancisce la non vincolatività della dichiarazione resa in violazione della disciplina prevista dal GDPR[29].

3.1. *Il principio di libertà del consenso nella giurisprudenza di legittimità*

Il requisito della libertà del consenso, ora contenuto nell'art. 4, par. 1, n. 11, del Regolamento, costituisce una riproposizione della precedente disciplina che già lo menzionava all'art. 2, par. 1, lett. h), della Direttiva 95/46/CE e all'art. 23, comma 3 del previgente codice della privacy. La normativa in questione si limita ad enunciare la necessità del medesimo, senza tuttavia indicare

[28] V. RICCIUTO, *La patrimonializzazione dei dati personali, contratto e mercato nella ricostruzione del fenomeno*, cit., p. 701; G. COMANDÈ, *Commento all'art. 11, l. n. 675/1996*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH, *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1997, p. 102.

[29] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 47.

in quali situazioni tale libertà sia carente, così da rendere necessaria un'attività ermeneutica volta a chiarire la portata del suddetto requisito.

Nel diritto comune, le ipotesi di consenso non libero, si rinvengono nei casi di incapacità, vizi del volere [30] e, in circostanze particolari, nelle situazioni di pericolo o di bisogno economico in cui si trova chi decide di contrarre. Si tratta dei casi sanzionati dal codice civile con i rimedi della annullabilità [31] e della rescissione del contratto [32].

---

[30] Cfr. A. TRABUCCHI, *Il dolo nella teoria dei vizi del volere*, Padova, 1937; ID., *voce Errore (diritto civile)*, in *Noviss. dig. it*., VI, 1960, p. 665 ss.; V. PIETROBON, voce *Errore. I) Diritto civile*, in *Enc. giur. Treccani*, XIII, Roma, 1989, p. 11 ss.; F. DI MARZIO, *Errore, violenza, dolo, azione di annullamento*, Torino, 2000; A. FASANO, *I vizi del consenso*, Torino, 2013; I. PAGNI, *Vizi del consenso e annullabilità della separazione consensuale omologata: lo sfuggente rapporto tra autonomia negoziale e controllo giudiziale*, in *Fam. e dir.*, 2005, 5, pp. 511-515; G. CIAN, *Sui vizi del volere nella dichiarazione testamentaria*, *Riv. dir. civ*., 5, pp. 1206-1214; A. GORGONI, *La riforma dei contratti in Francia. I vizi del consenso nel code civil: un confronto con la disciplina italiana*, in *Giur. it*., 2018, 1, p. 88 ss.; G. SICCHIERO, *Art. 768* quinquies *c.c. Vizi del consenso. Il patto di famiglia*, in *Nuove leggi civ. comm*., 2007, 1-2, pp. 63-81; G. CRISCUOLI, *Atti giuridici e vizi della volontà*, in *Riv. trim. dir. proc. civ*., 1993, 3, pp. 767-803; ID., *Errore di diritto e riconoscibilità*, in *Riv. dir. civ*., 1986, 4, pp. 383-412; P. GALLO, *I vizi del consenso*, in E. GABRIELLI (a cura di), *I contratti in generale*, *Trattato dei contratti*, Torino, 2006, pp. 457-537; R. SACCO, *Il consenso*, *ivi*, p. 423 ss.; M. LOBUONO, *I vizi della volontà*, in *Diritto civile*, diretto da Lipari e Rescigno, III, 2, *Il contratto in generale*, Milano, 2009, p. 1055; L. MENGONI, *Metus causam dans e metus incidens*, in *Riv. dir. comm*., 1952, I, p. 20 ss.; G. VETTORI, *Contratto e rimedi*, Padova, 2017, p. 484 ss.

[31] M. FRANZONI, *Dell'annullabilità del contratto*, Milano, 1997; F. GALGANO, *Della simulazione, della nullità del contratto, dell'annullabilità del contratto: art. 1414-1446*, Bologna-Roma, 1998; A. GORGONI, G. VETTORI, *L'annullabilità del contratto per incapacità legale. L'incapacità naturale e la circonvenzione di persone incapaci*, Padova, 2009; R. TOMMASINI, E. LA ROSA, *Dell'azione di annullamento*, in *Il Codice civile. Commentario*, fondato da Schlesinger, diretto da Busnelli, Milano, 2009; G. MARINI, *Il contratto annullabile*, in *Trattato del contratto*, diretto da Roppo, IV, *Rimedi*, a cura di A. Gentili, Milano, 2006, p. 307 ss.; G. VETTORI, *Contratto e rimedi*, Padova, 2017, p. 474 ss.; G.B. FERRI, *Appunti sull'invalidità del contratto*, in *Riv. dir. comm*., 1996, I, p. 367 ss.; U. MAJELLO, *La patologia discreta del contratto annullabile*, in *Riv. dir. civ*., 2003, I, p. 329 ss.; F. MESSINEO, voce *Annullabilità e annullamento,* in *Enc. dir*., II, Milano, 1958, p. 470 ss.; R. SACCO, voce *nullità e annullamento* in *Noviss. dig. it*., XV, 1965, pp. 662 ss.; S. PAGLIANTINI, *Tutela per equivalente di un contratto annullabile e principio di effettività: appunti per uno studio,* in *Nuove leggi civ. comm*., 2014, pp. 645 ss.; E. DEL PRATO, *Patologie del contratto: rimedi e nuove tendenze*, in *Riv. dir. comm*., 2015, I, p. 19 ss.; S. LANDINI, *Reticenze dell'assicurato e annullabilità del contratto*, in *Resp. civ. prev*., 2001, p. 629 ss.; C. CONSOLO, *Imprescrittibilità della c.d. eccezione di annullabilità e parte convenuta per l'esecuzione: spunti sistematici*, in *Corr. giur*., 2000, p. 93 ss.

[32] E. MINERVINI, *La rescissione del contratto*, in *Rass. dir. civ*., 1997, fasc. 4, pp. 764-809; G. BENEDETTI, *La rescissione nell'orizzonte della fonte e del rapporto giuridico*, in *Riv. trim. dir. proc. civ*., 2007, 1, pp. 15-33; ID. *La rescissione*, Torino, 2007; G. MIRABELLI, *La rescissione del contratto*, Napoli, 1951; F. DI MARZIO, *Simulazione, nullità, rescissione*, Torino, 2000; G. VET-

La dottrina maggioritaria ritiene che in questo settore, che risponde a logiche sue proprie, il richiamo alla libertà del consenso non possa essere ridotto all'applicazione delle normali regole dettate dal codice civile, ma che in ragione della generale posizione di debolezza in cui si trova l'interessato[33] e della rilevanza degli interessi in gioco, sia opportuna una interpretazione di questo requisito tale da garantirgli una più efficace tutela.

Al riguardo, l'orientamento cui aderisce il Garante per la protezione dei dati personali[34] è quello secondo cui il consenso non è libero, ma "necessita-

---

TORI, *Contratto e rimedi*, Padova, 2017, p. 555 ss.; A. BORGIOLI, *Contratto di società e rescissione*, in *Riv. soc.*, 1978, 2-3, pp. 421-438; M. COSTANZA, *Contratto preliminare e prescrizione dell'azione generale di rescissione*, in *Giust. civ.*, 1977, 9, pp. 1377-1385; R. LANZILLO, A. RICCIO, *Rescissione del contratto*, in *Commentario del cod. civ. Scialoja-Branca*, a cura di Galgano, Bologna-Roma, 2005, B. CARPINO, *La rescissione del contratto*, in *Il Codice civile, Commentario*, diretto da Schlesinger, Milano, 2000.

[33] In questo senso, V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, cit., p. 221: «*il consenso può essere ritenuto effettivamente libero solo se si presenta come manifestazione del diritto all'autodeterminazione informativa*»; S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, p. 460: «*è richiesto qualcosa di più e di diverso rispetto a ciò che deve ricorrere per configurare un consenso viziato in base agli articoli 127 e seguenti c.c.*»; A. FICI, E. PELLECCHIA, *Il consenso al trattamento*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., I, p. 511, secondo cui dovranno essere presi in considerazione «*tutti quegli eventi che possano comunque turbare il processo decisionale del soggetto nella scelta relativa all'abbandono della propria identità riservata. E, dunque, non solo alle ipotesi codicistiche dei c.d. vizi della volontà, ma altresì alle pressioni derivanti da una posizione di debolezza, anche informativa, dell'interessato, che lo costringono a cedere il dato pur di ottenere in cambio un bene o un servizio*»; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 419; V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998, I, p. 30; C. CAMARDI, *Mercato delle informazioni e privacy*, *Riv. crit. dir. priv.*, 1997, p. 567; G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, p. 324; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa dir. priv.*, 2, 2016, p. 517; ID., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 138.

[34] Provv. 3 novembre 2005, reperibile sul sito www.garanteprivacy.it, doc. web n. 1195215, in cui il Garante sottolinea che: la «*capacità di autodeterminazione non è assicurata quando si assoggetta in blocco l'accesso ai servizi alla previa autorizzazione a trattare i dati conferiti per i medesimi servizi allo scopo di perseguire una finalità diversa ed ulteriore, qual è l'invio di comunicazioni commerciali*». Ancora, provv. 22 luglio 2010, doc. web n. 1741988, in cui il Garante evidenzia che: «*l'unico consenso richiesto non può neanche definirsi liberamente prestato dall'utente, dal momento che la registrazione al sito web o la partecipazione ad un concorso sono subordinati all'autorizzazione dell'interessato di trattare i propri dati personali per finalità diverse, di profilazione e di cessione dei dati ad altre società per ulteriori scopi*»; Ancora, provv. 7 ottobre 2010, doc. web n. 1763037, in cui il Garante conferma che «*non può definirsi libero il consenso ad un ulteriore trattamento dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta*».

to" [35], quando l'interessato ha l'onere di prestarlo se vuole accedere al bene o al servizio richiesto. A ben vedere, si tratta di una prospettiva del tutto fisiologica nell'ambito dei rapporti improntati all'autonomia privata: di regola ogni contraente fornisce la sua prestazione al fine di ottenere in cambio la controprestazione resa dalla controparte.

Se si accogliesse l'impostazione seguita dai Garanti europei si produrrebbe il risultato di azzerare il mercato dei dati personali. Infatti, ove fosse garantita all'utente la possibilità di accedere al servizio pur negando il consenso al trattamento, nella maggior parte dei casi egli non fornirebbe tale consenso [36].

Questo modello di libertà, come detto, è ben diverso da quello tradizionalmente richiesto per tutelare la libertà del volere nell'ambito dei comuni atti di diritto privato. Si può ravvisare semmai una certa somiglianza tra questa impostazione e quella adottata rispetto agli atti di disposizione del corpo. Al riguardo, oltre alla norma prevista dall'art. 5 c.c. [37], si deve rammentare soprattutto l'art. 3 della Carta dei Diritti fondamentali dell'Unione europea che, al secondo comma, vieta espressamente «*di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro*». In forza di tale norma, gli atti di disposizione del corpo sono validi solo se posti in essere a titolo gratuito. Tradizionalmente, si ritiene che il principio della gratuità sia posto proprio a tutela della libertà e della spontaneità del consenso espresso dal soggetto interessato, poiché si vuole evitare che qualcuno «*possa essere spinto dal bisogno economico a distaccarsi*» da parti del proprio corpo [38].

---

[35] Così S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 138; ID., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa dir. priv.*, 2, 2016, p. 535.

[36] Ciò, in quanto, come rilevato da S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 139: «*L'erogazione di beni e servizi è infatti l'occasione principale per raccogliere dati personali. […] Se gli utenti devono essere liberi di accedere al servizio scegliendo se prestare o meno il consenso al trattamento dei dati, è infatti ben possibile che molti interessati decidano di negare il consenso, se, ciò nonostante, non viene loro impedito l'accesso al servizio*».

[37] L'art. 5 c.c. recita: «*Gli atti di disposizione del proprio corpo sono vietati quando cagionino una diminuzione permanente della integrità fisica, o quando siano altrimenti contrari alla legge, all'ordine pubblico o al buon costume*».

[38] A. GAMBARO, *I beni*, in *Trattato di diritto civile e commerciale*, diretto da Cicu, Messineo e Mengoni, Milano, 2012, pp. 200-201: «*I materiali biologici umani sono beni dai quali il loro titolare non può trarre alcun lucro, perché non si vuole che essi divengano oggetto di un mercato e perché, più radicalmente, non si vuole che qualcuno possa essere spinto dal bisogno economico a distaccarsi da essi*». A. GALASSO, *Il principio di gratuità*, in *Riv. crit. dir. priv.*, 2001, p. 205 ss.; G. RESTA, *La disposizione del corpo, regole di appartenenza e di circolazione*, nel *Trattato di biodiritto*, diretto da Rodotà e Zatti, II, *Il governo del corpo*, a cura di Canestrari, Ferrando, Mazzoni,

Bisogna chiedersi se possa valere la stessa limitazione anche nel settore dei dati personali.

Innanzitutto, occorre rilevare che la stessa Carta di Nizza, all'art. 8, relativo ai dati personali, non sancisce alcun divieto contenutistico, analogo a quello dell'art. 3 [39].

In secondo luogo, l'art. 7, par. 4, del GDPR nel concretizzare il requisito della libertà del consenso prevede che debba tenersi «*nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di un contratto*». La norma non introduce un divieto, si limita soltanto ad individuare uno dei (tanti) parametri da considerare al fine di determinare se il consenso sia stato prestato o meno in modo libero [40].

Occorre allora capire in quali circostanze risulti vietato subordinare l'accesso ad un bene o ad un servizio al consenso al trattamento dei dati personali. A tale scopo rileva la pronuncia della Corte di Cassazione n. 17278/2018 [41], in cui si afferma che questo tipo di operazioni è vietato quando la prestazione è «*ad un tempo infungibile ed irrinunciabile per l'interessato* [42]». La Corte, quindi, introduce due parametri per determinare se e quando il consenso sia stato prestato in mancanza di libertà. Il giudice di legittimità sembra concludere nel senso che manchi nel nostro ordinamento un divieto di scambiare i dati personali con servizi o contenuti, purché sussistano una serie di requisiti procedurali atti a garantire che la manifestazione volitiva dell'utente sia effettivamente libera e consapevole.

Rodotà e Zatti, I, Milano, 2011, p. 818; ID., *Contratto e persona*, in V. ROPPO, *Trattato del contratto*, IV, *Interferenze*, Milano, 2006, p. 17 ss.; M.C. VENUTI, *Atti di disposizione del corpo e principio di gratuità*, in A. GALASSO, S. MAZZARESE (a cura di), *Il principio di gratuità*, Milano, 2008, pp. 307-308.

[39] G. RESTA-V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 431.

[40] Si esprimono in questo senso, C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., 2021, p. 331; S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 140; G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., p. 432, i quali parlano della possibilità di rinvenire nell'art. 7, comma 4, GDPR una «*presunzione di invalidità del consenso prestato al fine di accedere a beni o servizi, ma deve essere chiaro che si tratta di una presunzione iuris tantum e non, invece,* iuris et de iure».

[41] Per un commento alla sentenza si veda F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 1, 2019, p. 34 ss.

[42] Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 2, 2019, p. 530 ss.

La fungibilità in questo contesto è intesa in senso atecnico per indicare un servizio o un contenuto che sia anche «*acquisibile per altra via*[43]», ed esprime quindi la necessità che sul mercato vi sia un'alternativa[44].

Il requisito della rinunciabilità attiene all'importanza della prestazione stessa per l'utente[45] ed alla possibilità di farne a meno senza un «*gravoso sacrificio*»[46].

Sulla scorta di tali parametri, si dovrà ritenere che se il servizio è sia infungibile che irrinunciabile, cioè qualora non abbia equivalenti sul mercato e sia fondamentale per il cliente, allora il consenso al trattamento non sarà stato prestato liberamente.

Laddove il servizio o il contenuto siano fungibili, ne conseguirà la rinunciabilità, in quanto se sul mercato è presente un servizio o un contenuto analogo, l'interessato potrà agevolmente indirizzarsi verso il servizio o contenuto alternativo. Con la precisazione che la fungibilità del servizio non comporta sempre e comunque la possibilità di subordinarne l'accesso al consenso al trattamento dei dati, poiché potrebbero esservi anche altre circostanze che incidano sulla spontaneità del consenso prestato, come situazioni di particolare debolezza e vulnerabilità dell'interessato.

La questione più delicata attiene all'ipotesi in cui il servizio sia infungibile ma non irrinunciabile. V'è da chiedersi, in sostanza, se possa considerarsi libero il consenso al trattamento dei dati personali prestato al fine di ottenere in cambio l'accesso ad un servizio che non presenta equivalenti sul mercato, ma di cui l'interessato possa fare a meno. A tal proposito è stata proposta una lettura restrittiva della nozione di rinunciabilità, che dovrebbe quindi riservarsi ai casi di evidente futilità del servizio, con la conseguenza che negli altri casi, qualora il servizio sia realmente infungibile, dovrà ritenersi anche irrinunciabile[47].

---

[43] *Ibidem*.

[44] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 142.

[45] *Ibidem*. Il tema della rilevanza dell'essenzialità del servizio era stato trattato anche da C. LO SURDO, *Il ruolo dell'obbligo di informativa*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., I, p. 736; A. ORESTANO, *La circolazione dei dati personali*, *ivi*, p. 188.

[46] Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it*., 2, 2019, p. 530 ss., secondo cui si dovrà considerare prestato liberamente il consenso che attenga al caso di un servizio agevolmente acquisibile per altra via, «*eventualmente attraverso siti a pagamento, se non attraverso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio*».

[47] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 143.

3.2. *La necessità di un consenso specifico ed informato*

Come visto, la giurisprudenza si è occupata con attenzione anche di un altro requisito che deve connotare il consenso, affinché possa costituire il fondamento di un lecito trattamento dei dati personali. La Suprema Corte, nella già citata pronuncia del 2018, chiarisce che il requisito della libertà del consenso deve essere inteso in stretta relazione con quello dell'informazione, per cui non potrebbe mai esistere un consenso libero ove il soggetto non sia stato adeguatamente informato. Dal principio di libertà del consenso discende quello del consenso informato, rispetto al quale la Corte richiama le considerazioni attinenti al settore delle prestazioni sanitarie [48], ove è avvertita l'esigenza di garantire la pienezza del consenso, in modo da assicurare il diritto di autodeterminazione dell'interessato, attraverso obblighi di informazione in favore della parte debole [49].

La disciplina contemplata dagli artt. 13 e 14 del Reg. UE 2016/679 sancisce una serie di obblighi di trasparenza in capo al titolare del trattamento. In particolare, l'interessato deve essere reso edotto di due diverse categorie di informazioni: un primo gruppo volto a richiamare la sua attenzione sui diritti che gli spettano e a garantire il loro effettivo esercizio (es. l'indicazione dei dati di contatto del titolare del trattamento); un secondo gruppo che riguarda invece gli utilizzi dei dati che il titolare realizzerà, in modo da circoscrivere l'og-

---

[48] A. DI MAJO, *La responsabilità da violazione del consenso informato*, in *Corr. giur.*, 2010, 9, pp. 1204-1208; E. BATTELLI, *Fine vita e consenso informato*, in *Riv. dir. priv.*, 2020, 4, pp. 561-590; V. ZENO-ZENCOVICH, *Il consenso informato e l'autodeterminazione informativa*, in *Corr. giur.*, 1997, pp. 915 ss.; U. SALANITRO, *Il consenso, attuale o anticipato, nel prisma della responsabilità medica*, in *Nuove leggi civ. comm.*, 2019, 1, pp. 125-151; P. ZATTI, *Brevi note sull'interpretazione della legge*, in *Nuove leggi civ. comm.*, 2019, 1, pp. 67-101; R. SENIGAGLIA, *Consenso libero e informato del minorenne tra capacità e identità*, in *Rass. dir. civ.*, 2018, 4, pp. 1318-1350; R. NATOLI, *Consenso informato e obbligazioni di risultato tra esigenze di compensation ed esigenze di deterrence?* in *Danno e resp.*, 2000, 7, pp. 732-739; U. PERFETTI, *La responsabilità civile del medico tra legge c.d. Gelli e nuova disciplina del consenso informato*, in *Giust. civ.*, 2018, 2, pp. 359-416; R. CALVO, *La nuova legge sul consenso informato e sul c.d. biotestamento*, in *Studium iuris*, 2018, 2, pp. 689-694; L. D'AVACK, *Consenso informato e scelte di fine vita: riflessioni etiche e giuridiche*, Torino, 2020. Per considerazioni in ambito penalistico, cfr. F. MANTOVANI, *Il consenso informato: pratiche consensuali*, in *Riv. ita., med. leg.*, 2000, 1, pp. 1-47; F. GIUNTA, *Il consenso informato all'atto medico tra principi costituzionali e implicazioni penalistiche*, *Riv. it. dir. e proc. pen.*, 2001, 2, pp. 377-410; M. POLVANI, *Il consenso informato all'atto medico: profili di rilevanza penale*, in *Giust. pen.*, 1993, 12, pp. 734-736.

[49] Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 2, 2019, p. 532. In questo senso anche A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* in *Notariato*, 4, 2021, p. 374.

getto del consenso che verrà prestato. Sebbene in quest'ultima accezione la nozione di consenso informato tenda a sovrapporsi con quella di specificità dello stesso, essa contribuisce ulteriormente a chiarire la portata della libertà del consenso che, appunto, per essere valido deve essere, oltre che libero, anche informato e specifico [50].

Il giudice di legittimità rinviene nell'esigenza di rimediare all'intrinseca situazione di debolezza dell'interessato, sotto il profilo della asimmetria informativa, nonché sul versante degli strumenti rimediali predisposti, la *ratio* ispiratrice della previsione di un consenso sì rafforzato. La disciplina in esame nasce con l'intento di «*affrontare i rischi per la persona posti dal trattamento in massa dei dati personali, così come reso possibile dall'evoluzione tecnologica* [51]». A tal riguardo, si potrà considerare informato soltanto quel consenso prestato dall'utente che «*abbia preventivamente avuto modo di rappresentarsi, singolarmente, con esattezza* [52]» gli effetti del trattamento. Non si potrà risolvere in un consenso generico, ma dovrà essere specificamente calibrato su di un determinato utilizzo del quale dovranno essere stati limpidamente chiariti i profili qualificanti quali, tra gli altri, l'oggetto, la finalità e la durata [53].

Con riferimento al requisito della specificità, la Corte di Cassazione, con la pronuncia n. 14381 del 2021, ha fissato uno standard particolarmente rigoroso, che implicitamente valorizza la modernità della disciplina della privacy recata dal Reg. 679/2016. Nel dettaglio, il giudice di legittimità ha rilevato l'invalidità del consenso prestato da parte degli aderenti ad una piattaforma onli-

---

[50] Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it*., 2, 2019, p. 533: «*Oltre che libero, il consenso, […], deve essere specifico: ed è manifesto che il requisito della specificità si pone, nel disegno normativo, in stretto collegamento con quello della libertà del consenso, così da risolversi in un'endiadi*»; in questo senso anche S. THOBANI, *Operazioni di tying e libertà del consenso*, in *Giur. it*., 2019, p. 537. A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* cit., p. 374, rinviene nella specificità del consenso «*una ben precisa portata funzionale, orientandosi esso ad assicurare l'autodeterminazione del singolo sulle informazioni a lui relative*».

[51] Cass. civ. sez. I, 2 luglio 2018, n. 17278, in *Giur. it*., 2, 2019, p. 533.

[52] *Ibidem*. A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* in *Notariato*, 4, 2021, p. 374 mette in luce che: «*non sarà utile un consenso non "informato", ossia non partorito nella piena consapevolezza delle informazioni di cui agli artt. 13-14 GDPR. L'omessa o lacunosa informativa impedisce infatti la formazione di una corretta autodeterminazione dacché non ponderate ne risulterebbero le scelte in merito alla protezione dei dati personali. Un consenso così pregiudicato non potrebbe dirsi realmente espresso finendo per invalidare il trattamento la cui liceità da questo dipendesse*».

[53] A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* cit., p. 374.

ne, i quali non conoscevano le modalità di funzionamento dell'algoritmo in base al quale sarebbero stati trattati i dati personali[54]. La Corte ha ritenuto che non fosse stato integrato il requisito del «*consenso espresso specificamente in riferimento ad un trattamento chiaramente individuato*», poiché non erano stati resi noti gli schemi esecutivi mediante i quali l'algoritmo si esprimeva[55].

Ma vi è di più. Il principio del consenso informato è arricchito da un ulteriore profilo sancito dalla Corte di Giustizia dell'UE, con la pronuncia *Orange Romania* del 2020, C-61/69. In tale decisione, il giudice sostiene che al fine di assicurare all'interessato un'effettiva libertà di scelta, il testo contrattuale non debba «*indurre la persona interessata in errore circa la possibilità di stipulare il contratto anche qualora essa rifiuti di acconsentire al trattamento dei suoi dati*». L'operatore, quindi, dovrà indicare chiaramente se il consenso al trattamento costituisca o meno un presupposto essenziale per la conclusione del contratto. Spetterà al giudice nazionale verificare l'esistenza di informazioni utili all'interessato a non cadere in errore rispetto ad una tale evenienza[56].

3.3. *La forma della manifestazione del consenso*

Il consenso al trattamento dei dati personali deve essere prestato in modo inequivocabile: ciò implica che lo stesso non debba essere connotato da tratti di ambiguità. È necessario che la manifestazione di volontà dell'interessato riveli limpidamente quali siano le sue intenzioni. Per tale ragione, essa deve scaturire da un suo comportamento commissivo, dotato di carattere dichiarativo, con conseguente esclusione delle «*manifestazioni di volontà tacite desunte da*

---

[54] Sul tema degli algoritmi cfr. G. PASSAGNOLI, *Ragionamento giuridico e tutele nell'intelligenza artificiale*, in *Pers. e merc.*, 2019, 3, p. 79 ss.; A. GAMBINO, *Vizi e virtù del diritto computazionale*, in *Dir. informazione e informatica*, 2019, 6, pp. 1169-1173; ID., *Intelligenza artificiale e tutela della concorrenza*, in *Giur. it.*, 2019, 7, pp. 1744-1748; M. FRANZONI, *Lesione dei diritti della persona, tutela della "privacy" e intelligenza artificiale*, in *Jus civile*, 2021, 1, pp. 4-20; U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civ.*, 2020, 6, pp. 1246-1276; L. D'AVACK, *Intelligenza artificiale: problematiche etiche e giuridiche*, in *I diritti dell'uomo*, 2020, 2, pp. 337-344; F. DONATI, *Intelligenza artificiale: quali spazi nel campo della giustizia?*, *ivi*, pp. 345-354; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di Biodiritto*, 2019, 1; G. ALPA, *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020; G. TEUBNER, P. FEMIA, *Soggetti giuridici digitali?: sullo status privatistico degli agenti software autonomi*, Napoli, 2019.

[55] Cass., 25 maggio 2021, n. 14381 in *Dir. e giust.,* 26 maggio 2021.

[56] C. ANGIOLINI, *A proposito del caso orange romania deciso dalla corte di giustizia dell'Ue: il rapporto fra contratto e consenso al trattamento dei dati personali*, cit., p. 259.

contegni meramente omissivi. Il silenzio, l'inattività o la preselezione di caselle», non integrano un volere decisivo [57].

La Corte di Cassazione, con la già citata sentenza n. 17278/2018, ritiene che se le informazioni fornite dal titolare, sono contenute in una diversa pagina rispetto a quella in cui è presente la casella di spunta per l'acquisizione del consenso, dovrà necessariamente esservi «*contezza che l'interessato abbia consultato detta altra pagina, apponendo nuovamente una diversa "spunta" finalizzata a manifestare il suo consenso*» [58].

In senso conforme, i Giudici di Lussemburgo, con la sentenza del 2020, che si pone in continuità con la sentenza *Planet49* del 2019, C-673/17, interpretano il requisito sancito dall'art. 4, par. 1, del Reg. 2016/679, ritenendo che il consenso debba consistere in una «*dichiarazione o azione positiva inequivocabile*», considerandolo assente nei casi in cui vi sia una casella già preselezionata che l'utente può soltanto deselezionare. In tali ipotesi, non si potrà infatti essere certi che l'interessato abbia consultato l'informativa ovvero abbia effettivamente visto la casella [59].

4. *L'applicazione del Codice del consumo secondo il Consiglio di Stato*

Terminata l'analisi sistematica in materia, giova tornare al recentissimo *decisum* del Consiglio di Stato da cui l'indagine ha preso le mosse.

Il giudice amministrativo, con la sentenza del 29 marzo 2021, n. 2631 si pronuncia al termine di una travagliata vicenda, originata dall'adozione da parte dell'AGCM nei confronti di Facebook di un provvedimento [60] – poi confermato nel 2020 dal TAR Lazio – che ha qualificato come pratica commerciale scorretta, *sub specie* di pratica ingannevole, la condotta posta in essere dalla piattaforma in relazione al trattamento dei dati degli interessati, nella parte in cui al momento della registrazione, Facebook invitava gli utenti ad iscriversi, proclamando la gratuità del servizio.

Per risolvere la questione, il giudice amministrativo ha dovuto prendere po-

---

[57] A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali,* cit., pp. 375-376.

[58] Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it*., 2, 2019, p. 532; S. THOBANI, *Operazioni di tying e libertà del consenso*, in *Giur. it*., 2019, p. 538.

[59] C. ANGIOLINI, *A proposito del caso Orange Romania deciso dalla corte di giustizia dell'Ue: il rapporto fra contratto e consenso al trattamento dei dati personali*, cit., p. 251.

[60] AGCM, Provvedimento n. 27432 del 29 novembre 2018.

sizione in merito alla «*possibilità di concepire la scelta del soggetto di consentire al trattamento dei propri dati personali anche come esercizio di libertà economica* [61]».

Facebook sosteneva a fini difensivi la tesi tradizionale, secondo cui i dati personali rappresenterebbero un bene *extra commercium*, insuscettibili di essere venduti, scambiati o in qualsivoglia modo essere ridotti ad un interesse economico, stante la loro attinenza ai diritti fondamentali della persona. Aderendo a questa impostazione si dovrebbe ritenere che i servizi digitali offerti non sarebbero prestati dietro un corrispettivo, ma sarebbero offerti nel contesto di un contratto da qualificarsi come gratuito. Il rapporto così instaurato sarebbe disciplinato esclusivamente dalla disciplina posta a tutela dei dati personali, cioè il GDPR.

Di tutt'altro avviso il Consiglio di Stato che fonda la sua decisione sull'irragionevolezza di una netta distinzione tra la disciplina che regola il mercato e la disciplina che protegge i dati personali; ciò in quanto ormai la maggior parte dei comportamenti umani coinvolge necessariamente dati personali, con la conseguenza che laddove si riconoscesse al settore dei dati personali una assoluta specialità, si giungerebbe ad escludere l'applicazione di ogni altra disciplina giuridica. Il giudice amministrativo, pur riconoscendo la centralità della c.d. "normativa *privacy*", afferma che laddove il trattamento dei dati «*investa e coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a tutela di altri valori e interessi* [62]» l'ordinamento esige l'applicazione di più corpi normativi, al fine di garantire la pienezza della tutela delle persone fisiche [63].

Sulla base di queste premesse è stato ritenuto che il patrimonio informativo costituito dai dati personali degli utenti sia dotato di un valore economico idoneo a configurare un rapporto di consumo anche in assenza di una controprestazione pecuniaria. Ciò in ragione del fatto che la società a cui i dati vengono "ceduti" di tali beni fa un uso commerciale, suscettibile di una chiara valutazione economica. Si giunge così ad affermare, in un'ottica giusrealistica, che il rapporto instaurato tra utente e piattaforma è soltanto apparentemente gratuito, poiché in esso si ravvisa l'esistenza di uno scambio tra le parti dell'operazione.

Per questi motivi, il Consiglio di Stato ha ritenuto applicabile la normativa

---

[61] V. RICCIUTO, C. SOLINAS, *Fornitura di servizi digitali e prestazione dei dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in *giustiziacivile.com*, n. 5, 2021, p. 3.

[62] Cons. Stato, 29 marzo 2021, n. 2631.

[63] Già la dottrina aveva sostenuto una posizione analoga, in particolare cfr. 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.*, n. 3, 2019, p. 500.

posta a tutela del consumatore anche alle operazioni nelle quali vengano forniti servizi digitali ed in cambio l'utente acconsente al trattamento dei propri dati personali [64].

Dopo aver accertato che i rapporti in questione rientrano nell'alveo di quelli regolati *anche* dal Codice del consumo, il giudice amministrativo rinviene nella carenza di adeguata informazione e nell'inadempimento all'obbligo di chiarezza l'integrazione di una pratica commerciale ingannevole ai sensi degli articoli 21, 22 e 23 del d.lgs. n. 206/2005. Il professionista forniva informazioni tali da indurre l'utente a credere che avrebbe fruito gratuitamente del servizio, «*omettendo di comunicare che, invece, ciò avverrà (e si manterrà) solo se (e fino a quando) i dati saranno resi disponibili a soggetti commerciali non definibili anticipatamente ed operanti in settori anch'essi non preindicati per finalità d'uso commerciale e di diffusione pubblicitaria*». In particolare, tra le censure sollevate dal giudice amministrativo, si dice che gli elementi di una pratica commerciale ingannevole vengono integrati, in quanto: «*Facebook non informa l'utente con chiarezza e immediatezza in merito alla raccolta e all'utilizzo, a fini remunerativi, dei dati dell'utente da parte del professionista e, conseguentemente, dell'intento commerciale perseguito, volto alla monetizzazione dei medesimi* [65]».

L'utente non sarebbe posto nella condizione di avere adeguata cognizione del fatto che per ottenere i benefici e i servizi egli è tenuto a cedere dati personali che non saranno utilizzati esclusivamente per far funzionare i servizi da lui anelati, ma che saranno sfruttati dalla piattaforma a fini di lucro. La dichiarazione di gratuità del servizio da parte di Facebook, e la carenza di una corretta informazione relativamente al valore dei dati, integra quindi una pratica ingannevole [66]. Peraltro, è evidente che nella realtà digitale il consumatore/utilizzatore sempre più spesso "paga" fornendo il consenso al trattamento dei dati personali, piuttosto che per mezzo di denaro. Ciò che manca è la consa-

---

[64] In senso favorevole già si erano espressi G. DE NOVA, *I contratti per l'accesso ad internet*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 1, 1996, pp. 42-43; F. DELFINI, *I contratti dei consumatori e internet*, in C. VACCÀ (a cura di), *Consumatori, contratti, conflittualità. Diritti individuali, interessi diffusi e mezzi di tutela*, Milano, 2000, p. 337; S.F. BONETTI, *La tutela dei consumatori nei contratti gratuiti di accesso ad internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in *Dir. informazione e informatica*, 6, 2002, p. 1129 ss.; P. SAMMARCO, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0*, in *Dir. informazione e informatica*, 4-5. 2010, p. 640; F. AGNINO, *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (vedi contratto FB)*, in *Giur. mer.*, 12, 2012, p. 2559.

[65] Cons. Stato, 29 marzo 2021, n. 2631.

[66] V. RICCIUTO, C. SOLINAS, *Fornitura di servizi digitali e prestazione dei dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in *giustiziacivile.com*, n. 5, 2021, p. 5.

pevolezza in merito al fatto che egli stia "pagando", ovvero eseguendo una prestazione a cui è attribuibile un valore economico. Nella maggior parte dei casi il consumatore considera, erroneamente, tale trasferimento gratuito [67].

Il Consiglio di Stato quindi impone «*di rendere esplicito il nesso sinallagmatico che, almeno di fatto, si instaura tra la fornitura di un bene o di un servizio e la prestazione del consenso al trattamento dei dati personali da parte degli utenti*» [68].

5. *Punti fermi e nuovi nodi da sciogliere*

Nel tentativo di individuare alcuni punti fermi nelle questioni di cui si discute, è opportuno tenere a mente quell'ambivalenza citata in avvio del saggio. Sarebbe ingenuo negare o nascondere il valore economico che i dati hanno assunto nell'economia digitale [69]. Al contempo, la natura di diritto fondamentale riconosciuta alla protezione dei dati personali impone di garantire una tutela peculiare della persona [70]. Il sentiero è quello tracciato dalla giurisprudenza.

Ci pare ormai impervio affermare che l'ordinamento vieti in radice la commercializzazione dei dati personali. Ciò in forza di numerose considerazioni.

In via preliminare, l'adozione di un'ottica giusrealistica spinge a prendere atto che nella realtà digitale lo scambio tra servizi e dati avviene quotidianamente, risultando una prassi difficilmente arginabile [71].

---

[67] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 85.

[68] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 134.

[69] Significativo in questo senso anche il considerando n. 13 della Direttiva 770/19: «*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. Tali specifici modelli commerciali si applicano in diverse forme in una parte considerevole del mercato. Introdurre una differenziazione a seconda della natura della controprestazione significherebbe discriminare alcuni modelli commerciali e incoraggerebbe in modo ingiustificato le imprese ad orientarsi verso l'offerta di contenuti digitali contro la messa a disposizione di dati. Vanno garantite condizioni di parità eque*».

[70] R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., p. 761.

[71] C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., 2021, p. 326: «*una tale operazione di scambio è ormai ben percepita sotto il profilo economico, ma fatica a trovare configurazione tecnico-giuridica nel contesto dei contratti a prestazioni corrispettive*». V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circo-*

Inoltre, a livello sistematico, occorre rilevare che nell'impianto della Carta dei Diritti fondamentali, mentre l'art. 3 vieta espressamente di trasformare il corpo e le sue parti in fonti di lucro, l'art. 8 garantisce la protezione dei dati personali, individuando nel consenso una delle possibili basi atte a legittimarne il trattamento [72]. Ma vi è anche un argomento di carattere letterale: l'art. 7 del Reg. 676/2016, stabilisce che al fine di verificare che sia stato prestato un consenso libero, si debba tenere "*nella massima considerazione*" il fatto che l'esecuzione di un contratto sia condizionato alla prestazione da parte dell'utente del consenso al trattamento di dati personali non strettamente necessari all'esecuzione del contratto stesso. La norma, nell'individuare uno dei parametri da considerare per accertare la sussistenza di un consenso libero, indubbiamente non fissa un divieto di commercio dei dati [73].

In questa direzione, del resto, sembrano orientarsi le principali pronunce esaminate: la sentenza del Consiglio di Stato che qualifica come ingannevole la pratica con cui Facebook proclamava il servizio come gratuito; nonché la pronuncia del 2018 della Corte di Cassazione in cui si osserva che la scambio di dati al fine di accedere ad un servizio è illecito quando il servizio è al contempo infungibile ed irrinunciabile.

Ma c'è un ulteriore aspetto di cui tenere conto. L'inesorabile crescita della realtà digitale ha messo in discussione gli equilibri faticosamente raggiunti nel sistema del diritto privato ed impone di adottare un approccio che presupponga una «*sinergia, senza precedenti, tra aree del diritto da sempre considerate come distinte* [74]». La pronuncia del giudice amministrativo conferma queste considerazioni: la regolazione del fenomeno presuppone la commistione tra la disciplina della protezione dei dati personali e quella che regola il mercato [75],

---

lazione dei dati personali, cit., p. 646, il quale fa riferimento ad «*una vera e propria scollatura tra l'interpretazione giuridica diffusa e la realtà socio-economica*».

[72] A. DE FRANCESCHI, *La vendita di beni con elementi digitali*, Napoli, 2020: «*proposito del legislatore europeo è promuovere la libera circolazione dei dati nel mercato interno, assicurando nel contempo la protezione dei dati personali, sorretta dai diritti di privacy nelle Costituzioni nazionali e nell'art. 8 della Carta dei Diritti fondamentali dell'Unione Europea*».

[73] G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, cit., pp. 432-433; R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., p. 761; F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 1, 2019, p. 43; V. RICCIUTO, *La patrimonializzazione dei dati personali, contratto e mercato nella ricostruzione del fenomeno*, cit., p. 700.

[74] A. DE FRANCESCHI, *La vendita di beni con elementi digitali*, Napoli, 2019, p. 9.

[75] 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.*, n. 3, 2019, p. 500, rileva la necessità di «*una combinazione di più codici disciplinari*» ed in parti-

al fine di garantire al soggetto una tutela che lo riguardi non solo come persona, ma altresì come parte dell'operazione economica[76]. Come già autorevole dottrina aveva rilevato, il riconoscimento della commerciabilità dei dati non comporta un *minus* nelle garanzie riconosciute all'individuo, bensì consente di ampliare il ventaglio di tutele apprestate in suo favore[77]. Pare, quindi, che la soluzione fornita dal Consiglio di Stato risulti fondata su solidi argomenti sistematici nonché su opportune valutazioni volte a garantire quanto più possibile l'effettività della tutela da riconoscersi al singolo.

Accertata la possibilità di scambiare dati personali (*rectius*: di scambiare il consenso al trattamento), occorrerà chiedersi se le modalità di tale commercializzazione possano dipendere soltanto dal rispetto delle norme attinenti alle modalità di manifestazione del consenso ovvero se, vista la particolare natura dei beni coinvolti in tali operazioni, non sia necessario un intervento pubblico che fissi una cornice di divieti e regole all'interno delle quali il suddetto consenso possa lecitamente essere prestato.

La soluzione fornita dal legislatore europeo, in ordine a tale questione, è consistita nel fissare, come visto, degli stringenti requisiti per la validità del consenso al trattamento.

Si tratta di un approccio che ha delle convincenti radici dogmatiche: come evidenziato da alcuni, in una società fondata sul principio dell'autodeterminazione dell'individuo, ricopre un ruolo centrale il riconoscimento al singolo del potere di scegliere relativamente alla quantità di informazioni sulla propria persona che egli intenda fornire[78]. In un settore così rilevante ai fini

---

colare «*la disciplina generale del contratto, la disciplina del diritto d'autore e la disciplina della protezione dei dati personali*», [in ragione della] «*complessità che contraddistingue anche semplicemente per questi aspetti le risorse e le attività che si definiscono intorno al fenomeno e nei mercati digitali, nell'ambito dei rapporti di diritto privato*».

[76] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., p. 643.

[77] 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*, cit., p. 500; C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, cit., 2021, p. 328; R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., p. 769; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., p. 659, il quale evidenzia che la prospettiva patrimonialistica: «*si aggiunge ma non elide né nega la considerazione della persona nell'ambito del fenomeno disciplinato. Semplicemente arricchisce la sfera delle tutele azionabili anche di quegli strumenti – tipicamente propri del diritto patrimoniale e contrattuale – che diversamente non sarebbero accessibili per l'interessato*»; V. CUFFARO, *Il diritto europeo sul trattamento dei dati*, cit., p. 1117.

[78] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 49; F. DONATI, in G. DEMURO, W.B. BOCK (a cura di), *Human Rights in Europe – Commentary of the charter of Fundamental Rights of the European Union*, Durham, 2009, p. 53.

della tutela dei diritti fondamentali, la questione in merito a ciò che è consentito o meno non può essere risolta mediante l'adozione di un criterio parametrato sul sentire comune, ma dovrà essere lasciata proprio alla scelta del singolo individuo [79].

Questa impostazione, però, non è andata esente da critiche. Altri hanno sostenuto che una disciplina sulla protezione dei dati personali fondata sul consenso al loro trattamento non sarebbe più attuale, in ragione dell'asimmetria informativa, ma anche cognitiva [80], tra gli utenti e chi procede all'acquisizione dei dati [81]. Del resto, sono stati sollevati dei dubbi in merito all'efficacia e all'adeguatezza di una tale normativa, in quanto volta a fronteggiare rischi che coinvolgono interessi pubblici, utilizzando però strumenti di tutela esclusivamente privatistici [82].

Si tratta di temi ancora non del tutto risolti, la cui attualità è confermata dal recente rinvio pregiudiziale con il quale il giudice amministrativo tedesco interroga la *C.G.U.E.* [83] al fine di accertare se Facebook abbia abusato della sua posizione dominante ed abbia altresì violato le regole poste dal GDPR.

Le soluzioni fornite dal Giudice di Lussemburgo, auspicabilmente, diraderanno alcuni dubbi interpretativi.

---

[79] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 49.

[80] L. GATT, R. MONTINARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2, 2017, p. 363 ss.

[81] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., p. 147; R. CATERINA, *Cyberspazio, social network e teoria generale del contratto*, in *Aida*, 1, 2011, p. 96; S. SICA, G. GIANNONE CODIGLIONE, *I social network sites e il "labirinto" della responsabilità*, cit., p. 2714; S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in A. MANTELERO, D. POLETTI, *Regolare la tecnologia: il reg. UE 2016/679*, Pisa, 2018, p. 163; J.P. ALBRECHT, *Das neue EU-Datenschutzrecht- von der Richtlinie zur Verordnung*, in *Computer und Recht*, 2016, pp. 88, 91.

[82] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente,* cit., p. 147; A. PLAIA, *Profili evolutivi della tutela contrattuale*, in *Eur. dir. priv*., 1, 2018, p. 69 ss.

[83] Causa C-252/21 del 24 marzo 2021.

IL VALORE NEGOZIALE DEI DATI PERSONALI DEL CONSUMATORE: SPIGOLATURE SUL RECEPIMENTO DELLA DIRETTIVA 2019/770/UE IN UNA PROSPETTIVA COMPARATA

di *Giuseppe Versaci*

1. *Dati personali e contratto alla prova del diritto derivato nazionale. Lo stato del recepimento della Direttiva 2019/770/UE*

Il valore economico acquisito dai dati personali, dimostrato empiricamente dalla sempre maggiore diffusione di modelli commerciali basati sul trattamento dei suddetti dati [1], impone di accostare il fenomeno in questione alle categorie e agli istituti del diritto privato patrimoniale [2], essendo noto come la patrimoniali-

[1] V. *supra*, Parte II, G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento di dati personali*. La letteratura sul tema è sempre più ampia: tra i molti, v. S.-A. ELVY, *Paying for Privacy and the Personal Data Economy*, in *Columbia Law Rev.*, 2017, p. 1369 ss.; per un'analisi più generale, v. ITMedia Consulting, col contributo dell'Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, 2018.

[2] Lungo tale direzione si snoda il discorso di V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., p. 642 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018,

tà costituisca un criterio di qualificazione e differenziazione dei regimi giuridici [3]. Questo solo elemento sarebbe di per sé sufficiente per intraprendere un discorso sulla relazione tra dati personali e contratto, assumendo quest'ultimo come la categoria tipica in grado di organizzare una regolazione di rapporti giuridici, tra due o più parti, di carattere patrimoniale (art. 1321 c.c.) [4].

D'altra parte, un simile discorso si giustifica ancor di più in ragione della concretizzazione attuata dalla Direttiva 2019/770/UE che, all'art. 3, par. 1, primo cpv., ha definitivamente riconosciuto il *valore negoziale* del rilascio di dati personali nell'ambito di una specifica operazione di consumo, vale a dire il contratto per la fornitura di contenuti o servizi digitali [5]. Con "valore negoziale" si vuole qui alludere semplicemente alla circostanza che la fornitura dei dati personali, da parte del consumatore, diviene un surrogato del pagamento di un prezzo al fine dell'applicazione di un determinato regime rimediale di natura contrattuale. Se tal riconoscimento attribuisca altresì un diverso valore allo statuto dei dati personali, e al peculiare istituto del consenso al trattamento, è indubbiamente una questione di grande interesse, che tuttavia non sarà oggetto di trattazione nelle prossime pagine [6]. Il focus di queste ultime verterà, piuttosto, sul *come* le disposizioni della Direttiva 2019/770, relative al rapporto tra dati personali del consumatore e contratto, sono state recepite, o stanno per essere recepite, negli ordinamenti nazionali. Lo scopo dello scritto, quindi, è principalmente informativo, col tentativo ulteriore di proporre una comparazione dei diversi modelli di recepimento in merito ad alcune rilevanti questioni lasciate aperte dal legislatore europeo.

A quest'ultimo riguardo, si tenga conto che il considerando 25 della Direttiva 2019/770 consente agli Stati membri di estendere le disposizioni di tutela consumeristica anche a situazioni in partenza escluse, come la raccolta, da parte dell'operatore economico, di soli metadati del consumatore o l'esposizione

---

p. 689 ss. L'autore, peraltro, rintraccia elementi per una lettura patrimonialistica già nelle prime discipline di protezione dei dati personali; a suo avviso, il GDPR e le nuove prassi di mercato non fanno altro che confermare, ed enfatizzare, una dimensione presente fin dagli albori.

[3] Cfr. D. LA ROCCA, *Diritti e denaro. Il valore della patrimonialità*, Milano, 2006, p. 39 ss.

[4] Sulla patrimonialità di molteplici rapporti instaurati sul web tra piattaforme ed utenti, v. C. CAMARDI, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Jus civile*, 2021, p. 916 ss.

[5] Cfr. K. SEIN, G. SPINDLER, *The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1*, in *Eur. Rev. Contr. Law*, 2019, pp. 263-265.

[6] V. *supra*, T. POLVANI, *Il consenso alla cessione dei dati personali nel dialogo tra le corti*. Di recente, è stata coniata la suggestiva espressione di «consenso "negoziato"»: C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021.

di quest'ultimo a messaggi pubblicitari come sola condizione di accesso a contenuti o servizi digitali. La Direttiva, inoltre, si è astenuta dal disciplinare le conseguenze contrattuali a seguito di una revoca, da parte del consumatore, del consenso al trattamento dei dati che lo riguardano, rimettendo espressamente la regolazione al diritto nazionale (v. il considerando 40). Pur non essendo esplicitato nel testo della Direttiva, i legislatori domestici possono altresì chiarire, di propria sponte, le ricadute contrattuali sia nei casi in cui il consenso al trattamento dei dati personali risulti essere stato prestato in modo invalido, sia nei casi in cui il consumatore eserciti i diritti che gli spettano come soggetto interessato al trattamento ai sensi degli artt. 15 ss. del Regolamento UE 2016/679 (Regolamento Generale per la Protezione dei Dati: c.d. RGPD). Sono molti, dunque, i motivi per i quali è meritevole soffermarsi sulle discipline nazionali di attuazione della Direttiva 2019/770, per lo più reperibili dal portale *online* dell'Unione europea che raccoglie le misure adottate dagli Stati membri[7].

Il termine per il recepimento è scaduto il 1° luglio 2021, tuttavia alcuni Stati vi hanno adempiuto solo in tempi recenti. È il caso dell'Italia, che ha attuato la Direttiva attraverso il d.lgs. 4 novembre, n. 173, frutto della delega al Governo contenuta nella legge 22 aprile 2021, n. 53 (legge di delegazione europea 2019-2020).

2. *La transtipicità consumeristica del valore negoziale dei dati personali: la lungimiranza dei legislatori di Francia e Germania e l'ambiguità di quello europeo*

Il modello di recepimento della Direttiva 2019/770 prescelto dal suddetto decreto legislativo si basa sull'inserimento di un nuovo capo (il capo I-*bis*) all'interno del titolo III della parte IV del Codice del consumo. Tale capo (artt. 135-*octies*-135-*vicies ter*) risulterà interamente dedicato ai «contratti di fornitura di contenuto digitale e di servizi digitali». Con questa scelta il legisla-

[7] V. https://eur-lex.europa.eu/legal-content/IT/NIM/?uri=CELEX:32019L0770&qid=1630853107741 (ultima consultazione: 5 dicembre 2021). Di alcune (proposte di) discipline di recepimento si ha notizia grazie a contributi accademici; ad esempio, per Paesi Bassi, Polonia ed Estonia si veda: M.BM. LOOS, *The (Proposed) Transposition Of The Digital Content Directive In The Netherlands*, in *JIPITEC*, 2021, pp. 229-240; M. NAMYSŁOWSKA, A. JABŁONOWSKA, F. WIADEREK, *Implementation of Digital Content Directive in Poland: A fast ride on a tandem bike against the traffic*, *ivi*, pp. 241-248; I. KULL, *Transposition Of The Digital Content Directive (EU) 2019/770 Into Estonian legal system*, *ivi*, pp. 249-259.

tore nostrano si allinea all'impostazione di altri Stati membri che hanno deciso, o stanno decidendo, di dare attuazione alla Direttiva in questione nell'ambito di una normativa dedicata ai rapporti di consumo [8]; nel caso specifico italiano, si riserva all'interno del Codice del consumo uno spazio apposito alla disciplina dei contratti di fornitura di contenuti e servizi digitali, senza incidere in tal modo sulle altre aree del codice. In sintesi, alla "specialità" del Codice del consumo [9] si associa l'ulteriore specialità dei contratti oggetto di regolazione.

È evidente che un intervento del genere, incidendo poco o nulla sulle disposizioni già esistenti, aspira ad avere risvolti minimali sul microsistema rappresentato dal codice di settore; in termini pratici, le disposizioni di nuovo conio non si estenderanno oltre il perimetro rigorosamente tracciato e non modificheranno nulla dell'architrave consumeristico. Tale scelta potrebbe dirsi in qualche modo obbligata, considerando sia il carattere di novità della disciplina che l'armonizzazione massima prevista dal legislatore unionale. In realtà, se tanto è vero per i profili riguardanti la fornitura del contenuto o servizio digitale e i rimedi esperibili dal consumatore in caso di non conformità [10], la

---

[8] In questo gruppo di Stati rientra certamente la Spagna e sembrerebbero rientrare anche Francia e Polonia: così J.M. CARVALHO, *Transposition of directives 2019/770 and 2019/771*, 2 luglio 2021, disponibile *online* su: https://novaconsumerlab.novalaw.unl.pt/transposition-of-directives-2019-770-and-2019-771/ (ultima consultazione: 5 dicembre 2021).

[9] È bene precisare che il Codice del consumo, pur essendo una disciplina speciale rispetto al codice civile, tende a porsi come normativa generale rispetto alle discipline di tutela del consumatore e, in taluni casi, anche rispetto al più ampio insieme delle discipline di tutela di una parte contrattualmente debole. Basti pensare, ad esempio, alla portata generale che può riconoscersi all'art. 36 del Codice del consumo in merito ai caratteri delle nullità di protezione: v. R. SACCO, G. DE NOVA, *Il contratto*, 4ª ed., Torino, 2016, p. 1504, nt. 67; G. D'AMICO, *Nullità virtuale – nullità di protezione (variazioni sulla nullità)*, in S. PAGLIANTINI (a cura di), *Le forme della nullità*, Torino, 2009, p. 14 ss.

[10] D'altra parte, è vero pure che il legislatore italiano avrebbe potuto compiere una scelta di campo del tutto diversa, inserendo l'intera disciplina dei rimedi relativi ai difetti di conformità – derivante dalle Direttive 770 e 771 del 2019 – all'interno del codice civile piuttosto che all'interno del codice consumo. In tal modo, avrebbe potuto disciplinare in modo più appropriato i rapporti tra i rimedi consumeristici validi per i difetti di conformità e i rimedi di diritto comune discendenti dalla garanzia per vizi. A tal proposito, è assolutamente eloquente la scelta del titolo del convegno organizzato dal Dipartimento di Giurisprudenza dell'Università di Ferrara il 16 e 17 giugno 2021: «*Verso la (ennesima) riforma del (solo) Codice del consumo. Il recepimento in Italia della Direttiva (UE) 2019/771 relativa ai contratti di vendita mobiliare conclusi da professionisti con consumatori*». La stessa critica viene mossa dalla dottrina polacca con riferimento alla scelta del legislatore nazionale di non recepire le due direttive nel codice civile: M. NAMYSŁOWSKA, A. JABŁONOWSKA, F. WIADEREK, *Implementation of Digital Content Directive in Poland: A fast ride on a tandem bike against the traffic*, cit., p. 245 ss.

questione è più complessa se si restringe l'angolo di visuale alla rilevanza contrattuale dei dati personali del consumatore.

La domanda da porsi è se tale rilevanza (che vede la fornitura dei dati personali del consumatore porsi in una logica sostanzialmente di scambio con la prestazione offerta dal professionista) possa essere riconosciuta anche in operazioni negoziali diverse dai contratti di fornitura di contenuti e servizi digitali. La scelta del legislatore italiano, e di altri legislatori nazionali (v., ad. es., Spagna [11] e Austria [12]), sembra escludere – stando al dettato letterale – tale possibilità, posto che non si prevede alcuna norma attraverso la quale il rapporto tra contratto e dati personali del consumatore possa assumere un respiro più generale rispetto a quello ritagliato dalla Direttiva 2019/770: in altri termini, una norma che attribuisca un carattere *transtipico* alla contrattualizzazione dei dati personali del consumatore [13].

Non manca, tuttavia, chi ha agito diversamente: è il caso, innanzitutto, del legislatore tedesco [14]. Quest'ultimo, intervenendo come prevedibile sul BGB che ingloba la disciplina dei contratti *b2c*, ha modificato il § 312 relativo all'ambito di applicazione di tale disciplina. In ragione di tale modifica (v. §

---

[11] La Spagna ha recepito la Direttiva 2019/770 con il «*Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores*». In particolare, per quanto riguarda la questione riferita nel testo, si veda il nuovo *apartado* 4 inserito nell'*artículo* 59 del *texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias*.

[12] In Austria, l'attuazione della Direttiva 2019/770 è avvenuta il 9 settembre 2021 attraverso la «*Bundesgesetz, mit dem ein Bundesgesetz über die Gewährleistung bei Verbraucherverträgen über Waren oder digitale Leistungen (Verbrauchergewährleistungsgesetz – VGG) erlassen wird sowie das allgemeine bürgerliche Gesetzbuch und das Konsumentenschutzgesetz geändert werden (Gewährleistungsrichtlinien-Umsetzungsgesetz – GRUG)*». Con riguardo alla questione riferita nel testo, si tenga conto che tale legge non incide sull'ambito di applicazione della disciplina generale di tutela del consumatore.

[13] A dire il vero, già la Direttiva 2019/770 potrebbe essere definita transtipica nella misura in cui il contratto di fornitura di contenuti o servizi digitali non impone la nascita di un nuovo tipo contrattuale, ma detta soltanto una disciplina, potenzialmente applicabile a diversi tipi contrattuali in base alle qualificazioni nazionali (K. SEIN, G. SPINDLER, *The new Directive on Contracts for the Supply of Digital Content and Digital Services*, cit., p. 260). Nel testo, tuttavia, si utilizza l'espressione "transtipicità" in un senso parzialmente atecnico, alludendo all'estensione della rilevanza contrattuale dei dati personali del consumatore oltre il perimetro applicativo della Direttiva 2019/770.

[14] La legge tedesca di recepimento della Direttiva 2019/770, approvata il 25 giugno 2021, riporta la seguente intestazione: «*Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen*».

312, comma 1a), le disposizioni relative ai principi dei contratti in questione e quelle relative ai contratti conclusi a distanza o fuori dai locali commerciali si applicano anche ai contratti di consumo in base ai quali il consumatore fornisce o si impegna a fornire dati personali al professionista. Tale previsione ha l'innegabile pregio di abbattere gli steccati normativi sopra descritti in vista di un'applicazione dello statuto consumeristico quanto più ampia possibile, raggiungendo operazioni negoziali – anche al di fuori del mercato digitale – nelle quali lo sfruttamento economico dei dati personali prende il sopravvento su altri elementi, come il pagamento di un prezzo. Non è da escludere, infatti, che nel prossimo futuro si diffondano sempre di più modelli commerciali che prevedano l'offerta di prestazioni, *diverse* dalla fornitura di contenuti e servizi digitali, in cambio del solo accesso ai dati personali del consumatore [15].

Lungo una direttrice simile a quella tedesca si è mosso anche il legislatore francese [16], che ha ampliato il raggio di rilevanza dello scambio contrattuale di dati personali del consumatore a tutto il settore della vendita di beni [17]. In particolare, ha previsto che, ai fini dell'applicazione degli obblighi di conformità nei contratti di vendita di beni, si considerano contratti di vendita anche i contratti in base ai quali il professionista consegna i beni e ne trasferisce la proprietà al consumatore e quest'ultimo fornisce qualsiasi altro beneficio, invece di o in aggiunta al pagamento di un prezzo (art. L. 217-1, *Code de la consommation*). Inoltre, sul piano degli obblighi di informazione precontrattuale, il nuovo art. L. 111-1 del medesimo *Code* stabilisce che, prima che il consumatore sia vincolato da un contratto a titolo oneroso, il professionista debba informarlo in modo leggibile e comprensibile circa il prezzo o qualsiasi altro beneficio fornito al posto o in aggiunta al pagamento di un prezzo. Pur non fa-

[15] Già adesso comunque sono presenti operazioni di questo tipo, diverse dalla fornitura di contenuti e servizi digitali, seppur in misura notevolmente inferiore a queste ultime. Nel dibattito olandese, ad esempio, si richiamano i «*cases where personal data are supplied 'in exchange' for the supply of 'free' toy cars, tennis balls and pregnancy boxes*»: M.B.M. Loos, *The (Proposed) Transposition Of The Digital Content Directive In The Netherlands*, cit., p. 238.

[16] La Francia ha dato attuazione alla Direttiva 2019/770 attraverso l'*Ordonnance n° 2021-1247 du 29 septembre 2021 relative à la garantie légale de conformité pour les biens, les contenus numériques et les services numériques*.

[17] D'altra parte, la giurisprudenza francese si era già espressa a favore dell'applicazione del diritto consumeristico anche in assenza del pagamento di un prezzo da parte del consumatore. Si possono qui richiamare tre sentenze emesse a stretto giro dal Tribunale di Grande Istanza di Parigi: *Tribunal de Grande Instance de Paris*, decisione del 7 agosto 2018, 1/4 social RG n. 14/07300 UFC – Que Choisir v. Twitter; *Tribunal de Grande Instance de Paris*, decisione del 12 febbraio 2019, RG n. 14/07224, *UFC – Que Choisir v. Google*; *Tribunal de Grande Instance de Paris*, decisione del 9 aprile 2019, *UFC – Que Choisir v. Facebook*. In tali sentenze, la materia del contendere riguardava l'applicazione della disciplina *b2c* sulle clausole contrattuali abusive.

cendosi esplicito riferimento allo sfruttamento commerciale dei dati personali del consumatore, è evidente che quest'ultimo costituisca la species principale del genus rappresentato dall'«*avantage procuré au lieu ou en complément du paiement d'un prix*».

Orbene, le scelte compiute dal legislatore tedesco e da quello francese appaiono indubbiamente più lungimiranti rispetto all'indirizzo intrapreso dal legislatore italiano e dagli altri che hanno preferito non *generalizzare* (per il momento) la rilevanza negoziale dei dati personali del consumatore [18].

Rimane, tuttavia, un dubbio: i lacci dell'armonizzazione massima di alcune direttive europee *b2c* consentono un simile salto in avanti, che si sostanzia in una tutela *in melius* per il consumatore? Nel momento in cui si vuole estendere l'apparato di protezione consumeristica ai contratti nei quali il consumatore non paga un prezzo al professionista, bensì fornisce dati personali per un trattamento degli stessi a fini commerciali, non è più un problema attinente al recepimento della Direttiva 2019/770 (il cui ambito di applicazione non viene alterato), quanto piuttosto delle altre direttive che, nei margini di un'armonizzazione massima, prevedono un campo di applicazione contrattuale circoscritto [19]. È evidente che il problema maggiore si pone rispetto alla Direttiva 2011/83, incidente su ampi settori della tutela dei consumatori.

A tal proposito, sebbene il legislatore europeo abbia recentemente esteso l'ambito applicativo di quest'ultima tramite la Direttiva 2019/2161 (c.d. Direttiva *Omnibus* o Direttiva di modernizzazione), rimangono comunque delle aree di incertezza. Invero, il considerando 31 della Direttiva *Omnibus* muove correttamente dal presupposto che la Direttiva 2011/83, nella sua versione originaria, già si applicava ai contratti per la fornitura di *contenuto digitale* (mediante un supporto non materiale) indipendentemente dal pagamento di un

---

[18] Bisogna tuttavia segnalare che, a livello giurisprudenziale, il nostro ordinamento ha già manifestato una significativa apertura verso un'ampia applicazione del diritto dei consumatori ai contratti nei quali il pagamento del prezzo è sostituito dalla fornitura di dati personali. A tal riguardo, valga il riferimento alla sentenza del Cons. Stato, 29 marzo 2021, n. 2631 (sulla quale v. *supra*, Parte I, V. PAGNANELLI, *Una "Valutazione d'impatto" della privacy sulle Big Tech. Riflessioni a margine della sentenza n. 2631/2021 della Sesta Sezione del Consiglio di Stato*). In tale sentenza, come si è visto, la disciplina consumeristica coinvolta era quella relativa al contrasto delle pratiche commerciali scorrette.

[19] A tal proposito, si è evidenziato che «*se generale è l'ambito applicativo tanto della Direttiva 93/13 che quello della 2005/29, è tutto da appurare invece se, rispetto al perimetro delle direttive 2008/48, 2011/83 e 2014/17, il diritto regolatorio europeo non abbia inteso tracciare una linea di displuvio tra tipi inclusi ed esclusi, selezionando la classe dei contratti armonizzabili attraverso il medio di un sinallagma nel quale è il professionista tenuto ad eseguire, a titolo oneroso, la prestazione caratterizzante*»: S. PAGLIANTINI, *Il consumatore "frastagliato". Istantanee sull'asimmetria contrattuale tra vicende circolatorie e garanzie*, Pisa, 2021, p. 43.

prezzo da parte del consumatore, mentre non si applicava ai contratti di *servizi* che non contemplassero siffatto pagamento. Conscio di ciò, il legislatore novellatore si è premurato di adeguare (esclusivamente) il presupposto oggettivo di applicazione della Direttiva 2011/83 a quello della Direttiva 2019/770, includendo anche «i contratti nel cui ambito il professionista fornisce o si impegna a fornire un servizio digitale al consumatore, e il consumatore comunica o si impegna a comunicare dati personali» (v. il considerando 33 della Direttiva 2019/2161). Orbene, se l'intento legislativo è stato certamente apprezzabile, non altrettanto può dirsi per la resa finale. Infatti, basandosi sulla lettera delle nuove disposizioni della Direttiva 2011/83 (v. art. 3, parr. 1 e 1-*bis*), restano ancora esclusi tutti i contratti *diversi* da quelli per la fornitura di contenuti e servizi digitali, che comunque prevedono (o prevedranno) la fornitura di dati personali del consumatore in sostituzione del pagamento di un prezzo.

In realtà, tale restrizione sembra scontrarsi con lo spirito che ha mosso la stessa introduzione dell'art. 3, par. 1, primo cpv., della Direttiva 2019/770, posto che dal considerando 24 di quest'ultima si evince la volontà di evitare discriminazioni di tutela tra classi di consumatori sol perché alcuni di essi si trovano coinvolti in modelli commerciali diversi da quelli canonici. Invero, proprio quest'*humus* innovatore ci aveva spinto in altra sede ad intravedere una transtipicità *in fieri* già nella Direttiva 2019/770[20]. L'auspicio, a questo punto, è che l'intervento tedesco sopra richiamato non resti isolato e che la Corte di giustizia sia presto chiamata a fornire un'interpretazione autentica, di marca antiletterale, del nuovo ambito applicativo della Direttiva 2011/83.

3. *L'influenza della protezione dei dati personali sul contratto*

Di là dal raggio d'azione assegnato alla fornitura di dati personali del consumatore in ambito contrattuale, l'attuazione nazionale della Direttiva 2019/770 va giudicata anche sotto un altro profilo di notevole rilievo. Invero, l'art. 3, par. 8 impone di salvaguardare il diritto in materia di protezione dei dati personali, senza tuttavia specificare come gli effetti giuridici discendenti dall'applicazione delle norme di *data protection* si ripercuotano sul contratto di fornitura di contenuti o servizi digitali. La scelta, seppur indolente, può dirsi coerente con il principio di proporzionalità che indirizza il riparto di competenze tra Unione europea e Stati membri in materia consumeristica. Questi ultimi,

[20] G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, pp. 165-168.

infatti, sono particolarmente gelosi di riservarsi la facoltà di disciplinare gli aspetti del diritto generale dei contratti, quali ad esempio le norme sulla formazione, la validità o l'efficacia del contratto (cfr. art. 3, par. 10, Direttiva 2019/770). Pertanto, dal momento che l'applicazione della disciplina di protezione dei dati personali potrebbe finire per impingere sui suddetti profili contrattuali, il legislatore europeo ha preferito astenersi dalla regolazione.

È opportuno, allora, esaminare l'atteggiamento dei diritti nazionali con riguardo alle fattispecie di maggiore interesse.

4. (Segue) *Le conseguenze della revoca del consenso al trattamento dei dati personali tra regole* ad hoc *e principi generali*

Come si è anticipato ad inizio dello scritto (§ 1), il legislatore europeo non si è solo astenuto dal regolare i profili sopra evocati, ma in un caso ha perfino rimesso in modo esplicito agli ordinamenti nazionali la definizione di certi effetti discendenti dall'applicazione dello statuto di *data protection*. Si sta alludendo alle conseguenze contrattuali della revoca, da parte del consumatore, del consenso al trattamento dei dati personali.

La fattispecie è piuttosto semplice. Assumiamo, infatti, che nell'ambito di un contratto per la fornitura di contenuti o servizi digitali, il consumatore fornisca al professionista propri dati (*rectius*, dati che lo riguardano) dietro la prestazione di un consenso al trattamento degli stessi (v. art. 6, par. 1, lett. a), RGPD). Com'è noto, in virtù dell'art. 7, par. 3 del RGPD, il consumatore – in qualità di interessato al trattamento – ha la facoltà di revocare il proprio consenso in qualsiasi momento, senza comunque arrecare pregiudizio alla liceità del trattamento svoltosi prima della revoca.

Sul piano contrattuale, è evidente che nel momento in cui la fornitura di contenuti o servizi digitali da parte del professionista si giustifica in virtù della fornitura di dati personali da parte del consumatore, venuto meno il presupposto giuridico (il consenso) affinché il professionista possa trattare lecitamente i dati del consumatore, la causa concreta del contratto di fornitura ne risulta alterata. Gli scenari prospettabili sono diversi, difficilmente riassumibili nel binomio semplificativo "prosecuzione/cessazione" degli effetti contrattuali. Basti dire, infatti, che un eventuale scioglimento di tali effetti, a seguito della revoca del consenso al trattamento, potrebbe dipendere dalla tipologia di contratto, con differenze tra i contratti ad esecuzione istantanea e quelli ad esecuzione continuata o periodica, oltre al fatto che lo stesso scioglimento potrebbe avvenire *ipso iure* o dietro esplicito impulso di una delle parti, presumibilmen-

te il professionista che si vede privato della possibilità di trattare (a fini commerciali) i dati del consumatore.

Prima di esaminare nel dettaglio le soluzioni domestiche al problema, è opportuno operare una prima distinzione tra gli ordinamenti che adottano regole specifiche per la regolazione della questione e gli ordinamenti che preferiscono affidarsi alle norme generali sul contratto, rinunciando all'invito della Direttiva europea di legiferare sul punto. Tra gli Stati della prima schiera si possono citare, a titolo esemplificativo, la Germania[21], la Spagna[22], i Paesi Bassi[23]; nel secondo gruppo, invece, possono menzionarsi, al medesimo titolo, l'Italia[24], l'Austria[25], la Polonia[26], la Francia[27], il Portogallo[28]; in posizione dubitativa si pone l'Estonia[29]. Le ragioni che inducono gli Stati di cui sopra a non adottare specifiche regole sulle conseguenze della revoca del consenso al trattamento non sono del tutto chiare; tuttavia, un'esplicita spiegazione è fornita dal Ministro della giustizia austriaco. Quest'ultimo, infatti, in ragione della diversità di casi che possono presentarsi in concreto, preferisce affidarsi alle

[21] § 327q, comma 2, BGB.

[22] Art. 119-*ter*, comma 7 del *texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias* (Real Decreto Legislativo 1/2007).

[23] Art. 7:50ab(5), BW (draft). Si tratta ancora di una proposta: per maggiori informazioni, v. https://zoek.officielebekendmakingen.nl/kst-35734-2.html#d17e1566 (ultima consultazione: 5 dicembre 2021).

[24] Il d.lgs. n. 173/2021 si limita a riprodurre il disposto dell'art. 3, par. 8 della Direttiva all'interno del futuro art. 135-*novies*, comma 6 del Codice del consumo, con la sola aggiunta di riferimenti alle discipline nazionali in materia di protezione dei dati personali. È del tutto silente, invece, sulle conseguenze che un'eventuale revoca del consenso al trattamento dei dati personali produce sul contratto.

[25] B. ZÖCHLING-JUD, *Digital Consumer Contract Law And New Technologies. Implementation Of The Digital Content Directive In Austria*, in *JIPITEC*, 2021, p. 226. In realtà, il contributo dell'autrice si riferisce a quello che era il testo della proposta austriaca di recepimento della Direttiva 2019/770. Nel frattempo, è stata emanata la legge federale (v. *supra,* nt. 12) senza che si registrino modifiche sulla questione in esame.

[26] M. NAMYSŁOWSKA, A. JABŁONOWSKA, F. WIADEREK, *Implementation of Digital Content Directive in Poland: A fast ride on a tandem bike against the traffic*, cit., p. 247.

[27] La disciplina francese di recepimento della Direttiva 2019/770 (v. *supra,* nt. 16) non fa alcun riferimento alla revoca del consenso al trattamento dei dati personali da parte del consumatore.

[28] La normativa portoghese di attuazione della Direttiva 2019/770 (*Decreto-Lei n.° 84/2021 de 18 de outubro – Regula os direitos do consumidor na compra e venda de bens, conteúdos e serviços digitais, transpondo as Diretivas (UE) 2019/771 e (UE) 2019/770*) non contiene specifiche indicazioni sul punto.

[29] I. KULL, *Transposition of the Digital Content Directive (EU) 2019/770 Into Estonian legal system*, cit., p. 255.

decisioni *case-by-case* della giurisprudenza, che sarà chiamata a compiere un bilanciamento degli interessi in gioco applicando i principi generali sul contratto [30]. È indubbio, però, che una soluzione del genere si ponga in aperto contrasto con le esigenze di certezza dei rapporti negoziali.

Tra gli ordinamenti che invece hanno deciso di intervenire con regole *ad hoc*, può ravvisarsi una discreta somiglianza delle soluzioni adottate. Ad esempio, sia la Germania (§ 327q, comma 2, BGB) che la Spagna (art. 119-*ter*, comma 7, Real Decreto Legislativo 1/2007) prevedono la facoltà per il professionista di recedere dal contratto di fornitura di contenuti o servizi digitali, una volta che il consumatore eserciti la revoca del consenso al trattamento dei dati personali. Inoltre, in entrambi gli ordinamenti tale facoltà riguarda soltanto i contratti nei quali la fornitura sia continua o consista in una serie di singoli atti, e comunque il professionista non può unire alla risoluzione del contratto una richiesta di risarcimento del danno eventualmente subito, escludendo in tal modo che la revoca del consenso possa essere paragonata ad un inadempimento contrattuale. Parzialmente diversa è l'impostazione adottata dal legislatore olandese, il quale non attribuisce una facoltà di recesso al professionista, bensì sembra ricondurre un effetto risolutorio del contratto direttamente alla revoca del consenso al trattamento da parte del consumatore [31].

Per quanto concerne l'ordinamento italiano, la mancanza di specifiche indicazioni del legislatore non può essere accolta con favore per le ragioni che seguono. Basandosi sulle norme vigenti, a fronte di un'operazione economica che vede instaurarsi una corrispettività, quanto meno indiretta, tra la fornitura dei contenuti o servizi digitali e la fornitura dei dati personali, la revoca del consenso al trattamento di questi ultimi può essere in qualche modo assimilata ad una impossibilità sopravvenuta parziale della prestazione, con conseguente applicazione analogica dell'art. 1464 c.c. Così facendo, si consentirebbe al professionista di ottenere una corrispondente riduzione della prestazione dovuta o di recedere dal contratto dimostrando l'assenza di un interesse apprezzabile nei confronti di un trattamento parziale dei dati personali del consumatore, vale a dire il (solo) trattamento svolto prima della revoca del consenso. Si tratta, tuttavia, di un'operazione ermeneutica sulla quale non tutti gli interpreti potrebbero convenire. Invero, dinanzi alla presente lacuna, l'applicazione dell'art. 1464 c.c. potrebbe risultare a taluni forzata, posto che per ravvisare l'*eadem ratio*, il caso simile che giustificherebbe l'attivazione della regola in

[30] È quanto riporta B. ZÖCHLING-JUD, *Digital Consumer Contract Law and New Technologies*, cit., p. 226 ss.

[31] «*The withdrawal of consent thus implies unilateral termination of the digital content contract*»: così, a proposito della proposta del nuovo art. 7:50ab(5), BW, M.B.M. LOOS, *The (Proposed) Transposition Of The Digital Content Directive In The Netherlands*, cit., p. 239.

questione non dovrebbe essere imputabile al contraente debitore, al pari dell'impossibilità sopravvenuta per cui è prevista la norma[32]. Nel caso della revoca del consenso al trattamento dei dati personali, è evidente che così non è. D'altronde, in assenza di un'esplicita previsione legislativa, è difficile ammettere che una delle parti – nel caso di specie, il consumatore che revoca il consenso al trattamento dei dati – possa alterare *volontariamente* il sinallagma contrattuale senza subire alcuna conseguenza negativa. Il dettato dell'art. 7, par 3, RGPD, tuttavia, impedisce che il consumatore possa subire pregiudizi a seguito dell'esercizio della revoca del consenso al trattamento e, allora, l'unica via per l'interprete appare la ricostruzione della regola (l'effetto contrattuale *post*-revoca) tramite un'*analogia iuris* che espone all'incertezza. Per rendersi conto di ciò, basterebbe riflettere sulla circostanza che l'ordinamento tedesco e l'ordinamento spagnolo, pur prevedendo una disciplina piuttosto simile, presentano comunque condizioni di ricorso al recesso, da parte del professionista, lievemente differenti. Mentre in Spagna è immediato a seguito della revoca del consenso al trattamento, in Germania il professionista può recedere senza osservare un termine di preavviso se, tenendo conto della portata del trattamento dei dati che continua ad essere ammissibile e ponderando gli interessi di entrambe le parti, è ragionevole interrompere il rapporto contrattuale prima della scadenza del contratto o prima della scadenza dell'eventuale termine di preavviso.

5. (Segue) *Le conseguenze dell'invalidità del consenso al trattamento dei dati personali: una questione negletta*

Alla luce di quanto sopra, si è preso coscienza che i dispositivi di protezione dei dati personali possono avere delle ripercussioni sul contratto nel quale la prestazione caratterizzante del professionista è strettamente collegata alla facoltà dello stesso di trattare, a fini commerciali, i dati personali del consumatore. Come si è visto, l'attenzione della Direttiva 2019/770 si è soffermata sugli effetti della revoca del consenso al trattamento con la chiamata in causa dei legislatori nazionali; tuttavia, vi sono altre vicende giuridiche che meritano una simile considerazione. Per lo stesso motivo in base al quale è rilevante la revo-

[32] A proposito dell'impossibilità parziale che produce gli effetti "alternativi" di cui all'art. 1464 c.c., si fa notare che essa deve essere «*naturalmente "sopravvenuta", "definitiva" e "precedente l'inadempimento"*» (S. PAGLIANTINI, *sub* art. 1464, in E. NAVARRETTA, A. ORESTANO (a cura di), *Dei contratti in generale*, Torino, 2011, IV, p. 577), ove con quest'ultima espressione può intendersi anche "non imputabile".

ca del consenso, è altrettanto significativa la sua invalidità. In ragione delle condizioni che tale tipologia di consenso deve soddisfare ai sensi degli artt. 4, n. 11, e 7, RGPD, non è certo improbabile che il consenso al trattamento dei dati rilasciato dal consumatore risulti affetto da vizi. Invero, se esso non si presenta libero, specifico, informato ed inequivocabile, non potrà dirsi validamente prestato, con la conseguenza che non potrà costituire la base giuridica per il trattamento commerciale dei dati personali da parte del professionista.

Nonostante l'evidente impatto che un consenso invalido *ab origine* può avere sul contratto in esame, al pari di un consenso revocato in corso d'opera, la questione è pressoché ignorata dai diritti derivati nazionali[33]. A dire il vero, però, un autore olandese riferisce che l'*Autoriteit Persoonsgegevens* ha sollevato la questione al governo in sede di preparazione della disciplina di recepimento della Direttiva 2019/770, suggerendo di introdurre «*the possibility for the consumer to invoke avoidance of the contract*»[34]. Il governo dei Paesi Bassi non ha accolto la proposta trincerandosi dietro l'argomento che l'atto di attuazione della Direttiva 2019/770 ha un ambito di applicazione circoscritto e non è adatto, dunque, a regolare aspetti di diritto contrattuale generale. Tale risposta, in realtà, dimostra in modo ancor più efficace quanto fosse opportuno un recepimento della Direttiva 2019/770 in una cornice normativa transtipica.

Al di là di ciò, e di quali saranno le (verosimilmente diverse) soluzioni nazionali sulla base delle rispettive strutture dogmatiche in tema di validità ed efficacia del contratto[35], è opportuno sottolineare un ulteriore profilo problematico. La difficoltà di regolare le conseguenze contrattuali di un'invalidità

---

[33] Il § 327q, comma 1, BGB afferma che la validità del contratto non è pregiudicata né dall'esercizio dei diritti di protezione dei dati personali, né dalla presentazione di dichiarazioni di protezione dei dati da parte del consumatore. Non appare chiaro, tuttavia, se tale disposizione si riferisca anche ad una dichiarazione di consenso al trattamento dei dati affetta da invalidità.

[34] M.B.M. LOOS, *The (Proposed) Transposition Of The Digital Content Directive In The Netherlands*, cit., p. 237.

[35] Si consideri, ad esempio, che nella dottrina tedesca è sostenuta la tesi in base alla quale l'invalidità del consenso al trattamento dei dati personali non dovrebbe influenzare la validità del contratto, e viceversa. Tale tesi, tuttavia, si poggia su una specifica struttura dogmatica interna, vale a dire l'*Abstraktionsprinzip*. In proposito, v. A. METZGER, *A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance – Contract Law 2.0?*, Baden-Baden, 2020, p. 33 s.; M. SCHMIDT-KESSEL, *Consent for the Processing of Personal Data and its Relationship to Contract*, in A. DE FRANCESCHI, R. SCHULZE (eds.), *Digital Revolution – New Challenges for Law. Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies, Blockchain Technology and Virtual Currencies,* München, Baden-Baden, 2019, p. 81 ss.

del consenso al trattamento dei dati personali è accresciuta, anche rispetto alle conseguenze della revoca, dal fatto che le cause di tale invalidità possono essere molteplici e non è chiaro se esse soggiacciono al medesimo regime, quanto meno sul piano delle ripercussioni che generano sul contratto. Orbene, una serie di quesiti può rendere più pregnante la questione evocata. Un consenso invalido perché disinformato è paragonabile ad un consenso invalido perché equivocabile o aspecifico, o un ad un consenso invalido perché prestato senza i requisiti minimi di libertà, o ancora ad un consenso invalido in quanto espresso da un minore di età inferiore a quella minima prevista dall'art. 8, RGPD o, in deroga consentita, dagli ordinamenti nazionali? [36] In altri termini, in questi casi la conseguenza contrattuale sarà la stessa? E ancora: l'invalidità frutto di una violazione commessa dal professionista (ad es., consenso disinformato o coartato) è assimilabile all'invalidità dettata da fattori esterni alla sfera del medesimo soggetto (ad es., consenso rilasciato da un minore)?

A fronte di simili interrogativi tuttora aperti [37], può osservarsi che è pur sempre nella facoltà degli Stati membri individuare le (eventualmente variegate) ricadute contrattuali, tuttavia è anche vero che la creazione di regimi diversi per *le invalidità* del consenso al trattamento dei dati potrebbe leggersi come un'illecita incursione nell'area di competenza dell'Unione europea, che ha scelto uno strumento molto rigido come il Regolamento per disciplinare gli aspetti generali della protezione dei dati personali, inclusa naturalmente la regolazione del consenso al trattamento [38]. È lecito attendersi, quindi, un dialogo (multivello) tra le corti sempre più fitto anche con riguardo alle questioni fin qui delineate, con la speranza che risultino più nitidi i confini di eurocompatibilità delle possibili soluzioni nazionali [39].

---

[36] Si tenga conto che in base alle Linee-guida dell'European Data Protection Board (EDPB), gli elementi che determinano un'invalidità del consenso al trattamento dei dati personali non vengono differenziati sul piano disciplinare. Come effetto comune a qualsiasi ipotesi di consenso invalido, si prevede (soltanto) che «*il titolare del trattamento non può passare dal consenso ad altre basi legittime [, in particolare] non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso*»: EDPB, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, 4 maggio 2020, p. 28.

[37] Si è cercato di offrire un tentativo di risposta in G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, cit., p. 176 ss.

[38] Un'attenta dottrina nota, infatti, che «*in the relationship between contract and consent one has to take into account the fact that consent is regulated at the EU-level, which – at least, in case of conflict – prevails over national law and national dogmatic structures*»: M. SCHMIDT-KESSEL, *Consent for the Processing of Personal Data and its Relationship to Contract*, cit., p. 77.

[39] Sul dialogo tra le corti in merito al consenso, v. T. POLVANI, *Il consenso alla cessione dei dati personali nel dialogo tra le corti*, in questo volume.

6. (Segue) *L'esercizio dei diritti dell'interessato durante il rapporto contrattuale: poche luci e molte ombre*

L'art. 3, par. 8, della Direttiva sui contratti di fornitura di contenuti e servizi digitali è molto netto nello stabilire che il diritto dell'Unione in materia di protezione dei dati personali è fatto salvo, a tal punto che prevale sulle disposizioni della Direttiva in caso di conflitto. È pacifico, dunque, che il consumatore, che fornisce dati personali al professionista, non può essere privato di alcuno dei diritti di cui gode in qualità di interessato al trattamento dei dati. Infatti, il considerando 38 precisa che la Direttiva, oltre a non alterare le condizioni di liceità del trattamento dei dati personali e quelle di validità del relativo consenso, non pregiudica nemmeno l'esercizio dei diritti dell'interessato, riportando gli esempi della cancellazione e della portabilità dei dati personali (artt. 17 e 20, RGPD). Tali diritti si applicano anche in caso di risoluzione del contratto da parte del consumatore, con l'art. 16, par. 2, che rafforza il concetto imponendo all'operatore economico – in sede di risoluzione – di rispettare gli obblighi applicabili a norma del RGPD. Da quest'ultima disposizione è interessante notare come emerga (implicitamente) un cumulo congiunto di diritti-rimedi: la risoluzione del contratto, da un lato, e la cancellazione o portabilità dei dati personali, dall'altro.

Non deve comunque dedursi che il consumatore, interessato al trattamento, possa esercitare i diritti di protezione dei dati nel solo momento risolutorio; l'esercizio dei diritti può certamente avvenire anche durante lo svolgimento del rapporto contrattuale, al solo ricorrere delle condizioni previste dal RGPD. Sul piano delle ricadute negoziali, il maggiore interesse volge ancora una volta verso la cancellazione e la portabilità dei dati, ma anche verso la limitazione del trattamento e l'opposizione allo stesso (artt. 18 e 21, RGPD). Si presentano, invece, piuttosto ininfluenti il diritto di accesso e il diritto di rettifica (artt. 15 e 16, RGPD), posto che essi non incidono sulla portata del trattamento da parte del professionista.

Prima di interrogarsi sulle sorti del contratto, suscettibili di variazione in ragione dei diritti sopra indicati, è necessario chiarire quali sono le condizioni per la proposizione degli stessi diritti. A tal riguardo, preme innanzitutto sottolineare che mentre la cancellazione dei dati e la limitazione del trattamento possono essere chieste a prescindere dalla base giuridica su cui si fonda il trattamento, la portabilità dei dati e l'opposizione al trattamento hanno un ambito di applicazione circoscritto ai trattamenti che si fondano solo su alcune basi giuridiche. In particolare, l'art. 20 RGPD concerne i trattamenti che si basano sul consenso o su un contratto; l'art. 21 RGPD, invece, presuppone che il trattamento si basi sul perseguimento di un legittimo interesse del titolare oppure

sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare.

Risulta, a questo punto, fondamentale individuare qual è la base giuridica del trattamento che sorregge la fornitura dei dati personali del consumatore nell'ambito della Direttiva 2019/770. Si può facilmente escludere la base giuridica di cui all'art. 6, par. 1, lett. e), RGPD, posto che l'operatore economico che fornisce un contenuto o servizio digitale chiaramente non richiede al consumatore di fornire dati personali per eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Inoltre, in considerazione dell'art. 3, par. 1, primo cpv., Direttiva 2019/770, che non ammette l'applicazione della Direttiva in questione laddove i dati del consumatore siano trattati dall'operatore economico esclusivamente per fornire il contenuto o il servizio digitale, può altresì escludersi – implicitamente – la base giuridica di cui all'art. 6, par. 1, lett. b), RGPD. Resterebbero così in campo le basi giuridiche del consenso e del legittimo interesse del titolare. Come si è evidenziato sopra, mentre la prima funge da presupposto per l'esercizio del diritto alla portabilità dei dati, la seconda svolge la medesima funzione per l'esercizio del diritto di opposizione al trattamento.

Orbene, pur nutrendo seri dubbi sull'effettiva possibilità di invocare il legittimo interesse del professionista per sfruttare i dati del consumatore a scopi commerciali [40], in questa sede si può anche ammetterla al solo fine di interrogarsi sull'eventuale conseguenza contrattuale di un'opposizione al trattamento *ex* art. 21 RGPD. Quest'ultima, infatti, è pressoché assimilabile – in termini effettuali – ad una revoca del consenso e possono quindi replicarsi i discorsi fatti in precedenza con riguardo all'alterazione del sinallagma negoziale. Tuttavia, a differenza dell'attenzione dedicata alla revoca del consenso al trattamento (indubbiamente influenzata da quanto previsto dal considerando 40 della Direttiva 2019/770), gli ordinamenti nazionali hanno finora trascurato le conseguenze di un'opposizione al trattamento. L'eccezione (positiva) è rappresentata anche in questo caso dal legislatore tedesco, che all'art. 327q, comma 2, BGB ha opportunamente equiparato revoca ed opposizione in termini di ripercussione sul contratto, consistente – come si è già visto – nella facoltà di recesso attribuita all'operatore economico. Ad ogni modo, nelle discipline nazionali che nulla prevedono, si può sopperire alla lacuna estendendo analogicamente la regola dettata (o ricostruita a livello interpretativo) per la revoca del consenso al trattamento dei dati, considerata la similitudine tra le due fattispecie.

Incertezze maggiori si pongono con riguardo alle conseguenze degli altri

[40] Sul punto, sia consentito rinviare a G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, cit., pp. 172-174.

diritti dell'interessato, anch'esse del tutto ignorate dai diritti derivati nazionali. Si supponga, ad esempio, che durante lo svolgimento del contratto il consumatore richieda al professionista di trasmettere i propri dati personali (trattati con mezzi automatizzati) a un altro titolare del trattamento. Si badi bene che la portabilità non implica automaticamente la revoca del consenso e la conseguente sospensione del trattamento dei dati da parte del professionista (v. considerando 68 RGPD). È dubitabile, dunque, che la richiesta della portabilità dei dati da parte del consumatore conduca ad uno scioglimento del contratto con il professionista, il quale peraltro, potendo ancora trattare i dati del consumatore, non può vedersi riconosciuta la facoltà di recedere. Si pensi, poi, all'ipotesi in cui il professionista tratti illecitamente i dati del consumatore, facendo sì che quest'ultimo richieda la cancellazione di tali dati (art. 17, par. 1, lett. d), RGPD) o la limitazione del trattamento (art. 18, par, 1, lett. b), RGPD). In tal caso, è ancor meno giustificabile un recesso del professionista, posto che le restrizioni nel trattamento hanno origine in suo comportamento illecito. Piuttosto, qualificando il trattamento illecito dei dati personali come una causa di non conformità del contratto [41], dovrebbe essere il consumatore a poter richiedere la risoluzione.

Vista l'eterogeneità delle fattispecie che possono presentarsi, è oltremodo evidente quanto sarebbe stato opportuno un chiarimento dei legislatori nazionali sul piano degli effetti contrattuali. Sul punto, a dire il vero, anche la normativa tedesca – senz'altro la più completa in confronto alle altre discipline di recepimento della Direttiva 2019/770 – è parca di indicazioni, limitandosi ad affermare che l'esercizio dei diritti dell'interessato non pregiudica la validità del contratto di fornitura del contenuto o servizio digitale (§ 327q, comma 1, BGB).

Per di più, tra i diritti dell'interessato, pur non essendo ricompreso nel Capo III del RGPD, rientra anche il diritto al risarcimento del danno subito a seguito di una violazione del Regolamento UE 2016/679 (art. 82 RGPD). A tal proposito, in realtà, non importa tanto definire le conseguenze contrattuali di un risarcimento di tal genere, quanto piuttosto la combinazione di quest'ultimo con i rimedi a disposizione del consumatore (ripristino della conformità del contratto e risoluzione), quando la non conformità derivi da un trattamento illecito dei dati personali. Non si può comunque pensare di affidare (anche) quest'ultima questione ai legislatori nazionali; d'altra parte, quando i rimedi che si cumulano sono tutti di conio europeo, la competenza non può che essere della stessa Unione, la quale avrebbe potuto certamente sforzarsi di più nel

[41] In tal senso si pongono anche i nuovi artt. L. 217-6 e L. 224-25-15 del *Code de la consommation*.

regolare i rapporti tra il diritto consumeristico e il diritto in materia di protezione dei dati personali.

7. *Conclusioni*

Dai paragrafi precedenti può evincersi che il confronto svolto tra le discipline nazionali di attuazione della Direttiva 2019/770, avente ad oggetto il rapporto tra dati personali del consumatore e contratto, non è stato semplice. Il principale scoglio è stato di ordine temporale, visto che gran parte degli Stati membri ha recepito la Direttiva in ritardo rispetto al termine previsto dal legislatore europeo (il 1° luglio 2021). Un ulteriore limite ha riguardato lo stesso contenuto degli interventi normativi, i quali non hanno dedicato particolare attenzione alle questioni riguardanti lo scambio contrattuale tra la fornitura di contenuti/servizi digitali e la fornitura di dati personali del consumatore. Ciononostante, le informazioni raccolte sembrano comunque sufficienti per designare un primo quadro della situazione.

Rispetto alle tematiche sopra selezionate, sembrano emergere due modelli normativi: l'uno – di marca tedesca – propenso a fornire una serie di indicazioni puntuali, seppur talvolta sintetiche, in sede legislativa; l'altro – non ascrivibile ad uno specifico ordinamento – proclive ad affidare la risoluzione delle questioni più spinose all'interpretazione dei principi generali, che inevitabilmente coinvolge la sede giurisprudenziale. A questo secondo modello appartiene un gruppo eterogeneo di Stati membri: vi rientrano, infatti, sia quelli che, dopo aver riflettuto, hanno ritenuto preferibile astenersi dalla definizione di regole *ex ante* in considerazione della fluidità delle fattispecie concretamente verificabili (emblematica in tal senso la posizione del Ministro della giustizia austriaco in merito alle ripercussioni negoziali della revoca del consenso al trattamento dei dati personali[42]), sia quegli altri la cui astensione è riconducibile con maggiore probabilità ad una mancanza di zelo nel legiferare.

Ad ogni modo, a prescindere dalle ragioni che possono spiegare l'atteggiamento degli ordinamenti che hanno sposato il secondo modello normativo, affiora l'impressione di un'occasione persa per questi legislatori nazionali, i quali avrebbero potuto approfittare del recepimento della Direttiva 2019/770 per regolare in modo più compiuto gli aspetti contrattuali della circolazione dei dati personali. Al contempo, peraltro, non può negarsi che lo stesso legislatore europeo, per quanto indubbiamente innovatore nell'introdurre una

[42] V. *supra* nt. 30.

norma come quella di cui all'art. 3, par. 1, primo cpv., della Direttiva in esame, è stato fin troppo sibillino nel definire le relazioni tra il diritto dei consumatori e il diritto sulla protezione dei dati personali, ambito nel quale gli Stati membri hanno ben pochi margini di manovra. La negatività di tali rilievi può essere comunque compensata osservando che la regolazione dell'economia dei dati è ancora in divenire: si vedano, ad esempio, le proposte del Regolamento *e-Privacy* e del *Data Governance Act*, oltre ai propositi di una futura legge sui dati[43]. In questo quadro di riforme europee, cresce allora l'auspicio che nei prossimi anni si avvii una riflessione anche in vista di un (primo) *restyling* del RGPD, al fine precipuo di fornire indicazioni che indirizzino in modo più chiaro il coordinamento dello stesso RGPD con le diverse aree del diritto privato patrimoniale, ove sempre più spesso si intrecciano i fili della legalità inter-ordinamentale composta dal livello nazionale ed unionale.

[43] Commissione europea, *Una strategia europea per i dati*, 19 febbraio 2020, COM(2020) 66 final, p. 15 ss.

PARTE V

AL DI LÀ DELLA "GRANDE DICOTOMIA" PUBBLICO-PRIVATO

SOLIDARIETÀ DIGITALE E CONDIVISIONE DEI DATI TRA PUBBLICO E PRIVATO

di *Matteo Giannelli*

SOMMARIO: 1. Premessa. Solidarietà, doveri e pandemia. – 2. Società digitale e solidarietà: un rapporto in via di definizione. – 3. Tra pubblico e privato: il percorso italiano della solidarietà digitale e i suoi inconvenienti. – 4. Solidarietà digitale e cultura della condivisione: dimensione locale e dimensione globale. – 5. Verso l'"altruismo dei dati"?

1. *Premessa. Solidarietà, doveri e pandemia*

Nell'affrontare il tema delle nuove declinazioni del principio di solidarietà nella società digitale è necessario partire dalla constatazione che le conseguenze socioeconomiche della pandemia da SARS-CoV-2 abbiano creato disuguaglianze ed emarginazioni riguardanti, in primo luogo, soggetti di fatto già discriminati [1].

Durante il primo *lockdown* e nelle fasi immediatamente successive – come normalmente accade durante i periodi di emergenza – il principio di solidarietà è stato richiamato in più occasioni nella narrazione operata sia da parte dei pubblici poteri che dai principali mezzi di informazione [2]. Si è trattato, tuttavia, di un appello vago, in mera funzione anti-individualistica, limitato a forme di solidarietà *nel lockdown* e del tutto disinteressato a quanto ci fosse

[1] Cfr, da ultimo, i contributi contenuti nel volume A. PAJNO, L. VIOLANTE, *Biopolitica, pandemia e democrazia*. Rule of law *nella società digitale*, vol. II, *Etica, comunicazione e diritti*, Bologna, 2021, e, in particolare, A. SIMONCINI, *L'uso delle tecnologie nella pandemia e le nuove disuguaglianze*, p. 225 ss. Inoltre, sia consentito rinviare a M. GIANNELLI, *I doveri costituzionali e la sfida della pandemia: quale solidarietà digitale?*, p. 81 ss., le cui riflessioni sono sviluppate in questa sede.

[2] Sul ruolo di questi ultimi nella pandemia e sulla loro natura di poteri privati o sociali, v. G.E. VIGEVANI, *Sistema informativo e opinione pubblica al tempo della pandemia*, in *Quad. cost.*, 2020, p. 779 ss.

da realizzare *a seguito* del *lockdown*, correndo così il rischio di apparire come puramente ideologico.

Una riflessione giuridica sul «*risveglio della solidarietà*»[3] non può, dunque, prescindere, dalle dimensioni enunciate dall'art. 2 della Costituzione – solidarietà politica, economica e sociale – e da una conseguente e precisa individuazione dei diversi soggetti ai quali sono riferibili i doveri costituzionali[4]. Ciò equivale a chiedersi se le diseguaglianze emerse nel corso della pandemia impongano, o meno, un nuovo modo di pensare a questi, ben al di là di alcune, più o meno recenti, contrapposizioni tra "età dei diritti" ed "età dei doveri"[5].

Sul punto, peraltro, non si può fare a meno di riconoscere che nella storia repubblicana la cultura dei doveri – o, per alcuni, delle responsabilità – sia rimasta in secondo piano[6]. Il coordinamento sistematico tra diritti e doveri, infatti, è stato sviluppato solo in parte dalla giurisprudenza[7] e dalla dottrina costituzionalistica[8], anche se, negli ultimi anni, è possibile registrare una certa inversione di tendenza[9] con la pubblicazione di lavori volti innanzitutto a ricostruire i fondamenti teorici del principio solidaristico, la loro compatibilità con il tema dei diritti e, perfino, la necessità di una "ri-

[3] Per utilizzare l'espressione di E. MORIN, con la collaborazione di S. ABOUESSALAM, *Changeons de voie. Les leçons du coronavirus*, Paris, 2020, trad. it. R. Prezzo, *Cambiamo strada. Le 15 lezioni del coronavirus*, Milano, 2020, p. 33 ss.

[4] Evidenziato da A. MORELLI nei numerosi lavori dedicati al tema: da ultimo si veda l'editoriale *Doveri costituzionali e principio di solidarietà*, in *Dir. cost.*, 2/2019, p. 5 ss.

[5] Per una proposta di lettura dell'art. 2 che abbia come riferimento la considerazione che la "Repubblica dei doveri inderogabili" e la "Repubblica dei diritti inviolabili" sono due gambe dello stesso corpo, le quali o stanno insieme o vengono fatalmente meno entrambe cfr. M. FIORAVANTI, *Art. 2*, Bari, 2017, p. 22.

[6] Basti pensare a quanto affermato da Noberto Bobbio in un dialogo con Maurizio Viroli: "se avessi qualche anno, che non avrò, sarei tentato di scrivere L'età dei doveri", così in N. BOBBIO, M. VIROLI, *Dialogo intorno alla Repubblica*, Roma-Bari, 2001, p. 40.

[7] Su cui cfr. E. LONGO, *Corte costituzionale, diritti e doveri*, in F. DAL CANTO, E. ROSSI (a cura di), *Corte costituzionale e sistema istituzionale. Giornate di studio in ricordo di Alessandra Concaro*, Torino, 2011, pp. 339 ss.

[8] Lo nota M. OLIVETTI, *Diritti fondamentali*, Torino, 2018, p. 14.

[9] Per questa affermazione E. ROSSI, *Relazione introduttiva*, in F. MARONE (a cura di), *La doverosità dei diritti: analisi di un ossimoro costituzionale?*, Napoli, 2019, p. 9 ss., cui si rinvia per i numeri riferimenti bibliografici, anche risalenti (a partire da G. LOMBARDI, *Contributo allo studio dei doveri costituzionali*, Milano, 1967), che non è possibile riportare in questa sede. Sul versante della giurisprudenza della Corte costituzionale si segnala la sentenza n. 114/2019 in cui viene esplicitato il legame tra garanzia dei diritti e adempimento dei doveri («*nell'architettura dell'art. 2 Cost. l'adempimento dei doveri di solidarietà costituisce un elemento essenziale tanto quanto il riconoscimento dei diritti inviolabili di ciascuno*»).

scoperta" dei doveri per la vita democratica, in modo da dare nuova linfa al concetto di etica repubblicana [10].

L'individuazione dell'oggetto e della latitudine dei doveri rappresenta, dunque, un problema persistente. Un processo reso ancora più complesso dalla svalutazione e dalla conseguente crisi del principio di solidarietà su cui essi si fondano [11], specie alla luce di quei tentativi che sembrano confinarlo in un terreno meramente altruistico [12].

2. *Società digitale e solidarietà: un rapporto in via di definizione*

Uno degli obiettivi principali della dimensione costituzionale della solidarietà, nella sua congiunzione con l'eguaglianza, è rappresentato dall'inclusione. Un fine ancora più arduo da raggiungere in un mondo "dilatato", come quello emerso durante la pandemia, in cui alla relazione si è sostituita la connessione [13].

Proprio a partire da questo contesto muove la riflessione sulla solidarietà digitale come forma di relazionalità che implica un *diverso* modo di pensare ai doveri costituzionali e di reagire alle diseguaglianze.

Gli autori che hanno riflettuto in maniera sistematica sul concetto di solidarietà digitale e sulle sue possibili declinazioni sono partiti dalla considerazione che questa potesse rappresentare una delle direttrici su cui lavorare per creare una via d'uscita dalla crisi economica e, in particolare, dai suoi inevitabili riflessi sociali, capaci di confinare i singoli nelle proprie individualità [14].

Nel 2013 il sociologo Felix Stalder si è servito del sintagma solidarietà digitale legandolo alla nozione di condivisione e alla rivalutazione del concetto di beni comuni online ("*digital commons*") al fine di teorizzare una forma di in-

---

[10] Su cui. M. VIROLI, *Repubblicanesimo*, Roma-Bari, 1999.

[11] Così A. APOSTOLI, *La svalutazione del principio di solidarietà*, Milano, 2012, spec. p. 141 ss.

[12] Mette in luce il rapporto tra carità, assistenza e solidarietà S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014, p. 57 ss.

[13] Di nuovo A. SIMONCINI, *L'uso delle tecnologie nella pandemia e le nuove disuguaglianze*, cit., pp. 225-226.

[14] Inevitabile il confronto con il pensiero di Émile Durkheim per il quale un fattore cruciale della solidarietà è rappresentato dall'"effervescenza collettiva", ossia quel sentimento che si prova a far parte di un gruppo che ci porta fuori dalla nostra individualità. Cfr. É. DURKHEIM, *De la division du travail social*, Paris, 1893 (trad, it. F. Airoldi Namer, *La divisione del lavoro sociale*, Milano, 1971, p. 231 ss.).

terconnessione in grado di fornire un potenziale strutturale al concetto stesso di solidarietà [15]. Evgeny Morozov, per altro verso, ha ricordato che le stesse infrastrutture tecnologiche possono esser utilizzate per creare democrazia o consumo, citando, a tal proposito, l'esempio della Cina dove il *Social Credit System* promuove la convivenza sociale con regole in linea con il controllo statale [16]. Morozov sottolinea come le disuguaglianze siano accentuate dai giganti digitali, ragion per cui risulta necessario trovare il modo per democratizzare la *ricchezza* e ridare slancio al ruolo dello Stato: il rischio che si corre, altrimenti, è quello di un'esplosione sociale causata dagli squilibri creati a livello globale dal mondo digitale [17].

Particolarmente significative sono anche le riflessioni sulle città come laboratori digitali per la democrazia e la sostenibilità, pur nella consapevolezza dell'impossibilità di una soluzione locale a problemi nazionali e globali. Un modello che, in ogni caso, appare in grado di formare reti e coalizioni sociali attraverso la sperimentazione di una serie di tecnologie che consentano la gestione di alcune politiche pubbliche (da quelle riguardanti i trasporti pubblici fino alle questioni abitative, passando per la sanità e l'istruzione) in una logica di solidarietà. Una simile declinazione del concetto di *smart cities*, dunque, potrebbe essere un veicolo attraverso cui istituzionalizzare forme di solidarietà anzitutto economica ma, allo stesso tempo, un'occasione per «mantenere la promessa di ridare alle città una dimensione adatta alle persone, e ciò significa anche democratizzare la proprietà e l'accesso alle tecnologie digitali» [18].

---

[15] F. STALDER, *Digital solidarity*, London, 2013, spec. p. 31 ss.

[16] Risale al 2011 il contributo in cui il sociologo bielorusso aveva constatato l'assenza di virtù palingenetiche della rete ed espresso le sue posizioni critiche, cfr. E. MOROZOV, *The Net Delusion: The Dark Side of Internet Freedom*, New York, 2011. Sull'esperienza cinese v. L. ORGAD, W. REIJERS, *How to Make the Perfect Citizen? Lessons from China's Model of Social Credit System* in *Robert Schuman Centre for Advanced Studies Research Paper* No. RSCAS 2020/28, disponibile in SSRN: https://ssrn.com/abstract=3586503.

[17] E. MOROZOV, *Digital Socialism? The Calculation Debate in the Age of Big Data*, in *New Left Review*, 116/117, March-June, 2019, p. 33 ss., spec. 54. Di recente cfr. ID., *The tech 'solutions' for coronavirus take the surveillance state to the next level*, in *The Guardian*, 15 April 2020.

[18] Così il Rapporto sull'investimento delle infrastrutture sociali in Italia (ricerca coordinata da E. TREVIGLIO), *Rilanciare le infrastrutture sociali in Italia*, promosso dalla Fondazione ASTRID e dalla Fondazione Collegio Carlo Alberto della Compagnia di San Paolo, e in particolare il par. 5.5 dedicato al caso di studio Barcellona. Sul punto v. anche F. BRIA, E. MOROZOV, *Rethinking the Smart City. Democratizing Urban Technology*, New York, 2018; con riferimento alla teoria del nudge, S. RANCHORDÁS, *Nudging Citizens through Technology in Smart Cities*, in *International Review of Law, Computers & Technology*, Vol. 33, 2019, Disponibile in SSRN: https://ssrn.com/abstract=3333111.

Al termine di questa breve rassegna, dovrebbe risultare evidente, che, pur nelle molteplici e possibili declinazioni, l'eventualità di riconoscere una dimensione giuridica vincolante al concetto di solidarietà digitale si connette, inscindibilmente, con l'individuazione dei destinatari di tale dovere [19]. Il tema è stato affrontato dal punto di vista giuridico – e, dunque, della sua capacità di tradursi in precise regole all'interno di singole disposizioni legislative o altre fonti – con riferimento ai rapporti tra privati che si realizzano nell'ambito degli *Smart contracts*, dove si è sostenuto che la solidarietà contrattuale deve lasciare spazio alla solidarietà digitale, idonea anzitutto a ricreare una forma di relazione tra i soggetti coinvolti [20].

Da un punto di vista di diritto costituzionale è, in primo luogo, necessario ricostruire i termini del rapporto tra pubblico e privato: è evidente che il ruolo primario dello Stato non potrà fare a meno di relazionarsi con le grandi società transnazionali.

La solidarietà digitale si traduce, infatti, in un principio capace di rivolgersi sia ai poteri pubblici sia, soprattutto, ai poteri privati. Se i primi, sia a livello nazionale che sovranazionale, possono – anzi devono – porre in essere delle azioni che abbiano come obiettivo primario il superamento il *digital divide* e la realizzazione delle condizioni per una vera e propria cittadinanza digitale, più incerti sembrano i contenuti giuridici degli obblighi di cui possono esser destinatari i secondi.

Tuttavia, sono proprio questi ultimi, in quanto detentori dei dati, a poter dare un contributo imprescindibile per il raggiungimento delle medesime finalità di interesse pubblico, in un'ottica capace di richiamare la dimensione orizzontale della sussidiarietà. In altre parole, la trasformazione digitale della società, unitamente al suo carattere trasversale rispetto a prospettive di regolazione sia nazionali che sovranazionali, richiede un cambio di paradigma anche rispetto ai soggetti destinatari dei doveri.

---

[19] Nella consapevolezza che l'impostazione legislativa dei doveri non esaurisca la sfera della solidarietà: per il riferimento alla dimensione costituzionale della "solidarietà spontanea" cfr. F. GIUFFRÈ, *I doveri di solidarietà sociale*, in R. BALDUZZI, M. CAVINO, E. GROSSO, J. LUTHER, *I doveri costituzionali: la prospettiva del Giudice delle leggi*, Torino, 2007, p. 42.

[20] F. GHODOOSI, *Digital Solidarity: Contracting in the Age of Smart Contracts*, September 7, 2019. Disponibile in SSRN: https://ssrn.com/abstract=3449674; che rinvia allo studio di D. MARKOVITS, *Arbitration's Arbitrage: Social Solidarity at the Nexus of Adjudication and Contract*, in *DePaul Law Review*, vol. 59, 2010, p. 431 ss.

3. *Tra pubblico e privato: il percorso italiano della solidarietà digitale e i suoi inconvenienti*

L'interpretazione che intendeva come destinatario dell'obbligo di solidarietà il solo potere statale deve oramai ritenersi superata[21]. Tale obbligo, che si concreta, innanzitutto, in una rimozione degli ostacoli digitali, non riguarda esclusivamente lo Stato, e le sue articolazioni, ma concerne tutti i soggetti e gli operatori coinvolti nell'utilizzo di tecnologie e servizi digitali, a partire dalle grandi multinazionali dell'innovazione tecnologiche (le c.d. Big Tech). Queste realtà sono, infatti, potenze economiche e digitali sempre più capaci di determinare e di orientare politiche, stili di vita e di lavoro, condizioni culturali e sociali.

Il rapporto che si verrà a creare tra questi poteri non dovrà, tuttavia, assumere le forme della beneficenza e generosità, da un lato, e della riconoscenza, dall'altro. Una simile costruzione del legame tra pubblico e privato si rinviene, invece, nel concetto di "solidarietà digitale" promosso, o per meglio dire *pubblicizzato*, dal Ministero per l'Innovazione tecnologica e la digitalizzazione italiano a partire dalla prima fase della pandemia nella primavera del 2020.

Questa iniziativa, che assumeremo come paradigmatica, ci aiuta a riflettere sul rapporto tra gratuità e solidarietà, tra spirito di liberalità e lo spirito di solidarietà e, in definitiva, sull'«agire non egoistico come deviazione da un modello di comportamento non razionale»[22]. Con essa i grandi monopoli privati (Amazon, Microsoft, Google, ecc.) offrono, attraverso una piattaforma pubblica[23], dei contenuti e dei servizi che sono solo apparentemente gratuiti, ma che, in realtà, rappresentano un'importante occasione di raccolta e utilizzo dei dati, per di più in ambiti cruciali – basti pensare alle cinque categorie individuate: connettività, *e-learning*, *smart working*, informazione e svago, supporto ai cittadini[24] – e senza la consapevolezza necessaria da parte degli utenti coinvolti.

In sintesi, si è trattato di un tentativo meritevole di attenzione dal punto di vista meramente formale della collaborazione tra istituzioni pubbliche e sog-

---

[21] Ci si sofferma con attenzione G. SCOTTI, *Alla ricerca di un nuovo costituzionalismo globale e digitale: il principio di solidarietà "digitale"*, in *Forum di Quad. Cost.*, 2, 2021, p. 415 ss.

[22] Sul punto v. G. RESTA, *Gratuità e solidarietà: fondamenti emotivi e irrazionali*, in *Rivista critica del diritto privato*, 2014, p. 39 ss.

[23] Consultabile al link: https://solidarietadigitale.agid.gov.it/.

[24] Per un'analisi dei contenuti e dei servizi cfr. P. ZUDDAS, *Covid-19 e* digital divide*: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio AIC*, 3/2020, p. 302 ss.

getti privati durante il *lockdown*. Il rapporto tra solidarietà privata e solidarietà pubblica, infatti, si pone come tema centrale, anche alla luce, della formulazione dell'art. 118 della Costituzione che ha aperto nuovi e inediti spazi per quanto riguarda la realizzazione di doveri inderogabili nell'ambito di talune attività di interesse generale[25].

Il principio di solidarietà, tuttavia, anche qualora si tratti di una solidarietà digitale, richiede primariamente un'azione positiva delle istituzioni pubbliche, nella specifica prospettiva dell'art. 3, comma 2, della Costituzione, che sia in grado di orientare e determinare la formazione di una serie di regole giuridiche, provenienti anche da soggetti privati. Per questa ragione, di pari passo con la promozione dei servizi offerti, il Governo italiano avrebbe dovuto stipulare, specie in assenza di codici deontologici, alcuni protocolli capaci di individuare e tutelare i dati sensibili delle persone, delle istituzioni e delle imprese coinvolte. È interessante notare come, al contrario, non vi fosse traccia di questi aspetti: alle aziende interessate veniva richiesto, in un'ottica di carattere puramente commerciale, di eliminare l'obbligo di rinnovo al termine del periodo dell'offerta (la cui descrizione non doveva esser redatta «in tono promozionale»), la diffusione della stessa su tutto il territorio nazionale, o su una o più regioni, e la creazione di un canale di adesione appositamente dedicato all'iniziativa[26].

4. *Solidarietà digitale e cultura della condivisione: dimensione locale e dimensione globale*

La solidarietà digitale potrà, dunque, tradursi in un veicolo di regolazione solo qualora si dimostri capace di assumere un contenuto giuridico che de-

---

[25] Così G. TARLI BARBIERI, *Doveri inderogabili*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 2072.

[26] Solo nella c.d. "fase 2" della solidarietà digitale – in cui la richiesta si è concentrata sulla ripartenza delle attività didattiche attraverso l'offerta di soluzioni innovative e servizi digitali a supporto dell'istruzione scolastica – sono stati definiti dei requisiti di partecipazione maggiormente stringenti: nell'allegato all'Avviso pubblico diffuso dal Ministero per l'Innovazione tecnologica e la digitalizzazione erano contenuti requisiti di partecipazione che facevano riferimento ai concetti di "sicurezza, affidabilità, scalabilità e conformità alle norme sulla protezione dei dati personali, nonché divieto di utilizzo a fini commerciali e/o promozionali di dati, documenti e materiali di cui gli operatori di mercato entrano in possesso per l'espletamento del servizio". Cfr. https://innovazione.gov.it/assets/docs/Didattica_Digitale_Avviso_Manifestazione_interesse_2020_09_28.pdf e https://innovazione.gov.it/assets/docs/Allegato%20A_Avviso__Pubblico_DidatticaDigitale.pdf.

termini, innanzitutto, nuove forme di partecipazione. Una solidarietà non fine a sé stessa, solitaria, ma determinata a creare fiducia reciproca e a incidere sulla declinazione attuale del concetto stesso di cittadinanza [27].

Da più parti, spesso in maniera retorica, si è sottolineato che, una volta superata la pandemia da Covid-19, non si potranno e non si dovranno ripetere le azioni passate. I termini di questo cambiamento, tuttavia, non sono stati chiariti, rimanendo vaghi e indefiniti.

Un'inversione di rotta sarà possibile, innanzitutto, attraverso una politica europea delle reti capace non solo di contrastare e regolare efficacemente il dilagare delle piattaforme digitali c.d. *Over The Top* [28] ma anche di porre una grande questione di controllo democratico sull'accesso ai dati e una finalità sociale delle tecnologie digitali [29]. Temi che sembrano attualmente assenti nel dibattito pubblico [30] e che, invece, sono stati richiamati dal Garante europeo per la protezione dei dati personali nel piano strategico per il quadriennio 2020-2024 [31]. Il paradosso della solidarietà digitale è, infatti, messo in luce dall'esperienza cinese, già richiamata, del *Social credit system*, dove l'accesso alla rete è sintomo di controllo sociale.

Negli ambiti chiave dell'istruzione e del lavoro, in cui si sono verificati le disuguaglianze più evidenti, la solidarietà digitale dovrebbe tradursi anzitutto in forme di consapevolezza critica nell'uso degli strumenti messi a disposizioni durante l'emergenza: accanto alle questioni infrastrutturali vi sono anche quelle, altrettanto fondamentali, delle competenze digitali. Inoltre, le istituzioni

---

[27] Cfr. ancora l'opera di S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., p. 115 ss.

[28] A partire dagli interventi che costituiscono la *Strategia europea per il digitale*. Si pensi all'impatto che potranno avere il *Digital services act* (DSA) e il *Digital Markets Act* (DMA) sulle piattaforme online, specie in termini di trasparenza e responsabilità dei processi algoritmici.

[29] Di recente per una prospettiva critica estesa al GDPR e, in particolare, all'eccessiva attenzione posta sulla protezione dei dati, definita come «religione», e non al loro uso, si veda il pamphlet V. MAYER-SCHÖNBERGER, T. RAMGE, *Access Rules. Freeing information to stop Big Tech, revive innovation, and empower society*, Berkeley, 2020, trad. it. E. Cianco, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, Milano, 2021.

[30] Si pensi al caso italiano della rete unica verticalmente integrata, su cui cfr. *Rete unica per sostenere Telecom Italia, una chiave di lettura,* in *HDblog.it*, 6 ottobre 2020; *Tim e Open Fiber: aspettiamo a seppellire la concorrenza*, in *Il Sole 24ore*, 22 settembre 2020, disponibile all'indirizzo: https://www.econopoly.ilsole24ore.com/2020/09/22/tim-open-fiber-concorrenza/.

[31] Dove si sottolinea la necessità di un approccio pan-europeo al contrasto della pandemia di Covid-19 basato sulla solidarietà digitale e sulla condivisione dei principi di protezione dati a tutela, innanzitutto dei soggetti più vulnerabili, https://edps.europa.eu/press-publications/press-news/news#news_5895.

pubbliche dovrebbero sviluppare dei *software open source*[32]: un investimento importante finalizzato a creare maggiore cognizione nell'utilizzo di questi strumenti, sulla scorta di coloro che hanno segnalato come l'impiego di programmi simili possa consentire una maggiore trasparenza come forma di democrazia digitale[33].

L'assenza di consapevolezza è tuttora una delle fonti da cui si alimenta il *digital divide* e ha reso le piattaforme di cui oggi disponiamo delle mere infrastrutture di consumo individualizzato, non di condivisione e assistenza reciproca.

Lo sviluppo dell'infrastruttura tecnologica e la promozione di una cultura digitale rappresentano, dunque, lo spazio in cui possono muoversi le ragioni della solidarietà digitale. Due orizzonti chiave, da un punto di visto politico-democratico, per realizzare quella «*piena appartenenza a una comunità*»[34] che conferisce significato al concetto di cittadinanza e al cui interno non può mancare quello spirito di solidarietà che «*è, e deve essere, alla base del rapporto permanente fra i cittadini e la collettività espressa e rappresentata dalle istituzioni pubbliche*»[35].

La riflessione sulla solidarietà digitale, tuttavia, non può esser limitata al solo contesto locale ma deve esser condotta anche nel contesto globale e, per questo, deve misurarsi con gli attori che lo popolano. La trasformazione digitale, con i suoi caratteri di universalità, e trasversalità, impone un punto di vista che sia riferito al potere esercitato dalle grandi multinazionali cui si è fatto riferimento.

---

[32] Sul concetto di "free software" e sulla sua necessaria declinazione in termini di trasparenza e conoscibilità cfr. L. LESSIG, *Foreword to the First Edition*, in *Free Software, Free Society: Selected Essays of Richard M. Stallman*, 3rd ed., Boston, 2015, p. vii, per cui «*Free software is control that is transparent, and open to change, just as free laws, or the laws of a "free society," are free when they make their control knowable, and open to change*».

[33] Nella dottrina italiana v. G. ZICCARDI, *Democrazia elettronica e libertà dei dati tra sistemi elettorali e WikiLeaks*, in *Ciberspazio e diritto*, 1/2011, p. 8 ss.; M.F. DE TULLIO, *Solidarietà e Covid-19*, in G. DE MINICO, M. VILLONE (cura di), *Stato di diritto – Emergenza – Tecnologia*", e-book disponibile su *Consulta Online*, 2020, p. 156 ss. Infine, con riferimento alle riforme della p.a. italiana e, in particolare, alla legge n. 124/2015, B. CAROTTI, *L'amministrazione digitale e la trasparenza amministrativa*, in *Giorn. dir. amm.*, 5/2015, p. 627.

[34] Così T.H. MARSHALL, *Citizenship and social class, and other essays*, Cambridge, 1950, tr. it. S. Mezzadra, *Cittadinanza e classe sociale*, Roma-Bari, 2002, p. 10. la cui riflessione sulle forme della cittadinanza risulta imprescindibile. Nella letteratura italiana P. COSTA, *Civitas. Storia della cittadinanza in Europa. Vol. 4. L'età dei totalitarismi e della democrazia*, Roma-Bari, 2001, spec. p. 483 ss.

[35] Così V. ONIDA, *Costituzione e corona virus. La democrazia nel tempo dell'emergenza*, Milano, 2020, p. 37.

La proiezione delle dimensioni della solidarietà oltre i confini dello Stato nazionale è, dunque, un ulteriore terreno su cui poter verificare le effettive possibilità della solidarietà digitale.

Sul punto può esser utile tornare alla primavera del 2020, al primo *lockdown*, quando Apple e Google hanno condiviso pubblicamente i dati sulla mobilità, mostrando il traffico di persone in vari contesti sociali: sulla base di tali dati i decisori politici hanno potuto trarre alcune importanti indicazioni sul rispetto delle misure di contenimento e gestione dell'epidemia da essi introdotte. In seguito alla pubblicazione di questi *Community Mobility Reports*, anche Facebook attraverso il suo programma *Data for Good* ha lanciato un'iniziativa per condividere i dati aggregati e anonimizzati in suo possesso con istituzioni, università e centri di ricerca in una serie di Paesi, tra cui l'Italia. L'obiettivo, in questo caso, era la formulazione di un modello predittivo di diffusione del contagio da coronavirus e la creazione di una mappa dei sintomi, in relazione alla presenza di persone in un determinato territorio.

5. *Verso l'"altruismo dei dati"?*

Nella medesima direzione sembra muoversi la proposta di Regolamento in materia di *governance* dei dati presentata dalla Commissione europea in data 25 novembre 2020[36]. In particolare, nel Capo IV (art. 15 e ss.) viene introdotto il concetto di "altruismo dei dati": un meccanismo in grado di consentire la raccolta e il trattamento dei dati messi a disposizione a titolo gratuito da persone fisiche e giuridiche a fini esclusivamente non commerciali e a vantaggio della collettività come, ad esempio, nel campo dei servizi pubblici o nell'ambito della ricerca scientifica. L'obiettivo è, in sintesi, quello di creare le condizioni per consentire ai cittadini e alle imprese di condividere i loro dati, sapendo che saranno gestiti da organizzazioni riconosciute e accreditate secondo quanto stabilito dal medesimo Regolamento[37].

La lettura dell'articolato evidenzia, tuttavia, alcune criticità in ordine alle

[36] Cfr. European Commission, *Proposal for a Regulation of the European parliament and of the Council on European data governance* (Data Governance Act), COM(2020) 767 final. L'obiettivo di fondo del Regolamento risiede nel miglioramento delle condizioni e dei meccanismi per la condivisione dei dati nel mercato interno, attraverso la creazione di un quadro armonizzato per lo scambio di dati, sia per l'accesso che per il loro riutilizzo.

[37] L'art. 22 della proposta prevede l'introduzione di un «modulo europeo comune di consenso all'altruismo dei dati» che permetterebbe raccogliere il consenso «in formato uniforme in tutti gli stati membri».

modalità di raccolta del consenso e alla possibilità di revocarlo, nonché in relazione alla definizione delle finalità per cui i dati possono essere riutilizzati, come sottolineato anche nel parere congiunto rilasciato il 10 marzo 2021 dal Comitato europeo per la protezione dei dati (EDPB) e dal Garante europeo della protezione dei dati (EDPS) [38].

Si tratta di una proposta che può esser confrontata con le iniziative *open data* delle Big Tech richiamate in conclusione del paragrafo precedente: entrambe, infatti, pur partendo da presupposti diversi, costituiscono un potenziale indice di una rinnovata sensibilità sociale.

L'atteggiamento delle grandi imprese private, tuttavia, va valutato attentamente: se da un lato può identificare la consapevolezza che il potere delle informazioni in loro possesso comporta un elevato livello di responsabilità nei confronti della società e, allo stesso tempo, qualifica come insufficienti le azioni volontarie finora intraprese; dall'altro potrebbe trattarsi di una mera donazione a fini tattici per «*generare qualche articolo positivo sui giornali*» e accontentare il decisore politico [39].

Una preoccupazione per certi versi fondata ma che, in via generale, sembra aver in qualche misura posto un aggravio di responsabilità «*all'uso delegato e oscuro dei dati di terzi*» dalla quale non ci si dovrebbe poter sottrarre, se non con la prova di aver fatto quanto era nelle proprie possibilità [40]. Una ricostruzione in cui il vincolo di solidarietà sociale, l'etica d'impresa, sia *off-line* che

---

[38] Il testo del parere è consultabile al link: https://edps.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. In termini generali, secondo le due autorità «la Commissione deve definire meglio le finalità di interesse generale di tale "altruismo dei dati". EDPB e GEPD ritengono che la mancanza di una definizione possa comportare l'incertezza del diritto e abbassare il livello della protezione dei dati personali nell'UE. A titolo di esempio, l'obbligo dell'organizzazione per l'altruismo dei dati di informare i titolari dei dati (ivi compreso l'interessato), in merito "alle finalità di interesse generale per le quali consentono il trattamento dei loro dati da parte di un utente dei dati" è in linea con il principio secondo il quale i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (principio della limitazione della finalità, a norma dell'articolo 5, lettera b), GDPR). È pertanto opportuno fornire nella proposta un elenco esaustivo di finalità chiaramente definite» (cfr. punto 172 del parere). Inoltre, si sottolinea la necessità di introdurre «un riferimento esplicito alla trasmissione di dati anonimizzati, ove possibile e opportuno ai fini del trattamento dei dati, in linea con il principio della minimizzazione dei dati, al fine di proteggere le persone interessate da rischi ingiustificati per i loro diritti e le loro libertà fondamentali, soprattutto nel caso del trattamento di categorie particolari di dati» (punto 189).

[39] È la posizione espressa da V. MAYER-SCHÖNBERGER, T. RAMGE, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, cit., pp. 309-310.

[40] Sul punto, anche per la citazione che precede, cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche*. Privacy *e* lex mercatoria, in *Dir. pubbl.*, 2019, p. 97.

on-line, acquistano una loro dimensione autonoma e prevalente sulla finalità lucrativa così come richiesto dalla gerarchia costituzionale dei valori [41].

Il comportamento delle Big Tech – si potrebbe citare anche il noto caso delle app di tracciamento – illustra chiaramente come il controllo sulle informazioni in un mondo guidato dai dati si sia spostato a favore di coloro che generano, archiviano e analizzano i flussi delle informazioni sulle loro piattaforme digitali.

Il concetto di solidarietà digitale si lega, quindi, inscindibilmente con la tematica della condivisione dei dati e con gli obiettivi del presente contributo. Se nella prospettiva della regolazione non sembra possibile, o addirittura pensabile, rompere i monopoli delle informazioni, risulta quantomai necessario ricavare degli spazi in cui stabilire degli obblighi: il caso dei dati sanitari anonimizzati e relativi alla ricerca, per esempio, potrebbe esser paradigmatico di una libera circolazione, condivisione e utilizzo a fini sociali. Il tutto in un contesto in cui oltre l'80% dei dati raccolti non viene usato nemmeno una volta [42] e che, dunque, anche per ragioni – per certi versi paradossali – connesse al valore dei dati medesimi, impone lo sviluppo di una nuova disciplina volta a estendere, promuovere e tutelare l'accesso libero ai dati accumulati da soggetti privati di grandi dimensioni da parte dei soggetti pubblici interessati a servirsene per obiettivi sociali o di informazione.

[41] *Ibidem*.

[42] V. MAYER-SCHÖNBERGER, T. RAMGE, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, cit., p. 203.

BIG DATA, BIG TROUBLES: COME SI CONTROLLA IL POTERE DEI DATI?

di *Elia Cremona*

SOMMARIO: 1. 'Dati' in cambio di servizi: è "giusto prezzo"? – 2. Concentrazione di dati e potere di mercato. – 3. I dati come prezzo, la privacy come nuova base giuridica dell'*enforcement* antitrust. – 4. I *big data* (e gli algoritmi che li processano) come *essential facilities* nel mercato della pubblicità online. – 5. L'assetto della regolazione: la forza dei princìpi, oltre teoria dei silos. – 6. Verso un sindacato del giudice amministrativo sull'eccesso di potere … privato?

1. *'Dati' in cambio di servizi: è "giusto prezzo"?*

Uno dei temi che più animava il dibattito tra i canonisti medievali della seconda e terza scolastica era quello del "giusto prezzo" delle merci [1]. In particolare, soprattutto la dottrina tomistica si interrogava sulla opportunità che i princìpi etici si imponessero sulle ragioni dell'economia, per «*togliere l'ingiustizia che proviene dal lasciare la determinazione della misura delle mercedi operaie, come quella dei prezzi delle merci, al giuoco spietato della domanda e dell'offerta*» [2].

[1] Sulle fasi della filosofica scolastica, si veda il classico J.A. SCHUMPETER, *History of Economic Analysis* (1954), Taylor & Francis e-Library, 2006, p. 79 ss., e, specificamente sul tema del giusto prezzo, pp. 89-90.

[2] Così A. SAPORI, *Il giusto prezzo nella dottrina di San Tommaso e nella pratica del suo tempo*, in *Arch. stor. it.*, 1932, vol. 90, n. 3, p. 3. L'Autore colloca la nascita del dilemma del 'giusto prezzo' nello sconvolgimento delle dinamiche dell'economia conseguente alle Crociate, che provocarono l'apertura di canali di commercio internazionale e – allo stesso tempo – la progressiva consunzione del potere delle Arti di controllare l'approvvigionamento dei materiali e la fissazione dei prezzi al dettaglio. In altre parole, «*la rottura dell'equilibrio tra domanda e offerta aveva le necessarie conseguenze sui prezzi del mercato che, già statici o relativamente statici, subivano ora inevitabili oscillazioni*». In tale contesto, Tommaso D'Aquino, mentre condanna le *commutationes* guidate dal solo criterio del lucro ("*propter lucrum quaerendum*"), giustifica

Così, al *pretium datum*, quello fissato sulla base delle accidentalità del mercato, si contrapponeva il *pretium iustum*, ovvero quello dato dall'oggettivo *valor rei*, rappresentato essenzialmente da tre fattori: il lavoro, le spese, la qualifica del lavoratore [3]. Si postulava cioè una equivalenza (*aequalitas iustitiae*) tra prezzo e valore, tra i due elementi costitutivi dello scambio economico [4].

Rileggere le attuali dinamiche dell'economia digitale alla luce di queste categorie è un'operazione molto interessante, e forse pure utile, con le dovute contestualizzazioni.

E difatti, siamo oggi abituati a considerare normale che la fornitura di contenuti o servizi digitali avvenga *senza* la corresponsione di un prezzo, venendo al più richiesto di esprimere un consenso al trattamento dei dati personali [5]. Servizi contro dati: è questo, in realtà, lo scambio sotteso alle relazioni economiche *online* [6]. Ma è un giusto prezzo?

Su questo tema si sono coagulati essenzialmente due filoni di pensiero: da un lato, secondo una prospettiva di maggiore realismo, v'è chi ha proposto di considerare i dati personali come beni di valore comparabile al denaro, dall'altro, secondo una prospettiva maggiormente idealista, v'è chi ha affermato il

---

quelle forme di lucro che siano contenute entro termini ragionevoli e volute per scopi onesti e onorevoli («*nihil prohibet lucrum ordinari ad aliquem finem necessarium vel etiam honestum*»); TOMMASO D'AQUINO, *Summa Theologiae*, II, 2, qu. CXVII, art. I, 3, b.

[3] A. SAPORI, *Il giusto prezzo*, cit. p. 25.

[4] TOMMASO D'AQUINO, *Summa*, cit., II, 2, qu. LXI, art. IV, 2, b, laddove afferma «*nomen contrappassi transfertur ad voluntarias commutationes, in quibus utriusque est actio et passio […] contrappassum importat aequalem recompensationem passionis ad actionem precedentem*».

[5] Cfr. A. QUARTA, *Mercati senza scambi. La metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020; P.A. ALCES, M.M. GREENFIELD, *They Can Do What!? Limitation on Use of Change-of-Terms Clause*, in *Georgia State University Law Review*, 26, 4, 2010, pp. 1099-1145; P. PALKA, *Terms of Service are not Contracts. Beyond Contract Law in the Regulation of Online Platforms*, in S. GRUNDMANN (a cura di), *European Contract Law in the Digital Age*, 2018, pp. 135-162, secondo il quale i termini di servizio non sono contratti in senso tradizionale. Sia consentito rinviare anche a E. CREMONA, *Fonti private e legittimazione democratica nell'età della tecnologia*, in corso di pubblicazione sulla Rivista *DPCE online*.

[6] Cfr. L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione*, in R. LENER, G. LUCHENA, C. ROBUSTELLA, *Mercati regolati e nuove filiere del valore*, Torino, 2021, p. 105 ss.; G. VERSACI, *La contrattualizzazione dei dati personali del consumatore*, Napoli, 2020; ID., *Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection*, in *European Review of Contract Law*, 2018, 14, 4, pp. 374-392; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, pp. 411-440; A. METZGER, *Data as Counter-Performance: What Rights and Duties Do. Parties Have?,* in *Journal of Intellectual Property, Information Technology and Electronic commercial law*, 2017, 8, 5; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, p. 164.

principio per cui i dati personali non possono essere considerati come una merce di scambio[7].

Si potrebbe molto indulgere sulla domanda *etica* in merito alla "giustizia" di un prezzo pagato in dati personali e pure sulla domanda *giuridica* sulla esatta qualificazione degli stessi. In entrambi i casi, il rischio che si corre è o quello di avallare acriticamente il fenomeno della patrimonializzazione dei dati personali (obnubilando la tutela di diritti e interessi diversi da quello alla speditezza dei traffici economici) o quello di rifiutare *tout court* le "magnifiche sorti e progressive" dell'economia digitale (censurando, cioè, la realtà di un fenomeno ormai globale).

Tale insidiosa dicotomia può essere però in questa sede evitata avviando una riflessione più pragmatica, che guardi cioè agli effetti dello sviluppo, sostanzialmente deregolato, del mercato digitale, senza rinunciare a esplorare qualche ipotesi *de iure condendo* e qualche possibile nuovo varco di tutela dei diritti, spesso di tenore costituzionale, in gioco nell'era digitale.

2. *Concentrazione di dati e potere di mercato*

Secondo la teoria classica, la concentrazione di potere di mercato e, soprattutto, l'abuso della conseguente posizione dominante, deve essere combattuta

[7] La portata del dibattito è ben resa dalle divergenze testuali riscontrabili tra la Proposta di Direttiva sulla fornitura di contenuti digitali avanzata dalla Commissione europea e il testo definitivamente approvato. E infatti, nel considerando n. 13 della Proposta era dato di leggere 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. Tali specifici modelli commerciali si applicano in diverse forme in una parte considerevole del mercato. Introdurre una differenziazione a seconda della natura della controprestazione significherebbe discriminare alcuni modelli commerciali e incoraggerebbe in modo ingiustificato le imprese ad orientarsi verso l'offerta di contenuti digitali contro la messa a disposizione di dati. Vanno garantite condizioni di parità eque*». Nel *drafting* finale della Direttiva 2019/770, la prospettiva "realista" sembra essere accantonata. Si legge al considerando n. 24: «*La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. […] Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente Direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali*». Cfr. Commissione europea, *Proposal for a Directive of the European Parliament and the Council on the aspects concerning contracts for the supply of digital content*, COM(2015), 634 final, 9 dicembre 2015; Direttiva UE 2019/770 del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

perché finisce per distorcere l'efficace allocazione delle risorse, mentre i prezzi perdono la loro funzione di indicatori della scarsità [8].

Nell'ambiente digitale, la "scomparsa" del prezzo ha posto più di un problema. Per un certo periodo di tempo, la dottrina dominante, essenzialmente riconducibile alla Scuola di Chicago, ha escluso l'intervento antitrust in caso di 'prezzi' bassi o nulli [9]. Ciò sull'assunto per cui il diritto antitrust protegge la concorrenza e non i concorrenti [10].

Senonché, nel mondo dei c.d. *multi-sided markets*, i prezzi nulli in un versante di mercato sono funzionali all'acquisizione di importanti quote di mercato sugli altri versanti: da lì giunge la remunerazione degli investimenti e la copertura dei costi di entrambi i versanti, senza che la piattaforma conosca mai perdite, neppure nel breve periodo [11].

Il tema del ruolo dei dati come volano per la concentrazione del potere di mercato ha iniziato a porsi con l'annuncio da parte di Google, dell'aprile del 2007, di acquisire la società DoubleClick, società operante nel campo delle inserzioni pubblicitarie online [12]. L'accordo di fusione ha sollevato preoccupazioni antitrust sia in Europa che negli USA, ma in entrambi casi la fusione è stata autorizzata, di fatto dando la stura ad una vera e propria stagione di cc.dd. *killer acquisitions* [13]. In particolare, la Commissione europea ebbe a rile-

---

[8] Cfr. A. EZRACHI, M.E. STUCKE, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, 2016.

[9] S. MANNONI, G. STAZI, *Is Competition a Click Away?*, Napoli, 2018, pp. 18-19.

[10] R.H. BORK, E.F. SIDAK, *What does the Chicago law School Teach About Internet Search and the Treatment of Google?*, in *Journal of Competition Law & Economics*, 8, 4, 2012, pp. 663-700.

[11] Per tale ragione si esclude l'applicabilità della dottrina dei prezzi predatori: in ogni caso la somma dei prezzi praticati ai gruppi di utenti dei versanti di mercato supera i costi marginali sofferti per l'offerta dei servizi. Cfr. M. MAGGIOLINO, *Concorrenza e piattaforme: tra tradizione e novità*, in G. COLANGELO, V. FALCE, *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Bologna, 2017, p. 59, nt. 30; J. WRIGHT, *One-Sided Logic in Two-Sided Markets*, in *Review of Network Economics*, 3, 2004, p. 48.

[12] La società DoubleClick sviluppava e forniva servizi per l'inserzione pubblicitaria online ed è stata definitivamente acquisita da Google nel marzo 2008, per oltre tre miliardi di dollari. DoubleClick offriva prodotti e servizi tecnologici che venivano venduti principalmente ad agenzie pubblicitarie e mass media che servivano aziende quali Microsoft, General Motors, Coca-Cola, Motorola, L'Oréal, Apple, Visa, Nike. La principale linea di prodotti dell'azienda era nota come DART (*Dynamic Advertising, Reporting, and Targeting*), che aveva lo scopo di aumentare l'efficienza di acquisto degli inserzionisti e ridurre al minimo l'invenduto per i *publisher*. Cfr. *DoubleClick Inc. 2004 Form 10-K Annual Report*, disponibile al seguente link: https://www.sec.gov/Archives/edgar/data/0001049480/000095012305003222/y06461e10vk.htm.

[13] Nel maggio 2007, la *Federal Trade Commission* statunitense ha richiesto ulteriori informazioni sull'accordo, anche a séguito delle sollecitazioni ricevute da Microsoft, che riteneva che la fusione avrebbe dato a Google un controllo eccessivo sulla pubblicità *online*; cfr. S. LOHR, *Mi-*

vare che l'effetto di *data collection* che si sarebbe venuto a creare non avrebbe conferito al soggetto incorporante un vantaggio competitivo non replicabile da parte di concorrenti come Microsoft o Yahoo [14].

La storia, com'è noto, ha smentito l'ottimistica previsione della Commissione, che per alcuni anni ha continuato, se non a sottovalutare, ad avallare le aspirazioni monopolistiche delle Big Tech. Ancora un fulgido esempio giunge dalla autorizzazione delle fusioni tra Microsoft/Yahoo, nel 2010, e Facebook/-Whatsapp, avvenuta nel 2014. Nel primo caso, la Commissione ritenne che la fusione avrebbe consentito di accrescere il livello di concorrenza nel mercato, grazie alla creazione di un competitor di Google su larga scala [15]. Nel secondo, la Commissione affermò che, se anche il soggetto esitante dalla fusione avesse raccolto e trattato i dati degli utenti di WhatsApp per migliorare i servizi di *targeting* su Facebook, la fusione non avrebbe pregiudicato il mercato (*theory of harm*) in quanto avrebbero continuato a residuare moltissimi dati di utenti online, utilizzabili per la pubblicità, non sotto controllo di Facebook [16].

---

crosoft Urges Review of Google-Double Click Deal, in *The New York Times*, 16 aprile 2007, disponibile al seguente link: https://www.nytimes.com/2007/04/16/technology/16soft.html. Il 20 dicembre 2007, la FTC ha approvato l'acquisto di DoubleClick da parte di Google dai suoi proprietari Hellman & Friedman e JMI Equity. In Europa, la Commissione ha concesso l'approvazione l'11 marzo 2008.

[14] Cfr. *Commission decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement, Case No COMP/M.4731 – Google/ DoubleClick*, disponibile al seguente link: https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf. In particolare, al punto 269 si legge che «*even the merged entity, let alone DoubleClick alone, would not have access to unique, non-replicable data because the type of information collected by DoubleClick is relatively narrow in scope. Other companies active in online advertising have the ability to collect large amounts of more or less similar information that is potentially useful for advertisement targeting*».

[15] *Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004, Case n. COMP/M.5727 – Microsoft/ Yahoo! Search Business*, disponibile al seguente link: https://ec.europa.eu/competition/mergers/cases/decisions/M5727_20100218_20310_261202_EN.pdf.

[16] *Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004, Case M.7217 – Facebook/ WhatsApp*, disponibile al seguente link: https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf. In particolare, al punto 188 si legge che «*the Commission refers to the results of the market investigation presented above (paragraph (177)), which indicate that, post-Transaction, there will remain a sufficient number of alternative providers of online advertising services. In addition, the Commission notes that there are currently a significant number of market participants that collect user data alongside Facebook. These include, first of all Google, which accounts for a significant portion of the Internet user data and, in addition, companies such as Apple, Amazon, eBay, Microsoft, AOL, Yahoo!, Twitter, IAC, LinkedIn, Adobe and Yelp, among others*». Allo stesso modo, anche nella valutazione dell'operazione Apple/Shazam, la Commissione ha ritenuto che l'integrazione dei database delle parti, contenenti dati sui rispettivi utenti, non avrebbe conferito al soggetto esitante dall'operazione di fusione un *"vantaggio non replicabile"*. Ciò in quanto i database contenevano dati non unici e

Una punta di resipiscenza compare invece nell'autorizzazione condizionata della fusione Microsoft/Linkedin, nel 2016 [17]. La Commissione in quel caso ha infatti specificato che la tutela della privacy, pur non rientrando direttamente nell'ambito del diritto europeo della concorrenza, può essere tenuta in considerazione nella valutazione antitrust nella misura in cui i consumatori la percepiscano come un fattore di qualità del servizio e le imprese concorrano tra loro anche sulla base di tale fattore. In questo caso, quindi, la Commissione ha affermato che i termini di protezione della privacy costituiscono un fattore concorrenziale importante tra gli operatori di social network e che tale parametro di qualità avrebbe potuto subire un abbattimento in conseguenza della concentrazione, in assenza degli impegni poi adottati da Microsoft [18].

Il trend descrive una maturata, ma forse non ancora matura, concezione dei *big data* come viatico per la formazione di monopoli (sorta di *essential facility*) [19].

---

non qualificabili come *input* importanti per la fornitura di prodotti a valle. Cfr. *Commission decision pursuant to Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation No 139/20041 and Article 57 of the Agreement on the European Economic Area*, *Case M.8788 Apple/Shazam*, disponibile al seguente link: http://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf.

[17] Al fine di superare le criticità emerse nel corso dell'istruttoria, Microsoft ha offerto l'assunzione di impegni, della durata di cinque anni, applicabili nello Spazio Economico europeo (SEE), che la Commissione ha accettato e reso vincolanti come condizione per l'autorizzazione della concentrazione. In particolare: (i) assicurare che i produttori e distributori di PC siano lasciati liberi di non installare LinkedIn su Windows e consentire agli utenti di rimuoverlo nel caso in cui i produttori e distributori di PC decidessero di pre-installarlo; (ii) consentire ai concorrenti di LinkedIn di mantenere gli attuali livelli di interoperabilità con i prodotti di Microsoft Office tramite il c.d. *Office add-in program* e *Office application programming interfaces*; (iii) garantire ai concorrenti di LinkedIn l'accesso a Microsoft Graph, un portale per sviluppatori di software, usato per sviluppare applicazioni e servizi che, con il consenso degli utenti, accedono ai loro dati immagazzinati sulla *cloud* di Microsoft, come ad esempio i contatti, le informazioni del calendario ed e-mail. Gli sviluppatori possono eventualmente utilizzare questi dati per spingere gli utenti ad abbonarsi ai propri social network professionali.

[18] *Commission decision pursuant to Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation No 139/20041 and Article 57 of the Agreement on the European Economic Area, Case M.8124 – Microsoft / LinkedIn*, disponibile al seguente link: https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

[19] Cfr. A. NICITA, M. DELMASTRO, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019. A suggerirne tale potenziale qualificazione come *essential facilities* è la stessa AGCM, nell'*Indagine conoscitiva sui Big Data*, a p. 109, laddove si legge che *«ai fini dell'analisi dell'indispensabilità tipica della dottrina antitrust dell'*essential facility *nel settore dei Big Data, almeno tre aspetti specifici appaiono potenzialmente rilevanti: – la natura personale o meno dei dati oggetto della richiesta di accesso; – se i dati in questione siano stati: i) volontariamente forniti dal soggetto a cui si riferiscono; ii) rilevati dall'operatore dominante; iii) ricavati tramite attività di analisi dei dati svolte dall'operatore in questione (*analytics*); – il grado di aggregazione dei dati*

L'esitazione a "colpire" le concentrazioni di dati deriva probabilmente da quanto detto in premessa: la concezione, o il mito[20], dei servizi digitali come servizi gratuiti ha indotto prudenza nell'intervento del regolatore che, non ravvisando nella cessione dei dati personali un costo per il consumatore, ha per molto tempo ritenuto massimizzato il suo benessere finale. Dunque, inutile, se non disutile, il suo intervento.

Oggi il paradigma sembra mutare, quantomeno in Europa, e ciò forse più grazie all'intervento delle autorità nazionali di regolazione che alla Commissione.

3. *I dati come prezzo, la privacy come nuova base giuridica dell'*enforcement *antitrust*

Germania e Italia costituiscono oggi, probabilmente, i due ordinamenti nei quali appare più evidente il processo di funzionalizzazione del diritto antitrust alla tutela di beni giuridici diversi dalla concorrenza e, in particolare, della privacy. In entrambi gli ordinamenti, il destinatario degli interventi delle Autorità è Facebook[21].

In Germania, il *Bundeskartellamt*[22] ha avviato nel 2016 un procedimento contro Facebook per abuso di posizione dominante e per la messa in atto di condotte anticoncorrenziali *per il tramite* della sistematica violazione delle norme in materia di protezione dei dati personali[23]. In particolare, la decisione

---

oggetto della richiesta di accesso potendo distinguere, dunque, tra dati a livello individuale, aggregati o bundled*. In ogni caso, la specificità, la quantità e la qualità dei dati possono configurare un ostacolo alla concorrenza e favorire una condotta abusiva, nella forma di un rifiuto a contrarre, solo laddove tali dati integrino i requisiti stringenti di una* essential facility *per la fornitura di un particolare servizio*». Cfr. I. GRAEF, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Alphen aan den Rijn, 2016.

[20] Cfr. J.H. NEWMANN, *The Myth of Free*, in *George Washington Law Review*, vol. 86, 2017, *University of Memphis Legal Studies Research Paper No. 163*, p. 3, dove si rileva come «*"Freeconomics" has replaced standard economics. The marginal costs of digital products supposedly fell to zero, causing prices to follow. Scarce goods are costly; abundant goods are Free. And standard economics cannot account for Free*».

[21] Per più approfondite analisi delle due pronunce, si rinvia ai contributi di V. PAGNANELLI e F. LAVIOLA, in apertura di questo volume.

[22] Decisione del 6 febbraio 2019; *Facebook Inc., Menlo Parc, U.S.A., Facebook Ireland Ltd., Dublin, Ireland, Facebook Deutschland GmbH/Verbraucherzentrale Bundesverband e. V.*, Berlin.

[23] La decisione in merito alla violazione del divieto di abuso di posizione dominante da parte

si è occupata della condotta consistente nell'inserimento, all'interno delle proprie condizioni contrattuali, di una serie di clausole che autorizzavano la società ad acquisire, combinare ed analizzare i dati generati dagli utenti nel corso delle loro attività online, non solo sulla piattaforma Facebook, ma anche dall'utilizzo di altri servizi di proprietà della stessa, come ad esempio WhatsApp o Instagram, nonché dall'interazione con siti web di proprietà di terze parti, ma che si avvalevano dei *Facebook business tools*.

Ad avviso del *Bundesrkartellamt*, l'assenza di un'informazione chiara agli utenti in merito a queste condizioni (appena descritte in modo generico e senza far riferimento ai singoli servizi considerati, all'interno dei *terms and conditions* di Facebook) sarebbe stata illegittima in quanto incompatibile con il diritto all'autodeterminazione informativa e alla privacy garantiti dalla Carta costituzionale tedesca, dall'art. 8 della Carta europea dei Diritti Fondamentali e del GDPR.

Peraltro, ha rilevato il *Bundesrkartellamt*, Facebook attraverso il ricorso a questa pratica è stata in grado di raccogliere una tale quantità di dati personali da porre l'azienda in una posizione di preminenza assoluta nel diverso versante di mercato rappresentato dalla vendita di servizi di pubblicità targettizzata, consentendo agli inserzionisti di sfruttare l'elevato grado di profilazione degli utenti del social network per proporre annunci a specifici gruppi di consumatori.

Per conseguenza, Facebook avrebbe sia leso la libertà di autodeterminazione informativa dei propri utenti sia pregiudicato il mercato concorrenziale dei servizi pubblicitari online, sfruttando la posizione di dominanza nel mercato dei dati, illecitamente acquisita.

La decisione è stata variamente commentata ed ha avuto alterne fortune nel vaglio giurisprudenziale[24]. Facebook ha impugnato la decisione dinanzi al tribunale regionale superiore competente, l'*Oberlandesgericht Düsseldorf*. In sede cautelare, l'istanza sospensiva è stata accolta, ritenendo i giudici sussistenti evidenti incongruità nell'apparato motivazionale della decisione, con particolare riferimento alla prova del pregiudizio alla concorrenza e alla sussistenza di

di Facebook è stata resa sulla base dell'asserita violazione del divieto di condotte abusive sancito all'art. 19 della normativa antitrust tedesca (*Gesetz gegen Wettbewerbsbeschränkungen*, GWB).

[24] V. COLANGELO, M. MAGGIOLINO, *Data Protection in Attention Markets: Protecting Privacy through Competition?*, in *Journal of European Competition Law & Practice,* 2017, 8, p. 363; G. DAVOLA, *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco*, cit., p. 63; R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, in *Merc. conc. reg.*, 3, 2020, p. 507 ss.; C. OSTI, R. PARDOLESI, *L'antitrust ai tempi di Facebook*, *ivi*, 2019, p. 195; A. GIANNACCARI, *Facebook e l'abuso da sfruttamento al vaglio del Bundesgerichtshof*, *ivi*, 2020, pp. 403-409.

un nesso di causalità tra la condotta commerciale di Facebook e il *vulnus* concorrenziale [25].

In buona sostanza, il tribunale ha ritenuto che non fosse affatto certo, in uno scenario controfattuale (*but-for*), che se anche i consumatori fossero stati messi nella condizione di graduare il livello di informazioni condivise con il social network, avrebbero scelto la soluzione più *privacy-preserving*. E in ogni caso, il consenso sarebbe stato raccolto da Facebook in maniera lecita, talché non si versava in una ipotesi di abuso di posizione dominante.

A sua volta, la decisione dell'*Oberlandesgericht Düsseldorf* è stata impugnata dinanzi alla Corte suprema federale tedesca, il *Bundesgerichtshof*, che ha di nuovo ribaltato la decisione, confermando quella del *Bundeskartellamt* [26]. Nella sentenza la Corte suprema ha affermato che le suddette condizioni contrattuali applicate da Facebook possono ben costituire un abuso di posizione dominante, indipendentemente dalla loro conformità al GDPR (così sfruttando la potenzialità del diritto antitrust di colpire anche comportamenti leciti, quando anticoncorrenziali).

Secondo i giudici, la fenomenologia dell'abuso sarebbe consistita nell'elisione della possibilità di scelta del consumatore (*fehlende Wahlmöglichkeit*), ovvero nella decisione di non offrire opzioni differenziate tra cui scegliere nella fruizione dei servizi di Facebook [27].

La questione, tornata all'*Oberlandesgericht Düsseldorf* per la cognizione di merito, è stata subito rimessa, nell'aprile 2021, alla Corte di Giustizia dell'Unione europea, che sarà perciò chiamata a districare la matassa che si è formata tra due dei più importanti plessi normativi del diritto unionale.

In dottrina è stato osservato come la decisione sostanzialmente recida il nesso causale tra la condotta e il pregiudizio alla concorrenza, arrestando l'indagine sull'abuso di posizione dominante sulla soglia della mera "compressione" della libertà di scelta del consumatore [28]. Si tratta di una novità non di poco conto, considerato che il rigoroso vaglio del nesso di causalità costituisce da sempre un argine importante al rischio della *imprevedibilità* dell'intervento delle autorità di regolazione antitrust, già caratterizzato dall'operare *ex post*.

---

[25] *Oberlandesgericht Düsseldorf*, decisione del 26 agosto 2019*,* VI-Kart 1/19 (V); *Bundeskartellamt c. Facebook.*

[26] *Bundesgerichtshof*, decisione del 23 giugno 2020; KVR 69/19; *Facebook.*

[27] *Ivi*, punto 103.

[28] A. WITT, *Excessive Data Collection as a Form of Anticompetitive Conduct - The German Facebook Case*, in *Antitrust Bulletin Jean Monnet Working Paper*, 1, 2020, p. 33; G. DAVOLA, *I vestiti nuovi*, cit., p. 69; R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati*, cit., pp. 524-527.

Peraltro, è tutto da dimostrare che i consumatori, posti nella possibilità di scegliere tra una esperienza del social network deteriore ma *privacy-preserving* e una esperienza migliore ma *privacy-sharing* prediligano la prima. Anzi, alcuni studi mostrano come i consumatori, nella più parte, *vogliano* essere profilati e ricevere pubblicità mirate[29]. Perciò, correttamente è stato sollevato il problema del rischio di una supervalutazione del ruolo concorrenziale dei *privacy terms*[30].

Alla saga tedesca, come anticipato, si accompagna quella italiana, definita dal Consiglio di Stato con sentenza del 29 marzo 2021[31], che ha confermato una parte delle sanzioni inflitte a Facebook dall'AGCM in applicazione della normativa a tutela del consumatore[32].

In quel caso l'Antitrust italiana ha contestato a Facebook due pratiche commerciali scorrette: una pratica ingannevole[33], consistente nell'informazione inadeguata al consumatore sul trattamento dei dati personali (peraltro fuorviata dal *claim* "Facebook è gratis e lo sarà sempre" che campeggiava nella pagina di accesso), e una pratica aggressiva, consistente in un indebito condizionamento del consumatore, costretto ad acconsentire a che Facebook o soggetti terzi effettuassero la raccolta e il trattamento dei dati personali, tramite la preselezione del consenso[34].

Per conseguenza, l'Autorità aveva condannato Facebook al pagamento di una sanzione amministrativa pari a cinque milioni di euro per ciascuna pratica commerciale scorretta e alla pubblicazione di una dichiarazione rettificativa sulla pagina di accesso al sito.

Di fronte al giudice amministrativo, il provvedimento è stato in parte confermato, con riferimento alla prima delle due pratiche scorrette, e in parte demolito, con riferimento alla seconda, sia in primo grado che in secondo grado, con sentenze sostanzialmente sovrapponibili nel contenuto.

Per quanto qui ci occupa, è interessante evidenziare alcuni princìpi molto importanti che sono certamente destinati ad avere séguito.

Innanzitutto, il giudice amministrativo ha affermato la sussistenza di una violazione della normativa consumeristica per pratiche commerciali scorrette[35] per il fatto che non v'era un *claim* chiaro sulla raccolta e l'uso a fini com-

[29] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *op. cit.*, p. 528.

[30] G. DAVOLA, *op. cit.*, p. 68.

[31] Cons. Stato, sez. VI, 29 marzo 2021, n. 2631.

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

[33] Ai sensi degli artt. 20, 21, 22 del d.lgs. 6 settembre 2005, n. 206 (Codice del consumo).

[34] Ai sensi degli artt. 20, 24, 25 del Codice del consumo.

[35] In tal sede, il Consiglio di Stato ha ricordato che «*l'espressione "pratiche commerciali scorrette" designa le condotte che formano oggetto del divieto generale sancito dall'art. 20 d.lgs.*

merciali, talché l'informazione al consumatore era "*non veritiera e fuorviante*" [36]. Ciò tantopiù a fronte del fatto che il 98% del fatturato di Facebook deriva da pubblicità online per la quale gli inserzionisti sono disposti a pagare proprio per poter raggiungere target di utenti profilati.

In più, la sentenza ha delineato una sorta di obbligo di posizione in capo alla piattaforma, in quanto il fenomeno della patrimonializzazione del dato personale "impone" agli operatori di rispettare nei confronti del consumatore «*obblighi di chiarezza, completezza e non ingannevolezza delle informazioni*" poiché questi "*deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio quale è quello di utilizzo di un* social network» [37].

Infine, rigettando l'eccezione di incompetenza dell'Autorità antitrust formulata da Facebook [38], ha affermato la complementarità tra la disciplina della *privacy* e quella del consumo nell'ottica di sviluppo di un sistema di tutele multilivello del soggetto "interessato-utente-consumatore" [39].

206/2005 (recante il Codice del consumo, in attuazione della Direttiva del Parlamento europeo e del Consiglio 11 maggio 2005, n. 2005/29/CE). La finalità perseguita dalla Direttiva europea consiste nel garantire, come si desume dal considerando 23, un elevato livello comune di tutela dei consumatori, procedendo ad un'armonizzazione completa delle norme relative alle pratiche commerciali sleali delle imprese, ivi compresa la pubblicità sleale, nei confronti dei consumatori. Scopo della normativa è quello di ricondurre l'attività commerciale in generale entro i binari della buona fede e della correttezza. Il fondamento dell'intervento è duplice: da un lato, esso si ispira ad una rinnovata lettura della garanzia costituzionale della libertà contrattuale, la cui piena esplicazione si ritiene presupponga un contesto di piena "bilateralità", dall'altro, in termini analisi economica, la trasparenza del mercato è idonea ad innescare un controllo decentrato sulle condotte degli operatori economici inefficienti". Perciò, "*le politiche di tutela della concorrenza e del consumatore sono sinergicamente orientate a promuovere il benessere dell'intero sistema economico*».

[36] TAR Lazio n. 260/2020, cit., ripreso da Cons. Stato n. 2631/2021, cit.

[37] *Ibidem*.

[38] Facebook aveva eccepito il difetto assoluto di attribuzione del potere in capo all'Antitrust per il fatto che – essendo il servizio "genuinamente gratuito" – non si verteva nell'ipotesi di acquisto ai sensi della disciplina del consumo, ma semmai di trattamento dei dati personali, di competenza del Garante (nel caso, irlandese quale autorità capofila). Curioso è anche il fatto – seppur forse solo dovuto a strategia processuale – che Facebook invochi l'applicazione della disciplina sulla privacy per difendersi dalle contestazioni dell'Autorità. Il fatto potrebbe essere invocato per corroborare la tesi contenuta nei paragrafi precedenti: che la regolamentazione europea sia in realtà più "confortevole" per le grandi piattaforme digitali.

[39] «*Ferma dunque la riconosciuta "centralità" della disciplina discendente dal GDPR e dai Codici della privacy adottati dai Paesi membri in materia di tutela di ogni strumento di sfruttamento dei dati personali, deve comunque ritenersi che allorquando il trattamento investa e coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a tutela di altri valori e interessi (altrettanto rilevanti quanto la tutela del dato riferibile alla persona fisica), l'ordinamento – unionale prima e interno poi – non può permettere che alcuna espropriazione applicati-*

Ora, si potrebbe rilevare che è un fatto che i dati personali, nella pratica del mercato, siano – da lungo tempo – considerati come una merce, una *commodity*. Ciò accade nonostante l'ordinamento euro-nazionale fatichi ad ammetterlo [40].

Sul piano del diritto interno, perciò, l'intervento dell'AGCM ha consentito di affrontare il tema apertamente, seppur tramite l'*escamotage* della informazione ingannevole, e di affermare finalmente la complementarietà tra i plessi normativi della *privacy*, del consumo e, si può considerare nello spirito dei provvedimenti giudiziari esaminati, anche antitrust.

Certo deve tenersi a mente che – comunque – una qualche differenza tra il pagamento di un servizio in 'dati personali' e il pagamento in 'denaro' continua a permanere: i dati, infatti, sono generalmente beni di tipo non-rivale; l'uso da parte di un soggetto non esclude la possibilità che un altro, contemporaneamente, utilizzi profittevolmente lo stesso dato, poiché l'uso non esaurisce la funzione né il dato stesso [41]. In altre parole, mentre il pagamento in denaro determina un 'impoverimento' dell'acquirente (uno spostamento di valore monetario da un soggetto ad un altro), all'esito di un pagamento in dati entrambi i soggetti "possiedono" i dati scambiati.

Ad ogni modo, per quanto qui ci occupa, sebbene il "valore economico" del dato personale sia stato accertato e la sanzione sia stata inflitta, il problema dello sfruttamento intensivo dei dati personali (all'insaputa) degli utenti è destinato a permanere.

L'irrogazione di tali sanzioni o l'innalzamento del livello di informazione del consumatore (per quanto ciò possa realizzarsi per il tramite di una "dichiarazione rettificativa" pubblicata da Facebook per 20 giorni) difficilmente

---

va di altre discipline di settore, quale è quella, per il caso che qui interessa, della tutela del consumatore, riduca le tutele garantite alle persone fisiche». Il giudice, quindi, rigetta l'idea di "compartimenti stagni di tutela", verso "tutele multilivello", che amplifichino "il livello di garanzia dei diritti, anche quando un diritto personalissimo sia "sfruttato" a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore". Così Cons. Stato n. 2631/2021, cit.

[40] Il dibattito che ha preceduto il *drafting* finale del considerando n. 24 della Direttiva UE 770/2019 è, in questo senso, emblematico: la Commissione, nella sua proposta, qualificava la cessione dei dati come una "*controprestazione*", mentre il testo finale della Direttiva afferma che i dati non possono essere considerati come una "*merce*". L'affermazione si risolve in una sorta di petizione di principio, alla quale non consegue l'adozione di misure supplementari rispetto a quelle già disposte dal GDPR.

[41] A. GALIANO, A. LEOGRANDE, S.F. MASSARI, A. MASSARO, *I dati non personali: la natura e il valore*, in *Riv. informatica di inf. e dir.*, fasc. 1/2020, p. 63. Cfr. H. ZECH, *Information as Property*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 6, 2015, n. 3, p. 192; A. DE FRANCESCHI, M. LEHMANN, *Data As Tradable Commodity and New Measures for Their Protection*, in *The Italian Law Journal*, vol. 1, 2015, n. 1.

consentirà di riequilibrare il rapporto asimmetrico tra piattaforma e utente-consumatore. E dal momento che Facebook non accenna a mutare il proprio modello di business, c'è da attendersi che le conseguenze di tali decisioni saranno ancora una volta "scaricate" sul consumatore, che sarà chiamato, forse, a spuntare qualche casella in più prima di accedere al servizio di social network.

Le due saghe mostrano perciò ad un tempo, da un lato, la buona volontà dei regolatori antitrust nazionali, protesi ad allargare la base normativa d'appoggio dell'*enforcement* antitrust a tutela dei (non più) nuovi diritti nell'ambiente digitale, ma dall'altro però ne confessano anche il limite, risultando abbastanza chiaro come i due procedimenti siano stati attivati a mo' di *strategic litigation*, e cioè più per soddisfare esigenze di controllo sostanziale dei poteri privati che per una effettiva, efficace, tutela della concorrenza e dei consumatori.

4. *I* big data *(e gli algoritmi che li processano) come* essential facilities *nel mercato della pubblicità online*

Se i precedenti appena evocati hanno fatto parlare di abbandono dell'approccio economico[42], l'istruttoria aperta dall'AGCM sulla pubblicità *online* sembra segnarne il ritorno, con un più saldo ancoraggio agli istituti tradizionali e ai metodi econometrici.

Si è detto che negli ecosistemi digitali, l'estrazione e la raccolta dei dati personali (e non personali) costituiscono un "fattore di prezzo". Perciò più sono le informazioni raccolte sugli utenti, meglio le piattaforme possono soddisfarne le preferenze, diventando più efficienti.

Proprio di questo si dolgono gli operatori pubblicitari il cui esposto ha determinato l'apertura di un'inchiesta dell'AGCM a carico di Google[43], il quale avrebbe posto in essere una condotta di discriminazione interna-esterna, consistente nel rifiutare di fornire le chiavi di decriptazione dell'Id Google e nell'escludere la possibilità di tracciamento dei pixel di terze parti. Ciò, peraltro, a fronte del contestuale utilizzo, da parte delle proprie divisioni interne, di strumenti di tracciamento che consentono di rendere i servizi di *advertising* di Google in grado di raggiungere una capacità di targettizzazione che altri concorrenti, pur altrettanto efficienti, non sono in grado di replicare, così venendosi a determinare un ingiustificato vantaggio competitivo.

---

[42] R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *op. cit.*, p. 527 ss.

[43] AGCM, Provvedimento A542 del 20 ottobre 2020.

In buona sostanza, ciò che è oggi contestato a Google è … l'utilizzo dei dati a sua disposizione e negati ai concorrenti (perché pseudonimizzati o aggregati) per il miglior tracciamento dei propri clienti.

I *big data* vengono così considerati come risorse essenziali[44], perché «*da essi dipendono caratteristiche fondamentali del servizio reso, in particolare in termini di innovazione e/o di personalizzazione*». L'Autorità intraprende quindi l'irta strada della dottrina delle *essential facilities*, che la giurisprudenza della Corte di Giustizia ha disseminato di ostacoli. Giova ricordare le fasi del test che è necessario superare prima di poter ritenere ammissibile la qualificazione di una risorsa alla stregua di una risorsa essenziale: anzitutto, si distingue tra mercato a monte e mercato a valle; dopodiché, occorre che l'impresa detentrice dell'*essential facility* sia dominante nel mercato a monte; quindi, che sia presente anche nel mercato a valle; infine, che l'accesso alla risorsa essenziale sia richiesto al fine di poter erogare un nuovo prodotto o servizio ai consumatori e che il diniego non sia sorretto da una giustificazione oggettivamente apprezzabile[45].

Effettivamente da qualche tempo una certa dottrina aveva preconizzato la possibilità di trattare l'enorme quantità di dati estratta dalle grandi piattaforme come *essential facilities*[46] e anzi qualche autore si è spinto a perorare la causa di un *data-sharing mandate* per le imprese in posizione dominante nei mercati digitali[47]. Questo pare essere il caso e lo svolgimento dell'istruttoria è tutto da seguire.

Ad ogni modo, a prescindere dall'esito del procedimento, quandanche fosse riconosciuta la natura di risorse essenziali dei dati in possesso di Google, bisogna osservare che probabilmente ciò non sarebbe sufficiente a liberare il mercato dal giogo del monopolio: è stato appropriatamente osservato che «*sono gli algoritmi a conferire ed estrarre valore dai dati grezzi mediante l'analisi descrittiva, predittiva e prescrittiva*»[48] e pertanto si dovrebbe prendere in con-

---

[44] Cfr. altresì l'*Indagine conoscitiva sui Big Data*, cit., p. 109 ss.

[45] Cfr. S. MANNONI, G. STAZI, *Is Competition a Click Away?*, cit., p. 46.

[46] I. GRAEF, *Eu Competition Law, Data Protection and Online Platforms. Data as Essential Facilities*, Alphen an de Rijn, 2016, p. 259. Sul tema si veda anche Commissione europea, *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 10 gennaio 2017, pp. 19-20.

[47] V. MAYER-SCHOMBERGER, T. RAMGE, *Reinventing Capitalism in the Age of Big Data*, Paris, 2018, p. 169. Cfr. S. MANNONI, G. STAZI, *Is Competition a Click Away?*, cit. p. 48, dove gli Autori sollevano – tra gli altri – un interrogativo fondamentale: risorsa essenziale è il dato o l'informazione? E se è l'informazione, «*il concorrente che chiede di considerare i dati dell'impresa dominante come risorsa essenziale come può sapere quale informazione ne potrà ricavare?*».

[48] S. MANNONI, G. STAZI, *Is Competition a Click Away?*, cit., p. 48.

siderazione l'ipotesi che sia la combinazione dei *big data* con *un certo algoritmo* ad erigere la barriera all'ingresso del mercato e quindi a porre i più seri problemi antitrust.

Il ragionamento, se portato agli estremi, finirebbe per includere l'algoritmo di Google nell'*essential facility* del mercato dell'*online advertising*, con rilevanti conseguenze sul piano antitrust: scenario, questo, che per il momento può essere preso in considerazione solo per pura speculazione teorica.

Quel che comunque appare sin da subito evidente è che l'approccio *privacy-oriented* che aveva caratterizzato la procedura intentata contro Facebook è in questo caso accantonato, in favore di uno più economico e di una garanzia della concorrenza, per così dire, "pura".

In questo caso l'Autorità non si cura della possibile violazione del diritto alla *privacy*, né – più sottilmente – del rischio di compromissione della libertà di scelta del consumatore, ma si occupa solo della utilizzazione dei dati a fini di profilazione e, dunque, si pone al di là del bene e del male, al di là delle ragioni e delle modalità con cui tali dati sono stati raccolti.

Se da un lato tale decisione ha il pregio di riportare l'*enforcement* antitrust entro i canoni della prevedibilità, dall'altro occorre però evidenziare come il susseguirsi di approcci differenti rischi di qualificare l'intervento dell'Autorità come *randomico* e la protezione degli interessi 'altri', come la *privacy* (pur se sempre intesa come forma di tutela della libertà economica del consumatore) solo occasionale.

5. *L'assetto della regolazione: la forza dei princìpi, oltre teoria dei silos*

Senza scadere nel catastrofismo, il fenomeno è più grave di quel che sembra, sia sotto il profilo della tutela dei diritti fondamentali nell'ambiente digitale, sia sul piano dell'adeguatezza dell'assetto della regolazione. La dinamica della regolazione del mercato in funzione della tutela della concorrenza, importata dal modello statunitense dello *Sherman Act*[49] e del *Clayton Act*, si muo-

[49] Lo *Sherman Antitrust Act* fu approvato nel 1890 ed è la più antica legge antitrust degli USA, volta a contrastare la formazione di monopoli e di cartelli. Per alcuni anni la legge rimase pressoché inapplicata, finché il Presidente Roosevelt non ne fece uso per combattere il trust ferroviario della *Northern Securities Company*, che nel 1902 fu sciolto; cfr. G.J. STIGLER, *Monopoly and Oligopoly by Merger*, in *The American Economic Review*, vol. 40, n. 2, *Papers and Proceedings of the Sixty-second Annual Meeting of the American Economic Association* (May, 1950), pp. 23-34. In seguito anche il Presidente William Howard Taft la utilizzò per colpire il monopolio della American Tobacco Company. Il più grande successo dello Sherman Act fu lo smembramento, in ben ventisei società, della Standard Oil.

ve ancor oggi secondo le logiche di regolazione *ex post*. I regolatori accertano fatti e comportamenti rispetto a norme previe: data una certa nozione di abuso di posizione dominante, l'Autorità di regolazione interviene sul mercato *una volta che* l'abuso si sia verificato e il danno alla concorrenza perpetrato (*theory of harm*) [50].

Se in un contesto di relativa stabilità delle dinamiche di mercato tale meccanismo di intervento pubblico nell'economia poteva ritenersi efficace, e anzi massimamente rispettoso della libera iniziativa economica dei soggetti privati, nel contesto di un mercato in continua, profonda e sempre più rapida trasformazione gli antichi paradigmi sembrano non soccorrere più. Tantopiù se oggetto di scambio commerciale non sono più beni materiali e valori monetari, ma dati personali e personalissimi.

L'inadeguatezza dell'assetto della regolazione emerge con ancora maggior chiarezza se si allarga lo sguardo alle confinanti discipline del consumo e dei dati personali, tutte trasversalmente impattate dall'avvento della *platform economy* [51]. Da circa trent'anni, infatti, l'Unione europea ha sviluppato discipline di settore, autonome e parallele (i cc.dd. silos regolatori verticali [52]), che solo di recente ha cercato – a fatica – di ricollegare fra loro, ora approntando nuovi princìpi generali, ora rafforzando norme intersettoriali [53].

Lo scenario che si si apre è allora quello di un regolatore che, se davvero vuole predisporre una regolazione *future-proof* [54], deve accettare di cedere parte del proprio potere regolativo ai protagonisti privati dell'evoluzione tecnologica (adottando una delle possibili soluzioni di *co-regulation* [55]), ma che deve rigua-

---

[50] Sulla inadeguatezza della "matrice regolatoria" a irregimentare il sempre crescente potere delle grandi piattaforme digitali, cfr. F. BASSAN, *Le piattaforme digitali tra co-regolazione, concorrenza e codificazione di diritto uniforme*, cit., p. 175.

[51] F. BASSAN *Le piattaforme digitali tra co-regolazione, concorrenza e codificazione di diritto uniforme*, cit., p. 175, nt. 23, afferma che «*le piattaforme digitali s'inseriscono infatti tra i silos verticali, operando nei diversi settori in ragione dei poteri delle autorità di regolazione e vigilanza nonché dello stato e del grado di resilienza dei mercati*».

[52] F. BASSAN, *Potere dell'algoritmo e regolazione dei mercati. La sovranità perduta sui servizi*, Soveria Mannelli, 2019.

[53] Emblematica in tal senso è la *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale* (c.d. AI ACT) presentata dalla Commissione europea il 21 aprile 2021, che introduce norme intersettoriali trasversali al settore (e al diritto) pubblico e privato. Cfr. A. SIMONCINI, E. CREMONA, *La AI tra pubblico e privato*, in corso di pubblicazione sulla rivista *DPCE online*, fasc. 1/2022.

[54] Cfr. S. RANCHORDÁS, M. VAN'T SCHIP, *Future-Proofing Legislation for the Digital Age*, in S. RANCHORDAS, Y. ROZNAI, *Time, Law, and Change*, Oxford, 2020; F. LAVIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *Osservatorio sulle fonti*, fasc. 3/2021, pp. 1163 ss.

[55] Cfr. F. BASSAN, *Le piattaforme digitali tra co-regolazione, concorrenza e codificazione di diritto*

dagnarne almeno altrettanto nella fissazione dei princìpi generali[56] e nel controllo giurisdizionale, a maglie larghe, sull'*effettivo* rispetto di quei princìpi.

Un circolo regolatorio, quindi, che il soggetto pubblico deve aprire e chiudere, ma che dovrà sempre più facilitare l'ingresso delle competenze e della capacità di regolazione uniforme dei soggetti privati[57] protagonisti del progresso tecnologico.

6. *Verso un sindacato del giudice amministrativo sull'eccesso di potere … privato?*

L'analisi della giurisprudenza delle corti nazionali sulle sanzioni irrogate dalle Autorità indipendenti alle piattaforme digitali, sopra accennata, offre pretesto per una riflessione conclusiva sulle prospettive di tutela giurisdizionale nei confronti dei poteri privati nell'ambiente digitale.

Prendiamo come paradigmatico il caso *Facebook c. Antitrust* deciso dal Consiglio di Stato. Questo pronunciamento ha senza dubbio un pregio che attiene al merito della decisione: il riconoscimento del valore patrimoniale dei dati personali non è effettuato al fine di squalificare un diritto fondamentale, di assoggettarlo alle logiche mercantilistiche, ma bensì ad innalzare il livello di tutela e promuovere l'avanzamento dei diritti.

Anzi. La sentenza smaschera una certa ipocrisia celata nel diritto europeo che regola il mondo digitale: dall'acronimo incompleto del GDPR (che menziona solo la protezione dei dati, ma non la loro libera circolazione, pure ri-

---

uniforme, cit., pp. 177-181; cfr. sul tema, G. TEUBNER, *Il trilemma regolativo. A proposito della polemica sui modelli giuridici post-strumentali*, in *Pol. dir.*, 1987, n. 1, p. 100 ss., il quale avverte che «*i confini della regolazione sono quindi definiti dai tre limiti dell'auto-produzione. La regolazione è efficace solo nella misura in cui conserva, nei sistemi regolati del diritto e della politica, le interazioni auto-riproduttive interne al sistema sociale regolato. Questa triplice relazione di compatibilità può essere chiamata "collegamento strutturale"*». Analogamente, a questo punto, possiamo formulare il *trilemma* regolativo: se la regolazione non rispetta le condizioni del collegamento strutturale fra diritto, politica e società, il risultato sarà necessariamente il *gap* regolativo.

[56] Cfr. G. VETTORI, *La forza dei principi. Ancora un inizio*, in *Pers. e merc.*, 1/2019, p. 4.

[57] Ormai organizzati come veri e propri ordinamenti giuridici privati. Cfr. O. LOBEL, *The Law of the Platform*, in *Minnesota Law Review*, 2016, p. 101, e spec. par. IV, *From Code as Law to Platform as Regulation*, p. 142 ss.; T.E. FROSINI, *Internet come ordinamento giuridico*, in *Perc. cost.*, 2014, fasc. 1, p. 13 ss.; per alcuni tali ordinamenti sarebbero addirittura dotati di un proprio territorio: «*Cyberspace is a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world"*», D.R. JOHNSON, D.G. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, vol. 48, p. 1378.

corrente nel titolo), al famoso considerando n. 24 della Direttiva 770/2019 (inizialmente formulato nel senso di una presa d'atto del valore economico del dato personale, poi censurato in sede di *drafting* finale), e tange altresì il tema del ruolo attribuito al consenso degli utenti online di fronte alle piattaforme [58]. È esperienza comune, e il tema è stato ampiamente affrontato in questo volume [59], che nell'ambiente digitale, la prestazione del consenso non è che un simulacro di una effettiva manifestazione di volontà.

Ma lasciando in disparte questi temi, si vuole qui concentrarsi su di un aspetto apparentemente "processuale", ma in realtà denso di ricadute sul piano del diritto sostanziale e in particolare sotto il profilo della possibilità di correggere le nuove asimmetrie nell'ambiente digitale.

Com'è noto, nell'ordinamento italiano, le sanzioni amministrative delle Autorità indipendenti sono soggette ad uno scrutino intrinseco da parte del giudice. La *full jurisdiction* [60], intesa come sindacato pieno e penetrante sull'azione amministrativa, porta – secondo le tesi più "spinte" – alla sostituzione del giudice all'amministrazione. Tale esigenza è stata avvertita più fortemente proprio con riferimento all'attività delle Autorità indipendenti, che in forza della propria indipendenza (che non è imparzialità [61]), pongono più seri problemi di rispetto del principio di legalità e in generale della tutela dei diritti dei soggetti interessati dal loro intervento [62].

Ebbene, nel caso delle sanzioni antitrust, la *full jurisdiction* diventa una sorta di lente d'ingrandimento grazie alla quale il giudice amministrativo diviene in grado di vedere cose che – nell'esercizio della normale giurisdizione di legittimità sugli atti e sui rapporti amministrativi – non vedeva.

---

[58] Riproduce questo *vulnus* all'autodeterminazione informativa, da ultimo, anche l'art. 5 del *Digital Markets Act*, che vieta ai *gatekeeper* la combinazione di dati personali provenienti da servizi diversi … salvo che l'interessato abbia prestato il proprio consenso.

[59] Si veda il contributo di Tommaso POLVANI in questo volume.

[60] Così sintetizza un complesso tema F. FOLLIERI, *La giurisdizione di legittimità e full jurisdiction. le potenzialità del sindacato confutatorio*, in *P.A. Persona e Amministrazione*, n. 2, 2018, pubblicato il 30 dicembre 2018: «*secondo recenti studi sul concetto di full jurisdiction nella giurisprudenza della Corte EDU sull'art. 6 della Convenzione, la full jurisdiction richiede che il giudice si sostituisca all'amministrazione, sia nella ricostruzione dei fatti (anche nei casi di c.d. "discrezionalità tecnica"), sia nella decisione circa la misura da adottare e il relativo assetto di interessi (la c.d. "discrezionalità amministrativa" o "discrezionalità pura"). In altre parole, secondo quest'interpretazione della giurisprudenza della Corte, la full jurisdiction coincide con il sindacato diretto o sostitutivo (permesso solo in giurisdizione di merito) e non invece con il sindacato indiretto o confutatorio (permesso in giurisdizione di legittimità)*».

[61] Come ricorda Corte cost. n. 13/2019.

[62] Si pensi alla lunga saga delle sanzioni Consob e Banca d'Italia. Cfr. E. BINDI, A. PISANESCHI, *Sanzioni Consob e Banca d'Italia. Procedimenti e "doppio binario" al vaglio della Corte EDU*, Torino, 2018.

In particolare, il giudice amministrativo mentre rivede o riforma la sanzione amministrativa irrogata dall'autorità di regolazione finisce per censurare quasi *direttamente* l'attività del soggetto privato, "saltando" l'intermediazione dell'Autorità amministrativa e confrontandosi direttamente col *fatto* più che con l'*atto*[63].

La mediazione dell'atto amministrativo gravato d'impugnazione, poi, si fa ancor più evanescente quando l'Autorità, come nel caso di specie fa uso di norme a fattispecie aperta che richiamano clausole generali, come ad esempio quelle contenute nel Codice del consumo, dove si configurano come fondamentali i diritti «*ad una adeguata informazione e ad una corretta pubblicità*», «*all'esercizio delle pratiche commerciali secondo principi di buona fede, correttezza e lealtà*» e «*alla correttezza, alla trasparenza ed all'equità nei rapporti contrattuali*»[64].

È stato osservato che per certi versi le Autorità che sono abilitate ad applicare norme a fattispecie aperta riescano ad essere spesso più incisive rispetto a quelle che esercitano poteri nomativi. Ed è effettivamente così: esse, prima, "chiudono la fattispecie" e poi la applicano[65].

L'utilizzo di tali norme elastiche, allargando molto il margine di discrezionalità rimesso all'amministrazione, finisce per trasformare il sindacato del giudice amministrativo sulla loro attività da un sindacato sulla *violazione di legge* ad uno scrutinio sull'*eccesso di potere*.

Ma non (solo) dell'amministrazione, ma del potere … privato, che esercita la propria "discrezionalità" nella veste della libertà d'impresa[66].

---

[63] Il percorso di allontanamento della giurisdizione amministrativa dal modello di giudizio sull'atto è da lungo tempo stato messo in evidenza dalla dottrina.

[64] Così l'art. 2 del Codice del consumo. Il successivo art. 5, comma 3, del medesimo codice, stabilisce, inoltre, che «*le informazioni al consumatore, da chiunque provengano, devono essere adeguate alla tecnica di comunicazione impiegata ed espresse in modo chiaro e comprensibile, tenuto anche conto delle modalità di conclusione del contratto o delle caratteristiche del settore, tali da assicurare la consapevolezza del consumatore*». La giurisprudenza soggiunge che «*l'obbligo di estrema chiarezza gravante sul professionista deve essere da costui assolto sin dal primo contatto, attraverso il quale debbono essere messi a disposizione del consumatore gli elementi essenziali per un'immediata percezione della offerta pubblicizzata*» (cfr. Cons. Stato, sez. VI, 14 ottobre 2019, n. 6984, 15 luglio 2019, n. 4976 e 23 maggio 2019, n. 3347).

[65] Cfr. G. DE MINICO, *Regole. Comando e consenso*, Torino, 2005, *passim*.

[66] In questo senso, poco importa che i principi siano codificati. La dottrina da tempo ha chiarito che «*la trascrizione del principio in una norma non è sufficiente, di per sé, per trasformare il tipo di sindacato necessario per applicare il principio*»: non si transita cioè, sol per questo, da un sindacato sull'eccesso di potere ad un sindacato sulla violazione di legge. Cfr. C. MARZUOLI, *Discrezionalità amministrativa e sindacato giurisdizionale: profili generali*, in *Dir. pubbl.*, 1998, p. 150, cit. in C. CUDIA, *Eccesso di potere e clausole generali*, in S. TORRICELLI, *Eccesso di potere e altre tecniche di sindacato sulla discrezionalità. Sistemi giuridici a confronto*, Torino, 2018, p. 66.

Questa giurisprudenza ne è un esempio piuttosto chiaro: il Giudice amministrativo si è appuntato più sul comportamento del soggetto privato destinatario della sanzione che sulla sanzione stessa. Cioè in qualche modo ha sindacato l'esercizio della "discrezionalità" di *Facebook*, che – in quanto privato – assume le forme (non della discrezionalità amministrativa ma) di una libera decisione sul tipo di informazione da dare ai propri utenti in merito al trattamento dei dati.

Si tratta di uno spunto importante, perché attiene alla qualità del sindacato giurisdizionale sull'attività economica dei privati.

Facciamo qualche passo indietro. È noto che la libertà di iniziativa economica privata nasce già funzionalizzata all'interesse sociale con l'art. 41 della Costituzione; anzi essa storicamente non è mai uguale a sé stessa: si contrae e si riespande a seconda delle temporanee esigenze di regolazione del mercato.

Tale funzionalizzazione, tuttavia, non ha mai consentito uno scrutinio dell'attività dei soggetti privati alla luce del solo parametro dell'assolvimento di una qualche funzione sociale, spingendosi il sindacato del giudice tuttalpiù fino alla c.d. *business judgment rule* o all'uso di clausole generali, come la buona fede e la correttezza, al fine di preservare il vincolo solidaristico contenuto nei rapporti contrattuali, specie se asimmetrici [67].

Fino a non molto tempo fa, ad esempio, la libertà di impresa di queste piattaforme è stata esercitata in modo pressoché incontrollato nell'ambiente digitale. Anzi, c'è chi sostiene che tali piattaforme siano il più grande successo della *deregulation* e la prova dell'esistenza della mano invisibile, salvo che ad arricchirsi – al posto delle nazioni – sono le grandi piattaforme [68].

Così, esse hanno assunto posizioni di potere incontrastato sui mercati. Ad ogni modo, oggi c'è una ampia letteratura che si intrattiene sulla natura di 'potere' di questi soggetti privati, a partire proprio dalla loro capacità di incidere unilateralmente sui diritti e le libertà fondamentali (la raccolta dei dati personali è solo *uno* dei modi d'essere di queste piattaforme che incide sui diritti fondamentali). Si ripropone, nell'ambiente digitale il dilemma fondamentale del diritto costituzionale: il rapporto tra potere e libertà [69].

---

[67] G. SIGISMONDI, *Le analogie tra sindacato sul potere pubblico e sui poteri privati*, in G. FALCON, B. MARCHETTI, *Pubblico e privato nell'organizzazione e nell'azione amministrativa*, Padova, 2013, e *amplius* ID., *Eccesso di potere e clausole generali. Modelli di sindacato sul potere pubblico e sui poteri privati a confronto*, Napoli, 2012.

[68] Il richiamo è alla notissima formula della mano invisibile di Adam Smith, ne *La ricchezza delle Nazioni*.

[69] Esattamente nei termini in cui lo pose oltre cinquanta anni fa G. LOMBARDI, *Potere privato e diritti fondamentali*, Torino, 1970. Cfr. A. SIMONCINI, *Sovranità e potere nell'era digitale,* in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), *Diritti e libertà in internet*, Firenze,

Ciò posto, il tenore costituzionale del problema potrebbe indurre a salutare di buon occhio questo fenomeno che abbiamo descritto come la trasformazione del sindacato del giudice amministrativo per violazione di legge sulle sanzioni delle autorità indipendenti in un sindacato sull'eccesso di potere dei soggetti privati.

Questo per una ragione invero molto semplice. Storicamente, il vizio dell'eccesso di potere si è configurato come strumento versatile per il sindacato dell'esercizio del potere pubblico *da un punto di vista sostanziale*[70].

Ne è nota la traiettoria evolutiva, cui la Costituzione del '48 ha impresso una accelerazione decisiva[71]. In altre parole, nell'epoca del predominio del potere pubblico, la figura dell'eccesso di potere è stato il "grimaldello" attraverso il quale si è potuta superare l'idea di un controllo meramente formale sul 'potere' (cioè di valutazione di mera conformità ad uno schema legale) e si è potuti accedere – dapprima – ad una misura della devianza dalla funzione, della devianza dal perseguimento dell'interesse pubblico, e – da ultimo – ad un giudizio sintetico del risultato economico-sociale dell'azione amministrativa[72].

Tornando al nostro tempo, e cioè in un'epoca di predominio di poteri privati, uno scrutinio giurisdizionale sull'uso del potere da parte di questi soggetti (certo, sempre mediato dalle Autorità di regolazione) potrebbe fare tremendamente comodo in termini di tutela dei soggetti deboli nell'ambiente digitale.

Quando, ad esempio, si afferma che il fenomeno della patrimonializzazione del dato personale "impone" alle grandi piattaforme di rispettare «*obblighi di chiarezza, completezza e non ingannevolezza*» il giudice amministrativo sta sostanzialmente sindacando l'esercizio del potere *discrezionale* di Facebook (cioè l'esercizio della sua libera impresa) e allo stesso tempo conformando l'attività

2017, p. 19 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, p. 67; sia consentito rinviare anche a E. CREMONA, *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in *Oss. fonti*, fasc. 2/2021, p. 879 ss.

[70] A. POLICE, *L'eccesso di potere nel prima della Costituzione repubblicana*, in S. TORRICELLI, *Eccesso di potere e altre tecniche di sindacato sulla discrezionalità. Sistemi giuridici a confronto*, cit., 2018, p. 41 ss.

[71] Dall'originaria figura dello straripamento di potere, dallo sviamento di potere, si è passati alla elaborazione delle figure sintomatiche, autonomizzandole dalla figura dello sviamento e trasformandole in un catalogo aperto suscettibile, tra l'altro, di essere ridotto per effetto della codificazione di alcune ipotesi e, dall'altro, incrementato attraverso il riferimento a nuovi diritti di respiro costituzionale (tra i quali, appunto, alcune clausole generali: ragionevolezza, proporzionalità, buona fede, affidamento, che hanno allargato la prospettiva dell'art. 97 Cost.). Cfr. A. POLICE, *op. ult. cit.*, p. 52.

[72] Cfr. C. CUDIA, *Funzione amministrativa e soggettività della tutela. Dall'eccesso di potere alle regole del rapporto*, Milano, 2008.

del soggetto titolare del potere (privato, non amministrativo) al perseguimento di un interesse pubblico, in assenza di una regola *specifica* che a ciò vincoli, ma piuttosto facendo governo di princìpi costituzionali e clausole generali.

Questa giurisprudenza, perciò, non ha solo il pregio di avere definitivamente fatto luce sulla natura patrimoniale della cessione di dati personali, ma altresì di avere aperto un varco di tutela delle situazioni soggettive dell'"interessato-utente-consumatore" nei confronti del 'potere', per privato che sia.

Finito di stampare nel mese di aprile 2022
nella Stampatre s.r.l. di Torino
Via Bologna 220

DIMENSIONE GIURIDICA | LEGAL DIMENSION

Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

---

Volumi pubblicati:

1. D. BIANCHI-M. RIZZUTI (a cura di), *Funzioni punitive e funzioni ripristinatorie. Combinazioni e contaminazioni tra sistemi*, 2020.
2. S. COCCHI-A. SIMONI (eds.), *Freedom v. Risk? Social Control and the Idea of Law in Covid-19 Emergencies*, in corso di pubblicazione.
3. D. BIANCHI (a cura di), *Distribuzione del rischio sanitario tra responsabilità dell'organizzazione e responsabilità individuali*, 2021.
4. E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, 2022.