PA Persona e Amministrazione
Ricerche Giuridiche sull'Amministrazione e l'Economia

Renato Rolli
Professore Associato presso il Dipartimento di Scienze Aziendali e Giuridiche dell'Università della Calabria
renatorolli@hotmail.com
Mariafrancesca D'Ambrosio
Dottoressa in Giurisprudenza, cultrice di Contabilità di Stato presso il Dipartimento di Scienze Aziendali e Giuridiche dell'Università della Calabria
dambrosio.mfrancesca@gmail.com

Consenso e accountability: i poli del commercio dei dati personali online

Consent and accountability: the poles of online personal data trade

Sintesi

Sin dagli albori del nuovo millennio, la rapidissima diffusione del web ha stravolto ogni aspetto della quotidianità, forse anche in modo latente. Il *world wide web* costituisce uno strumento in grado di colorare di nuove sfumature la libertà di espressione del pensiero, di esplorare l'ignoto e di trovare risposta ad ogni quesito. Tuttavia, la fruizione di questo incredibile strumento ha un prezzo: la dazione totale dei *personal data* ed il conseguente annullamento della *privacy*. Navigando in Internet, infatti, si rendono disponibili ad una platea indefinita di destinatari, i "dati personali" di ciascun utente. Tale espressione potrebbe allora risultare ossimorica: cosa rimane di "personale" nei dati immessi in rete? La diffusione dei dati sensibile apre la strada ad un'ulteriore questione: chi detiene il controllo e, dunque, chi è responsabile di tale diffusione?
La risposta a tali quesiti rende necessario esaminare la natura dei dati immessi in Rete nonché la fitta trama del sistema di *accountability* va che delineandosi nella giurisprudenza delle Corti nazionali e sovranazionali.

Abstract

Since the dawn of the new millennium, the rapid spread of the web has disrupted every aspect of everyday life, perhaps even in a latent way. The world

wide web is a tool that can add new shades of colour to the freedom of expression, it can explore the unknown and it can find answers to every question. However, the use of this incredible tool comes at a price: the total disclosure of personal data and the consequent loss of privacy. In fact, surfing the Internet makes the 'personal data' of each user available to an indefinite number of recipients. This expression could then be oxymoronic: what remains of 'personal' in the data put on the web? The dissemination of sensitive data opens the way to a further question: who is in control, and therefore who is responsible for this dissemination?

The answer to these questions makes it necessary to examine the nature of the data placed on the Net, as well as the dense weave of the accountability system that is emerging in the jurisprudence of the national and supranational Courts.

PAROLE CHIAVE: big data; consenso; privacy; libertà di manifestazione del pensiero; responsabilità.

KEYWORDS: big data; consent; privacy; freedom of speech; accountability.

1. *Big data* e consenso inconsapevole

Con il termine inglese *Big Data* (cosiddetti megadati) si suole indicare una quantità di dati ed informazioni così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza. L'espressione viene utilizzata, cioè, per indicare la capacità di analizzare ovvero di estrapolare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati – grazie a sofisticati metodi statistici e informatici di elaborazione – al fine di scoprire i legami tra fenomeni diversi – ad esempio, correlazioni – e prevedere quelli futuri.

Tanto premesso, mette conto osservare come tali dati possano costituire oggetto di molteplici attività:

- statistica, intesa quale raccolta di dati e informazioni in forma esclusivamente aggregata e anonima volta a verificare il corretto funzionamento del sito;
- sicurezza, da intendere alla stregua di raccolta di dati e informazioni diretta a tutelare la sicurezza del sito (filtri antispam, *firewall*, rilevazione virus) e degli Utenti ed a prevenire o a far emergere frodi o abusi a danno del sito web;
- attività accessorie, quali la comunicazione dei dati a terze parti che svolgono funzioni necessarie o strumentali all'operatività del servizio – es. box commenti;
- consulenze e incarichi professionali, rispetto ai quali l'utilizzo dei dati è finalizzato alla valutazione dell'incarico, nonché all'eventuale adempimento dello stesso.

È di tutta evidenza che un flusso costante di informazione possa divenire *res in commercio*.

Occorre osservare altresì che la crescita di questi dati segue un andamento tridimensionale[1] (modello delle 3V). Ne discende che con il trascorrere del tempo ne aumenta:
- la varietà: i dati arrivano in modo disomogeneo, trattandosi di foto, documenti, valori alfanumerici, video, audio;
- il volume: la grande quantità di dati proviene da sorgenti differenti (*social media*, transazioni finanziarie, acquisti *online*);
- la velocità: intesa quale velocità di affluenza dei dati ed alla conseguente necessità di utilizzarli in modo tempestivo.

Per le suesposte caratteristiche i megadati sono oggetto, tipicamente, di due azioni: il *Management*, inteso quale serie di processi concernenti l'acquisizione e la memorizzazione di informazioni; l'*Analytics*, ossia l'analisi dei dati da svolgersi in tempi rapidi.

1Il presente contributo è opera dell'analisi e dell'approfondimento congiunto di Renato Rolli e Mariafrancesca D'Ambrosio. In particolare Renato Rolli ha curato l'introduzione e i paragrafi 2, 5. Mariafrancesca D'Ambrosio si è occupata dei paragrafi 1, 3, 4.
Teoria elaborata nel 2001 dall'analista Doug Laney.

Tanto conduce a delineare il ciclo di vita dei *Big Data*, scandito in una serie di processi che dalla raccolta delle informazioni conduce, attraverso successive modifiche, al loro utilizzo passando, talvolta, per la fase di bonifica, necessaria allorquando nel pacchetto vi siano informazioni non più utili ai fini dell'elaborazione.

Più precisamente, l'acquisizione avviene mediante canali (*Application programming interface*, c.d. API[2]) che al momento dell'accesso al sito importano i dati da *database* preesistenti ovvero interpretano ed estrapolano il flusso di dati che passa in rete; o, ancora, tramite *cookie*, frammenti di dati sugli utenti memorizzati sul computer e utilizzati per personalizzare la navigazione.

Successivamente, la grande quantità di dati raccolta viene stoccata ed archiviata: prende avvio, dunque, la fase relativa all'analisi, alla modellazione – tramite algoritmi ideati per consentire lo studio, l'analisi ed il confronto del flusso dei dati, al fine di estrapolarne informazioni utili per studi futuri – ed alla conseguente interpretazione delle informazioni. Invero, i *Big Data* sono estremamente eterogenei giacché provengono da una molteplicità di siti e di fonti. Tanto ne rende necessaria e – certamente non agevole – l'interpretazione.

Com'è noto, ciascun utente quotidianamente utilizzando lo *smartphone*, il *tablet* o il PC genera, anche inconsapevolmente, una ingente quantità di informazioni: ebbene, gli assai diffusi social network –tra tutti *Instagram* e *Facebook* (ora Meta) – i blog, i siti di vendita online – per tutti, *Amazon* – i motori di ricerca – come *Google*, Safari – ed ancora i più svariati siti internet, registrano le azioni compiute dagli utenti per poi indirizzarle e canalizzarle nelle ricerche future: basti pensare che il mero compimento di una ricerca su Google o la semplice navigazione nel web, genera una grande quantità di informazioni.

2 Le API, quindi, sono delle interfacce grafiche che sviluppatori e programmatori terzi possono utilizzare per espandere le funzionalità di programmi, applicazioni e piattaforme di vario genere (software e non solo). Rappresentano, quindi, l'interfaccia aperta attraverso la quale interagire con programmi (o parti di essi) altrimenti inaccessibili.
Utilizzando un'API, un programmatore può far interagire due programmi (o due piattaforme, o un programma e una piattaforma) altrimenti tra loro incompatibili. Utilizzando, quindi, degli "artifici" di programmazione, si possono estendere le funzionalità di un programma ben oltre le reali intenzioni dello sviluppatore o della software *house* che l'ha realizzato.

Il conferimento del consenso[3] al trattamento dei dati così forniti avviene tramite un banner posto – generalmente – in fondo alla pagina web, ovvero tramite il solo utilizzo o la consultazione del sito, quale comportamento concludente: in tal modo visitatori e utenti approvano l'informativa privacy e acconsentono al trattamento dei loro dati personali ed anche alla eventuale diffusione a terzi se necessaria per l'erogazione di un servizio.

D'altro canto, deve osservarsi come il conferimento e, quindi, il consenso alla raccolta e al trattamento dei dati, sia facoltativo: in altri termini, l'utente può negare o revocare in qualsiasi momento un consenso già fornito. Tuttavia, negare il consenso può comportare l'impossibilità di erogare alcuni servizi e l'esperienza di navigazione nel sito risulterebbe compromessa.

Ebbene, tanto conduce a chiedersi sino a che punto si possa effettivamente decidere se acconsentire alla diffusione dei propri dati, posto che, allo stato, la fruizione totale del servizio in rete parrebbe subordinata alla necessaria prestazione del consenso. Si può, allora, correttamente asserire che la scelta sia rimessa al titolare dei dati?

2. Il valore economico dei *Big data*

Tanto premesso, giova osservare come tanto la raccolta di una quantità di dati sempre più elevata, tanto la conseguente estrazione delle informazioni che si ritengono necessarie costituiscano due operazione centrali nell'ambito di qualsivoglia business: invero, grazie all'utilizzo di questa risorsa è possibile accrescere l'efficienza dei processi produttivi e delle capacità decisionali, prevede-

3 In riferimento alla natura giuridica del consenso, con riguardo alla disciplina dettata dalla l. 31 dicembre 1996, n. 675, v. S. Patti, Art. 11. Consenso, in C. M. Bianca, F. Busnelli, A. Bellelli, F. P. Luiso, E. Navarretta, S. Patti, P. M. Vecchi (a cura di), *Tutela della privacy, cit.*, 359; V. Zeno Zencovich, *Il consenso informato e l'autodeterminazione informativa*, in Corr. giur., 1997, 915.
In epoca più recente, con riferimento alla previgente disciplina dettata dal codice della privacy, v. S. Mazzamuto, Il principio del consenso e il problema della revoca, in R. Panetta (a cura di), *Libera Circolazione e protezione dei dati personali*, t. I, Milano, 2006, 1016; A. Orestano, *La circolazione dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 188. E, in riferimento alla rilevanza che il consenso assume nel regolamento 2016/679 UE, v. F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in Il nuovo Regolamento Europeo sulla privacy e sulla protezione dei dati personali.

re con maggiore accuratezza le tendenze attuali e future e, in conseguenza di ciò, rendere più mirate e precise le attività commerciali nell'individuazione del proprio target di mercato. È evidente, allora, che lo sfruttamento dei dati personali possiede un vero e proprio valore economico.

È doveroso premettere, tuttavia, che i dati non hanno valore intrinseco (ossia quali dati grezzi): le informazioni in essi contenute, invero, assumono valore nella misura in cui costituiscano oggetto delle attività di organizzazione, gestione, filtraggio ed estrazione[4].

A tal fine viene in rilievo la distinzione che intercorre tra le attività commerciali proprie del campo del *business* riguardante i dati: vi rientrano, da un alto, le attività che permettono l'accesso a servizi e/o beni dietro il rilascio di dati personali – ai quali si aggiungono dati ulteriori, per effetto delle attività che l'utente svolge sulle piattaforme digitali – nelle quali il prezzo del servizio è ridotto a fronte dell'accesso ai suddetti dati; dall'altro, vi sono le attività di raccolta e vendita dei dati effettuate da brokers e aventi quali destinatari gli operatori interessati a possederli ai fini di una più ottimale profilazione degli utenti. I *data broker* sono il chiaro esempio di come l'informazione sia denaro: *nella società della conoscenza in cui viviamo le informazioni digitali costituiscono il nuovo petrolio di cui sono disponibili immensi giacimenti che i data broker scandagliano H24 tutti i giorni dell'anno, senza che al momento nessun privato e nessuna autorità pubblica li controlli*[5].

Si comprende, allora, perché con sentenza del 10.1.2020, n. 261 il Tar Lazio abbia ritenuto ingannevole l'informativa fornita da *Facebook*, con la quale si affermava la gratuità dell'iscrizione in fase di prima registrazione, posto che i dati personali sono suscettibili di sfruttamento economico e, conseguentemente, assumono valore commerciale[6]. I Giudici hanno ritenuto che i dati persona-

4 S. MARCELLI, *Il valore dei dati: prospettive e caratteristiche dei big data*, nota [5]: I dati sono prodotti da innumerevoli fonti, per quanto concerne la loro gestione e organizzazione non si può poi prescindere da sistemi automatici o semiautomatici, come processori e/o algoritmi (si pensi ai sistemi di *machine learning)*, nonché in fase di filtraggio mediante processi di estrazione (c.d. *knowledge discovery in database)* tramite appositi software (*data mining, text mining ecc. ecc.)*

5 D. TALIA, *I data broker ci conoscono senza essere nostri amici.*

6 Il giudizio verte sulla legittimità del provvedimento con il quale l'Agcm aveva accertato l'illiceità della pratica commerciale di Facebook che in fase di registrazione dell'utente a fronte di

li, «*in quanto asset disponibili ad assurgere nell'ambito di un contratto alla funzione di "controprestazione"*, oltre a essere tutelati quale espressione di un diritto della personalità dell'individuo, debbano essere protetti *quale possibile oggetto di una compravendita tra operatori economici, ovvero tra questi ultimi e i soggetti interessati*[7]. Invero, *il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "social network"*»[8].

L'innovativa pronuncia del Tar – riconoscendo l'idoneità dei dati personali ad assumere rilievo economico e, conseguentemente, ad assolvere alla funzione di controprestazione in senso tecnico di un contratto – oltre a garantire una tutela ulteriore in materia di *privacy*, impone la rivalutazione tanto del valore delle informazioni di cui sono in possesso degli enti pubblici, tanto dei rapporti tra i cittadini e le stesse amministrazioni pubbliche detentrici dei loro *personal data*.

Alle delicate *quaestiones* relative alla tutela della *privacy* – che si affronterà *funditus* nel successivo paragrafo – si accompagnano una serie di criticità relative alle possibili derive anticoncorrenziali derivanti dalla loro attitudine ad incidere profondamente sulle corrette dinamiche di mercato.

---

un claim sulla gratuità del servizio offerto ("Iscriviti è gratis e lo sarà per sempre") ometteva di comunicare che le informazioni relative alla raccolta e all'uso a fini commerciali dei dati personali da parte della Società. L'Autorità aveva ritenuto il messaggio non veritiero e fuorviante, in quanto la raccolta e sfruttamento dei dati degli utenti a fini remunerativi si configurava come controprestazione del servizio offerto dal social network (tant'è vero che i ricavi provenienti dalla pubblicità on line, basata sulla profilazione degli utenti a partire dai dati forniti da questi ultimi, costituivano l'intero fatturato della società). La società aveva contestato la carenza di potere dell'Agcm, poiché in assenza di un corrispettivo patrimoniale e, quindi, di interesse economico dei consumatori da tutelare, gli obblighi violati avrebbero riguardato esclusivamente il profilo del trattamento dei dati personali degli utenti disciplinato dal Regolamento privacy e conseguentemente le attribuzioni del Garante per la protezione dei dati personali. Sul punto si rinvia a https://www.irpa.eu/il-tar-lazio-riconosce-il-valore-economico-commerciale-dei-dati-personali/.

7 Tar Lazio sentenza del 10.1.2020, n. 261.

8 Ibidem.

Invero, nell'ambito dell'economia digitale, tale fenomeno è particolarmente rilevante rispetto ai modelli di business operanti nei mercati a più versanti (c.d. *multi-sided platforms*)[9]: la raccolta di ingenti quantità di dati determina, per le aziende così organizzate, un notevole vantaggio informativo a discapito delle piattaforme che operano sul singolo versante.

Si impone poi la considerazione secondo la quale i *big data* non sono a tutti accessibili e, soprattutto, non lo sono con le medesime possibilità. Non può certamente porsi a confronto la potenza dei grandi colossi del digitale – avallata dall'operato dei *brokers*, quali intermediari nella vendita di pacchetti ingenti di dati – con quella degli operatori minori.

Ne discende che soltanto le aziende in possesso di una grande quantità di dati possono realizzare analisi sempre più approfondite e sofisticate dei megadati e avere, dunque, un assai incisivo potere di impatto sulle scelte di mercato.

In questo contesto va delineandosi una nuova economia che si caratterizza per la volontà/necessità di monetizzare questo ingente flusso di dati, del cui potenziale sono in grado di avvalersi solo poche aziende. Esempio lampante è *Google*, sorto come mero motore di ricerca e divenuto negli anni una macchina in grado, non soltanto di raccogliere le informazioni provenienti dalle ricerche e dalle navigazioni in rete, ma anche di conoscere ogni interesse, gusto, preferenza politica di chiunque ne faccia uso.

Emerge, a questo punto, un interrogativo: fino a che punto è accettabile una simile influenza sull'andamento dei mercati?

3. Il diritto alla protezione dei dati personali

9 Esempi di mercati a più parti sono quelli delle carte di credito (formato da coloro che possiedono una carta e i commercianti); sistemi operativi (utilizzatori finali e sviluppatori); pagine gialle (inserzionisti e consumatori); console di videogiochi (giocatori e sviluppatori di giochi); siti di reclutamento (persone che cercano lavoro e agenzie di collocamento); motori di ricerca (inserzionisti e utenti); e reti di comunicazione, come Internet. Esempi di aziende conosciute che utilizzano mercati a due parti sono American Express (carte di credito), eBay (negozio online), Taobao (negozio online in Cina), Facebook (social network), LinkedIn (social network professionale), Mall of America (centro commerciale), Match.com (piattaforma di appuntamenti), AIESEC (associazione studentesca che aiuta i giovani talenti a trovare un posto in un'azienda), Monster.com (piattaforma di reclutamento), e Sony (console di giochi).

La protezione dei dati[10] è colonna portante di una società nella quale le relazioni si svolgono *in toto* – o, comunque, in modo rilevante – secondo modalità digitali[11]. In tal senso, la protezione dati deve studiarsi e applicarsi quale tecnica di coesione sociale, non solo quale forma di tutela di un diritto fondamentale[12].

Lo sviluppo dilagante ed invasivo del *web* nella vita quotidiana ha accesso l'attenzione sulla questione *privacy*. Invero, nell'odierna società dell'informazione il concetto di *privacy* è intimamente legato a quello di diritto – consacrato in disposizioni nazionali ed internazionali – alla protezione dei dati personali, il cui emergere si deve allo sviluppo delle tecnologie digitali ed al ruolo centrale assunto dell'informazione nell'odierno contesto sociale ed economico. Tali considerazioni delineano le due facce della medaglia: la necessità – scaturente dalla piena appartenenza alla società attuale – di non ostacolare la circolazione di dati; i pericoli per i diritti e le libertà individuali derivanti da tale circolazione.

Ebbene, dirimente sarebbe l'attribuzione all'interessato di un potere di controllo sui dati che lo riguardano. In tal senso, il diritto alla protezione dei

---

10 Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica. Tra essi: i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa); i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale; i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

11 Sul dilagante uso del digitale nel settore pubblico si veda E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in Giornale di diritto amministrativo, 2015, n.2, p. 148-157; D. U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT;* A. G. OROFINO – *La semplificazione digitale*, in Il diritto dell'economia anno 65, n. 100 (3 2019), pp. 87-112.

12 F. PIZZETTI, *Dal GDPR al valore dei dati e delle informazioni*, in *privacylab.it.*

dati personali si sostanzierebbe nel diritto a che detti dati, ove trattati da terzi, siano protetti secondo le modalità stabilite dalla legge, sì da garantire un controllo sulla circolazione delle informazioni, nonché sulle condizioni e sui limiti del trattamento delle stesse: la ratio sarebbe individuabile nella valorizzazione della dignità e dell'autodeterminazione della persona umana mediante il conferimento di facoltà e poteri che conferiscono il controllo sulle qualità corporee ed immateriali che costituiscono l'individualità. Una simile configurazione ben si comprende se si considera che tale diritto è pacificamente ricondotto alla categoria dei diritti della personalità[13].

13 Come noto ai civilisti, la nozione dei diritti della personalità è conquista giuridica relativamente recente. Basti considerare che, generalmente, la loro nascita come categoria viene fatta risalire all'opera di O. Gierke, *Deutsches Privatrecht*, Lipsia, 1895, la quale contiene un capitolo dedicato ai «*persönlichkeitsrechte*». Le motivazioni che sono alla base di siffatto «ritardo», in quello che potrebbe definirsi come «processo di valorizzazione» della persona umana, vanno ricercate prevalentemente nella visione che il Codice civile italiano del 1942 ci consegnava dell'uomo, ovverosia quella di un soggetto il cui obiettivo principale consisteva nella accumulazione della ricchezza e nello scambio di beni e servizi, e la cui protezione era bensì garantita, ma affidata a complessi normativi altri rispetto al diritto civile, primo tra tutti quello del diritto penale. Si deve, quindi, agli sforzi della dottrina e della giurisprudenza, prima, e all'intervento del legislatore nazionale e sovranazionale, poi, il pieno sviluppo di un impianto giuridico, costituito da una unica, o da una pluralità, a seconda che si acceda alla tesi monista o a quella pluralista, di situazioni giuridiche soggettive, aventi ad oggetto gli attributi della persona, anche giuridica, in tutte le sue manifestazioni e sviluppi, passati, presenti, e futuri. Alla base del sistema dei diritti della personalità vi è, dunque, l'esigenza, avvertita sempre più fortemente con l'evoluzione della società, di proteggere tutti quegli interessi della persona ritenuti meritevoli di tutela da parte dell'ordinamento giuridico. Le forme di protezione più rilevanti che circondano tali situazioni giuridiche possono facilmente essere individuate nel diritto penale, da una parte, e nel diritto civile, dall'altra. In questa sede, non ci si soffermerà oltre sul tema brevemente accennato: si rimanda a A. De Cupis, *I diritti della personalità*, in Trattato di diritto civile e commerciale, diretto da A. Cicu, F. Messineo, Milano, 1959; A. Di Majo, *Profili dei diritti della personalità*, in Riv. trim. dir. proc. civ., 1, 1962, 69 ss.; D. Messinetti, *voce Personalità (diritti della)*, in Enc. dir., Milano, 1983; O. T. Scozzafava, *Nuovi e vecchi problemi in tema di diritti della personalità*, in Riv. crit. dir. priv., 1983, 207 ss.; A. Gambaro, *I diritti della personalità*, in Riv. dir. civ., 1984, 421 ss.; P. Rescigno, *voce Personalità (diritti della)*, in Enc. giur., Roma, 1991; V. Zeno-Zencovich, *voce Personalità (diritti della)*, in Dig. disc. priv., Sez. civ., Torino, 1996; Id., *I diritti della personalità*, in Diritto civile, diretto da N. Lipari, P. Rescigno, Milano, 2009; G. Alpa, G. Resta, *Le persone fisiche e i diritti della personalità*, in Trattato di diritto civile, diretto da R. Sacco, Torino, 2006. Nella letteratura straniera, si veda, in generale, R. Savatier, *Le métamorphoses èconomiques et sociales du droit privé d'aujourd'hui, Troisième série, Approfondissement d'un droit revouvelé*, Parigi, 1959, 5 ss.; P. Tercier, *Der Entwicklungsstand des Persönlichkeitsschutzes* in Kontinentaleuropa, in Aa.Vv., Das Persönlichkeitsrecht im Spannungsfeld zwischen Informationsauftrag und Menschenwürde: Vortragsveranstaltung, München, 1989, 71 ss.; K. Peifer, *Individualität im Zivilrecht: Der Schutz persönlicher, gegenständlicher und wettbewerblicher Individualität im Persönlichkeitsrecht, Immaterialgüterrecht und Recht der Unternehmen*, Tubinga, 2001; N. Witzleb, *Geldansprüche bei Persönlichkeitsverletzungen durch Medien*, Tubinga, 2002. Per importanti spunti comparatistici Stig Strömholm, *Right of Pri-*

Tanto imporrebbe che ogni sua limitazione non possa spingersi sino ad intaccare il contenuto essenziale dello stesso diritto.

D'altro canto, giova osservare che «*la qualificazione adottata non deve condurre ad un appiattimento del diritto alla protezione dei dati personali sugli altri, più tradizionali, diritti della personalità ed impedire di cogliere i tratti peculiari della relativa disciplina*»[14]. Esempio di tale ricostruzione è il Regolamento UE 679/2016 (cd GDPR) che, ad es., all'art. 89[15] legittima il trattamento dei dati personali per

vacy and Rights of the Personality: A Comparative Survey, Stoccolma, 1967, in particolare 25 ss.

14 V. M. Donofrio, *La protezione dei diritti nell'era digitale: tratti essenziali e capisaldi normativi*, in altalex.com.

Ed ancora sulla natura dei diritti R. Alexy, *Teoria dei diritti fondamentali*; G. Zagrelbesky, *La legge e la sua giustizia*, Bologna, Il Mulino, 2008, 283 ss; R. Guastini, *L'interpretazione dei documenti normativi*, in A. Cicu – F. Messineo – L. Mengoni (a cura di), *Trattato di diritto civile e commerciale*, Milano, Giuffrè, 2004, 246 ss.; M.Barberis, *Etica per giuristi*, Roma-Bari, Laterza, 2006).

É in questa dimensione che nessun principio ha la capacità di limitarne nessun altro. Solo qui, perciò, può parlarsi di «assolutezza» dei principi fondamentali, e in una accezione semantica definita: sul piano normativo i valori non esprimono di per sé ragioni capaci di relativizzazione reciproca (R. Alexy, *Teoria dei diritti fondamentali*, cit., 119 ss.). È proprio questa caratteristica della comunicazione tra i principi fondamentali a fare del c.d. bilanciamento la tecnica della soluzione dei conflitti che insorgono nella prassi (R. Alexy, *Teoria dei diritti fondamentali*, cit., 133). Infatti, è unicamente il problema concreto della vita, per le caratteristiche peculiari con cui «interroga» il diritto, ciò che rende possibile bilanciare i principi; «soppesarli» rispetto alle esigenze del caso concreto. Con altre parole: la ponderazione in cui il bilanciamento consiste è giuridicamente pensabile soltanto nel riferimento al caso concreto; la eventuale prevalenza di un valore fondamentale su un altro valore fondamentale è comprensibile non come questione di assolutezza bensì come posterius del singolo giudizio di bilanciamento; è un fatto occasionale, dipendente dalle circostanze del caso concreto (R. Alexy, *Teoria dei diritti fondamentali*, cit., 106 ss.). Dunque, se il principio del pluralismo democratico include, normalizzandola, la possibilità del conflitto tra i valori ultimi (tra i principi fondamentali) senza precludere a priori alcuna ipotesi risolutiva, allora fa anche in modo che ciascun diritto possa essere occasionalmente recessivo rispetto ad ogni altro interesse costituzionalmente rilevante – anche quando quest'ultimo non sia incorporato nella forma di una libertà individuale o di un diritto soggettivo.

15 La norma così dispone: il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18,

scopi di ricerca scientifica, storica o per l'analisi statistica, considerando tali finalità di pubblico interesse. Il rispetto del diritto alla protezione dei dati personali viene considerato quale precondizione per l'esercizio di altri diritti civili, politici e sociali, essendo questo un diritto fondamentale, di natura costituzionale, posto a garanzia della dignità della persona.

Da tanto discende il superamento di una prospettiva puramente individualistica e l'adozione di un sistema di meccanismi di controllo e di rimedi basato sull'interazione tra privato e pubblico[16]. Ed infatti, il complesso apparato di rimedi di natura civilistica, amministrativa e penale non tutela soltanto i diritti dei singoli interessati, ma garantisce altresì l'interesse dei consociati e dell'ordinamento alla legittimità, liceità e correttezza dei trattamenti di dati personali effettuati[17]: sono all'uopo previsti il controllo sul trattamento dei dati personali svolto dal soggetto interessato ed i poteri di vigilanza e protezione del trattamento di dati sensibili – o a rischio specifico – attribuiti al Garante per la protezione dei dati personali.

La tutela riconosciuta a tali dati è dunque dinamica, atta a seguire i dati nella loro circolazione. Ecco perché il diritto alla tutela dei *personal data* deve delinearsi, non come ostativo al soddisfacimento di interessi altrui altrettanto meritevoli di tutela, quanto piuttosto come esigenza di trasparenza e di protezione della persona in un complesso sistema di interessi contrapposti.

19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

16 Ibidem.

17 Sul significato e sulla funzione del riferimento alla correttezza v. F. D. BUSNELLI, Spunti per un inquadramento sistematico, in C. M. BIANCA, F. D. BUSNELLI, A. BELLELLI, F. P. LUISO, E. NAVARRETTA, S. PATTI, P. M. VECCHI (a cura di), *Tutela della privacy*, Padova, Cedam, 1999, 228. L'autore osserva che «con la direttiva sul trattamento dei dati personali la correttezza spinge verso la responsabilità, ma il moto di base di questo indirizzo è lo stesso: il recupero di regole elastiche come quella della correttezza per far fronte agli odierni problemi di tutela dei soggetti deboli». Sia consentito di rinviare anche al mio contributo, Spunti di riflessione su taluni «diritti dell'interessato», in N. ZORZI GALGANO (a cura di), *Persona e Mercato dei dati. Riflessioni sul GDPR*.

4. La libertà di manifestazione del pensiero sui social network

La possibilità di navigare in internet consente di accedere ad un numero potenzialmente infinito di informazioni e di esprimere idee ed opinioni rivolgendosi ad una platea indefinita di destinatari. Il diritto di manifestare il proprio pensiero risulta, tuttavia, accresciuto e compresso ad un tempo: invero, la libertà di espressione trova un limite, nel continente europeo, nell'esigenza di protezione della collettività. Ne deriva che un'idea non potrà trovare diffusione se nociva per la collettività o lesiva della sicurezza e l'ordine pubblico.

Diversamente sarebbe ove vigesse il principio d'oltreoceano del *free market place of ideas,* secondo il quale le idee sono soggette ad una selezione naturale nella quale sono destinate ad emergere solo le idee migliori.

Nel nostro ordinamento, per espressa previsione costituzionale (art. 21 Cost), la libertà di espressione del pensiero trova un limite nel rispetto del buon costume ed è passibile di ulteriori limitazioni ove bilanciata con altri diritti e libertà costituzionalmente tutelati.

Stante l'indefinito numero di utenti raggiungibili mediante le piattaforme online, occorre chiedersi se sia conforme al dettato costituzionale esigere il preventivo controllo della veridicità del pensiero che si intende manifestare e diffondere in Rete: occorre, cioè, stabilire se la veridicità del pensiero sia preminente rispetto alla libertà di manifestarlo.

La Costituzione e, in senso lato, le norme che disciplinano la libertà di espressione non menzionano un diritto a ricevere un'informazione corretta e/o veritiera: oggetto di tutela è il pensiero in sé, dunque anche il fatto oggettivamente errato, qualora ritenuto vero da chi ne afferma l'esistenza. D'altro canto, vengono in rilievo tutte quelle situazioni giuridiche idonee ad imprimere un limite al contenuto del pensiero liberamente espresso, ossia i diritti della perso-

nalità[18] e i diritti di natura pubblicistica volti, cioè, alla tutela di interessi collettivi costituzionalmente rilevanti[19].

Se giustificato è il bilanciamento tra valori parimenti tutelati, una aprioristica censura finirebbe per svuotare di contenuto lo stesso art. 21 Cost., ponendo un limite implicito sulla scorta della sola veridicità o meno del pensiero espresso. Non meritevole di pregio si presenta tale considerazione, atteso che non sono sempre noti i criteri per stabilire se l'informazione diffusa sia vera o falsa.

5. Il complesso sistema di accountability online

La libertà di esprimere idee, opinioni, dati e contenuti di qualsivoglia genere sulle piattaforme online, pone il problema dell'individuazione del soggetto responsabile del controllo di tali informazioni.

Controverso è stabilire se il controllo sulla diffusione di contenuti online spetti ad un ente pubblico – Stato – ovvero ad un privato – *provider*.

Tale obbligo di vigilanza potrebbe assumere due forme, potendo configurarsi alla stregua di controllo preventivo – da esercitare *ex ante* – ossia impedendo l'upload dei contenuti illeciti da parte dell'utente; ovvero come controllo successivo, che consiste nella rimozione, su richiesta dell'utente, di una notizia già caricata in Rete.

Sul tema, il Tribunale di Milano con sentenza del 2010 si era espresso a favore del controllo preventivo condannando i manager di *Google* per il reato di trattamento illecito di dati, ex art. 167 D.Lgs. 196/2003 (c.d. codice della *privacy*) sulla scorta della considerazione secondo la quale *Google* avrebbe dovuto rendere edotti gli utenti circa gli «*obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli"; obbligo derivante, secondo il Tribunale, dall'art. 13 del D.Lgs. 196/2003 oltre che dal "buon senso*"» [20]. I giudici

18 Tra essi il diritto all'onore, alla reputazione, alla dignità sociale. Si pensi alle fattispecie del codice penale che puniscono la diffamazione, l'ingiuria.
19 Quali, ad esempio, l'amministrazione della giustizia e la sicurezza dello Stato.
20 "Google Vivi Down", Tribunale di Milano, 12 aprile 2010, n. 1972: il processo scaturisce dalla pubblicazione di un filmato sull'*host* Google Video, che ritrae un ragazzo disabile umiliato

avevano ritenuto, dunque, che sussistesse un necessario controllo preventivo in capo ai gestori della piattaforma. La pronuncia venne impugnata in Appello e successivamente in Cassazione. Confermando la decisione dei giudici di seconde cure, la Suprema Corte aveva accertato l'assenza di una posizione di garanzia in capo ai provider, poiché nessuna disposizione «*prevede che vi sia in capo al provider, sia esso anche un hosting provider, un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito"; parimenti, nessuna norma incriminatrice punisce un ipotetico obbligo dei provider di ricordare agli utenti di rispettare la legge*».

Tale principio affonda le sue radici nella normativa sul commercio elettronico di cui al d.lgs. 70/2003, frutto della direttiva europea 2000/31/CE: l'art. 17 del decreto citato esclude per il *provider* un generale dovere di sorveglianza sui contenuti degli *uploader*; ed ancora, l'art. 16 sancisce l'irresponsabilità del provider per le condotte illecite tenute dagli utenti, qualora non ne fosse a conoscenza e se, una volta avvisato dall'autorità, abbia provveduto alla rimozione dei contenuti stessi[21].

Tali premesse conducono ad affermare che la responsabilità del *provider* presuppone che costui abbia un atteggiamento "attivo" nella gestione dei contenuti, consistente nella loro manipolazione: egli, cioè, sarà responsabile nelle ipotesi nelle quali abbia creato il contenuto, lo abbia indirizzato verso una pla-

---

da alcuni compagni all'interno di un edificio scolastico; nella ripresa si sentono anche frasi ingiuriose nei confronti dell'associazione Vivi Down. Per ciò che qui interessa, tre manager di Google venivano originariamente imputati per non aver impedito il delitto di diffamazione nei confronti del minore e dell'associazione (artt. 40 cpv. e 595 c.p.) e per aver trattato illecitamente dati personali attinenti alla salute del ragazzo ripreso (art. 167 D.Lgs. 196/2003, c.d. codice della privacy).
Nel giudizio di primo grado, il Tribunale di Milano assolveva gli imputati dal delitto di diffamazione, escludendo che vi fosse in capo all'*host provider* un obbligo di impedire reati commessi dagli utenti; tale esclusione era motivata sia da ragioni giuridiche (la direttiva sul commercio elettronico, attuata nel nostro ordinamento con il D.Lgs. 70/2003, esclude un obbligo di vigilanza sul contenuto dei materiali diffusi dagli utenti), sia da considerazioni di tipo fattuale (l'impossibilità in concreto di filtrare ex ante i contenuti degli *uploader*). Il Giudice ambrosiano riteneva, invece, integrato il delitto di illecito trattamento di dati personali: Google avrebbe dovuto avvisare gli *uploader* degli "obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli"; obbligo derivante, secondo il Tribunale, dall'art. 13 del D.Lgs. 196/2003 oltre che dal "buon senso".
21 Per un'approfondita analisi della sentenza della corte di cassazione si rinvia a la sentenza della Cassazione sul caso Google, in dirittopenalecontemporaneo.it

tea selezionata di destinatari ovvero lo abbia modificato. Occorre considerare, peraltro, che ostano al riconoscimento di un controllo preventivo tanto l'assetto costituzionale del nostro ordinamento – che esclude forma preventive di censura – tanto la disciplina europea orientata verso un generale esonero di responsabilità per gli operatori della Rete[22].

Esclusa la via del controllo preventivo, la giurisprudenza ha accolto l'opzione del controllo postumo, affidando ai gestori delle piattaforme *web* il potere/dovere, sollecitato dall'interessato, di rimuovere i contenuti illeciti.

In questo senso si è espressa la Corte di giustizia che, nella sentenza *Google Spain*, ha onerato il gestore del motore di ricerca del compito di stabilire, caso per caso, se l'informazione possa restare online o debba essere rimossa. I giudici muovono dall'assunto secondo il quale i gestori delle piattaforme sono configurabili alla stregua di titolari del trattamento dei dati personali e come tali responsabili di tale trattamento. Solo ove costoro rimangano inerti, l'interessato potrà esercitare il suo diritto dinanzi alla pubblica autorità, chiamata a decidere se quella specifica notizia costituisca legittimo esercizio della libertà di espressione o, al contrario, sia mezzo di offesa. Ne discende un *iter* di rimedi ben definito: l'interessato rivolge la propria richiesta dapprima al *provider* e, solo a fronte di diniego o inadempienza di quest'ultimo, potrà adire l'autorità di protezione dei dati.

Ebbene, ritenuta preferibile la strada del controllo successivo, occorre chiarire in quali casi la titolarità del trattamento, e la conseguente responsabilità, sia ascrivibile al gestore del sito.

Nel recente caso *Fanpage*, la Corte di giustizia ha riconosciuto una contitolarità tra l'amministratore della f*anpage* e *Facebook*, ossia tra utente e *social network*: osservano i giudici come non sia revocabile in dubbio che la società americana *Facebook* e la sua succursale europea *Facebook Ireland*, avente sede in Ger-

22 L. CALIFANO, *La liberta' di manifestazione del pensiero ... in rete; nuove frontiere di esercizio di un diritto antico. Fake news, hate speech e profili di responsabilità dei social network*, in *federalismi.it*, 17 novembre 2021.

mania, siano responsabili del trattamento dei dati personali degli utenti che utilizzando il social network, in quanto tenute al rispetto della Direttiva 95/46/CE. Tuttavia, non si tratta della responsabilità di un singolo, bensì di una forma di responsabilità solidale atteso che «*l'amministratore di una fanpage può chiedere di trattare dati che riguardano i destinatari degli annunci contenuti nella pagina impostando personalmente i parametri con cui regolare il proprio campo o settore di intervento*»[23].

Non può escludersi allora che attraverso l'elasticità dei concetti di "titolare" e di "trattamento", alla luce delle rafforzate garanzie del GDPR, le Autorità di controllo o i giudici possano giungere ad estendere il sistema di *accountability* dei *social network* non solo in relazione ai problemi connessi all'utilizzo delle piattaforme, ma anche rispetto al contenuto e alla portata delle comunicazioni rese dagli utenti a mezzo di quelle stesse piattaforme.

6. Conclusioni

Quotidianamente milioni di utenti diffondono in Rete flussi di dati in grado di rivelare una quantità indefinita di informazioni.

Non è assurdo ritenere che al *Big Brother* orwelliano, misterioso personaggio in grado di controllare la società mediante speciali teleschermi, si siano sostituiti gli algoritmi di internet, affamati captatori di informazioni, capaci di prevedere ed influenzare le scelte degli utenti. Se certamente non può immaginarsi – né è auspicabile – un arresto della rete deve, tuttavia, rilevarsi la necessità di un uso consapevole del *web*.

Se indubbio è che la piena integrazione nella rapidissima società moderna non possa prescindere da simili meccanismi di diffusione delle informazioni, è parimenti necessario che il progresso della realtà digitale sia accompagnato da una attenta e profonda tutela dei dati personali, realizzabile già solo attribuendo a ciascun utente un potere di controllo sulla diffusione dei propri dati.

---

23 Corte di Giustizia, Sez. Grande, sentenza 05/06/2018 n. C-210/16 in Altalex, 14 giugno 2018.

Il vantaggio, del resto, è *in re ipsa*: una posizione attiva dell'utente-consumatore non può che tradursi in un uso più consapevole dei motori di ricerca e maggiormente aperto all'accettazione della fruizione di dati sensibili utili ad indirizzare le risposte del mercato. È auspicabile, in tal senso, che la protezione della persona sia contemperata con l'indefettibile esigenza di far circolare i dati personali.

Non può negarsi, infatti, che la globalizzazione della società e del mercato, lungi dall'assecondare il *right to be alone*[24] di ciascun individuo, renda sempre più urgente la soddisfazione del bisogno di fruire liberamente delle informazioni altrui.

Tanto trova riscontro, non soltanto, nel principio secondo cui il diritto alla protezione dei dati personali debba essere «contemperato» alla luce «della sua funzione sociale»[25] con «altri diritti fondamentali, in ossequio al principio di proporzionalità»; ma anche nell'idea che la tutela dell'identità personale o della riservatezza, potendo determinare il sacrificio di altri «diritti fondamentali» come «la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa»[26], non possa giustificare di per sé l'introduzione di limiti alla libera circolazione delle informazioni[27].

---

24 A Samuel Warren e Louis Brandeis si deve una delle prime definizioni di privacy come right to be alone, traduzione di diritto di essere lasciati "soli".

25 Sul tema, anche per la dettagliata ricostruzione della giurisprudenza europea e italiana in ordine ai limiti della protezione dei dati personali, v. A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in Contr. Impr., 2017, 609.

26 Considerando n.4 regolamento ue

27 Tema, questo, indagato diffusamente nella letteratura civilistica. A tale riguardo, senza alcuna pretesa di completezza, ma anzi con la consapevolezza che una rassegna ordinata risulterebbe del tutto disagevole a fronte dei numerosi contributi offerti dalla dottrina, è opportuno il riferimento a E. Navarretta, *Libertà fondamentali dell'U.E.* e rapporti fra privati: il bilanciamento di interessi e i rimedi civilistici, in Riv. dir. civ., 2015, I, 878; G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, Esi, 2015, 105; a F. Di Ciommo, *Il diritto all'oblio nel Regolamento (UE) 2016/679*. Ovvero, di un "tratto di penna del legislatore" che non manda al macero alcunché, in Corr. giur., 2018, 16; e a D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in Riv. crit. dir. priv., 1998, 339.