Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*

Emma Garzonio

Abstract

Il Regolamento (UE) 2016/679, in vigore dal 25 maggio 2018, nello stabilire nuovi obblighi e responsabilità per gli intermediari digitali – i *provider*, fra cui le piattaforme di *social networking* – ha integrato, ed in parte superato, le precedenti disposizioni in materia. Il contributo in oggetto, dopo un breve *excursus* che ripercorre nella giurisprudenza europea ed italiana le tappe evolutive dei fondamenti normativi delle responsabilità sancite oggi dal GDPR, ne vuole verificare l'applicabilità alle piattaforme *social*, partendo dalla definizione stessa del concetto di piattaforma e delle sue funzioni, anche avvalendosi di contributi tratti dai *media* e *cultural studies*.
L'obiettivo è analizzare l'equilibrio non sempre stabile fra gli obblighi per i Social Network Provider ed i diritti degli interessati nel delicato campo della comunicazione politica sulle piattaforme *social*: è su questi "campi di battaglia" infatti che si sono recentemente verificati "scandali" quali quello di Cambridge Analytica, che hanno rinnovato l'attenzione sui rischi del trattamento automatizzato dei dati personali e sulla possibilità di *data breach*. L'articolo vuole dunque verificare la tenuta degli strumenti dispiegati dal GDPR - in primo luogo contro la profilazione degli utenti e l'aggregazione delle tracce digitali tramite algoritmo - quando questi si debbono applicare a scapito degli interessi delle major di Internet.

The new General Data Protection Regulation no. 2016/279, entered into force on May 25, 2018, has established and codified new duties and responsibilities for intermediary service providers, including social network platforms, overtaking and completing the pre-existing rules.
The research at hand, after a brief excursus which retraces within the European and

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco"

Italian legal systems the grounds on which the GDPR today ratifies new responsibilities, aims at verifying the GDPR enforceability vis-à-vis social network platforms. To do so, it will start from a defining framework for the term "platform" itself and then analyse the concept and its functions conveying also relevant essays from media and cultural studies.
The objective is to analyse the trembling balance between Social Network Providers duties and individuals' rights with specific regards to political communication strategies on social networks. Within the political propaganda framework, in fact, scandals such as the Cambridge Analytica affaire have emerged, renewing public opinion's attention on the risks linked to the automated processing of personal data and on the possibilities of data breach.
This essay aims then at verifying the resilience of the tools laid out by the GDPR in the field of personal data protection – with specific attention to profiling activities and digital footprints aggregation through algorithmic codes - when they have to be used to the detriment of the interests of major Web companies such as Facebook, which is not new to a quite unscrupulous employment of its users' personal data.

Sommario

Keywords

Piattaforme, Privacy, GDPR, Algoritmi, Comunicazione politica

1. Le piattaforme: dal concetto alle responsabilità

Per approcciare l'ampia materia che riguarda i nuovi obblighi ed adempimenti codificati dal Regolamento (UE) 2016/679 – d'ora in avanti citato con l'acronimo inglese GDPR, *General Data Protection Rules* –, specificamente rispetto alle piattaforme *social*, è necessario innanzitutto muovere qualche passo definitorio di quelli che sono i concetti chiave per la nostra ricerca: gli Internet Service Provider, le piattaforme digitali, la responsabilità di questi soggetti ed i rischi connessi alle loro attività in merito al trattamento automatizzato dei dati.
Sarà inoltre utile compiere un breve excursus delle tappe che hanno costituito l'impianto normativo dell'attuale Regolamento e hanno preceduto, nella giurisprudenza europea ed italiana, la approvazione e l'entrata in vigore del GDPR.
Innanzitutto il concetto stesso di "piattaforma" e le funzioni ad essa legate mostrano una natura estremamente trasversale e continuamente mutevole che non si presta a

una catalogazione statica, specialmente quando si tratta di piattaforme che si nutrono di relazioni sociali reticolari[1] e si basano sulla condivisione orizzontale di contenuti.
Il termine "piattaforma" è emerso recentemente nel nostro orizzonte lessicale ed è divenuto di utilizzo sempre più familiare – sia come autodefinizione da parte dell'*establishment* di tali *network*, sia come termine riconosciuto nel più vasto discorso pubblico creato dagli utenti, dalla stampa, dai *commentators* – quando si vogliono descrivere i servizi prestati online dai cosiddetti intermediari di contenuti.
La parola "piattaforma" dice ben poco della posizione che tali intermediari si stanno ritagliando grazie alle funzioni digitali che sono in grado di espletare: YouTube, per fare un esempio, fornisce il proprio servizio non solo ai suoi *users* ma anche ai pubblicitari, ai grandi produttori di media che spera di assicurarsi come partners, ai soggetti che hanno il potere di elaborare e determinare orientamenti e strategie sociali e politiche – i cosiddetti *policymakers*. In questo contesto il concetto estensivo di "piattaforma" ci aiuta a svelare come YouTube o un social network o un motore di ricerca divengano palcoscenico per tali clienti, rendendo loro possibile una perpetua attività di campagna elettorale (o di marketing politico), con capacità di penetrazione sempre più estese e progressive, grazie al crescente numero di utenti interconnessi[2].
Queste funzionalità si basano sulle caratteristiche intrinseche della piattaforma, specialmente quella di elidere gli attriti inerenti al servizio che prestano: tensioni fra *user-generated* e *commercially produced content*[3], fra il nutrire lo spirito della *community* e creare spazi pubblicitari, fra la possibilità di intervento sul contenuto e la capacità di rimanere neutrali.
La posizione occupata nella pratica discorsiva da questi attori ha a che vedere con le regole etiche, morali, le convenzioni sociali e le azioni formali da cui derivano i comportamenti e gli atti linguistici – e per estensione, comportamenti ed atti comunicativi online – e fa affidamento su termini ed idee che sono sufficientemente specifici da significare qualcosa, ma anche sufficientemente ampi da operare in luoghi differenti e verso audience differenziate[4]. Dunque definire il proprio servizio online come "piattaforma" non è affermazione priva di significato, ma certamente non è priva di difficoltà concettuali. Come altre metafore strutturali – si pensi ai termini ormai consueti di *network, broadcast, channel* – il termine "piattaforma" dipende dalla propria ricchezza semantica, che seppure possa forse rimanere inavvertita dall'ascoltatore casuale, conferisce alla parola una certa risonanza discorsiva.
Qualsiasi contraddizione possa sussistere nell'essere allo stesso tempo strumento che rafforza le capacità dell'utente individuale, che veicola robuste operazioni di marketing e che diffonde contenuti *mainstream* di grandi produttori viene elusa dalla versatilità

[1] Per il concetto di rete digitale si veda M. Castells, *Comunicazione e potere*, Milano, 2017, 13 ss.

[2] M. Airoldi, *Potrebbe interessarti anche: recommender algorithms e immaginario, il caso YouTube,* in *Im@go, a journal of the social imaginary*, 6, 2015, 132 ss. Sulle audience ibride di YouTube, H. Jenkins - S. Ford - J. Green, *Spreadable media. I media tra condivisione, circolazione, partecipazione*, San Marino, 2013, 97 ss.

[3] Sul concetto di *agency* dei creatori di contenuti si veda J. Van Dijk, *Users like you? Theorizing agency in user-generated content*, in *Media, Culture & Society*, 31-1, 2009, 41 ss. Sul tema del *produsage*, A.Bruns, *Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage,* Berna, 2008.

[4] T. Gillespie, *The Politics of 'Platforms'* in *New Media & Society*, 3, 2010. Del medesimo autore sul potere selettivo delle piattaforme, *Platforms Intervene*, in *Social Media + Society*, 1-2, 2015.

ed elasticità dell'essere "piattaforma" e dal potente fascino dell'idea che essa veicola. Talmente fascinosa da divenire concetto persuasivo probabilmente anche nella prospettiva giuridica, capace di incorniciare i servizi degli intermediari in un *framework* metaforico familiare: prospettare la funzione delle piattaforme come semplice e neutrale attività di fornitura di contenuti al pubblico di utenti, quale veicolo e non quale produttore di contenuti od informazioni (notizie), ben si presta a lasciar ricadere la responsabilità rispetto a tali contenuti sugli *users* della piattaforma stessa. Ovvero, specialmente quando si parla di responsabilità delle piattaforme, il termine stesso può servire non per enfatizzare, ma per minimizzare il ruolo degli intermediari: gli *online content providers*, non producendo ma veicolando informazione, risultano rispetto ad essa limitatamente responsabili.

Per poter limitare la propria responsabilità non solo giuridica ma anche, se vogliamo, culturale – nel diffondere contenuti frivoli e puerili, quando non addirittura infondati o inattendibili – gli intermediari hanno dunque bisogno di potersi posizionare come semplici *host* o *provider*.

Questo tentativo di eludere le proprie responsabilità, a partire da quelle giuridiche, risulta in stridente contrasto a con la realtà odierna della comunicazione, non più univoca (*one-to-one*) né molteplice (*one-to-many)* come presunta dai mass media di vecchio stampo, ma addirittura collettiva (*many-to-many*)[5]. Vero è che gli utenti non si limitano più ad utilizzare un servizio per ricevere contenuti, ma in qualche modo producono essi stessi il servizio – la condivisione di informazioni – attraverso la connessione reticolare su cui le piattaforme di *sharing* (che siano video, *tweet*, contenuti privati, notizie dal mondo) si basano.

Gli *users* diventano dunque anche *producers*[6]*,* mentre i *provider* non sono solamente intermediari neutrali ma «sempre più spesso intervengono, con procedure non sempre trasparenti, nell'organizzazione e nella gestione dei contenuti. La loro attività quindi può essere paragonata –

con qualche approssimazione, ma non infondatamente – a quella degli editori tradizionali, riflessione che impone un radicale ripensamento delle loro responsabilità.»[7]

Parole come "piattaforma" non emergono spontaneamente dal discorso pubblico, ma derivano dal vocabolario culturale reso disponibile ad un dato momento storico dagli *stakeholders* della comunicazione: essi sono portatori di interessi specifici e le parole che immettono nel discorso nascono per trovare risonanza presso audience specifiche. Sono termini che esprimono non solo la volontà di vendere, persuadere, condannare o proteggere determinate tecnologie ma di stabilire ed affermare che cosa siano o non siano in realtà e che cosa dovremmo aspettarci da esse.

Queste parole sono importanti tanto per quel che nascondono che per quel che rivelano: nonostante le premesse e le promesse, le piattaforme sono molto più simili

[5] D. McQuail*, Sociologia dei media*, Bologna, 2007.

[6] M. Castells, *La nascita della società in rete*, Milano, 2014, 408.

[7] M.R Allegri, *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018. Per una trattazione sul tema della responsabilità degli ISP all'interno dell'ordinamento penale italiano, cfr. T. Giovannetti, *Governance della rete e ricorso alla sanzione penale: il caso della responsabilità dell'Isp tra tentazioni punitive e rispetto dei principi costituzionali*, in M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione. Atti del convegno (Pisa, 21-22 novembre 2013)*, Torino, 2014, 315 ss.

alle strutture dei media tradizionali di quanto non vogliano lasciar trasparire. Così, esattamente come per le comunicazioni di massa e l'editoria tradizionale, le scelte su che cosa possa essere trasmesso e come debba essere organizzato, monetizzato, eventualmente rimosso o proibito coincidono con interventi reali e sostanziali all'interno del discorso pubblico[8].

2. Quali responsabilità per i Social Network Provider: i fondamenti normativi

Un'ulteriore differenziazione deve essere compiuta all'interno della famiglia dei *provider*.

La sigla ISP (Internet Service Provider, o fornitore/prestatore di servizi via Internet) si riferisce a «qualsiasi persona fisica o giuridica che presta un servizio della società dell'informazione», servizi definiti come «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»[9].

Il carattere piuttosto ampio di questa definizione fa sì che essa risulti applicabile non solo ai *provider* di servizi online

«così come operavano agli inizi degli anni Duemila, ma anche a quei soggetti che oggi prestano servizi di tipo più moderno ed evoluto, quali ad esempio i motori di ricerca e i *social network provider* (Snp). È vero che la definizione sopra riportata fa riferimento a servizi prestati "dietro retribuzione", mentre una delle caratteristiche salienti dei social media o dei motori di ricerca è la loro gratuita disponibilità; tuttavia, l'avverbio "normalmente" allude al fatto che la retribuzione non sia un requisito assolutamente necessario, ma solo un elemento frequentemente previsto dalla prassi […]»[10]

La c.d Direttiva E-Commerce del 2000 e il decreto legislativo di attuazione approvato nel 2003[11] prevedono essenzialmente tre categorie di intermediari digitali.

La prima comprende i prestatori di servizi di "semplice trasporto" (attività di *mere conduit*), laddove il prestatore non è considerato responsabile delle informazioni trasmesse a condizione che egli non dia origine alla trasmissione, non ne selezioni il destinatario e non ne modifichi i contenuti/informazioni. Nella prestazione del servizio le attività di trasmissione e di fornitura di accesso possono includere la memorizzazione automatica delle informazioni, a condizione che essa serva solo allo scopo di trasmissione, che sia transitoria e di durata non eccedente «il tempo ragionevolmente neces-

[8] T. Gillespie, *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale, 2018.

[9] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, 8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, art. 2, lett. *b)*, recepita in Italia con d. lgs. 70/2003.

[10] M.R. Allegri, *op.cit.*, 54.

[11] D. lgs. 70/2003, "Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico", in *Gazzetta Ufficiale* n. 87, 14 aprile 2003.

sario a tale scopo» (art.12). Appartengono a questa categoria, ad esempio, i fornitori di servizi di connettività ad Internet.
L'art. 13 definisce le casistiche di irresponsabilità del *provider* rispetto alla memorizzazione temporanea (attività di *caching*) di informazioni, cioè la «memorizzazione automatica, intermedia e temporanea di informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro delle stesse ad altri destinatari». Rientrano in questa categoria, fra gli altri, i fornitori di servizi di posta elettronica o i motori di ricerca.
Rilevante rispetto all'oggetto della nostra ricerca è il successivo art. 14, che riguarda i prestatori di servizi che memorizzano – non temporaneamente, ma durevolmente – le informazioni fornite dai destinatari del servizio o utenti (attività di *hosting*). Questa definizione può riferirsi, ad esempio, ai prestatori che consentono operazioni di *upload* dei contenuti degli utenti in uno spazio dedicato, che sia un sito Internet, un blog o una pagina di un social network.
Le disposizioni contenute all'interno della direttiva sul commercio elettronico – e del relativo d.lgs. 70/2003 – in tema di regime di responsabilità degli intermediari e dei gestori di social network non si applicano però alle questioni relative alla protezione dei dati personali: tale materia è invece regolata dalle successive direttive europee più specificamente attinenti all'ambito[12]. Questo corpus costituisce l'impianto normativo che è stato sostituito dal GDPR.
Nel decennio successivo e fino ai giorni nostri sono evidentemente cambiate le funzionalità ed il raggio di azione dei prestatori di servizi e così anche la portata delle loro responsabilità. Se in una prima fase giurisprudenziale gli ISP – essendo considerati privi di responsabilità editoriale sui contenuti trasmessi tramite le piattaforme da essi gestite – non erano stati inclusi fra i soggetti i cui ricavi concorrevano a formare il Sistema Integrato delle Comunicazioni (SIC)[13], più recentemente quest'ultimo ha interessato anche gli introiti derivanti «da pubblicità on line e sulle diverse piattaforme anche in forma diretta, incluse le risorse raccolte da motori di ricerca, da piattaforme sociali e di condivisione».[14] Rispetto al SIC, la rete Internet non è stata altresì presa in considerazione fin dall'origine, se non in ordine all'editoria elettronica "anche via Internet"[15]. La successiva assimilazione, sia pure sotto il solo profilo dei ricavi, degli ISP ai soggetti dotati di responsabilità editoriale sui contenuti (*content provider*) può essere considerato un segnale delle più evolute funzionalità dei *provider* nella gestione e nell'organizzazione dei contenuti informativi[16].
Ai fini della presente ricerca, l'analisi del regime di responsabilità previsto per i *provider*

[12] 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.

[13] Definito nel d.lgs. 177/05 come riformato dal d. lgs. 44/2010.

[14] L. 16 luglio 2012, n. 103, "Conversione in legge, con modificazioni, del decreto-legge 18 maggio 2012, n. 63, recante disposizioni urgenti in materia di riordino dei contributi alle imprese editrici, nonché di vendita della stampa quotidiana e periodica e di pubblicità istituzionale", art. 3, c. 5-*bis* M.R. Allegri, *op. cit.,* 61.

[15] R. Borrello, *Alcune riflessioni preliminari (e provvisorie) sui rapporti tra i motori di ricerca ed il pluralismo informativo,* in *questa Rivista,* 1, 2017, 68 ss.

[16] M.R. Allegri, *op. cit.,* 61.

e degli strumenti dispiegati dalla più recente regolamentazione risulta utile per verificare l'operatività e l'efficacia degli stessi nei confronti delle piattaforme caratterizzate da attività di *hosting*, quali appunto i social network. Posto che la presunta neutralità delle operazioni dell'*hosting provider* così come inteso nella direttiva e nella relativa legge nazionale ad oggi non può sussistere, il GDPR ha voluto codificare in un più attuale quadro normativo quelli che sono i nuovi obblighi per le piattaforme che maneggiano informazioni e categorie di dati relativi ai propri *users*.

L'esigenza di approvare un regolamento in luogo delle precedenti direttive e relative legislazioni nazionali coincide innanzitutto col bisogno di assicurare che le norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche, con riguardo al trattamento dei dati personali, vengano applicate in modo uniforme e coerente in tutta l'Unione europea, eliminando le difformità fra ordinamenti nazionali. Queste sono considerate fonte di incertezza rispetto all'effettivo uso del dato personale una volta immesso in Internet: una volta online infatti, oltre all'impossibilità di prevenirne la libera circolazione, è anche estremamente arduo impedire che venga incrociato con altre informazioni (personali e non), con modalità di trattamento e per finalità diverse da quelle previste originariamente.

Secondo l'art. 3, relativo all'ambito di applicazione territoriale, la nuova disciplina si applica dunque «al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»[17] nonché da parte di un titolare o responsabile stabilito fuori dall'Unione europea nel caso in cui il trattamento abbia ad oggetto i dati personali di coloro che si trovano all'interno di essa, oppure inerisca all'offerta di beni o servizi nel territorio dell'Unione.

Ricordiamo che il Regolamento "relativo alla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" è stato approvato il 25 maggio 2016 e viene applicato in tutto il territorio dell'Unione dalla stesa data dell'anno corrente: l'abrogazione della precedente direttiva 95/46/CE in materia è stata resa effettiva a decorrere dal 25 maggio 2018 secondo quanto contenuto nell'art. 94 GDPR.

La scelta dell'Unione europea di muoversi verso le scelte poi confluite nella più recente regolamentazione trova le sue basi nel riconoscimento del diritto alla protezione dei dati personali quale diritto fondamentale del cittadino europeo[18]. Tale identificazione è operata dal Trattato di Lisbona – ufficialmente in vigore dal 1° dicembre 2009 – sia tramite interposto riconoscimento del valore giuridico dei diritti contenuti nella precedente Carta dei diritti dell'Unione[19] (o Carta di Nizza, proclamata in prima battuta il

[17] 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.

[18] L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016 e F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 153 ss. Per un' introduzione generale al GDPR, cfr. G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati,* in Le Nuove Leggi Civili Commentate, 1, 2017, 1 ss.

[19] F. Donati, Art. 8, *Protezione dei dati di carattere personale*, in R. Bifulco - M. Cartabia - A. Celotto,

7 dicembre 2000) sia all'art. 16 del Trattato sul Funzionamento dell'Unione Europea. La prima riporta, all'art. 8:
«Protezione dei dati di carattere personale
1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».[20]
L'art. 16 TFUE specifica invece che
«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati».[21]
Come sottolinea Franco Pizzetti[22], sono due gli elementi di innovazione contenuti in tale articolo: il primo è che esso non solo riconosce il diritto alla protezione dei dati personali quale diritto di carattere personalistico, ma assegna al Parlamento europeo ed al Consiglio il compito specifico di adottare le norme necessarie affinché tale diritto risulti effettivo nell'ambito dell'Unione. Di conseguenza viene fondata la competenza specifica dell'Unione a disciplinare la materia, competenza mancante nel precedente Trattato CE in base al quale fu adottata la citata direttiva 95/46. Il secondo elemento meritevole di considerazione è che a queste medesime istituzioni è assegnato anche il compito di assicurare la libera circolazione dei dati all'interno dell'Unione, principio che dunque viene strettamente legato, tramite questa norma, al diritto alla protezione dei dati personali stessi: questo collegamento fra diritto alla protezione e principio di libera circolazione dei dati caratterizzerà profondamente il GDPR.
Il regime di responsabilità per gli ISP – nel nostro caso, più specificamente per i *Social Network Provider* o SNP – previsto dalla direttiva si compenetra dunque con gli adempimenti rispetto al trattamento dei dati codificati nel GDPR.
Il diritto fondamentale è riconosciuto alla persona fisica già nei summenzionati articoli, caratteristica che coerentemente troveremo nel GDPR, specialmente nel considerando 1 e negli artt. 1, par. 1, relativamente all'oggetto del Regolamento e 4 relativa-

L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea, Bologna, 2001, 83 ss.

[20] Carta dei diritti fondamentali dell'Unione Europea, (2016/C 202/02), in *Gazzetta ufficiale dell'Unione europea* n. C 202/389 del 7 giugno 2016.

[21] Trattato sul funzionamento dell'Unione Europea, versione consolidata, in Gazzetta ufficiale dell'Unione europea n. C 326 del 26/10/2012

[22] F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di) *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 8 ss.

mente alla definizione di dato personale.
Ai sensi dell'art. 4, par. 7, del nuovo Regolamento europeo, il "titolare" del trattamento dei dati è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»: tale definizione, dunque, è applicabile a qualsiasi tipo di *provider*, compresi i gestori dei social network, purché possa essere dimostrata la sua attitudine a determinare finalità e mezzi del trattamento. Al comma successivo invece è definito "responsabile" del trattamento «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».
Rispetto alla precedente direttiva europea, che indicava nel *data controller* il "responsabile" del trattamento, la disciplina attuale compie un ulteriore distinguo fra quest'ultimo – oggi *data processor* –, colui che effettua il trattamento per conto del "titolare" ed il titolare stesso, ovvero il soggetto che determina le modalità e i mezzi del trattamento[23]. Tale distinzione può avere rilevanza nel caso del *provider* che affida ad un altro soggetto la responsabilità del trattamento dei dati, come accade fra società madre e relative controllate.
Ai fini della presente ricerca, tale classificazione può inoltre servire ad inquadrare meglio il ruolo dei gestori dei social network. Infatti, sebbene possa sussistere incertezza sulla qualifica di "titolare" attribuibile al SNP – poiché è l'utente a determinare finalità e mezzi del trattamento, sottoscrivendo i *terms of service* della piattaforma e gestendo la condivisione dei propri dati sulla propria pagina personale – si può comunque applicare al *provider* la qualifica di "responsabile", poiché tratta i dati personali in base al consenso prestato dagli utenti e alle modalità e finalità da essi definite.
Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'art. 5 GDPR, quali la liceità, correttezza e trasparenza del trattamento nei confronti dell'interessato; la limitazione della finalità del trattamento e la minimizzazione dei dati (ossia, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento); l'esattezza e l'aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; la limitazione della conservazione, che non deve coprire un tempo superiore rispetto agli scopi per i quali è stato effettuato il trattamento; infine l'integrità e la riservatezza, al fine di garantire la sicurezza adeguata dei dati personali oggetto del trattamento.
Il par. 2 del medesimo articolo richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo": tale principio è detto di "responsabilizzazione" (*accountability*) e viene poi esplicitato ulteriormente dall'art. 24, par. 1, dove si afferma che «il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento».

[23] Sul mutamento di strategia dalla direttiva al nuovo regolamento, cfr. A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1, 2017, 144 ss.

3. Social network, *privacy by design/default* ed attività di profilazione

La peculiarità delle piattaforme di *social networking* è quella di basarsi sulla costruzione di pagine personali da parte degli utenti, che si identificano – teoricamente fornendo il reale nominativo – ed interagiscono con altri *users* fornendo volontariamente e costantemente informazioni sulla propria attività online ed offline, condividendo immagini delle loro vite, esternando le proprie preferenze ed inclinazioni, "geolocalizzandosi" per segnalare agli altri la propria posizione in uno dei loro luoghi preferiti.
«Sui *social* le persone vengono private silenziosamente e inesorabilmente di una parte molto intima di sé, ottenendo spesso in cambio una identità altra,
accettata passivamente o per comodo, perché copre esigenze istantanee, spesso orientate al consumo di beni e servizi o all'informazione di superficie. […] Chi desidera muoversi in questi spazi – privati, ma che si atteggiano a spazi pubblici – di fatto è costretto in un recinto, tanto più stretto quanto più appaiono libere e incondizionate la sua capacità comunicativa e la sua facoltà di dialogo con i consociati».[24]
Il fulcro delle attività della piattaforma è dunque incentrato pressoché interamente sulla raccolta dei dati personali, spesso anche sensibili, concessi di buon grado dagli utenti e fatti inevitabilmente circolare all'interno della loro rete di contatti, quando non dell'intera *community,* in conseguenza di scelte poco attente per quanto riguarda le impostazioni della privacy del profilo ("visibile a tutti" in luogo di "solo agli amici" selezionati, o di un più ampio "amici degli amici").
La rete delle utenze connesse al proprio profilo è decisa e gestita dall'utente stesso – che sceglie quindi "chi" fra i contatti possa vedere "che cosa" dei contenuti – ma è estremamente difficile riuscire a mantenere il controllo totale sulla circolazione dei propri dati all'interno del *network*. Cedendo volontariamente parte della nostra sovranità sui contenuti *uploadati* e sulle informazioni che ci riguardano, possiamo sì selezionare quale sarà la nostra audience e mantenere la guardia sui livelli di privacy rispetto alla nostra lista di contatti, ma difficilmente avremo piena coscienza di come ci stiamo interfacciando con la piattaforma stessa, ossia di quale potere di controllo – selezione, filtraggio, memorizzazione, condivisione con terzi – essa abbia sui nostri contenuti.
Precedentemente all'entrata in vigore del GDPR era diffuso in via maggioritaria il principio di autotutela od *opt-out*, in base al quale le informazioni condivise da ciascun utente sulla propria pagina erano accessibili a tutti gli altri utenti della piattaforma a meno che non fosse stato l'utente stesso a scegliere impostazioni di privacy più rigide: l'onere di vigilare sulla circolazione delle informazioni era dunque riversata su quest'ultimo, mentre i SNP potevano declinare ogni responsabilità legata alla diffusione dei dati personali degli utenti nonché ai contenuti immessi sulla piattaforma.
Il contrario e attuale principio di *opt-in* invece richiede che la protezione dei dati personali sia assicurata al massimo livello possibile dal gestore della piattaforma fin dalla progettazione per impostazione predefinita (*privacy by default*[25], art. 25 GDPR), a meno

[24] G. L. Conti - M. Pietrangelo - F. Romano (a cura di), *Social media e diritti. Diritto e social media*, in *Informatica e diritto*, 1-2, 2017, 21.

[25] Cfr. S. Sica - V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano,

che non sia l'utente stesso a scegliere una tutela meno rigida. In ogni fase del trattamento dei dati inoltre i *provider*, in qualità di titolari del trattamento, devono adottare ogni misura tecnica e organizzativa atta a garantire il massimo livello di protezione dei dati, minimizzando i rischi inevitabilmente connessi al trattamento stesso (*privacy by design*[26]).

La differenza più evidente consiste nel fatto che quest'ultima è una metodologia che il titolare del trattamento deve tenere presente dall'inizio alla fine del trattamento stesso e che può essere ricalibrata sulla base degli eventuali rischi riscontrati in fase di revisione, mentre la *privacy by default* riguarda essenzialmente la fase di progettazione dei trattamenti ed impone al titolare di assicurarsi che siano trattati, per impostazione predefinita, solo i dati personali necessari per le specifiche finalità del trattamento (art. 25, par. 2). Al contrario della *privacy by design* dunque, che impone il costante rispetto delle regole e modalità di trattamento, la *privacy by default* si applica anteriormente all'avvio del trattamento e ogni volta che esso riprende dopo eventuali interruzioni: opera sulla base di un automatismo inserito nel trattamento stesso e scatta di norma al suo avviarsi[27]. Anche per questa ragione, essa si presta particolarmente per i trattamenti che comportano elevati livelli di automatismo od elevato ricorso a strumenti tecnologici, di carattere eminentemente digitale[28].

L'accattivante pagina relativa ai "Termini e normative di Facebook", dove l'utente interessato può consultare le condizioni d'uso accettate con la sottoscrizione alla piattaforma nonché la normativa sui dati rivista alla luce del GDPR, si limita a rimandare alle impostazioni privacy del profilo personale – dal quale l'utente può gestire i livelli di condivisione dei contenuti con la propria lista di contatti e di reperibilità da parte di altri utenti, nonché le proprie attività - e a ricordare che

«Il General Data Protection Regulation riconosce il diritto di accedere ai propri dati, rettificarli, trasferirli ed eliminarli […] Hai anche il diritto di opposizione e il diritto di limitare l'elaborazione dei tuoi dati. Ciò comprende:

Il diritto di opporsi al trattamento dei propri dati per il marketing diretto, che può essere esercitato mediante il link di annullamento dell'iscrizione contenuto in tali comunicazioni di marketing;

Il diritto di opporsi al trattamento dei propri dati quando svolgiamo un'attività nell'interesse pubblico o nel perseguimento degli interessi legittimi di Facebook o di terzi. Puoi esercitare tale diritto su Facebook e su Instagram».[29]

La sfida, oggi che la persona digitale prende il sopravvento su quella fisica nella definizione della sua identità – e che quindi il nostro status è quasi perennemente online – è quella di riuscire a tutelare non solo il dato nella sua interezza, ma anche e so-

2016, 79 ss.

[26] S. Calzolaio, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg.Ue 2016/679*, in *Federalismi.it*, 24, 2017. Dello stesso autore cfr. *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, 31, 2016, 185 ss.

[27] Cfr. A. Cavoukian, *Privacy by Design: Leadership, Methods, and Results*, in S. Gutwirth - R. Leenes - P. de Hert - Y. Poullet (a cura di), *European Data Protection: Coming of Age*, New York, 2013, 175.

[28] F. Pizzetti, *op.cit.*, 112

[29] www.facebook.com/privacy/explanation.

prattutto le tracce, i frammenti digitali che lo vanno a comporre. La frammentazione all'interno dell'universo digitale dell'informazione che ci riguarda può essere superata e ricomposta dall'efficienza e dal potere di aggregazione degli algoritmi che si trovano alla base dei meccanismi di *engagement* delle piattaforme, soprattutto di quelle di *social networking*[30].

È proprio sulla presenza di *feed algoritmici* infatti che si basa la funzionalità e l'esistenza stessa delle piattaforme – di *social networking* ma non solo - che tramite la riaggregazione delle tracce digitali e la profilazione degli utenti selezionano tematiche in evidenza, contenuti consigliati, prodotti "che ti potrebbero interessare" o correggono cortesemente le parole che "forse stavi cercando". La finalità è sempre quella di aumentare l'*engagement* ed il profitto della piattaforma che stiamo utilizzando e che vogliamo continuare ad utilizzare, intrappolati in un *autoplay* senza fine o galleggiando nella *filter bubble* che l'algoritmo ha creato per noi, sulla base delle nostre preferenze, raccogliendo le briciole dei *cookies* che abbiamo lasciato navigando e sfruttando la conoscenza dei dati che più o meno consciamente disseminiamo in Internet.

Così, mentre magari abbiamo la percezione di essere in grado di mantenere il controllo dei nostri dati più sensibili, ci può sfuggire l'ampiezza e la profondità delle tracce frammentarie che abbiamo lasciato online durante la navigazione e non abbiamo il potere di controllare quale rappresentazione di noi e delle nostre attività emerga dalla riaggregazione di tali frammenti operata dagli algoritmi.

Il considerando 30 del GDPR relativamente a tale questione infatti recita:

«Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

Un rilevante aspetto relativo alla protezione dei dati personali degli utenti dei social network infatti è inerente alle pratiche commerciali di profilazione operate dagli intermediari digitali per offrire agli utenti servizi ed inserzioni commerciali sempre più mirati e personalizzati, più efficaci e pervasivi rispetto all'*advertising* generico. Si tratta di sfruttamento commerciale dei profili, in questo caso *social*, che fornendo preziose informazioni sulle inclinazioni al consumo dell'utente possono acquisire un rilevante valore di mercato.

Un "mi piace" su Facebook od un "segui" su Instagram, solo per menzionare le due piattaforme più usate in Italia – la seconda è società controllata dalla prima e basata sul medesimo algoritmo – non sono mai azioni neutrali, ma una dichiarazione *open air* delle nostre attitudini, preferenze, dei nostri gusti ed interessi, veri valori commerciali su cui la piattaforma ruota e che il gestore, munito di algoritmo può aggregare, identificare e profilare.

[30] T. Gillespie, *The relevance of algorithms*, in T. Gillespie - P. J. Boczkowski - K. A. Foot (eds.), *Media Technologies: Essays on Communication, Materiality, and Society,* Cambridge (MA), 2014. Sul tema della pervasività dell'algoritmo nella vita fuori e dentro i social network, C. Figueiredo - C. Bolaño, *Social Media and Algorithms: Configurations of the Lifeworld Colonization by New Media*, in *International Review of Information Ethics*, 26, 2017, 26.

«La Macchina vuole sapere in continuazione cosa sta succedendo, quali scelte operiamo, dove stiamo andando, con chi ci fermiamo a parlare. Tutto ciò mentre i nostri dati personali diventano parte del "data-mining" [31], tralasciando il fatto che la nostra individualità semi-privata e per lo più pubblica va rendendo incredibilmente ricchi i proprietari dei social media. È questo il prezzo della libertà e sembriamo più che disposti a volerlo pagare».[32]

Questa pratica comporta inevitabilmente il trattamento dei nostri dati personali e finanche sensibili, poiché riesce a carpire tramite le nostre espressioni di gradimento o preferenza molti aspetti della nostra personalità individuale.

La difficoltà nel creare una regolamentazione che sia efficace e realmente vincolante rispetto alle attività di una piattaforma di *social networking* – di cui noi, intesi come la nostra attenzione ed i nostri dati, siamo il prodotto commercializzato – è l'esistenza di una vasta zona grigia per quanto riguarda la definizione delle attività della piattaforma – è commerciale, è sociale, è editoriale, pretende di creare informazione – che va di pari passo con un certo grado di incoscienza con cui gli *users* si rapportano ad esse. Nonostante l'esistenza del GDPR, un utente medio che vada a sfogliare i termini d'uso di Facebook e voglia capire più a fondo quali e quanti dei propri dati siano profittevolmente sfruttati non vedrà del tutto chiariti i propri dubbi a causa di una certa vaghezza espositiva che caratterizza i *Terms of service* circa la possibilità di registrare ed immagazzinare i dati degli utenti da parte della piattaforma.

Il gestore della piattaforma è naturalmente consapevole di quale sia il valore del dato personale dei suoi utenti e di come farne profitto ed è grazie allo sbilanciamento fra tale consapevolezza e l'incoscienza dei comportamenti messi in atto dagli utenti che l'esistenza stessa di colossi come Facebook – che al primo trimestre di quest'anno, nonostante l'esplosione del caso Cambridge Analytica mostrava ricavi a quota 11,97 miliardi di dollari[33] - è resa possibile.

La nostra identità è la merce di scambio: sul piatto ci sono infiniti contenuti gratuiti a cui possiamo accedere tramite ogni tipo di *device*. La nostra stessa attenzione è bene cruciale e carente sul mercato della comunicazione e le aziende che riescono a convogliare tale attenzione possono realizzare enormi guadagni[34]: è per questo che qualsiasi nostra azione sul web è tramutabile in dato ed ogni nostro click è monetizzabile.

La *datafication* (in italiano "datizzazione") ovvero la trasformazione in dati elaborabili di tutto ciò che facciamo, pensiamo, preferiamo o detestiamo e di tutte le relazioni che intratteniamo con privati e con istituzioni e compagnie, ci porta in un territorio assolutamente nuovo in cui si sono già profilati dei raccoglitori globali di informazioni, i c.d. *mega data set*, che potrebbero costituire una seria minaccia a causa dell'eccesso di potere che stanno accentrando intorno alla loro conoscenza dei nostri dati[35].

---

[31] Sulla differenza fra *data mining* e *data warehousing*, si veda N. Moinet*, Intelligence economica. Saggio sulle moderne tecniche di strategia d'impresa*, Roma, 2013.

[32] G. Lovink, *Ossessioni collettive. Critica dei social media*, Milano, 2012, 17.

[33] A. Salvadori, *Facebook brilla anche nel 1° trimestre 2018: ricavi pubblicitari a +50%,* in www.engage.it, 25 maggio 2018.

[34] C. R. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, 2003, 33.

[35] S. Lohr, The age of Big Data, in www.nytimes.com , 11 febbraio 2012. Sul tema, cfr. V. Mayer-

La privacy ai tempi dei *social* acquisisce dunque carattere polisemico, includendo un insieme di poteri che consentono agli utenti, almeno in teoria, il controllo non solo sulle modalità di trattamento dei propri dati da parte di soggetti sia pubblici che privati che hanno accesso a tali dati ma anche un diritto alla riservatezza di
«connotazione pluralistica: non un singolo diritto, ma un insieme di diritti, tutti riconducibili all'unità e all'integrità della persona umana, fra cui spiccano il diritto all'identità personale come rappresentazione veritiera della propria personalità, il diritto alla riservatezza del proprio domicilio, della propria corrispondenza, delle proprie comunicazioni, in generale, il diritto alla protezione e al controllo dei propri dati personali, ovunque essi siano archiviati, ovvero il pieno controllo del proprio "corpo elettronico"».[36]

4. SNP, privacy e propaganda: la comunicazione politica dopo Cambridge Analytica

Ci sono parole ricorrenti nell'universo *social* con cui la maggioranza degli utenti ha a che fare e che, all'insaputa dei più, costituiscono i termini di riferimento fondamentali per il misterioso funzionamento dell'algoritmo. Innanzitutto quest'ultimo serve a smistare e filtrare per noi i contenuti da visualizzare nelle nostre personalizzate *news feed* – la selezione di notizie nella paginata *home* – da tempo non più in semplice ordine cronologico, criterio che mostrava minor *appeal* e minor capacità di risvegliare la partecipazione attiva degli *users*.
Quello che sappiamo rispetto al funzionamento dell'algoritmo – una parte del meccanismo, va da sé, poiché gli "ingredienti segreti" devono rimanere tali come per la paradigmatica ricetta della Coca Cola – è che esso segue quattro fasi distinte.
La fase di *inventory* si attiva ad ogni nostro accesso alla piattaforma: il sistema recupera le notizie pubblicate dal nostro *network* di "amici" e "pagine seguite" compiendo un vero e proprio inventario delle "giacenze" di informazioni e *post* che ancora dobbiamo vedere.
I *signals* – segnali di contesto e di contenuto – determinano e comunicano al sistema la situazione attuale dell'utente (orario e luogo di accesso, tipologia di connessione e *device* utilizzati) e delle notizie da fargli visualizzare (per tipologia di contenuto, autore, "freschezza" e capacità attrattiva della notizia misurabile in commenti, reazioni e condivisioni, eventuali *feedback* negativi, tempo medio trascorso da altri utenti sulla medesima notizia). Alcuni segnali hanno un peso maggiore di altri, ad esempio se siano rilevanti rispetto al numero e consistenza delle interazioni che una notizia possa far scaturire – *meaningful interactions*.[37]
Sulla base dei segnali l'algoritmo opera poi una previsione personalizzata (*prediction*)-

Schönberger - K.N. Cukier, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013 e G. D'Acquisto - M. Naldi, *Big data e privacy by design,* Torino, 2017.

[36] M.R. Allegri, *op. cit.*, 77.

[37] V. Cosenza, *Come funziona l'algoritmo di Facebook: i fattori di posizionamento 2018*, in www.vincos.it, 20 febbraio 2018

per ognuno degli utenti connessi, cercando di aumentare l'*engagement* della piattaforma proponendo contenuti che, verosimilmente, piacciano, stimolino lettura e condivisione, *click* e reazione, commento ed ulteriore traffico di dati.
Nell'ultima fase di *score* viene assegnato un punteggio di rilevanza ad ognuno dei contenuti disponibili nell'inventario e saranno poi le notizie frutto di questa ulteriore selezione ad essere visualizzate nel nostro *news feed*. Sono i diversi gradi di interazione fra i fattori di posizionamento di Facebook – in questo caso – basati sull'analisi della nostra attività precedente a determinare la nostra esperienza di fruizione della piattaforma e la godibilità dei contenuti appositamente filtrati per noi, un'esperienza sempre più vicina al "Daily Me" preconizzato dall'informatico Nicholas Negroponte[38].
Questo procedimento di selezione e filtraggio si applica ai contenuti commerciali e di intrattenimento così come all'informazione ed alla comunicazione politica, che sia sotto forma di inserzioni sponsorizzate, articoli di testate online di evidente taglio politico o post condivisi dalle pagine ufficiali dei nostri rappresentanti politici. Oggi è imprescindibile per le personalità politiche che vogliano dispiegare una propaganda efficace e pervasiva essere presenti sui social, Facebook e Twitter in primis: sono cambiati i termini, gli spazi ed i "caratteri a disposizione" della comunicazione politica. Proprio sul campo delle inserzioni politiche su Facebook si sono già giocati alcuni degli scandali più grossi, che non hanno in ogni caso saputo travolgere il colosso di Menlo Park ma che ancora alimentano pesanti dubbi sul risultato di alcune elezioni, nello specifico le più recenti presidenziali americane ed il referendum per la Brexit in contesto europeo.
Nell'aprile 2018[39], in seguito agli eventi legati ai casi Cambridge Analytica, emersi il mese precedente, e Russiagate – inchiesta giudiziaria nata a seguito di sospette ingerenze da parte della Russia nella campagna elettorale per le elezioni presidenziali Usa del 2016, basate sull'attività fraudolenta di falsi profili *social* – la piattaforma di Zuckerberg aveva confermato la stretta, almeno in ambito americano, sugli annunci sponsorizzati a scopo politico.
La vicenda di Cambridge Analytica, dal nome della società accusata di aver utilizzato illecitamente i dati personali di milioni di utenti del social network Facebook, ha avuto origine nel 2015 in seguito all'avvio di una collaborazione tra la piattaforma e lo sviluppatore di un'applicazione denominata "*thisisyourdigitallife*", Aleksandr Kogan, ricercatore presso l'Università di Cambridge e titolare della società Global Science Research.
La Cambridge Analytica, fondata nel 2013 ed attualmente chiusa per insolvenza nel Regno Unito e per bancarotta negli Usa, è stata una società specializzata nella raccolta di dati provenienti dall'utilizzo dei social network con finalità di profilazione di carattere politico. Mediante il trattamento di tali dati la società poteva procedere ad un'analisi combinata degli stessi e alla creazione di modelli predittivi da utilizzare durante le campagne elettorali.[40] In seguito all'accusa di aver utilizzato in maniera illegittima – a

[38] Cfr. N. Negroponte, *Being digital*, New York, 1995, 153.

[39] S. Biagio, *Stretta di Facebook sulle inserzioni politiche: sapremo chi le paga e da dove arrivano*, in www.ilsole24ore.com, 7 aprile 2018.

[40] D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda*

causa dell'assenza del consenso esplicito dei soggetti interessati – milioni di dati personali raccolti tramite la *app* di Kogan, la società ha cessato le proprie attività.
La combinazione fra le condizioni di uso di Facebook dell'epoca, meno restrittive rispetto a quelle attuali e la già menzionata "incoscienza" con cui spesso gli utenti rilasciano il proprio consenso - per poter utilizzare la piattaforma stessa, nonché *app* ed estensioni gratuite - hanno fatto sì che tramite il semplice consenso dell'utente che decideva di scaricare *thisisyourdigitallife*, Facebook consentiva a quest'ultima di ottenere non solo le molteplici informazioni presenti sul profilo ma anche quelle ricavabili direttamente ed indirettamente dai profili di tutti gli "amici" del soggetto interessato. In questo modo la *app* è arrivata a carpire le informazioni di più di 80 milioni di profili in tutto il mondo – di cui circa 215mila italiani – a partire dall'iscrizione di appena 270mila utenti. Tali preziose informazioni personali sono poi state vendute da Kogan alla Cambridge Analytica per le sue attività di profilazione di carattere politico.
Facebook è una piattaforma di lancio per migliaia di pagine, siti web ed *app* che propongono i propri servizi e prodotti tramite il social network, spesso suggerendo l'accesso a questi ultimi con le medesime credenziali utilizzate dagli *users* per il *social*. Con questa prassi estremamente comune – di cui l'*app* in questione e lo "scandalo" Cambridge Analytica sono stati estremo esempio – le informazioni presenti nel nostro profilo – nonché spesso quelle relative ai nostri contatti, ai "luoghi salvati", ai *like* dati - vengono condivise dalla piattaforma *social* che stiamo utilizzando e dalla pagina od *app* a cui stiamo accedendo, rendendo arduo riuscire a controllare quali e quante informazioni vengono estrapolate e cedute[41].
Il caso *Cambridge* è stato un esempio di *data breach* e di violazione della privacy degli utenti con finalità politiche – ed ovviamente di profitto - da parte di società di privati ma più estensivamente il campo della comunicazione politica sui *social*, anche quando scevro da meccaniche sotterranee di manipolazione, è settore estremamente sensibile e che necessita più di altri di specifica regolamentazione.
Sulla scia dello scandalo, da ottobre 2017 era stato annunciato che solo gli inserzionisti autorizzati avrebbero potuto gestire gli annunci elettorali su FB ed Instagram, mentre questo requisito sarebbe stato presto esteso a chiunque avesse mostrato "annunci sensibili" – come argomenti politici di rilievo a livello nazionale. Per ottenere l'autorizzazione alla pubblicazione gli inserzionisti devono confermare identità e posizione ed attendere in ogni caso il nullaosta della piattaforma prima della condivisione di annunci di carattere politico od elettorale.
Questi ultimi devono essere chiaramente identificabili ed etichettati come "annuncio politico" – dicitura che gli utenti americani troveranno in alto a sinistra rispetto al post – assieme ad informazioni cruciali come "pagato da", così che sia chiara l'origine ed il finanziamento dell'annuncio. Come per la rimozione di contenuti inappropriati o la sospensione di account fittizi, l'intervento della piattaforma in caso di annunci politici non etichettati si basa sulla segnalazione dei propri utenti – un intervento *ex-post* dunque e non un'azione preventiva.

"Cambridge Analytica", in *Federalismi.it*, 20, 2018

41 Sui fattori di rischio nel Web 2.0 si veda E. Morozov, *L'ingenuità della rete. Il lato oscuro della libertà di Internet*, Torino, 2011.

Dal 24 maggio 2018, col rafforzamento della *Political Ads Policy* di Facebook, è stata inoltre prevista la pubblicazione di un archivio pubblico di annunci politici, contrassegnati dal marchio "*Political Ad*", che assieme all'immagine ed al testo dell'annuncio mostra ulteriori informazioni come la quantità spesa e le informazioni demografiche del pubblico per ogni annuncio[42].

In Italia la novità relativa al monitoraggio della propaganda politica sui *social* e l'archiviazione dei relativi contenuti è stata introdotta il mese successivo. È ora dunque possibile navigare su qualsiasi pagina Facebook – ad esempio quella di un partito o di una personalità politica – e vedere l'elenco dei contenuti sponsorizzati attivi in quel momento. Nella sezione "Informazioni e inserzioni" infatti viene pubblicato l'elenco delle inserzioni attive gestite da quel profilo; in aggiunta viene anche data la possibilità di monitorare tutte le volte che la pagina ha cambiato nome nel tempo.

Nulla ancora per quanto riguarda la "Libreria delle inserzioni" di carattere politico, attivata da Facebook al momento solamente negli Usa, in India, in Brasile – in vista delle ultime elezioni generali di ottobre 2018 - e nel Regno Unito. Per questi paesi l'archivio include le inserzioni di Facebook ed Instagram classificate come di "natura politica" in base ai loro contenuti o relative a questioni nazionali di importanza pubblica: vi si possono reperire inserzioni sui candidati eletti, catalogate per temi o per candidato, con sponsorizzazioni attive o meno, a decorrere dal 7 maggio 2018 e disponibili alla visione da parte degli utenti per sette anni a partire da questa data.

Sono allo stesso modo registrate le prestazioni delle inserzioni, dall'ammontare delle cifre di sponsorizzazione catalogate per fascia di spesa, al numero di visualizzazioni, passando per tutti i dettagli del pubblico (età, sesso e luogo).

L'archivio è disponibile in italiano ma non è ancora operativo in Italia - non è ancora possibile per gli utenti segnalare contenuti politici e visualizzare quelli che riguardano il nostro paese – sebbene sia da segnalare un'interessante iniziativa di Openpolis (www.openpolis.it) che rilancia il *Political Ad Collector* creato dalla testata indipendente americana *ProPublic*. Si tratta di un database di più di un migliaio di inserzioni, monitorate e registrate grazie al contributo degli utenti che hanno installato sul proprio browser l'estensione dedicata.

Un esempio, relativo alle recenti elezioni provinciali in Trentino, riguarda l'inserzione politica con finalità elettorali pubblicata dal candidato PD Gabriele Bertoldi: assieme allo slogan, «Il 21 ottobre vota per un'autonomia forte e giusta» possiamo leggere la dicitura "*sponsored*" ed altre specifiche raccolte sotto le *Targeting information* che spiegano perché una determinata categoria di utenti visualizzerà quello specifico annuncio:

«One reason you're seeing this ad is that Gabriele Bertoldi - Partito Democratico wants to reach people interested in *Happiness*, based on activity such as liking Pages or clicking on ads. There may be other reasons you're seeing this ad, including that Gabriele Bertoldi - Partito Democratico wants to reach people ages 18 and older who live near Trento, Trentino-Alto Adige. This is information based on your Facebook profile and where you've connected to the internet»[43]

---

[42] R. Leathern, *Shining a Light on Ads With Political Content*, in www.newsroom.fb.com/news, 24 maggio 2018.

[43] Per questo ed altri annunci di natura politica selezionati tramite l'estensione di Political Ad Collector

5. Considerazioni conclusive

Iniziative come queste possono tracciare un sentiero di buone pratiche per quanto riguarda una maggiore regolamentazione della propaganda politica messa in atto sui *social* ed una sempre maggiore spinta alla trasparenza rispetto ai contenuti politici, che si rende necessaria di fronte alle capacità pervasive e totalizzanti delle piattaforme. L'utente ha diritto di conoscere la natura dell'informazione che gli viene proposta e di poter uscire dalla propria "bolla" preconfezionata di contenuti.

Il corto circuito fra la necessaria neutralità dell'informazione politica e la proposta personalizzata – e quindi affetta per natura da un certo grado di *bias* politico – è intrinseco nella natura stessa delle piattaforme *social*: questa è l'impasse attuale più gravosa da superare.

Facebook si pone come soggetto promotore e fornitore di informazione, ma di quale informazione?

Basta un'etichetta o un *fact checking* su di un'inserzione per farci capire che quel contenuto è diretto specificamente all'immagine aggregata del nostro Io-online, ricreata dall'algoritmo grazie al nostro comportamento digitale?

I rischi dell'udire sempre e solo il costante eco delle proprie opinioni politiche riverberato da contenuti appositamente scelti per noi sulla base della sola godibilità e piacevolezza sono evidenti[44]. Le condizioni elettroniche personalizzate – peraltro solo in parte dall'utente tramite una scelta consapevole: come abbiamo visto, il "lavoro sotterraneo" di filtraggio lo compie l'algoritmo – che contengono esattamente ciò che il lettore desidera ed escludono ciò che non vuole vedere – si parla di un futuro pulsante *dislike* su Facebook, forse per semplificare ulteriormente questa selezione – non sono condizioni favorevoli alla crescita di un'informazione sana.

Finché i nostri dati e la nostra attenzione saranno il valore commerciale di scambio sulle piattaforme *social*, è piuttosto naturale e conseguente ad una certa logica di mercato che ci vengano proposti prodotti e servizi che tengano alta la nostra attenzione, che amplifichino l'*engagement* della piattaforma e ci spingano a continuare a condividere le nostre informazioni. Nessun buon venditore sponsorizzerebbe contenuti "scomodi", spiacevoli, punti di vista fastidiosi, approfondimenti politici di opposta fazione, sebbene si parli di una certa volontà di stimolare la «proattività degli utenti nell'informarsi ampliando le proprie reti sociali»[45].

Permane sempre il dubbio sull'efficacia di questa spinta alla proattività rispetto alla reale qualità ed imparzialità dell'informazione politica disponibile sul *social*: sforzarci di seguire qualche pagina che riporta contenuti fuori dal nostro coro o aggiungere al nostro *network* esponenti di pensiero differente ci renderebbe veramente consumatori

in Italia, si v. www.propaganda.openpolis.it.

[44] Si veda T. Bucher, *If..Then. Algorihtmic power and politics*, Oxford, 2018 e F. Antinucci, *L'algoritmo al potere. Vita quotidiana ai tempi di Google*, Bari, 2009. Sul tema di Web 2.0 e partecipazione politica, cfr. F. Marcelli - P. Marsocci - M. Pietrangelo (a cura di), *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015.

[45] Da un incontro con Laura Bononcini, Head of Public policy di Facebook per l'Europa meridionale, nell'ambito di un ciclo di seminari organizzati dal prof. B. Caravita di Toritto presso l'Università La Sapienza, "Social network, formazione del consenso ed istituzioni politiche", 12 novembre 2018.

di informazione non filtrata?
Si può davvero ricondurre la polarizzazione dell'opinione politica ormai cavalcante sui *social* al semplice frutto della selezione dell'utente nel libero mercato dell'informazione o si può scorgere un certo grado di responsabilità della piattaforma stessa nel voler mettere il valore di un *like* al di sopra dell'ampiezza dell'orizzonte politico dei suoi *users*?
Il crescente potere di controllo da parte dei privati sulla comunicazione già si ripercuote sugli istituti fondanti della democrazia, in primis il libero scambio di differenti opinioni come fattore di crescita e non di disgregazione del discorso pubblico, mentre le nuove forme di interazione del web sembrano aver già alterato la capacità del cittadino di sentirsi tale e come tale di governarsi.
Sono molte le difficoltà definitorie ed applicative determinate dall'ampiezza e dalla flessibilità di ruoli e funzioni dei network stessi e la tenuta della giovane regolamentazione in materia di dati personali, in vigore da poco più di un semestre, deve ancora essere verificata sul campo dei *social*.
Certo è che non si possono sottovalutare i potenti strumenti di formazione del consenso politico che una piattaforma come Facebook può dispiegare e che questo importante passo in materia di tutela del diritto alla protezione dei dati costituisce una sfida all'ingerenza dei colossi dello *sharing* non solo nel campo della privacy personale ma anche in quello della formazione e consolidamento dell'opinione politica