UNIVERSITÀ DEGLI STUDI DI PAVIA
DIPARTIMENTI DI GIURISPRUDENZA, INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE,
SCIENZE ECONOMICHE E AZIENDALI, SCIENZE POLITICHE E SOCIALI, STUDI UMANISTICI

CORSO DI LAUREA INTERDIPARTIMENTALE IN
COMUNICAZIONE, INNOVAZIONE, MULTIMEDIALITÀ

RITORNO AD UN FUTURO DECENTRALIZZATO:
LA RISPOSTA AL DILEMMA DELLE PIATTAFORME SOCIALI

Relatore:
Chiar.mo Dott./Prof. Paolo Costa

Correlatore:
Chiar.mo Dott./Prof. Guido Legnante

Tesi di laurea di
Stefania Giulia Tonelli
Matricola 476393

ANNO ACCADEMICO 2019/2020

SOMMARIO

INTRODUZIONE 5

CAPITOLO 1 - RITORNO AL FUTURO 9

1) Dal Web delle origini all'era dei social network 9

2) Verso un Web di piattaforme centralizzate 17

2.1) Reddit e Usenet: un confronto esemplificativo 18

2.2) I vantaggi delle piattaforme centralizzate 19

3) I problemi con le piattaforme centralizzate 24

3.1) Privacy e data protection 24

3.2) Moderazione del discorso online 26

3.3) Non-persistenza dei dati 28

3.4) Monopolizzazione del mercato 29

3.5) Modello economico pubblicitario 31

3.6) I social network nel dibattito pubblico 32

4) La proposta di un ritorno ad una logica dei protocolli 35

4.1) Il ritorno ad un futuro decentralizzato 37

4.2) Gli elementi costitutivi di un web decentralizzato 38

5) Social network su protocollo decentralizzato 43

5.1) L'architettura di un DOSN 44

5.2) I benefici della decentralizzazione per i servizi di social networking ...46

CAPITOLO 2 - UN'INNOVAZIONE DISRUPTIVA 53

1) Dalle criptovalute al social networking 54

2) La tecnologia della blockchain 56

3) Le transazioni all'interno di una blockchain 62

3.1) Crittografia e criptazione 63

3.2) Firma digitale 64

3.3) Indirizzi e *wallet* 65

3.4) Transazioni.....65

4) Consenso e *mining* 66

5) Immutabilità nella blockchain.....69

CAPITOLO 3 - IL RISPETTO DELL'UTENTE.....71

1) Il business della sorveglianza.....72

2) La tutela della privacy.....76

2.1) Il concetto di privacy 76

2.2) La minaccia del business della sorveglianza 78

2.3) Lo scandalo e la speranza 81

2.4) Approccio decentralizzato alla tutela dei dati.....87

3) La moderazione del discorso online 92

3.1) Minaccia alla libertà di espressione 92

3.2) Le derive della libera espressione 98

3.3) La ricerca di un compromesso 102

3.4) Decentralizzazione della responsabilità.....105

4) Le piattaforme sociali nel dibattito pubblico 110

4.1) Persuasione e manipolazione nella comunicazione politica 111

4.2) The Social Dilemma 118

4.3) Trasparenza e autodeterminazione dell'ambiente informativo.....124

PROSPETTIVE E CONCLUSIONI 129

a) Dalla teoria alla pratica.....129

b) Verso un futuro ibrido 138

BIBLIOGRAFIA 143

SITOGRAFIA 147

FILMOGRAFIA 153

INTRODUZIONE

L'11 dicembre 2019 Jack Dorsey, fondatore e CEO di Twitter, ha annunciato l'istituzione di Bluesky, un team di ricerca indipendente finalizzato allo studio di un protocollo aperto e decentralizzato per i social media. L'informatico ha rivelato che lo scopo di tale progetto è che Twitter possa in futuro diventare *client* di questo eventuale standard. Successivamente, con un *tweetstorm* Dorsey ha spiegato che l'investimento è motivato da alcune difficoltà che attualmente ostacolano le piattaforme centralizzate e ha chiarito i benefici che il proprio social network trarrebbe da una simile prospettiva.

Il fondatore di Twitter non è l'unica personalità nel mondo dell'*hi-tech* che ha manifestato interesse per il concetto di decentralizzazione, ma a cosa ci si sta riferendo? Cos'è un protocollo decentralizzato e cosa comporta per un social network esserne *client*? A quali difficoltà risponde tale frontiera dell'informatica e quali sono i vantaggi che potrebbe apportare ai servizi centralizzati? Partendo da questi interrogativi si ha sviluppato il presente elaborato, con l'obiettivo di presentare il *Ritorno ad un futuro decentralizzato* come *la risposta al dilemma delle piattaforme sociali*.

Innanzitutto, un servizio online si definisce decentralizzato quando insiste su una struttura distribuita e l'autorità del sistema è condivisa fra i vari nodi del network. Architettura distribuita, a sua volta, significa che in un network i nodi che lo compongono non sono distinti in *client* e *server*, ma ogni *host* ricopre entrambi i ruoli ed è gerarchicamente pari agli altri. Ciò si contrappone al funzionamento delle piattaforme centralizzate che monopolizzano il web. Queste, infatti, possono sì fare affidamento ad una struttura distribuita per migliorare la propria scalabilità, ma le funzionalità vengono espletate unicamente dai nodi server controllati dall'unica autorità che fornisce il servizio. Dopo quest'iniziale e necessaria precisazione, si procederà ora ad accennare la struttura dell'elaborato in questione.

Il primo capitolo della tesi discussa spiega l'espressione "ritorno al futuro", evidenziando come la prospettiva decentralizzata non rappresenti tanto una nuova

ipotesi, quanto la riproposta di un panorama che ha caratterizzato le origini della rete. Risalendo, infatti, al progetto originario di Tim Berners-Lee per il World Wide Web, si può riscontrare come l'applicazione che ad oggi garantisce la fruizione dei contenuti di Internet a milioni di utenti sia nata come progetto pubblico e accessibile a tutti. Successivamente, una serie di fattori ha portato lo spazio aperto e universale della rete ad essere monopolizzato da poche, onnipresenti piattaforme centralizzate. Dopo un iniziale ed immenso successo, tuttavia, queste ultime devono oggi affrontare diverse difficoltà che minano il pieno giovamento da parte dei loro utenti di determinati diritti e principi fondamentali. Per questo motivo da più parti si auspica un ritorno alla libertà e alla democraticità dell'Internet decentralizzato delle origini.

L'invocazione di tale prospettiva è permessa dai recenti sviluppi tecnologici, i quali permetterebbero di superare le problematiche che hanno caratterizzato il primo panorama decentralizzato. In particolare, si fa riferimento all'innovazione introdotta da Satoshi Nakamoto, l'ignoto inventore del Bitcoin, e illustrata nel secondo capitolo di questo elaborato: la blockchain. Quest'ultima viene definita come tecnologia disruptiva, ovvero destinata a creare una rottura tra il presente e il futuro del mercato in cui si insedia. La blockchain garantisce, infatti, determinate proprietà che ne fanno la chiave per il destino della decentralizzazione.

Il terzo capitolo del presente scritto affronta la questione centrale della tesi sostenuta, ovvero qual è il dilemma che affligge le grandi piattaforme e come la decentralizzazione di tali servizi possa apportare dei benefici per la sua risoluzione. Innanzitutto, viene illustrato il cosiddetto capitalismo della sorveglianza, il modello di business dei sistemi centralizzati che monopolizzano l'infosfera odierna. Come conseguenza di tale processo economico, vengono approfondite le tre maggiori problematiche che caratterizzano le piattaforme sociali e come queste mettano in pericolo il godimento di determinati diritti da parte degli utenti. In primo luogo, si affronta la questione della privacy, messa a repentaglio dal business della sorveglianza, che si basa sull'estrazione massiccia di informazioni personali degli individui dalla loro esperienza online. In tale contesto si evidenzia, inoltre, come

il mercato dei dati rappresenti un pericolo per la *data protection*, a causa dell'ambiguità e della vulnerabilità delle policy per la protezione della privacy e alla difficoltà di controllo della condivisione di dati con soggetti terzi da parte dei servizi a cui vengono ceduti. In secondo luogo, viene mostrata la situazione di *impasse* in cui si trovano le piattaforme centralizzate per quanto riguarda la moderazione del discorso online. Da un lato, infatti, gli utenti e le autorità di regolamentazione esigono dai colossi del web una vigilanza dei contenuti pubblicati all'interno dei loro *walled gardens*, costringendoli ad investire costantemente nello sviluppo di algoritmi e nell'assunzione di impiegati addetti alla moderazione. Dall'altro lato, tuttavia, le persone si aspettano dai servizi online anche il rispetto della libertà di espressione, pretesa in tali contesti in quanto le piattaforme sono ormai equiparate a spazio di discorso pubblico. Infine, come terza problematica connessa alla centralizzazione viene approfondita l'influenza di tali sistemi sul dibattito pubblico e politico. In tale sede, infatti, si evidenzia come la proposta personalizzata e microtargettizzata dei contenuti rappresenti una minaccia per lo sviluppo autonomo del pensiero, per il confronto libero e civile delle opinioni e, in generale, per la salvaguardia di diversi principi democratici. Per ognuna delle problematiche accennate, vengono approfonditi i relativi benefici apportati a tali difficoltà da un approccio decentralizzato. La particolarità di una simile proposta è che offre un'alternativa dal punto di vista tecnico al problema dell'individuazione di una soluzione normativa alle questioni evidenziate.

In seguito, a completamento dell'argomentazione, viene offerta una panoramica delle iniziative concrete nell'ambito delineato, ponendo particolare attenzione all'interesse mostrato in tale direzione da parte dei rappresentanti dei più noti servizi centralizzati. Infine, si propone una prospettiva percorribile per la concretizzazione dei concetti discussi, illustrando come un sistema ibrido - composto da funzionalità sia centralizzate che decentralizzate - possa rappresentare una soluzione ad oggi realistica al dilemma delle piattaforme sociali.

CAPITOLO 1 - RITORNO AL FUTURO

Secondo il report *Digital 2020*[1], realizzato da We Are Social in collaborazione con Hootsuite, in un anno l'utente Internet medio spende online un tempo pari a oltre 100 giorni, ovverosia 6 ore e 43 minuti al giorno. Più di un terzo di questo tempo, 2 ore e 24 minuti al giorno, viene trascorso sui social network. Questi dati mostrano come le piattaforme digitali siano ormai diventate parte integrante della vita quotidiana della maggior parte della popolazione mondiale. I social media interagiscono con il mercato, la vita politica, le relazioni personali e molti altri ambiti, influendo sul nostro modo di vivere e persino di pensare. E questo potere fa capo a un ristretto numero di piattaforme che hanno conquistato posizioni dominanti - praticamente monopoliste - non solo nel mercato dell'attenzione, ma anche in quello economico e nella sfera di influenza politica e culturale. Tuttavia, l'iniziale sentimento generale a favore di Internet e dei social media come mezzi per agevolare la libertà di espressione e lo sviluppo di idee sta affrontando un declino. L'espansione indisturbata dei grandi colossi dell'hi-tech si sta ora scontrando con esigenze quali la privacy degli utenti, la regolamentazione del mercato e la moderazione del discorso online. A ciò si cerca di far fronte con lo sviluppo di una governance del settore, che tuttavia è ostacolata dalle dimensioni dello stesso, in particolare dalla globalità del fenomeno e dalla «massa critica raggiunta da tali concentrazioni»[2]. Per questo motivo, un'ipotesi che sta riscontrando sempre più interesse è quella di un ritorno al Web delle origini: un ecosistema democratico, aperto e decentralizzato.

1) Dal Web delle origini all'era dei social network

Sorge spontaneo l'interrogativo di come un sistema libero e decentralizzato possa contribuire a fronteggiare le questioni accennate. Può sembrare contraddittorio,

[1] *Cfr.* We Are Social, *Digital 2020*, in "wearesocial.com" (https://wearesocial.com/digital-2020, consultato il 5 agosto 2020).

[2] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

infatti, che ad esigenze di controllo e regolamentazione si risponda con un'ipotesi che prevede la decentralizzazione delle decisioni. Per questo motivo è bene fare un passo indietro e tornare alle origini del Web, quello spazio universale, aperto e slegato da logiche commerciali, così come pensato dal suo stesso inventore: Tim Berners-Lee.

> Quando cominciai a trafficare con il programma che avrebbe poi fatto nascere l'idea del World Wide Web, lo chiamai Enquire, da *Enquire Within upon Everything*, "entrate pure per avere informazioni su ogni argomento". […] Quel libro dal titolo che sapeva di magia era un portale su un intero universo di informazioni, a proposito di qualsiasi argomento. […] Forse non sarà la perfetta analogia con il Web, ma può servire come rudimentale punto di partenza[3].

Così Tim Berners-Lee inizia il suo racconto delle tappe che lo hanno portato all'invenzione del Web, nel manuale da lui scritto *L'architettura del nuovo Web*. Un volume che presenta un sottotitolo emblematico: «Dall'inventore della rete il progetto di una comunicazione democratica, interattiva e intercreativa»[4]. La democraticità emerge quindi fin da subito come elemento chiave di quell'applicazione che ogni giorno permette a miliardi di persone la fruizione dei contenuti online. Il World Wide Web si definisce infatti come quel servizio di Internet costituito da un sistema di documenti in formato ipertestuale, posti in relazione per mezzo di link e accessibili attraverso la Rete[5]. Berners-Lee lo descrive per la prima volta il 12 marzo 1989 nel paper *Information Management: A Proposal*, un documento che prospetta un sistema per gestire la grande mole di informazioni legata agli esperimenti scientifici al CERN di Ginevra, in cui Berners-Lee lavora[6]. L'elaborato discute i problemi di perdita di informazioni dei sistemi complessi in evoluzione - a partire dal contesto del centro di ricerca svizzero - e propone una soluzione basata

---

[3] Tim Berners-Lee, *L'architettura del nuovo Web*, Milano, Giangiacomo Feltrinelli Editore, marzo 2001, p. 15.

[4] *Ivi*, frontespizio.

[5] *Cfr.* Alberto Marinelli, *Internet e World Wide Web*, in *Scienza e tecnica, Istituto dell'Enciclopedia italiana*, Roma, 2008, pp. 339-349.

[6] *V.* Tim Berners-Lee, *Information Management: A Proposal*, in "CERN Document Server", marzo 1989 (https://cds.cern.ch/record/369245/files/dd-89-001.pdf, consultato il 5 agosto 2020).

sulla registrazione di tali dati in documenti ipertestuali interconnessi da link. La visualizzazione di tali contenuti è resa possibile attraverso un applicativo che prende il nome di web browser, installabile sui client degli utenti. In questo modo il potenziale di Internet diviene accessibile a chiunque sia dotato di un computer - inteso nel senso più ampio del termine - e dell'apposito software.

In poco più di un anno Berners-Lee sviluppa le tecnologie alla base del Web e il 6 agosto 1991 appare il primo sito internet della storia. Si tratta di una pagina con un'interfaccia grafica estremamente semplice, che presenta una sintesi del progetto World Wide Web e rivela i primi dettagli del suo funzionamento. In quel momento, tuttavia, gli unici a possedere gli strumenti per poter fruire del servizio sono Berners-Lee e gli altri ricercatori del CERN. È solo nel 1993 che il Web inizia a diffondersi al di fuori del mondo della ricerca e diventa accessibile all'utente medio. Il 23 gennaio 1993 nasce infatti Mosaic, il primo browser dotato di interfaccia grafica utente ed utilizzato a livello commerciale. Il Web si apre così al mondo e il suo inventore intuisce che, solo se il servizio fosse stato gratuito e fruibile da tutti, il potenziale della rete sarebbe stato veramente sfruttato. Così, pochi mesi dopo - il 30 aprile 1993 - il CERN, su proposta di Berners-Lee, decide di rendere pubblico il Web. Si tratta di una scelta che cambia per sempre la storia della rete. Con le parole del padre del Web: «Se la tecnologia fosse stata proprietaria e sotto il mio totale controllo, probabilmente non sarebbe decollata. La decisione di rendere il web un sistema aperto fu necessaria per renderlo universale. Non puoi proporre qualcosa come uno spazio universale e al tempo stesso mantenere il controllo su di esso»[7].

L'anno successivo, nell'ottobre 1994, Berners-Lee fonda il World Wide Web Consortium (W3C) presso il Massachusetts Institute of Technology. A tale organizzazione viene affidato il compito di realizzare standard che assicurino che tutti i siti del nascente Web funzionino secondo gli stessi principi di conformità.

[7] Andrea Daniele Signorelli, *Storia di internet e del world wide web*, in "Wired.it", 11 marzo 2019 (https://www.wired.it/internet/web/2019/03/11/internet-world-wide-web-storia/?refresh_ce=, consultato il 6 agosto 2020).

Grazie a quest'ultimo tassello prende così definitivamente il via quell'ondata di innovazione che ha reso la rete uno strumento universale, decentralizzato e accessibile a tutti.

Negli anni successivi, in un arco di tempo che arriva fino al 2000, si sviluppa velocemente quell'ecosistema di tecnologie, processi comunicativi e modelli di business che è andato a costituire il cosiddetto Web 1.0. È un contesto composto ancora da documenti testuali con poche immagini e rari video o file audio. La rete è accessibile tramite connessioni con larghezza di banda molto limitata, che non agevolano lo sviluppo di formati multimediali. Nonostante l'instabilità della tecnologia, l'imperfezione delle prime pagine HTML ed altre difficoltà tecniche, il Web di Tim Berners-Lee riscontra comunque un immediato successo che ne permette la transizione dal mondo accademico - legato soprattutto alle possibilità di *free publishing* e di diffusione universale della conoscenza - a quello commerciale e della comunicazione. Si sviluppa così l'esigenza, in ogni contesto sociale, di far parte di quell'universo emergente[8].

In poco tempo le pagine pubblicate online crescono quantitativamente e qualitativamente. Il risultato immediato è un ecosistema libero e aperto, ma caotico. In questo contesto si affacciano così i primi motori di ricerca, con lo scopo di fornire un servizio agli utenti per un recupero agevole dell'informazione online. Nel 1994, in particolare, nasce Yahoo!, dalle menti di David Filo e Jerry Yang. Il progetto embrionale è costituito da una raccolta di link funzionale all'indicizzazione delle diverse pagine online. Tuttavia, la crescita esponenziale del numero di siti web ostacola la performance del software così strutturato, per la difficoltà di aggiornamento del deposito di link. La soluzione a questo problema viene proposta pochi anni dopo da Larry Page e Sergey Brin, due studenti dell'Università di Stanford. Il 15 settembre 1997, infatti, i due giovani lanciano un nuovo motore di ricerca destinato a diventare il punto di riferimento degli utenti per il reperimento dell'informazione online. Il neonato Google consente, infatti, di rintracciare il

[8] *Cfr.* Alberto Marinelli, *Internet e World Wide Web*, in *Scienza e tecnica, Istituto dell'Enciclopedia italiana*, Roma, 2008, pp. 339-349.

contenuto desiderato sul Web grazie ad un sistema di parole chiave e alla gerarchizzazione dei contenuti. Quest'ultima, in particolare, è permessa da un algoritmo ispirato al sistema accademico di valutazione dell'impatto dei paper: la posizione gerarchica di un contenuto viene misurata in base alla quantità di link che vi fa riferimento.

Il servizio così offerto dai motori di ricerca fa da detonatore al definitivo boom economico della rete. In particolare, le società commerciali comprendono che la loro presenza online non è accessoria, ma distintiva di una nuova era del mercato. Inoltre, anche il loro utilizzo del Web cambia: da semplice vetrina online attraverso la quale mostrare un duplicato della brochure aziendale, a contesto interattivo in cui gestire le relazioni con i clienti e attivare nuove attività transattive[9].

Il grande successo commerciale vede contestualmente l'affermarsi di imprese destinate ad essere le protagoniste nella nuova fase di sviluppo del Web. Sono Yahoo!, Google, Amazon e eBay i primi colossi digitali[10]. La diffusione di questi servizi determina lo sviluppo di nuove tendenze nel contesto della rete. Grazie alla comparsa di moderni assetti tecnologici e allo sviluppo di nuovi comportamenti sociali, l'ecosistema della rete affronta una nuova trasformazione. Si tratta del passaggio dall'era del Web 1.0 a quella del 2.0. Le società di telecomunicazione investono nei sistemi di connettività permettendo un ampliamento della larghezza di banda. Ciò consente di facilitare l'elaborazione e la visualizzazione dei formati multimediali, ma soprattutto asseconda la condivisione di file in modalità *peer-to-peer*. Quest'ultima espressione significa che nel Web 2.0 non esiste più esclusivamente l'architettura di rete client-server, in cui gli *host* (i dispositivi di calcolo che interconnessi tra loro formano la rete di Internet) assumono dei ruoli fissi come client o server, ma singoli nodi fra loro gerarchicamente equivalenti svolgono entrambe le funzioni[11].

---

[9] *Ibid*.

[10] *V.* James F. Kurose, Keith W. Ross, *Reti di calcolatori e Internet*, 7a ed., Milano-Torino, Pearson Italia, 2017, p. 62.

[11] *Ivi*, pp. 84-86.

Grazie a questa modalità, si diffonde velocemente, tra il 1999 e il 2000, la pratica del *file sharing*. In quegli anni nasce infatti Napster, un servizio che mediante il sistema del peer-to-peer permette la condivisione fra utenti di contenuti musicali. Il programma, tuttavia, non è completamente decentralizzato fra i diversi nodi di pari, ma fa ricorso ad un registro collocato su dei server centrali, gestiti dai creatori del sistema, Shawn Fanning e Sean Parker. Ciò permette alle major discografiche di identificare dei responsabili del programma di *file shari*ng e di intentare loro una causa per violazione del copyright. La vicenda non ferma comunque la diffusione dei sistemi in modalità peer-to-peer, che da quel momento si sviluppano senza alcun ricorso a registri centralizzati. La pratica del *file sharing* si estende così dal settore esclusivamente musicale a tutti i prodotti dell'industria culturale. La rivoluzionaria modalità di accesso e fruizione dei contenuti digitali comporta il sorgere di nuovi bisogni tra le persone e, ben presto, il traffico generato dai sistemi peer-to-peer raggiunge quantitativamente quello tradizionale in modalità client-server. Inoltre, l'evoluzione tecnologica favorisce lo sviluppo di comportamenti sociali di tipo collaborativo tra gli utenti della rete[12].

Negli stessi anni si diffondono anche i *blog*, pagine web dinamiche costruibili, personalizzabili e aggiornabili direttamente dagli utenti. Queste diventano un luogo di espressione individuale online, in cui i soggetti possono raccontare le proprie esperienze, annotare pensieri e stati d'animo, esprimere opinioni e, soprattutto, condividere informazioni. Il blog, infatti, non è uno spazio vissuto esclusivamente in maniera individuale, ma i contenuti postati online possono essere letti e commentati anche dagli utenti che non ne sono autori. Inoltre, le relazioni si sviluppano non solo attraverso la partecipazione alle conversazioni così createsi, ma anche mediante lo scambio di link, il suggerimento di contenuti agli altri membri della comunità e la condivisione di risorse nell'ambiente di rete. La diffusione di questi

[12] *Cfr.* Alberto Marinelli, *Internet e World Wide Web*, in *Scienza e tecnica, Istituto dell'Enciclopedia italiana*, Roma, 2008, pp. 339-349.

comportamenti rende i Blog uno dei contesti comunicativi che innescano la ridefinizione dei confini tra «spazio privato e spazio pubblico»[13].

Dall'inizio del nuovo millennio si diffondono sempre più profondamente le tecnologie di accesso ad Internet ad alta velocità, grazie alla banda larga. Inoltre, parallelamente alle innovazioni nel contesto della rete, si assiste allo sviluppo di numerosi strumenti per la produzione di foto, video e audio in formato digitale. Entrambi questi elementi contribuiscono alla proliferazione dell'offerta di servizi web basati sulla distribuzione di contenuti multimediali. Il pubblico che fruisce di tali forme di comunicazione è sempre più esteso e non si limita a beneficiare delle stesse, ma contribuisce alla «produzione, classificazione e ridistribuzione»[14]. Fra le imprese che emergono in questo contesto ve sono alcune che riescono particolarmente ad intercettare le nuove esigenze degli utenti della rete e sviluppano *web service* in grado di rispondervi. Queste realtà riscontrano un successo straordinario che ne fa le protagoniste dell'era del Web 2.0 e che, inoltre, dà vita a un nuovo ambiente economico legato ai servizi della rete.

Sono in particolare i social network l'innovazione che attira l'attenzione di tutti gli utenti del Web. Gli anni a cavallo fra i due millenni vedono, infatti, il proliferare di piattaforme per il social networking, in particolare a partire dal caso Friendster, sito di incontri che mette in contatto le persone secondo il principio amici-di-amici. Nonostante il madornale fallimento di questa piattaforma - a causa di diverse questioni che travalicano l'interesse di questo elaborato - grazie alla sua popolarità si diffonde nella rete la necessità di un luogo di incontro, in cui instaurare relazioni con persone legate da interessi affini. In tutto il mondo nascono e si diffondono servizi per il social networking con differenti caratteristiche, che catturano l'attenzione di diverse basi di utenti. La maggior parte delle piattaforme di quegli anni trova successo in contesti nazionali, come Orkut in Brasile e India, Mixi in Giappone, LunarStorm in Svezia, Hyves in Olanda, Bebo nel Regno Unito,

[13] *Ivi*, p. 346.
[14] *Ivi*, p. 347.

in Nuova Zelanda e Australia, e molti altri ancora[15]. Inoltre, *web service* di comunicazione già popolari, come quelli di messaggistica, i forum e i servizi per il blogging, iniziano ad implementare funzionalità di social networking. Tuttavia, nonostante alcune di queste piattaforme contino su una base di utenti anche maggiore di quella di MySpace, è quest'ultimo il primo social network a spopolare in un contesto fondamentale, quello degli Stati Uniti e dei media di lingua inglese.

A determinare il successo di MySpace è un misto di funzionalità distintive e di circostanze sociali. La piattaforma californiana nasce per attirare gli utenti delusi da Friendster. Un particolare sottogruppo di questi è costituito dalle band indie-rock, espulse dal social network per non essersi attenute al regolamento dei profili. Il riversarsi di gruppi musicali su MySpace porta, a sua volta, l'ingresso dei relativi fan. La piattaforma acquisisce così un'immediata popolarità, ma sono due in particolare i servizi che ne decretano il successo: da un lato MySpace aggiunge costantemente nuove funzionalità sulla base della domanda e dei suggerimenti degli utenti; dall'altro permette agli stessi di personalizzare le proprie pagine modificandone il codice HTML. Inoltre, un altro particolare gruppo di utenti si unisce al social network in massa. Si tratta dei teenager, esclusi da numerose altre piattaforme non aperte ai minori. My Space dà così il via all'era dei servizi di social networking universali, utilizzati in tutto il mondo e destinati a rompere definitivamente i confini spazio-temporali nei rapporti inter-relazionali.

Parallelamente allo sviluppo di questi network di massa, nascono e si diffondono numerosi servizi di nicchia. Uno di questi è Facebook, piattaforma pensata per supportare le reti sociali di college prestigiosi. Infatti, il social network oggi più diffuso al mondo nasce in realtà come piattaforma ad accesso ristretto ai soli possessori di indentificativi di determinate università. Ciò contribuisce a diffondere tra gli utenti la percezione del sito come una comunità privata e intima. Solo dal 2005 Facebook viene aperto anche agli studenti delle scuole superiori, alle reti aziendali e, infine, a chiunque. Da quel momento prende il via la diffusione

[15] *Cfr.* Danah M. Boyd, Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, in "Journal of Computer-Mediated Communication", 13 (2008), pp. 210-230.

della piattaforma a livello mondiale che elegge Facebook a "The Social Network", cioè a social network per eccellenza[16].

2) Verso un Web di piattaforme centralizzate

Nei primi anni 2000 diventano così evidenti la strategicità del coinvolgimento degli utenti nella creazione di contenuti e l'importanza della dimensione del social networking. Le piattaforme si configurano come un ambiente sociale in cui valorizzare la propria identità e sviluppare ed intrattenere relazioni mediate dalla tecnologia[17]. Attraverso i social network gli utenti esprimono la propria personalità pubblicando immagini, video, parole e condividendoli con una rete di persone più o meno ampia. A differenza delle prime *community* online e dei forum di discussione, le piattaforme per il social networking non sono organizzate per tematiche e interessi, ma sono strutturate attorno alla rete di contatti che ogni utente si costruisce. Il successo di questo tipo di *web service* è dovuto alla loro capacità di rispecchiare le strutture sociali reali, articolate, appunto, in network di relazioni più che in gruppi di interesse[18].

Nel Web del social networking, quindi, quello che conta è la rete di contatti che ognuno si crea, definita *social environment*[19] (ambiente sociale). All'interno di una determinata piattaforma l'utente accumula nel tempo una pluralità di relazioni che sono essenziali per la sua stessa esperienza in quel contesto. La differenza fra i social network e altri *web service* per l'espressione della propria identità online, come i blog, è che i primi sono incentrati proprio sull'interazione fra utenti, piuttosto che sulla valorizzazione della personalità individuale. Con la diffusione capillare dell'online social networking nella vita quotidiana delle persone si sviluppa così il fenomeno della vetrinizzazione, per il quale gli utenti percepiscono la

---

[16] *Ibid.*

[17] *Cfr.* Vanni Codeluppi, *Mi metto in vetrina*, Milano, Mimesis Edizioni, 2015, p. 22.

[18] *Cfr.* Danah M. Boyd, Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, in "Journal of Computer-Mediated Communication", 13 (2008), pp. 210-230.

[19] Bortoli Stefano, Bouquet Paolo, Palpanas Themis, *Social networking: Power to the people*, in *Papers presented in W3C Workshop on the Future of Social Networking Position*, Barcellona, gennaio 2009.

necessità di esporsi nelle vetrine digitali e catturare l'attenzione degli altri. La propria presenza online e il relativo riconoscimento altrui diventano quindi strumentali alla certificazione dell'esistenza stessa dell'individuo nel Web e persino nella realtà offline[20].

2.1) Reddit e Usenet: un confronto esemplificativo

Dopo aver evidenziato l'importanza del *social environment* che ognuno si crea attraverso l'esperienza all'interno dei social network, a sostegno della tesi discussa in questo elaborato è bene mettere a confronto due tipologie di piattaforme che hanno caratterizzato l'inizio dell'era del social networking: quella centralizzata e quella basata su un protocollo aperto. A tale scopo si farà riferimento a due esempi semplificativi, Reddit e Usenet. Si tratta di due social network concettualmente molto simili. Infatti, entrambi sono strutturati in una serie di forum di discussione connessi a differenti tematiche. Tuttavia, a livello tecnico, Reddit consiste in una piattaforma centralizzata controllata da un'unica società, mentre Usenet si basa su un protocollo aperto (il Network News Transfer Protocol, o NNTP) a cui chiunque può avere accesso tramite diverse applicazioni. Per utilizzare Usenet, infatti, un utente deve accedere a un server della rete sottostante il protocollo tramite un'applicazione *client* per la fruizione dei contenuti. Nel corso del tempo, proprio grazie alla struttura del social network basata su un protocollo aperto, diverse organizzazioni hanno sviluppato numerose interfacce utente per Usenet, introducendo così varie funzionalità aggiuntive. Tuttavia, la struttura così composta del social network comporta alcuni problemi. Innanzitutto, l'assenza di un'entità centralizzata che stabilisca delle norme univoche del sistema a cui tutti devono attenersi fa sì che all'ingresso di nuovi utenti gli altri debbano farsi carico della loro formazione, per assicurarne la conformità agli standard. In secondo luogo, il fatto che Usenet poggi su una rete di *host* comporta che i contenuti distribuiti nei diversi server possano essere strutturati in maniera diversa. Inoltre, la decentralizzazione rende

[20] *Cfr.* Vanni Codeluppi, *Mi metto in vetrina*, Milano, Mimesis Edizioni, 2015, pp. 14-15.

complessa l'implementazione di qualsiasi modifica al protocollo, poiché richiede il consenso delle numerose parti in causa per l'approvazione degli aggiornamenti. In Reddit, al contrario, le innovazioni vengono sviluppate da un team dedicato che le stabilisce e le applica. Infine, il problema maggiore di Usenet è la questione della monetizzazione, ossia la difficoltà di stabilire un modello di business efficace. In un sistema centralizzato, invece, la singola entità che controlla la piattaforma può trarne profitto - normalmente grazie alla proprietà dei dati degli utenti e alla pubblicità[21].

2.2) I vantaggi delle piattaforme centralizzate

Grazie al confronto esemplificativo fra Reddit e Usenet è possibile riassumere i presupposti che, agli albori dell'era del social networking, hanno determinato l'affermazione delle piattaforme centralizzate a discapito di quelle basate su standard aperti e decentralizzati. La centralizzazione, infatti, comporta che una singola organizzazione gestisca e amministri le funzionalità offerte agli utenti. Non vi è quindi, innanzitutto, il problema degli aggiornamenti e dell'introduzione di nuovi servizi, come visto in precedenza, perché spetta esclusivamente al soggetto centralizzato decidere eventuali implementazioni. La possibilità di strutturare ed evolvere la piattaforma a proprio piacimento, inoltre, comporta la facoltà di poter incorporare nel sistema un determinato modello di business di cui l'entità centrale è l'unica a beneficiare. I finanziamenti per la manutenzione del social network nel contesto centralizzato provengono quindi - solitamente - dal capitale investito dall'organizzazione che vi è dietro (anche questa componente è assente in una realtà decentralizzata) e da proventi ricavati dal modello di business. Quest'ultimo è tipicamente basato sulla vendita di spazi pubblicitari e dei dati degli utenti per la targetizzazione delle inserzioni stesse. Il circolo vizioso che si crea fra risorse economiche, implementazione delle funzionalità ed efficienza del modello di business

[21] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

fa sì che gli utenti optino per i servizi centralizzati, meglio performanti e costantemente aggiornati[22].

Tornando ora alla questione del *social environment* precedentemente discussa, non rimane che approfondire un ultimo elemento che ha determinato il successo delle piattaforme centralizzate a fronte di quelle decentralizzate. Con la concentrazione degli utenti in determinati social network facenti capo a singole entità si è amplificato esponenzialmente il fenomeno dell'importanza della rete di contatti che ogni utente si crea online. La centralizzazione comporta infatti che i dati personali dei suoi fruitori siano di proprietà del soggetto che gestisce una piattaforma. In questi dati sono compresi i contenuti che nel tempo un utente ha prodotto e pubblicato online e anche il sistema di relazioni che ha costruito. Ciò significa che se un individuo volesse raccogliere quest'insieme di informazioni personali per esportarle in altre applicazioni, in particolare in altri social network, non potrebbe farlo. Le piattaforme centralizzate rappresentano oggi dei *walled gardens*, dei giardini recintati, all'interno dei quali ad ogni utente viene data l'impressione di avere il controllo sui propri dati, ma da cui tuttavia non è possibile semplicemente trasferire le proprie informazioni personali e, soprattutto, la propria rete di contatti in un altro social network[23].

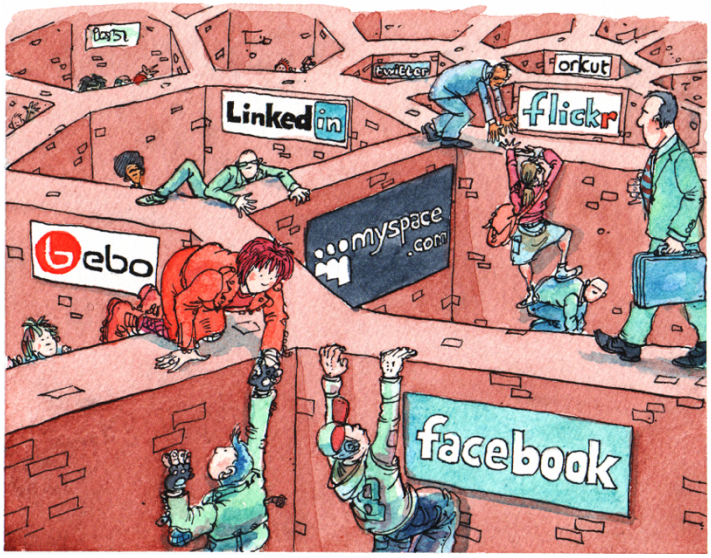

Figura 1: Il concetto di *walled gardens* rappresentato in un'illustrazione di David Simonds, in *Everywhere and nowhere*, in "The Economist, Business", 19 marzo 2008 (https://www.economist.com/business/2008/03/19/everywhere-and-nowhere, consultato il 15 settembre 2020).

[22] *Ibid.*

[23] *V.* Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, Tim Berners-Lee, *Decentralization: The future of online social networking*, in *W3C Workshop on the Future of Social Networking Position Papers*, vol. II, gennaio 2009, pp. 2-7.

Si crea così il cosiddetto *lock-in effect* o *vendor lock-in*, fenomeno per cui, in economia, fra cliente e fornitore di beni o servizi si instaura un rapporto di dipendenza. Quest'ultima è dovuta al fatto che per il cliente rivolgersi a un fornitore differente di beni o servizi analoghi comporta rilevanti costi e rischi[24]. Nel caso dei social network il costo è la perdita dei contenuti prodotti e, soprattutto, della rete di contatti creata. L'importanza di quest'ultima può essere spiegata dalla legge di Metcalfe, l'inventore del protocollo Ethernet. Tale principio afferma infatti che «per ogni persona che vi si aggiunge una rete diventa sempre più utile»[25]. È la quantità di membri di un network, quindi, a renderlo vantaggioso e la centralizzazione fa sì che lasciare una comunità sia particolarmente oneroso. Tuttavia, nel contesto delle piattaforme centralizzate, gli utenti devono creare account diversi per ogni sito di social networking e costruire nuovamente una propria rete di relazioni[26].

L'interesse dei social network a trattenere gli utenti all'interno dei propri *walled gardens* è dovuto sicuramente allo scopo di massimizzare le visualizzazioni delle loro pagine, segno di popolarità del sito. Tuttavia, il vantaggio maggiore è derivato dal fatto che i modelli di business che sostengono le piattaforme sono «inerentemente connessi alla concentrazione dell'utenza»[27]. Infatti, le funzionalità che generano maggior profitto per le organizzazioni proprietarie dei social network - come la pubblicità - e alcuni fra i servizi forniti più importanti - la raccomandazione di acquisti e consumi o la targetizzazione dei contenuti per il pubblico - sono permessi grazie alla profilazione degli utenti, realizzata attraverso algoritmi che lavorano su basi statistiche e quindi su ingenti quantità di informazioni. È vero che le grandi piattaforme si basano su sistemi di gestione dei dati distribuiti per incrementare la propria scalabilità - ovvero la capacità di garantire prestazioni ottimali anche all'aumentare dei volumi dei dati in circolazione. Tuttavia, per assicurare il

---

[24] *Cfr.* Wikipedia, *Vendor lock-in*, in "Wikipedia", 21 ago 2020 (https://it.wikipedia.org/wiki/Vendor_lock-in#cite_note-ITIL_p157-1, consultato il 15 settembre 2020).

[25] Eli Pariser, *Il Filtro*, Milano, il Saggiatore S.p.A., 2012, pp. 37-38.

[26] *V.* The Economist, *Everywhere and nowhere,* in "The Economist, Business", 19 marzo 2008 (https://www.economist.com/business/2008/03/19/everywhere-and-nowhere, consultato il 15 settembre 2020).

[27] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, p. 43.

controllo del t*hroughput* (la «quantità di dati trasmessi per unità di tempo»[28]) è necessario che i nodi interconnessi risiedano su dorsali proprietarie. Quest'ultimo costituisce quindi un altro elemento che fa della centralizzazione la condizione ottimale per il successo delle piattaforme per il social networking nell'infosfera.

Come appena accennato, il carattere di centralizzazione non fa strettamente riferimento ad architetture accentrate, in quanto solitamente le grandi piattaforme si affidano a sistemi tecnici distribuiti. Piuttosto, ad essere centralizzate e controllate da un unico soggetto tecnico e giuridico sono le funzionalità offerte agli utenti, come le politiche di accesso e distribuzione, gli algoritmi e, soprattutto, la proprietà dei dati. Una simile configurazione è dovuta sicuramente a fattori "storici", in primo luogo al fatto che i maggiori social network e gli altri *web service* centralizzati sono frutto del genio di determinate personalità come Mark Zuckerberg, Jeff Bezos, Larry Page e Sergey Brin. È comprensibile infatti che questi soggetti abbiano un interesse a mantenere il controllo sulle proprie tecnologie e aziende[29].

In aggiunta, alcuni fenomeni sociali hanno beneficiato di determinati vantaggi che le piattaforme centralizzate detengono, a differenza di quelle decentralizzate. Innanzitutto, i sistemi centralizzati rispondono all'esigenza di integrare i dati eterogenei e potenzialmente contraddittori prodotti dalle diverse fonti informative all'interno dell'infosfera. Il non dover rendere conto del proprio funzionamento interno, della logica degli algoritmi, fa sì che le piattaforme centralizzate possano assumersi «una sorta di "responsabilità epistemica" davanti ai problemi aperti della *knowledge fusion*»[30]. Un simile ruolo è permesso dal fatto che nei *web service* centralizzati gli utenti fruiscono passivamente del servizio, aderendo implicitamente a un patto di "fede" nel sistema. Secondo lo stesso ragionamento, le piattaforme centralizzate assumono una funzione integrativa anche per quanto riguarda il linguaggio. Infatti, l'adozione generalizzata di tali sistemi fa sì che ad essi faccia capo anche una capacità normativa del complesso sistema linguistico-

[28] *Ivi*, p. 45.
[29] *Ivi*, p. 43.
[30] *Ivi*, p. 44.

concettuale che caratterizza l'infosfera. Le piattaforme sociali plasmano la semantica del Web «promuovendo specifici modelli di comportamento, sia in modo manifesto […], sia in modo implicito o indiretto, ad esempio imprimendo alle conversazioni specifiche strutture dialogiche»[31]. Tutto ciò rappresenta un vantaggio dal punto di vista sociale, perché risponde ad una necessità di chiarificazione.

Sono molti quindi i fattori che hanno favorito l'affermazione e il consolidamento nell'infosfera delle piattaforme centralizzate a scapito di quelle basate su protocolli aperti e decentralizzati. E nonostante le loro dimensioni monopolistiche possano rappresentare una minaccia sotto diversi punti di vista, contrastarle con interventi legislativi porterebbe inevitabilmente a dover affrontare un paradosso. Andando a contenere la massa critica di tali concentrazioni, infatti, si danneggerebbe la qualità delle funzionalità offerte e si limiterebbe la possibilità di innovazione. In aggiunta, i servizi forniti dalle piattaforme di social networking sono oggi percepiti come essenziali, poiché sono entrati a far parte della vita quotidiana delle persone. Sarebbe quindi "socialmente/politicamente" controindicato procedere ad una limitazione di tali sistemi. Inoltre, l'argomentazione di incentivare la concorrenza nel settore andando a restringere i monopoli esistenti, non può essere invocata dal momento che i servizi di social networking sono offerti gratuitamente[32].

Tuttavia, il panorama odierno delle piattaforme centralizzate non è completamente roseo. Al contrario, come già accennato, l'iniziale sentimento generale a favore di Internet e dei social media ha subìto una battuta di arresto. Nuovi interessi e nuove necessità sono sorti e contrastano con i monopoli dei social network centralizzati. Da più parti si invoca il ritorno all'equilibrio del Web delle origini, di quell'Internet decentralizzato e aperto così come era stato pensato da Tim Berners-Lee. L'infosfera odierna piuttosto che essere il frutto di un apporto collettivo, sembra essere diventata il prodotto di singoli soggetti che attirano e bloccano gli utenti all'interno di *walled gardens*, spettacolari ma comunque vincolanti. La visione iniziale di Internet come mezzo per incentivare l'universale libertà di espressione e

[31] *Ivi*, p. 45.
[32] *Ivi*, pp. 45-46.

lo sviluppo di idee sembra essere decaduta in favore di una generale tendenza al gregarismo[33].

Al contrario, l'open web si definisce propriamente come piattaforma su cui chiunque può intervenire, basata su standard (come il protocollo HTTP) e su una complessa tecnologia (server, dispositivi, browser…). Si tratta di una struttura che, per definizione, implica l'apporto degli utenti per la sua innovazione, per l'utilizzazione e per l'implementazione. Si mantiene così la promessa originale di Internet quale universo in cui tutti sono connessi e in cui ogni contenuto può ricevere l'attenzione che merita, a prescindere da sponsorizzazioni o connessioni[34].

3) I problemi con le piattaforme centralizzate

Si è accennato ad alcune difficoltà che caratterizzano il panorama odierno monopolizzato dalle piattaforme centralizzate. Sorge spontaneo l'interrogativo di quali siano queste problematicità tali da reprimere l'entusiasmo per dei servizi completamente gratuiti, costantemente aggiornati e modernizzati e che soddisfano l'egocentrismo degli individui ponendoli al centro di personali reti di relazioni. Si procederà ora ad introdurre tali problematiche.

3.1) Privacy e data protection

Gli utenti dell'infosfera hanno a lungo beneficiato dei servizi offerti dalle grandi piattaforme online senza necessariamente interrogarsi su una questione fondamentale. In un normale scambio commerciale la fruizione di un servizio o il consumo di un bene sono soggetti ad un costo. Al contrario, nel contesto dei *web service* centralizzati l'accesso alle funzionalità offerte è generalmente gratuito. E come recita un aforisma sempre più utilizzato proprio per descrivere il modello di business dei servizi web: «Se non stai pagando per il prodotto, allora il prodotto sei

[33] *Ivi*, p. 46.

[34] Cfr. Charlie Terenzio, *How Walled Gardens Like Facebook Are Cannibalizing Media Publishers*, in "Forbes", 6 giugno 2018 (https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/06/how-walled-gardens-like-facebook-are-cannibalizing-media-publishers/#5703c6f65101, consultato il 15 settembre 2020).

tu»[35]. La moneta che gli utenti offrono inconsapevolmente a Facebook, Google, Amazon e agli altri colossi del web, infatti, non sono altro che le informazioni che quotidianamente cedono loro attraverso qualsiasi attività svolta all'interno di quei preziosi *walled gardens*. Riprendendo Eric Hobsbawn, importante storico britannico, nell'era contemporanea «il plusvalore è creato dai consumatori digitali che, usando Internet, "lavorano" gratuitamente per i produttori e dunque pagano con le loro attività di utenti le nuove tecnologie dell'informazione»[36]. La prima questione che oggi genera criticità e avversione nei confronti delle piattaforme decentralizzate è quindi una conseguenza del loro modello di business. Il guadagno di un social network come Facebook dipende, infatti, dal numero dei suoi utenti, in particolare dalla quantità di dati di cui dispone su di essi. Per anni gli individui online hanno ceduto queste informazioni senza preoccuparsi di ciò, assuefatti dal fascino e dalla comodità dei sistemi fruiti gratuitamente. Tuttavia, dopo quest'iniziale fase di cecità nei confronti del business incentrato sui dati personali degli utenti, questi ultimi hanno finalmente iniziato a prendere coscienza di stare cedendo un proprio diritto fondamentale, quello alla *privacy*[37]. In particolare, in seguito a vicende quali lo scandalo di Facebook e Cambridge Analytica, la campagna referendaria per la Brexit e le elezioni presidenziali del 2016 negli USA (contesti che si avrà modo di approfondire in seguito), i cittadini dell'infosfera hanno iniziato a comprendere le potenzialità di quelli che vengono definiti come «il petrolio del terzo millennio», ovvero i dati. Chi ne dispone in grandi quantità - si parla infatti di Big Data - ed è in grado di sfruttarli, ne trae un vantaggio competitivo inedito rispetto a chi è escluso da un simile mercato[38]. Per quanto riguarda le grandi piattaforme costruite sul World Wide Web, queste sono distribuite su dei server proprietari a cui gli utenti possono accedere tramite un web browser o un'applicazione mobile. La centralizzazione del sistema fa sì che ad avere il controllo delle informazioni salvate

[35] Tristan Harris in *The Social Dilemma* (Jeff Orlowski, 2020).

[36] Domenico Talia, *La Società Calcolabile e i Big Data*, Soveria Mannelli, Rubbettino Editore, 2018, p. 48.

[37] *Ibid.*

[38] *Ivi*, p 39.

in quei server sia solo il soggetto proprietario, il quale ha in questo modo a disposizione un grande potere. Il possesso dei dati gli permette di sfruttarli per fornire agli utenti servizi personalizzati basati sulla targetizzazione del pubblico, di usarli a fini commerciali e di vendere queste informazioni all'industria pubblicitaria o a chi ne è interessato. Ciò ha suscitato preoccupazioni sia da parte degli utenti, sia delle autorità di regolamentazione, per il timore che le piattaforme possano approfittare di questo potere o che non proteggano adeguatamente i dati raccolti[39]. Inoltre, la ricerca nel settore ha evidenziato quanto effettivamente è possibile conoscere di un individuo analizzando le informazioni trasmesse attraverso l'utilizzo dei social e della rete in generale. La pervasività delle nuove tecnologie nella quotidianità delle persone e la digitalizzazione (quindi la conversione in dato digitale di qualsiasi informazione possibile) fanno sì che, attraverso l'attività online, gli utenti lascino continuamente delle tracce che rivelano di loro molto più di quanto possano fare i tradizionali dati sociodemografici. Per questo motivo, l'attenzione della popolazione nei confronti di queste tematiche sta crescendo sempre di più e così anche l'interesse delle persone nei confronti della propria privacy. La *data protection* costituisce quindi una delle maggiori difficoltà che le piattaforme centralizzate di oggi si trovano a dover affrontare.

3.2) Moderazione del discorso online

Una seconda grande questione che si sta rivelando sempre più problematica per i soggetti responsabili dei grandi social network centralizzati riguarda la moderazione del discorso online. Questa difficoltà deriva da un paradosso che le piattaforme per il social networking si trovano oggi a dover fronteggiare. Anche in questo caso è in ballo un diritto fondamentale: quello alla libertà di espressione. I social network centralizzati tecnicamente costituiscono dei servizi web proprietari, all'interno dei quali gli utenti devono adattarsi ai protocolli di comportamento

[39] *Cfr.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

unilateralmente stabiliti. L'amministratore di una community dovrebbe quindi essere in condizione di definirne gli obiettivi, i limiti e le conseguenze di eventuali violazioni. Tuttavia, per quanto riguarda le piattaforme di social networking di dimensioni globali, come Facebook ad esempio, l'approccio "casa nostra, regole nostre" non è ammesso[40]. Si tratta di un contesto eccezionale in cui, ponendosi come piattaforme aperte per la libera espressione, i social media hanno più difficoltà di chiunque altro, come spiega Andrew Losowsky, responsabile del progetto Coral che ambisce a valorizzare l'interazione tra community online[41]. L'enorme diffusione dei servizi di social networking tra l'utenza della rete, infatti, ha fatto sì che le piattaforme vengano oggi considerate degli spazi di discorso pubblico, in cui è preteso il principio della libera espressione. Ciò, essenzialmente, non rappresenta una problematica. La difficoltà per i responsabili dei social network si pone nel momento in cui è richiesta loro anche la garanzia della qualità del discorso online. Come afferma Mike Masnick nel suo saggio *Protocols, Not Platforms: A Technological Approach to Free Speech*, infatti, la centralizzazione del controllo nelle piattaforme ha portato con sé «la richiesta di responsabilità, inclusa una sempre maggiore sorveglianza dei contenuti ospitati su queste piattaforme». Secondo il CEO di Twitter Jack Dorsey nei servizi di social networking «la centralizzazione […] agevola un meccanismo non virtuoso per il quale si sarebbe portati a "focalizzare l'attenzione su contenuti e conversazioni che generano polemiche e indignazione, piuttosto che conversazioni che informano e promuovono la conoscenza"[42]». Ciò ha portato nel tempo allo sviluppo di derive patologiche del web come l'*hate speech*, le fake news, la disinformazione, la polarizzazione, il *trolling* ed altri ancora[43]. Si avrà modo di approfondire più avanti le conseguenze della centralizzazione sulla qualità del discorso online, quello che si vuole evidenziare

[40] *Cfr.* Emily Bell, *Facebook's moderation is of public interest. It should be public knowledge*, in "Columbia Journalism Review", 23 marzo 2017 (https://www.cjr.org/tow_center/facebook-moderation-guardian.php, consultato il 23 settembre 2020).

[41] *Ibid.*

[42] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[43] *Ibid.*

al momento è - come accennato in precedenza - il paradosso che le piattaforme di social networking sono chiamate ad affrontare. Da un lato, infatti, è richiesto loro di intervenire nella regolamentazione dei fenomeni di deterioramento della conversazione online accennati. Dall'altra gli utenti dell'infosfera reclamano la garanzia della libertà di manifestazione del pensiero. La ricerca di un tale compromesso costituisce, tuttavia, per i servizi di social networking, un lavoro svantaggioso. Sempre secondo Dorsey, infatti, il perseguimento di un equilibrio tra la libertà di espressione e la moderazione dei contenuti porta le piattaforme «a dover impegnare ingenti risorse economiche e umane in uno sforzo che prevede investimenti con ritorni limitati»[44]. L'approccio tradizionale alla regolamentazione del discorso online determina quindi delle diseconomie di scala difficilmente risolvibili.

3.3) Non-persistenza dei dati

Come approfondito in precedenza, la proprietà dei dati a carico delle piattaforme di social networking determina per gli utenti e per le autorità di regolamentazione delle preoccupazioni relative allo sfruttamento di tali informazioni. In aggiunta, vi sono altre due problematicità connesse al possesso centralizzato dei dati. Innanzitutto, il controllo univoco dei sistemi di memorizzazione dei dati da parte dei soggetti che gestiscono le piattaforme dà origine ad un ulteriore timore. Come accennato precedentemente, i maggiori servizi di social networking odierni si basano su un'architettura client-server. Ciò implica che le informazioni prodotte in un dato sistema siano salvate sui server proprietari dell'autorità a capo dell'applicazione. Nel caso dei grandi social network, ovviamente, i dati non risiedono in un unico server, ma all'interno di *data center*, ossia strutture composte da diversi host che «creano un potente server virtuale»[45]. I servizi più diffusi fanno riferimento anche a più *data center*. Google controlla dai 50 ai 100 centri, per un totale di 2,5 milioni

[44] *Ibid.*

[45] James F. Kurose, Keith W. Ross, *Reti di calcolatori e Internet*, 7a ed., Milano-Torino, Pearson Italia, 2017, p. 85.

di server stimati a luglio del 2016[46]. Si tratta di un numero in costante crescita, proporzionale all'espansione della capacità del servizio e all'aggiornamento dell'infrastruttura hardware. Ciò significa che il soggetto proprietario di un dato servizio è responsabile della persistenza dell'enorme massa di dati relativa al proprio *walled garden*. Tuttavia, le architetture centralizzate sono di per sé più vulnerabili rispetto ad un sistema distribuito. In quest'ultimo, infatti, i dati sono ridondati su diversi server decentralizzati. Ciò garantisce che, qualora la memoria di uno di questi dovesse essere danneggiata, il complesso di informazioni del sistema non venga intaccato. Al contrario, «fino a quando i dati restano salvati in database centralizzati rimarrà sempre la possibilità che vengano persi, cancellati»[47].

3.4) Monopolizzazione del mercato

La seconda problematica connessa al possesso dei dati da parte di soggetti centralizzati è una questione che ha a che fare con la regolamentazione del mercato. Come già accennato, molti degli odierni colossi del web sono nati da un settore di nicchia o, comunque, marginale. Facebook, ad esempio, si rivolgeva inizialmente solo agli studenti dei più importanti college americani; Google ha iniziato dal mercato delle ricerche online, che, ai tempi, era secondario; Amazon ha puntato sulla vendita di libri, un settore sicuramente più ridotto rispetto al campo d'azione raggiunto. Tutte queste aziende hanno preso piede nel proprio ambito di riferimento e successivamente hanno incrementato sempre più il proprio capitale di rischio per cercare di espandersi nel mercato generale, alla massima velocità[48]. Una simile crescita è stata resa possibile dall'enorme espansione e dal costante aggiornamento dell'infrastruttura del mondo digitale. Un altro fattore, inoltre, ha determinato il successo di queste attività: il già accennato *network effect*, l'effetto rete. L'esempio

---

[46] Data Center Knowledge, *Google Data Center FAQ*, in "DataCenter Knowledge", 17 marzo 2017 (https://www.datacenterknowledge.com/archives/2017/03/16/google-data-center-faq, consultato il 3 ottobre 2020).

[47] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 3442.

[48] *Cfr.* The Economist, *Everybody wants to rule the world*, in "The Economist", 27 novembre 2014 (https://www.economist.com/briefing/2014/11/27/everybody-wants-to-rule-the-world, consultato il 3 ottobre 2020).

perfetto di questo meccanismo è rappresentato da Facebook. Con la crescita dell'utenza del social network sono aumentate le persone con cui interagire all'interno della piattaforma, il che ha significato maggiori vantaggi dell'iscrizione, che, a loro volta, hanno attirato nuovi membri. Allo stesso modo, tutti gli altri web service che hanno conseguito un grande successo hanno fatto affidamento sull'effetto rete. Un meccanismo simile, inoltre, è quello del modello di business alla base dell'economia delle piattaforme. Quest'ultima consiste in attività economiche e sociali facilitate dallo strumento del *matchmaker* (piattaforma), concetto con cui ci si riferisce a contesti online per cui l'obiettivo principale non è la vendita di beni o servizi, ma, appunto, il collegamento di diversi gruppi di utenti[49]. Ad oggi, i colossi del web controllano il settore all'interno del quale si sono espansi grazie a tali meccanismi e di fatto «possiedono uno spazio»[50] nel mercato di Internet. Potranno nascere continuamente aspiranti concorrenti delle Big Tech, ma dovranno sempre confrontarsi con le capacità di dati e algoritmiche conquistate dai giganti del web. Come già affermato, si tratta di un vantaggio competitivo difficile da recuperare. Gli algoritmi di raccomandazione o di ricerca di Amazon, Facebook e Google sono costantemente alimentati e mantenuti aggiornati dall'enorme massa di dati accumulata. I colossi del web hanno a disposizione team di esperti e professionisti della *data analysis* in grado di incrementare sempre di più la rilevanza dei risultati di ricerca e degli annunci mostrati. Il *network effect* incentiva costantemente la crescita dell'utenza e quindi quella dei dati registrati. Anche se servizi concorrenti sono disponibili e facilmente accessibili nell'infosfera, gli utenti hanno sviluppato una dipendenza nei confronti dei web service offerti dalle Big Tech. Le persone hanno stabilito delle abitudini e una routine in riferimento a questi servizi, che per questo motivo diventano irrinunciabili[51]. Soprattutto se un dato *walled garden*, come Google ad esempio, aggiunge alla funzionalità iniziale (quella di motore di ricerca) sempre nuove *features* (la posta elettronica, le mappe…), gli utenti

[49] Cfr. Wikipedia, *Platform Economy*, in "Wikipedia", 26 novembre 2020 (https://en.wikipedia.org/wiki/Platform_economy#The_platform_business_model, consultato il 26 novembre 2020).

[50] *Ibid.*

[51] *Ibid.*

rimangono intrappolati in queste concentrazioni cedendo loro sempre più dati, prodotti proprio attraverso la fruizione di tutti i diversi servizi. Ad oggi non c'è quindi possibilità di competizione con i giganti del web che «possiedono enormi risorse economiche, la quasi totalità del traffico web e una potenza di calcolo pressoché illimitata»[52]. Da più parti si invoca l'esigenza di una regolamentazione del mercato dei dati monopolizzato dai colossi dell'hi-tech. Come ha detto John Sherman, il senatore che ha dato il suo nome alla legge antitrust originale americana: «Se non tolleriamo un re come potere politico, non dovremmo accettare un re per la produzione, il trasporto o la vendita di qualsiasi necessità della vita»[53]. Tuttavia, ad oggi il vantaggio dei Tech-Giants come Facebook o Google nella raccolta di dati sugli utenti si traduce in un monopolio del settore dei Big Data, in particolare per quanto riguarda i servizi di *targeting*. Come spiegato precedentemente, a differenza delle concentrazioni nei mercati tradizionali quali l'energia, i trasporti o le telecomunicazioni, nel caso dei web service non è possibile evocare il principio della concorrenzialità per limitare lo sviluppo di monopoli, perché le funzionalità offerte dalle piattaforme sono concesse gratuitamente[54]. Esperti e autorità di regolamentazione stanno da tempo cercando soluzioni per ridurre questa difficoltà.

3.5) Modello economico pubblicitario

Si è sottolineato più volte come il possesso dei dati degli utenti costituisca la base del modello economico delle piattaforme centralizzate. L'insieme delle attività di profilazione - la capacità di accumulare informazioni personali sugli utenti - e di *tracking* - il tracciamento delle attività di ciascuno sulla rete - rappresenta il *business core* dei web service accentrati. Tali funzioni, infatti, permettono alle piattaforme di «selezionare, per ogni messaggio, i destinatari più appropriati

---

[52] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 3442.

[53] *Cfr.* The Economist, *Everybody wants to rule the world*, in "The Economist", 27 novembre 2014 (https://www.economist.com/briefing/2014/11/27/everybody-wants-to-rule-the-world, consultato il 3 ottobre 2020).

[54] *Cfr.* Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, p. 46.

(*targeting*)»[55] e, soprattutto, di vendere tali informazioni agli inserzionisti pubblicitari. Ma il modello economico basato sull'*attention economy* inizia ad accusare i primi problemi[56]. I guadagni dei creatori di contenuti, come gli *youtuber* ad esempio, stanno man mano calando, probabilmente in conseguenza *dell'information overload*, il sovraccarico di informazioni. Citando il premio Nobel per l'economia, Herbert Simon: «L'informazione consuma attenzione. Quindi l'abbondanza di informazione genera una povertà di attenzione e induce il bisogno di allocare quell'attenzione efficientemente tra le molte fonti di informazione che la possono consumare»[57]. A guadagnare dalla monetizzazione dei dati sono quindi solo i fornitori dei servizi che traggono profitto dalle attività di targeting e non gli utenti stessi, né i creatori di contenuti. Tuttavia, è controproducente anche per le piattaforme che i propri fruitori siano meno stimolati a produrre materiali e informazioni. Inoltre, si è visto come il meccanismo dell'*attention economy* incentivi la creazione di contenuti polemici e provocatori, in quanto in grado di attirare maggiormente l'attenzione del pubblico. Ciò va a discapito della costruzione di conversazioni informative e divulgative di conoscenza. Tutti questi meccanismi sono favoriti dalla centralizzazione e dal *business core* basato sulla pubblicità. Al contrario, in un web service decentralizzato è possibile creare un modello economico che permetta la monetizzazione dei materiali prodotti dagli utenti, come incentivo alla creazione di contenuti di qualità.

3.6) I social network nel dibattito pubblico

Infine, c'è un'ultima questione che preoccupa le piattaforme centralizzate. Si è già parlato dell'importante ruolo di spazio di discorso pubblico ricoperto dai web service come Facebook. In ragione di questa funzione le piattaforme di social networking rappresentano oggi dei veri e propri attori sociali all'interno della scena

---

[55] *Ivi*, p. 42.

[56] *Cfr*. Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 3442.

[57] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

pubblica e politica. Recentemente, alcune particolari occasioni, quali l'uscita del Regno Unito dall'Unione Europea e l'elezione del presidente americano Trump, hanno evidenziato come i social network rappresentino oggi uno dei giocatori più importanti nel campo della politica odierna. In un contesto così sensibile preoccupa l'influenza sul dibattito online di attori digitali e automatizzati. Ciò che più spaventa, in particolare, è la difficoltà di misurare l'impatto che le reti sociali online possono avere sull'opinione pubblica. Si è già accennato più volte, infatti, a come i social network centralizzati tendano ad incentivare la proliferazione di contenuti polemici, la disinformazione e la polarizzazione. Nel terzo capitolo di questo elaborato, in particolare, verrà approfondita la visione drammatica di questo tema data da un documentario recentemente distribuito da Netflix, *The Social Dilemma*. Tuttavia, in questa sede è sufficiente che sia chiaro come la partecipazione dei social network al dibattito pubblico rappresenti un pericolo.

La caratteristica di automazione di tali web service comporta, inoltre, un'altra preoccupazione. Come sostenuto da Emily Taylor, amministratore delegato di Oxford Information Labs e redattore del *Journal of Cyber Policy*: «Oggi noi esistiamo in questi ambienti curati, dove non vediamo mai nulla al di fuori della nostra bolla e non ci rendiamo conto di quanto siano curati»[58]. Il riferimento ovviamente è alle piattaforme centralizzate e ai servizi offerti dalle stesse, puntualmente targettizzati e personalizzati per il profilo di un dato utente. Gli algoritmi alla base di questi web service, infatti, sono programmati per identificare le preferenze di ogni individuo e fornirgli contenuti che le soddisfino. In questo modo, «creano un universo di informazioni specifico per ciascuno di noi, una "bolla dei filtri", che altera il modo in cui entriamo in contatto con le idee e le informazioni»[59]. È intuitivo come questi meccanismi possano rappresentare un pericolo per lo sviluppo dell'opinione personale e della conoscenza degli individui. Il fatto che attraverso gli algoritmi gli utenti siano esposti a contenuti che rispecchiano ciò che già

[58] Alex Hern, *How social media filter bubbles and algorithms influence the election*, in "The Guardian", 22 maggio 2017 (https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles, consultato il 10 ottobre 2020).

[59] Eli Pariser, *Il Filtro*, Milano, il Saggiatore S.p.A., 2012, pp. 14-15.

conoscono e preferiscono implica che la cosiddetta "bolla dei filtri" non mostri informazioni che contrastino con il corpo di conoscenze di un dato soggetto. Tuttavia, come spiega Siva Vaidhyanathan nel suo libro *La googlizzazione di ogni cosa*, apprendere implica di per sé l'incontro con qualcosa di sconosciuto o che non si ha mai concepito o, addirittura, con qualcosa che non si sarebbe mai ritenuto possibile[60]. Mentre ciò a cui la bolla espone gli utenti è un ignoto vicino, che non mette in discussione le credenze di una persona, ma soddisfa la sua necessità di apprendere nuove informazioni.

Infine, un ultimo timore connesso alla partecipazione dei social network al dibattito pubblico è suscitato dalla capacità degli algoritmi di tali web service di riprodurre i *bias* sociali e culturali incorporati nella base di dati che implementa l'algoritmo stesso. Per spiegare quest'affermazione si procederà con un esempio descritto da Hannah Fry nel libro *Hello World: Essere umani nell'era delle macchine.* Si immagini di utilizzare un algoritmo che individui il rischio che una persona possa commettere un omicidio. Poiché secondo i dati utilizzati da Hannah Fry il 96% degli assassini sono maschi, il meccanismo potrà essere ritenuto accurato solo se i soggetti identificati come ad alto rischio saranno per la maggior parte di sesso maschile. Supponendo che l'algoritmo in questione abbia una precisione del 75%, si avrà che tre quarti degli individui che risulteranno ad alto rischio lo saranno realmente. Su un campione di 100 persone classificate come potenziali assassini risulterà che 96 di queste saranno di sesso maschile e 4 di sesso femminile in base alle statistiche. Data la percentuale di precisione dell'algoritmo, si avrà che un quarto degli uomini (24) e un quarto delle donne (1) saranno individui classificati erroneamente come potenziali omicidi. La differenza fra i valori assoluti 24 e 1 non significa che la percentuale di errore sia maggiore per i maschi e minore per le femmine, ma consegue semplicemente dal fatto che statisticamente gli uomini commettono più omicidi delle donne. Inoltre, il risultato non è dovuto alla caratteristica in esame (il rischio di commettere omicidi), né all'algoritmo: «è solo una

[60] *Ivi*, p. 75.

certezza matematica. Il risultato è squilibrato perché lo è la realtà»[61]. Gli algoritmi di *machine learning* come quelli alla base dei social network, infatti, implicano una base di dati che li alimenti. Ma queste informazioni riflettono la realtà a cui si riferiscono e ne incorporano *bias* e pregiudizi. Di conseguenza gli algoritmi ereditano le distorsioni di un dato contesto e le replicano: descrivono il presente o ipotizzano il futuro sulla base del passato.

4) La proposta di un ritorno ad una logica dei protocolli

È giunto il momento di tirare le fila di questo primo capitolo. L'infosfera odierna appare monopolizzata da un ridotto numero di web service strutturati in piattaforme centralizzate. Si è accennato al fatto che tale realtà debba oggi affrontare una serie di difficoltà per le quali si invoca da più parti il ritorno ad una rete libera, aperta e decentralizzata secondo il progetto originario del World Wide Web di Tim Berners Lee. Si è quindi risaliti alla nascita di quell'applicazione che, ad oggi, permette a miliardi di persone di accedere e consultare i contenuti online: il web, appunto. Seguendo lo sviluppo storico dei fatti si è notato come, dal progetto originario di un'infosfera accessibile a tutti, senza vincoli e distribuita, si sia gradualmente passati ad un contesto centralizzato e monopolizzato da un ristretto numero di soggetti a capo di determinate piattaforme. Particolare attenzione è stata posta ai servizi di social networking, in relazione ai quali si è evidenziato come i vantaggi offerti dalla centralizzazione abbiano portato alla nascita di un web strutturato in enormi bacini di utenza racchiusi all'interno di giardini murati. Questi ultimi "intrappolano" gli utenti rendendoli dipendenti dai servizi offerti grazie alla proprietà esclusiva dei loro dati. Dopo aver quindi chiarito come la centralizzazione abbia - finora - vinto sulla logica decentralizzata, si sono introdotte le difficoltà che negli ultimi anni sono sorte in relazione a tale struttura.

Riassumendo, le problematicità che le piattaforme centralizzate si trovano oggi ad affrontare sono: la *data protection* e la garanzia del diritto alla privacy

[61] Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, pp. 27-28.

degli utenti; la ricerca di un compromesso fra la necessità di moderazione del discorso online e la libertà di espressione; una struttura tecnica che mette in pericolo la persistenza dei dati degli utenti; le criticità della monopolizzazione del mercato dei dati e dell'attenzione; il sorgere di problemi per il modello economico basato sulla pubblicità; infine, i timori per l'influenza delle piattaforme di social networking nel dibattito pubblico e, in particolare, nella scena politica.

Di fronte a tale scenario, esperti, professionisti del settore e autorità di regolamentazione si stanno interrogando su come intervenire per arginare e/o risolvere le questioni elencate. È opportuno sottolineare come le problematiche introdotte non siano le uniche vigenti, quanto le più importanti e interessanti per questo elaborato. Come ripetuto più volte, in risposta a tali difficoltà è stato proposto da diverse voci il ritorno alla logica decentralizzata e basata su protocolli del progetto originario del web pensato da Tim Berners Lee. Ha riscosso particolare attenzione l'interesse mostrato per tale alternativa dal fondatore e CEO di Twitter Jack Dorsey. L'11 dicembre 2019 l'informatico statunitense ha infatti annunciato l'istituzione di Bluesky, un team di ricerca indipendente finalizzato allo sviluppo di un protocollo aperto e decentralizzato per i social media. Dorsey ha anche rivelato l'obiettivo per Twitter di diventare *client* di questo eventuale standard[62].

Figura 2: L'annuncio di Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).

Con una successione di *tweet* Jack Dorsey ha in seguito spiegato le principali motivazioni di tale interesse e ha rivelato di essere stato ispirato dal saggio di Mike

[62] Cfr. Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).

Masnick *Protocols, Not Platforms: A Technological Approach to Free Speech*[63]. In quest'ultimo il fondatore di Techdirt descrive il progetto di una struttura per il social networking basata su protocolli e illustra come tale configurazione potrebbe contribuire alla risoluzione delle difficoltà affrontate dalle piattaforme centralizzate. Tuttavia, prima di approfondire tale prospettiva, si vuole in questa sede introdurre lo scenario generale di un Internet decentralizzato e spiegarne i meccanismi.

4.1) Il ritorno ad un futuro decentralizzato

Nel giugno 2016 Internet Archive, storica biblioteca digitale della conoscenza online, ospita nella sua sede a San Francisco il primo vertice Web Decentralizzato, fra un gruppo di appassionati, archivisti, giornalisti e politici[64]. In tale contesto Brewster Kahle, fondatore dell'importante archivio digitale, annuncia il suo progetto: «Locking the Web Open»[65]. Con queste parole l'informatico statunitense invita quel primo gruppo di sviluppatori a condividere la sua prospettiva futura per un web decentralizzato. Il desiderio di Kahle è quello di ristrutturare il web in modo che continui a garantire ciò che gli utenti chiedono e si aspettano da un simile strumento comunicativo ed espressivo, senza tuttavia compromettere la sua inclusività. Secondo Kahle ciò dev'essere fatto incorporando nella codifica stessa del web i valori che si vuole vengano implementati. Tali principi imprescindibili, secondo l'informatico statunitense, sono la libertà di espressione, la privacy e l'accesso universale alla conoscenza. La necessità di ristrutturazione, secondo Kahle, è dovuta al fatto che tali valori non fanno al momento parte dell'essenza stessa del web. Innanzitutto, il web non è ugualmente accessibile in tutto il mondo, spiega l'informatico, argomentando che in Cina, ad esempio, l'accesso ad Internet

[63] Mike Masnick, op. cit., in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[64] *Cfr.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[65] Brewster Kahle, *Locking the Web Open: A Call for a Decentralized Web*, in "Brewster Kahle's Blog", 11 agosto 2015 (http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/, consultato il 20 agosto 2020).

Archive e ad altri siti è bloccato ai cittadini. Il web, inoltre, non garantisce la privacy e, al contrario, permette potenzialmente a chiunque di entrare in possesso dei dati personali degli utenti e consente persino lo spionaggio[66].

Le difficoltà individuate da Kahle rispecchiano quindi quelle esaminate in questo elaborato. Allo stesso modo, i principi ritenuti fondamentali dal fondatore di Internet Archive riecheggiano i diritti e le necessità degli utenti che si è detto non essere garantiti dal sistema delle piattaforme centralizzate. Tuttavia, secondo Kahle c'è una caratteristica importante che, nella ristrutturazione del web, è fondamentale conservare: il divertimento. Il web è così facile da usare e stimolante, spiega l'informatico, che milioni di persone sono portate a condividervi incessantemente contenuti interessanti. Gli utenti costruiscono una rappresentazione delle proprie vite online. Nuove caratteristiche e funzionalità vengono costantemente introdotte grazie al fatto che il web permette di sviluppare liberamente implementazioni sulla sua struttura. «Tutto sommato», sottolinea Kahle, «l'apertura del web ha portato alla partecipazione di molti»[67]. Secondo il fondatore di Internet Archive è possibile costruire un web sicuro, rispettoso della privacy e allo stesso tempo divertente. Per fare ciò bisogna realizzare un web decentralizzato e distribuito.

4.2) Gli elementi costitutivi di un web decentralizzato

È importante, innanzitutto, chiarire la differenza fra due termini: decentralizzato e distribuito. Un sistema decentralizzato è una particolare configurazione di uno distribuito. Un esempio di quest'ultimo è rappresentato da Internet. La struttura della rete delle reti è tale che, qualora uno dei nodi che la compone dovesse venire meno, il funzionamento sarebbe comunque garantito facendo affidamento alle parti operative del sistema. Ciò è permesso grazie alla struttura distribuita, la quale prevede la distribuzione e la condivisione dell'elaborazione fra più nodi. Un sistema decentralizzato si affida ad un'architettura distribuita e, in aggiunta, i nodi che lo compongono spartiscono anche il potere decisionale e la custodia delle

[66] *Ibid.*
[67] *Ibid.*

informazioni. Un sistema non decentralizzato può essere comunque distribuito, ma avere un unico punto che prende le decisioni e ne è responsabile[68]. Come già accennato, infatti, le grandi piattaforme centralizzate odierne fanno affidamento ad un'architettura distribuita per questioni di scalabilità.

Molte delle pagine che compongono il web non sono distribuite. Nella maggior parte dei casi, infatti, i dati di un sito sono memorizzati in un unico luogo fisico. Perciò, se l'hardware di tale nodo dovesse smettere di funzionare, il sito non sarebbe più visibile. In questo senso il web è centralizzato: se un unico soggetto controlla l'hardware di un sito o la linea di accesso a tale sito, allora ne ha l'autorità/potere esclusiva di tutti gli utilizzi.

Sorge spontaneo l'interrogativo, quindi, di come dovrebbe strutturarsi un web distribuito e decentralizzato. Sono tre gli elementi fondamentali di tale progetto: software *open-source*, protocolli comunicativi e database condivisi. Questi blocchi costitutivi non sono tecnologie nuove; al contrario, esistono già e sono ampiamente impiegate da programmi e applicazioni centrali nelle vite quotidiane delle persone e in particolare in alcuni settori, come quello economico. Innanzitutto, i software *open-source* sono applicativi che possono essere letti, copiati, modificati o condivisi da chiunque, senza necessità di autorizzazione da parte del soggetto proprietario. WordPress, ad esempio, la nota piattaforma di blog e *content management system* che alimenta il 30% dei siti web[69], è un software *open-source* «progettato per tutti, con particolare attenzione all'accessibilità, alle prestazioni, alla sicurezza e alla facilità d'uso»[70]. Al contrario, i programmi delle grandi piattaforme centralizzate sono segreti e controllati dai soggetti proprietari. Per questo motivo, ad esempio, è difficile misurare l'influenza dei social network all'interno del dibattito pubblico e politico, perché i meccanismi di funzionamento degli

---

[68] *Cfr*. MaRi Eagar, *What is the difference between decentralized and distributed systems?*, in "Econova", 4 novembre 2017 (https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462, consultato il 20 aprile 2020).

[69] Cfr. Marvin Ammori, *The Coming Decentralized Decade*, in "Morning Consult", 6 gennaio 2020 (https://morningconsult.com/opinions/the-coming-decentralized-decade/, consultato il 14 giugno 2020).

[70] Cfr. WordPress, *Democratize Publishing*, in "WordPress.org" (https://wordpress.org/about/, consultato il 15 ottobre 2020).

algoritmi di personalizzazione dei contenuti e dei messaggi pubblicitari e propagandistici sono sconosciuti[71].

In secondo luogo, i protocolli sono i linguaggi di comunicazione fra computer e stabiliscono «il formato e l'ordine dei messaggi scambiati tra due o più entità»[72]. La possibilità di condividere informazioni fra calcolatori diversi permette di aumentare esponenzialmente le capacità di un singolo elaboratore. Il protocollo più noto è il cosiddetto "IP", l'Internet Protocol, lo standard che permette a milioni di computer di comunicare fra loro attraverso un linguaggio comune. Tim Berners Lee ha sviluppato i protocolli alla base del web, come l'HTTP (Hypertext transfer protocol), dedicato al trasferimento dati in formato ipertestuale, e l'HTML (Hypertext markup language), il linguaggio per la codifica degli ipertesti.

Infine, la tecnologia più recente fra quelli che si è visto essere gli elementi fondamentali per il progetto di un web decentralizzato è rappresentata dalla blockchain. Chi ha familiarità con questo termine ne è probabilmente venuto a conoscenza nel contesto delle criptovalute. La blockchain, infatti, è il database distribuito impiegato per conservare il libro mastro delle transazioni in Bitcoin, la più nota criptovaluta. La blockchain sviluppata da Satoshi Nakamoto, pseudonimo dell'ignoto inventore del Bitcoin, e le altre tecnologie simili costituiscono dei registri di tutte le transazioni di criptovalute che avvengono all'interno di una rete di nodi e tale database, strutturato a blocchi, è condiviso e validato dalla rete stessa[73]. Inoltre, anche l'aggiornamento del registro è un processo collettivo affidato al gruppo di nodi. La differenza con le piattaforme centralizzate è che queste ultime conservano i dati in grandi database accentrati, mentre con la tecnologia della blockchain viene meno la necessità di fare affidamento ad un'autorità centrale. In questo modo si risolve un problema fondamentale del contesto centralizzato,

---

[71] Alex Hern, *How social media filter bubbles and algorithms influence the election*, in "The Guardian", 22 maggio 2017 (https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles, consultato il 10 ottobre 2020).

[72] *V.* James F. Kurose, Keith W. Ross, *Reti di calcolatori e Internet*, 7a ed., Milano-Torino, Pearson Italia, 2017, p. 8.

[73] *Cfr.* Roberto Garavaglia, *Tutto su Blockchain*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2018, posizione 1191.

quello della fiducia. Nel sistema della blockchain «la fiducia non dipende da nessuna istituzione o dalle intenzioni di nessun particolare attore coinvolto. In una blockchain non è necessario fidarsi di nessuno, ma allo stesso tempo si può essere sicuri che le transazioni verranno elaborate correttamente senza alcuna manomissione o censura»[74]. Con le piattaforme centralizzate, invece, è l'autorità centrale ad avere il controllo e a poter intervenire sulle informazioni conservate, ad esempio «con determinazioni di immediata efficacia come il blocco di un utente o la censura di determinate tipologie di contenuti»[75]. Il meccanismo della validazione collettiva delle transazioni nella blockchain garantisce, quindi, anche l'immutabilità delle informazioni salvate. Questi e gli altri vantaggi della tecnologia della blockchain verranno approfonditi nel secondo capitolo, che sarà dedicato all'infrastruttura tecnica necessaria per la realizzazione di piattaforme di social networking decentralizzate.

Riprendendo il progetto di Brewster Kahle, secondo il fondatore di Internet Archive vi sono alcuni altri elementi che contribuirebbero a tale prospettiva. Il web decentralizzato sarebbe innanzitutto basato su un'architettura peer-to-peer, che, come visto in precedenza, è un sistema che non dipende da un host centrale. In questo modello i nodi facenti parte della rete contribuirebbero fornendo larghezza di banda e spazio di archiviazione per il sistema. Ogni singolo sito sarebbe memorizzato su più server, quindi, al crescere del numero di nodi componenti la rete, aumenterebbero la ridondanza, la sicurezza e la velocità della struttura. Per soddisfare la necessità di privacy interverrebbero due meccanismi. Innanzitutto, la distribuzione dei bit attraverso la rete permetterebbe di ostacolare considerevolmente il tracciamento del fruitore di un dato sito connesso da un unico punto o collegamento. Inoltre, nel web immaginato da Khale sarebbe possibile realizzare un

[74] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 1582.

[75] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

sistema distribuito di autenticazione, senza ricorrere a un database centralizzato di username e password[76].

Il fondatore di Internet Archive, infine, prospetta anche la possibilità di introdurre nuove funzionalità nel web decentralizzato. Khale propone innanzitutto di registrare le informazioni del web nel tempo, ovvero creare una memoria storica delle varie evoluzioni dei contenuti digitali nei siti web. Ciò sarebbe possibile attraverso il "versioning", il controllo delle versioni multiple di un insieme di informazioni. In questo modo si garantirebbe uno storico e l'affidabilità del crescente patrimonio digitale[77]. Inoltre, potrebbero essere introdotti dei semplici meccanismi a disposizione dei lettori per pagare gli autori dei contenuti. Questo permetterebbe lo sviluppo di modelli di business ulteriori rispetto a quello basato sulla pubblicità e sul mercato di dati personali. La decentralizzazione, infine, contribuirebbe ad aumentare quel divertimento che per Kahle è un tratto distintivo ed essenziale del web. L'assenza di un soggetto proprietario dei software che azionano i diversi web service creerebbe un sistema stimolante per lo sviluppo di innovazioni, una piattaforma tecnologica che ognuno può implementare e modificare senza dover avere il permesso di alcuna autorità[78]. Inoltre, i costi di innovazione sarebbero enormemente ridotti grazie alla possibilità per gli sviluppatori di interagire con gli strumenti *open-source* e aggiungere funzionalità ai vari sistemi, senza dover ricostruire l'intera esperienza di un dato web service[79].

Come sostiene Marvin Ammori, dirigente di Protocol Labs, azienda focalizzata sul miglioramento di Internet e dell'elaborazione di dati in generale attraverso protocolli web decentralizzati:

> Internet fa ciò che sa fare meglio quando funge da forza democratizzante, abbattendo le barriere e unendoci in nuovi modi. Considerando i suoi recenti usi oscuri nelle elezioni e

[76] Brewster Kahle, *Locking the Web Open: A Call for a Decentralized Web*, in "Brewster Kahle's Blog", 11 agosto 2015 (http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/, consultato il 20 agosto 2020).

[77] *Ibid.*

[78] *Ibid.*

[79] V. Cfr. Marvin Ammori, *The Coming Decentralized Decade*, in "Morning Consult", 6 gennaio 2020 (https://morningconsult.com/opinions/the-coming-decentralized-decade/, consultato il 14 giugno 2020).

la sua tendenza a fomentare rabbia e divisioni, spetta a noi oggi ripensare al modo in cui facciamo rete, siamo coinvolti online e rivendichiamo i nostri dati. E inizia con la decentralizzazione[80].

5) Social network su protocollo decentralizzato

Da un primo sguardo alla prospettiva di un web decentralizzato si è già intuito che un simile progetto potrebbe apportare diversi benefici all'infosfera, contribuendo a risolvere le difficoltà affrontate dalle piattaforme centralizzate. In questo paragrafo si procederà, quindi, ad introdurre quali sono i vantaggi che la decentralizzazione produrrebbe per un particolare tipo di web service: i social network.

Un social network si definisce come «una piattaforma online che:

a. fornisce servizi agli utenti per costruire un profilo più o meno pubblico e per dichiarare esplicitamente la connessione tra il proprio profilo e quello degli altri utenti;
b. consente a un utente di condividere informazioni e contenuti con utenti scelti o con il pubblico generale;
c. supporta lo sviluppo e l'utilizzo di applicazioni sociali con le quali l'utente può interagire e collaborare con amici e sconosciuti»[81].

Gli attuali social network più popolari sono centralizzati, il che, come si è visto, implica l'esistenza di un'autorità centrale che ha il controllo sui dati personali degli utenti, sui software che implementano la piattaforma, la responsabilità della moderazione del discorso interno alla rete e che ricava profitti da un modello economico prevalentemente pubblicitario. Come discusso nel secondo paragrafo di questo primo capitolo, l'affermazione dei social network centralizzati a discapito di quelli decentralizzati è dovuta ad una serie di difficoltà del modello basato su protocolli che, in un primo momento storico, hanno favorito l'ascesa delle piattaforme *closed*. Tuttavia, l'enorme crescita affrontata da tali web service ha prodotto nel

[80] *Ibid.*

[81] Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 349.

tempo diverse conseguenze e complicazioni che i social network centralizzati si trovano oggi ad affrontare. E la soluzione a questi problemi sembra riproporre proprio il ritorno a quell'architettura decentralizzata del web delle origini, resa ad oggi più favorevole grazie all'introduzione di nuove tecnologie.

5.1) L'architettura di un DOSN

Un social network decentralizzato è «una rete sociale online implementata su una piattaforma distribuita. In un DOSN (Decentralized Online Social Network) non esiste un unico fornitore di servizi, ma un insieme di nodi che cooperano per garantire tutte le funzionalità offerte da un OSN centralizzato»[82]. Come si è visto per il progetto generale di un web decentralizzato, vi sono alcune tecnologie chiave per lo sviluppo di un servizio di social networking basato su protocolli. Innanzitutto, come da definizione, un DOSN implica l'implementazione su una piattaforma distribuita, che può essere costituita da una rete di server fidati, da un sistema peer-to-peer o da un network opportunistico. Le differenze fra queste tecnologie non sono interessanti al fine di questo elaborato, pertanto si rimanda alla definizione di architettura peer-to-peer, vista in precedenza, come generale illustrazione degli altri modelli nominati. Inoltre, mentre un social network centralizzato si presenta come un'interfaccia costruita per mostrare i contenuti immagazzinati in un database accentrato, un DOSN fa affidamento ad un database distribuito, come quello implementato dalla tecnologia blockchain, a cui già si ha accennato. Protocolli open-source provvedono, in aggiunta, a far interagire fra loro i nodi.

Per quanto riguarda alcune funzionalità specifiche dei social network, come la possibilità di reagire ad un post o a un'immagine, il monitoraggio delle relazioni fra gli utenti e la raccomandazione dei contenuti, la decentralizzazione pone alcune sfide. Tuttavia, la soluzione non sembra essere impraticabile. Guido Vetere,

[82] Barbara Guidi, Marco Conti, Andrea Passarella, Laura Ricci, *Managing social contents in Decentralized Online Social Networks: A survey*, in "Online Social Networks and Media", 7 (2018), pp. 12-29.

docente di Intelligenza Artificiale presso l'Università degli Studi Guglielmo Marconi di Roma, illustra alcune possibili alternative.

Nel caso delle piattaforme di social networking centralizzate, la reazione che un utente può apporre ad un contenuto, come un post o un'immagine, si concretizza in una traccia (record[83]) registrata in un database. Pertanto, i calcoli applicati per stabilire con chi un utente interagisce di più non sono altro che delle interrogazioni, delle *query*, eseguite fra le tracce salvate. Nel caso di un social network decentralizzato, invece, i record lasciati dagli utenti sono distribuiti fra i vari nodi della rete e, allo stesso modo, deve essere distribuita la *query*. Dal punto di vista teorico, spiega Vetere, la questione non pone ostacoli insormontabili. Tuttavia, nella pratica, potrebbero manifestarsi alcuni problemi tecnici, «come impredicibili latenze o fallimento di singoli nodi, e richiederebbero accorgimenti implementativi non banali»[84]. Un'interessante possibilità in questo senso è offerta dalla tecnologia della blockchain. Il meccanismo dei registri distribuiti che la implementano, infatti, può essere applicato al *tracking* e alla durevolezza delle interazioni nella rete. Si è già accennato al funzionamento del database distribuito, replicato e collaborativamente validato della blockchain e si procederà ad approfondire i dettagli della questione nel secondo capitolo di questo elaborato. Ciò che è interessante al fine di questo contesto è che, come con i Bitcoin si affida il tracciamento delle transizioni ad un livello separato e autonomo rispetto a quello di ciascun nodo, cioè alla comunità di nodi che partecipano alla rete, così, per il *tracking* delle interazioni fra gli utenti, grazie alla distribuzione del registro, si ottiene la persistenza dei dati[85].

Per quanto riguarda, invece, i meccanismi di raccomandazione, ci si riferisce a quella funzionalità dei social network che consiste nel proporre i contenuti

---

[83] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

[84] Donald Kossmann, *The State of the Art in Distributed Query Processing*, in Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

[85] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

prodotti dagli utenti di una comunità a profili affini o che potrebbero trovare interessante quel materiale. Le piattaforme decentralizzate oggi esistenti, invece, offrono una presentazione dei contenuti cronologica ed integrale. Tale processo non sembra essere dovuto direttamente alla struttura distribuita di tali social network, quanto piuttosto all'onerosità computazionale delle operazioni necessarie per «la selezione dei contenuti e l'ordinamento della *timeline*»[86]. Come spiega Guido Vetere, si tratta di costo sostenibile in relazione ad un proporzionale ritorno. Si è già discusso, infatti, come la possibilità per una piattaforma di offrire servizi e funzionalità ottimali e sempre aggiornati sia strettamente legata alla capacità di ricavarne profitto. La sfida per i social network decentralizzati è quindi quella di individuare il giusto bilanciamento fra i servizi proposti e gli oneri necessari.

La proposta di Guido Vetere per le piattaforme decentralizzate è quella di distaccarsi dai modelli di business basati sulla profilazione degli utenti, la raccomandazione di contenuti e messaggi pubblicitari personalizzati e il mercato dei dati. Il punto di forza della decentralizzazione, secondo Vetere, è la possibilità di stimolare la creatività e di instaurare un rapporto di collaborazione e fiducia con l'utente. Ciò contribuirebbe al miglioramento della qualità dell'esperienza e dei contenuti nell'infosfera[87].

5.2) I benefici della decentralizzazione per i servizi di social networking

Si è quindi visto come, dall'iniziale vantaggio delle piattaforme centralizzate su quelle decentralizzate, si sia ora passati alla proposta di un ritorno ad una logica dei protocolli. Si è poi introdotto cosa significhi tecnicamente la decentralizzazione e come possa essere applicata ai servizi di social networking. Infine, in questo sotto-paragrafo si procederà a tratteggiare quali sono, effettivamente, i benefici che una struttura decentralizzata può portare alle piattaforme di network sociale.

Innanzitutto, dal punto di vista tecnico la decentralizzazione apporta diversi vantaggi. Un'architettura basata su protocolli, che prevede la distribuzione dei dati

[86] *Ibid.*
[87] *Ibid.*

e del carico computazionale attraverso una rete di nodi, comporta, come si è già accennato, che non esista un «single point of failure»[88], un unico punto di errore che, se compromesso, determina il fallimento dell'intero sistema. Al contrario, per un social network avere una struttura interamente distribuita, sostenuta da una tecnologia come quella della blockchain, implica che, in caso di fallimento di un nodo, il lavoro di elaborazione venga distribuito fra le restanti parti operative della rete. Inoltre, la ridondanza delle informazioni memorizzate su diversi server del network fa sì che sia maggiormente garantita la persistenza dei dati. Un'architettura distribuita comporta anche una più elevata scalabilità, dal momento che la potenza e le risorse a disposizione della rete aumentano al crescere della base di utenti[89]. Infine, per una piattaforma centralizzata un aumento di popolarità comporta sì un incremento dei ricavi, ma, allo stesso tempo, anche la crescita dei costi di gestione e manutenzione dell'infrastruttura per garantire una performance costante. Con la decentralizzazione, invece, non c'è un unico fornitore del servizio che deve farsi carico di ciò, ma una rete di nodi che vi contribuisce.

Come si è più volte affermato, un social network decentralizzato è particolarmente favorito rispetto ad uno centralizzato per quanto riguarda la questione della privacy. Da un lato, infatti, l'assenza di un soggetto centrale implica che non vi sia una raccolta accentrata dei dati e che gli incentivi economici per la pubblicità siano ridotti; dall'altra, inoltre, la decentralizzazione fa sì che manchi un'autorità che decida o cambi a piacimento i termini della privacy. Per accedere ad un social network decentralizzato, infatti, un utente sceglie un server di fiducia che "ospiti" i suoi dati[90]. All'interno del sistema, quindi, le informazioni risiedono su diversi server indipendenti connessi fra loro e fra i quali le trasmissioni di dati avvengono

[88] Barbara Guidi, *When Blockchain meets Online Social Networks*, in "Pervasive and Mobile Computing", 62 (2020).

[89] *V.* Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 357.

[90] *Cfr. V.* Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, Tim Berners-Lee, *Decentralization: The future of online social networking*, in *W3C Workshop on the Future of Social Networking Position Papers*, vol. II, gennaio 2009, pp. 2-7.

secondo il meccanismo del consenso e della validazione collettiva[91]. Ogni utente, pertanto, è in possesso e ha il controllo dei propri dati personali, i quali rimangono al sicuro anche nel momento della condivisione delle informazioni, la quale avviene solo previa autorizzazione esplicita dell'utente autenticato e mediante sistemi di criptazione a chiave pubblica e privata (si avrà modo di specificare questi meccanismi nel prossimo capitolo). La crittografia, infatti, permette contemporaneamente di rendere sicure le comunicazioni e di poterle "firmare" per ostacolare la contraffazione[92]. Tutto ciò fa sì che l'utente possa decidere con chi condividere i suoi dati e, soprattutto, con quali restrizioni. In aggiunta, il controllo personale sulle proprie informazioni contrasta anche il *data mining*[93] - l'estrazione massiccia dei dati - e il generale mercato dei dati, assicurando all'individuo online di una maggiore conoscenza di come e da chi le proprie informazioni vengano utilizzate.

L'assenza di un'autorità centrale apporta benefici anche dal punto di vista della libertà di espressione. È intuitivo, infatti, come in un contesto decentralizzato, in cui la responsabilità spetta all'utente stesso o, al massimo, è collettivamente esercitata, venga a mancare quel controllo sui contenuti esercitato dai *provider* di servizi centralizzati. Ciò permette di evitare la censura o l'imposizione di costrizioni da parte del soggetto autorevole[94]. In questo modo viene meno anche la difficoltà di dover trovare un compromesso tra la necessità di moderazione del discorso online e la rivendicazione della libera espressione. Ciò non significa che un social network decentralizzato sia terra fertile per il libero e incondizionato sviluppo di comportamenti abusivi. Un sistema basato su protocolli, invece, sposta semplicemente il processo decisionale in merito a ciò che può essere considerato abusivo o meno ai terminali della rete, piuttosto che affidarlo ad un'entità centrale,

---

[91] *Cfr.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[92] *Cfr.* Brewster Kahle, *Locking the Web Open: A Call for a Decentralized Web*, in "Brewster Kahle's Blog", 11 agosto 2015 (http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/, consultato il 20 agosto 2020).

[93] Cfr. Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 357.

[94] *Ibid.*

con i relativi bias e condizionamenti. In questo modo, in un contesto decentralizzato, ognuno è in grado e ha il potere di decidere a quali contenuti essere esposto e quali invece considera offensivi o illeciti[95]. Ciò è permesso dalla possibilità di scegliere fra una moltitudine di interfacce e servizi diversi tramite cui accedere ai contenuti del database distribuito.

In un contesto decentralizzato, spiega Mike Masnick nel suo già citato *Protocols, Not Platforms: A Technological Approach to Free Speech*, si può avere un protocollo specifico per ogni tipo di piattaforma oggi esistente, ad esempio quelle di social networking. Per implementare poi un singolo protocollo possono essere sviluppate infinite interfacce fra loro concorrenti, permettendo così ad ogni utente di scegliere quella preferisce. In questo senso, un sistema basato su protocolli rappresenta di per sé un contesto fertile per l'innovazione. Non vi è un soggetto centrale che definisce e offre tutte le funzionalità di una piattaforma. Al contrario, ognuno è libero di progettare nuovi servizi, *tool*, filtri, applicazioni e molto altro per migliorare l'esperienza online. Come si è già detto, inoltre, la decentralizzazione comporta un'ingente riduzione dei costi per la modifica, l'aggiornamento e l'implementazione del sistema. La possibilità per gli utenti di scegliere fra software concorrenti per accedere al corpus generale di contenuti comporta, in aggiunta, un aumento della competizione. Di conseguenza, gli sviluppatori sono stimolati ad implementare servizi sempre migliori e aggiornati per guadagnarsi la predilezione degli utenti[96].

Un ulteriore beneficio apportato dalla decentralizzazione è rappresentato dalla possibilità di introdurre dei modelli di business diversi da quello pubblicitario. Quest'ultimo, infatti, comporta la proprietà dei dati degli utenti e un'architettura che agevoli gli algoritmi di profilazione e targetizzazione. Come si è visto dall'analisi della questione di Guido Vetere, tali processi incontrano alcuni ostacoli nel contesto decentralizzato. Quest'ultimo, invece, potrebbe e dovrebbe

[95] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[96] *Ibid.*

incentivare modelli di business che valorizzino la creatività degli utenti e la collaborazione al fine miglioramento del sistema. Come già accennato, uno dei problemi delle prime piattaforme basate su protocolli era proprio la difficoltà nell'implementare un modello di business che garantisse sufficienti ricavi. In un primo momento hanno pertanto prevalso i servizi centralizzati. Tuttavia, ad oggi, lo sviluppo di nuove tecnologie sembra offrire la possibilità di sperimentare nuovi e diversi *business model* profittevoli anche in un sistema basato su protocolli. La decentralizzazione, inoltre, favorirebbe un incremento della competizione in quest'ambito, portando man mano al perfezionamento di modelli di business adeguati al contesto[97].

Vi è in particolare un meccanismo che potrebbe contribuire a rendere sostenibile e più allettante il sistema decentralizzato. I recenti sviluppi nel settore delle valute virtuali hanno reso teoricamente possibile costruire un protocollo che utilizzi una criptovaluta o un token (letteralmente "gettone") a cui è associato un valore che aumenta al crescere dell'utilizzo di tali *item*. Ciò rappresenta un notevole incentivo all'utilizzo di un dato protocollo al fine di incrementare il valore della moneta associata. Alcuni progetti ipotizzano anche la possibilità di trattenere una percentuale della valuta di riferimento a favore di un'organizzazione responsabile del protocollo, che si occupi, grazie a tale risorsa, di finanziare la manutenzione e il funzionamento del sistema. Criptovalute e token potrebbero fungere, in aggiunta, da stimolo per lo sviluppo di interfacce, *tool*, filtri e software vari per l'implementazione del protocollo. Infine, anche i creatori di contenuti potrebbero beneficiare di un simile sistema di incentivi. Ad esempio, si potrebbe costruire un'architettura che ricompensi gli utenti per la produzione di materiali valevoli, riconosciuti dal resto della rete[98]. Un simile meccanismo favorirebbe il miglioramento della qualità dei contenuti, contribuendo ad affrontare il problema delle fake news, della disinformazione, dei comportamenti abusivi.

---

[97] *Ibid.*
[98] *Ibid.*

Infine, la decentralizzazione offre una soluzione per un'importante problematica affrontata dalle piattaforme centralizzate. Grazie al sistema basato su protocolli, infatti, diminuiscono enormemente per gli utenti i costi di trasferimento da un'implementazione ad un'altra. Come si ha già avuto modo di vedere, nel contesto decentralizzato il corpus di dati è distribuito nel generale protocollo per il social networking. Gli utenti sono liberi di scegliere e cambiare l'interfaccia e i software con cui accedere a questi dati, senza dover ogni volta ricostruire da capo la propria rete di contatti e lo storico dei contenuti. Diminuisce, quindi, l'effetto di *lock-in* e si crea un sistema che favorisce l'allineamento con le preferenze e gli interessi degli utenti[99].

Si sono visti fin qui i benefici apportati dalla decentralizzazione ad un servizio di social networking. Nel terzo capitolo di questo elaborato si procederà ad approfondire nel dettaglio come un DOSN possa contribuire a superare le due maggiori difficoltà delle piattaforme centralizzate: la questione della privacy e la moderazione dei contenuti. In vista di ciò, nel prossimo capitolo si esaminerà con maggiore specificità l'infrastruttura tecnica di un social network decentralizzato.

[99] *Ibid.*

CAPITOLO 2 - UN'INNOVAZIONE DISRUPTIVA

Nel primo capitolo di questo elaborato si è visto come un'architettura decentralizzata possa apportare diversi benefici al web in generale e, soprattutto, alle piattaforme di social networking. Si è proceduto quindi a delineare quali siano gli elementi costituitivi di eventuali servizi decentralizzati, cominciando dalla distinzione tra un sistema distribuito e uno decentralizzato. È opportuno specificare che, a livello tecnico, sono molte le variabili possibili, a partire dalle diverse modalità di strutturare la piattaforma distribuita. Come si è già accennato nel capitolo precedente, infatti, la rete di nodi alla base dell'architettura può essere costituita da un network di server fidati, da un sistema peer-to-peer o da una rete opportunistica[100]. Non si procederà ad illustrare il significato di questi termini - in quanto non rilevante al fine di questo elaborato. Ci si limiterà a specificare che si tratta di diverse possibilità tecniche per mettere in relazione i nodi di una rete, gerarchicamente pari fra loro, affinché assumano e condividano le attività necessarie per azionare un servizio di social networking. Nel corso del tempo sono state proposte diverse soluzioni per la costruzione di un DOSN, ma il punto di svolta si è avuto con l'introduzione di un'importante tecnologia: la blockchain. Quest'ultima è considerata un'innovazione «*disruptive*»[101], ossia in grado di cambiare il modo in cui una data industria, un dato settore operano, apportando una tale efficienza da rivoluzionare il mercato in cui si instaura[102]. Per questo motivo si procederà ora ad analizzare questa tecnologia e le possibilità offerte ai servizi di social networking. La blockchain sembra essere, infatti, la chiave di volta per rispondere sia all'iniziale insuccesso dei sistemi decentralizzati, sia alle difficoltà attuali delle piattaforme centralizzate.

---

[100] *Cfr.* Barbara Guidi, *When Blockchain meets Online Social Networks*, in "Pervasive and Mobile Computing", 62 (2020).

[101] *Ibid.*

[102] *Cfr.* Cambridge Dictionary, *Disruptive*, in "Cambridge Dictionary" (https://dictionary.cambridge.org/it/dizionario/inglese/disruptive, consultato il 28 ottobre 2020).

1) Dalle criptovalute al social networking

Il concetto di blockchain viene introdotto per la prima volta nel 2008 da Satoshi Nakamoto, pseudonimo dell'ignoto inventore del Bitcoin, la più famosa criptovaluta. Nakamoto presenta tale tecnologia nell'articolo *Bitcoin: A Peer-to-Peer Electronic Cash System*, con cui spiega la sua proposta per un sistema di valuta elettronica che consenta i pagamenti online senza l'intermediazione di un'istituzione finanziaria[103]. Tuttavia, è importante specificare che la blockchain è un elemento a sé stante, svincolato dal Bitcoin. Quest'ultimo, infatti, rappresenta solo una delle molte e diverse applicazioni della rivoluzionaria tecnologia introdotta da Satoshi Nakamoto. L'architettura della blockchain garantisce determinate proprietà ai servizi sviluppabili tramite essa, tali da apportare vantaggi ai sistemi tecnologici dei più svariati settori. Facendo riferimento al testo *Tutto su Blockchain* di Roberto Garavaglia è possibile delineare il panorama dei numerosi ambiti di applicazione nei quali la blockchain è già stata introdotta. Procedendo solo ad elencarli, i maggiori settori che beneficiano dei vantaggi apportati dalla tecnologia introdotta da Nakamoto sono: *agrifood*, assicurazioni, *banking*, digital marketing, donazioni, finanza, identità digitale, industria mediatica, settore pubblico, *sharing economy*, trasporti, turismo, *utilities*, welfare[104]. In aggiunta, nel testo *Blockchain 2.0: spiegata semplicemente - ben oltre il bitcoin*, Julian Hosp spiega quali sono, per ogni proprietà garantita dalla tecnologia in questione, gli ambiti di business che ne hanno tratto vantaggio. Secondo Hosp sono sette le peculiarità della blockchain che ne determinano altrettanti metodi di applicazione:

1. descrizione irrevocabile e incensurabile della proprietà
2. salvaguardia dei dati e garanzia della privacy
3. *smart contract* (contratti digitali)
4. rappresentazione di qualsiasi valore in *token*
5. trasparenza e autenticità totali

---

[103] *Cfr.* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, in "Bitcoin.org", 31 ottobre 2008 (https://bitcoin.org/bitcoin.pdf, consultato il 28 ottobre 2020).

[104] *V.* Roberto Garavaglia, *Tutto su Blockchain*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2018.

6. ridondanza e persistenza
7. inclusività[105].

Per ognuno dei punti in elenco Hosp presenta diversi ambiti rivoluzionati dall'introduzione della blockchain in quanto tecnologia «dirompente»[106]. La maggior parte di essi, ovviamente, beneficia di più di una delle proprietà offerte dall'innovazione di Satoshi Nakamoto. Tuttavia, per semplicità, si procederà ora a nominare i settori che secondo Hosp hanno tratto vantaggio dalla tecnologia in questione seguendo la suddivisione introdotta nel testo di riferimento. Innanzitutto, oltre all'intuitivo contesto delle criptovalute, hanno beneficiato dell'identificazione incensurabile della proprietà all'interno della blockchain i programmi di raccolta punti, il *gaming*, la condivisione di contenuti multimediali o documenti digitali, la certificazione dell'identità e la registrazione di brevetti e marchi. La garanzia della privacy ha giovato alla salvaguardia dei dati medici, ai sistemi di comunicazione elettronica e al salvataggio di password o altri dati di accesso. Gli *smart contract* hanno permesso l'implementazione di settori quali l'amministrazione fiduciaria, il mercato delle scommesse, il gioco d'azzardo, le assicurazioni, incentivi e sanzioni, il crowdfunding e gli investimenti di private-equity, gli accordi globali, il sistema legale e, inoltre, l'intelligenza artificiale. La tokenizzazione ha apportato benefici alla gestione di titoli, come azioni e obbligazioni, o del registro delle imprese, al mercato immobiliare e a quello dei metalli preziosi. Gli ambiti che traggono giovamento dalla trasparenza garantita dalla blockchain sono la contabilità, gli audit, la logistica, il traffico di pietre preziose, l'industria farmaceutica, il copyright, il sistema elettorale, la fornitura elettrica, l'educazione stradale, le donazioni, le tasse, la decentralizzazione di Stati, organizzazioni e corporazioni; e ancora, la reputazione personale o istituzionale, l'informazione (attraverso il contrasto alle fake news), l'istruzione scolastica, il mercato del lavoro e le piattaforme di valutazione. La ridondanza del sistema di dati rappresenta un vantaggio per quanto riguarda la

[105] *V.* Julian Hosp, *Blockchain 2.0: spiegata semplicemente - ben oltre il bitcoin*, Kindle ed., 2019.

[106] *Ivi*, posizione 1725.

tecnologia di droni, aerei e macchine autopilotati, per i Big Data e il *machine learning*. Infine, l'inclusività permessa dalla blockchain rappresenta un elemento fondamentale per la resistenza alla censura mediatica o governativa, l'assistenza allo sviluppo dei Paesi in difficoltà, la gestione dei rifugiati, l'Internet of things, la trasmissione di comunicazioni nello spazio e, per concludere, l'imprenditoria[107].

Si sono voluti nominare tutti i settori analizzati da Hosp per i quali la tecnologia della blockchain rappresenta un elemento dirompente al fine di evidenziare come tale innovazione, grazie alle proprietà che la caratterizzano, abbia rivoluzionato ambiti eterogenei e lontani fra loro. Si è voluto sottolineare, inoltre, come le criptovalute rappresentino solo una delle applicazioni possibili di questa tecnologia. L'analisi di Hosp, infine, raccoglie e distingue efficacemente i diversi benefici apportati dalla blockchain, che si procederà ad approfondire in seguito. Nei prossimi paragrafi, invece, verrà discusso più dettagliatamente il sistema tecnico che implementa l'innovazione di Satoshi Nakamoto.

2) La tecnologia della blockchain

Il padre dei Bitcoin ha introdotto la blockchain con uno scopo preciso: risolvere «il problema di come una comunità possa salvare informazioni digitali immodificabili, senza una struttura di gestione centralizzata»[108]. Come spiega Hosp nell'opera già citata, nell'ecosistema digitale è possibile creare, modificare, replicare o cancellare informazioni gratuitamente e con grande semplicità. Per questo motivo ad oggi la maggior parte dei servizi online è gestita da un organismo centralizzato che crea consenso e fiducia per quanto riguarda l'informazione di un dato sistema. Negli ultimi anni, però, in molti si sono interrogati sulla possibilità di realizzare una struttura che gestisca i dati digitali efficacemente ed affidabilmente senza la necessità di un'autorità centralizzata. La risposta è stata fornita nel 2008 proprio da Satoshi Nakamoto con la proposta della blockchain. Una prima definizione di quest'ultima può articolarsi in questo modo:

[107] *Ivi*, posizione 1725-4679.
[108] *Ivi*, posizione 788.

«Una blockchain è un file digitale, che contiene i dati di una comunità. Ogni membro del gruppo è uguale agli altri e nessuno può decidere per altri. Per fare in modo che tutti abbiano sempre lo stesso file e non si creino malintesi, tutti devono aggiornarsi regolarmente al sopraggiungere di nuove informazioni. Per far parte del gruppo si copia il file da un altro partecipante, e in questo modo si ottengono tutte le informazioni. Dal momento che questi aggiornamenti avvengono ad intervalli di tempo e vengono agganciati al file, il file viene chiamato blockchain»[109].

Si procederà ora a sviscerare quest'iniziale spiegazione rivelando i dettagli tecnici di funzionamento della tecnologia in questione.

Innanzitutto, per perseguire il suo scopo ed essere accessibile a chiunque, in tutto il mondo, la blockchain deve insistere su un network. Quest'ultimo si definisce come un gruppo di macchine interconnesse - chiamate nodi - che comunicano fra loro tramite appositi canali e regole stabilite da un protocollo[110]. Si è già visto come, attraverso i criteri dell'architettura e dell'autorità, sia possibile distinguere fra rete centralizzata, distribuita e decentralizzata. La blockchain si fonda su un network strutturalmente distribuito e decentralizzato dal punto di vista dell'autorità. In realtà tale tecnologia può essere sviluppata implementando diversi gradi di centralizzazione o decentralizzazione per quanto riguarda l'autorità. Tuttavia, per l'interesse di questa tesi si considererà la blockchain come sistema distribuito e decentralizzato[111].

Per garantire la fiducia e il consenso all'interno di un sistema così costituito, la tecnologia introdotta da Satoshi Nakamoto implementa un particolare meccanismo. La blockchain, infatti, è essenzialmente un libro mastro (*ledger*) pubblico e distribuito, responsabile dell'archiviazione dei dati condivisi tra i partecipanti del network. Il termine "blockchain" è riferito alla modalità di registrazione delle informazioni, le quali vengono raggruppate in blocchi (*block*) concatenati tra loro

[109] *Ivi*, posizione 898.

[110] *V.* Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 745.

[111] *Ivi*, posizione 820.

(*chain*), uno successivamente all'altro[112]. Ogni blocco aggiunto alla catena contiene l'*hash* crittografico del blocco precedente, una marca temporale e i dati di transazione. Questi elementi sono necessari per impedire la manomissione dei blocchi. Il registro, inoltre, è distribuito e pubblico per tutti gli utenti del network, viene costantemente aggiornato e mantenuto sincronizzato. Quando dei nuovi dati devono essere archiviati, l'informazione viene crittata e verificata dai nodi della rete. La registrazione di nuovi dati è considerata valida e può essere aggiunta al libro mastro solo se conquista il consenso della maggior parte degli utenti della comunità[113]. Il risultato è un sistema aperto e neutrale, e allo stesso tempo sicuro, affidabile e consensuale. In questo modo la possibilità di utilizzare il servizio e di averne fiducia non dipende più da singole entità centralizzate, ma risiede nella codifica stessa della tecnologia[114].

Da quest'iniziale spiegazione del meccanismo della blockchain è emerso come uno degli scopi principali di questa tecnologia sia quello di salvare informazioni. È importante specificare che le informazioni archiviabili nel sistema possono essere di qualunque tipo, come transazioni di *asset*, contratti, certificati di proprietà, dichiarazioni di autenticità e anche i dati social degli utenti[115]. Per descrivere semplicemente ed efficacemente la tecnologia in esame si farà riferimento alle transazioni originali operate attraverso la blockchain: quelle di monete virtuali.

Partendo quindi dal primo elemento introdotto nell'iniziale esposizione del funzionamento di una blockchain, si specifica che il libro mastro o *ledger* riprende il concetto di un tradizionale registro della contabilità, ovvero uno strumento che permette di «registrare transazioni di ogni categoria di bene»[116]. La differenza tra

---

[112] Cfr. Nathaniel Popper, *What is the Blockchain? Explaining the Tech Behind Cryptocurrencies*, in "The New York Times", 27 giugno 2018 (https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-information.html?action=click&module=RelatedLinks&pgtype=Article, consultato il 6 agosto 2020).

[113] Cfr. Barbara Guidi, *When Blockchain meets Online Social Networks*, in "Pervasive and Mobile Computing", 62 (2020).

[114] *V*. Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 594-603.

[115] *V*. GO-Science, *Block chain technology*, in "YouTube", 19 gennaio 2016 (https://youtu.be/4sm5LNqL5j0, consultato il 6 agosto 2020).

[116] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 621.

un *ledger* tradizionale e quello della blockchain è l'evoluzione della tecnologia che li supporta, con il passaggio da un archivio cartaceo ad uno digitale. La funzione di salvataggio di informazioni può far assimilare il concetto di *ledger* a quello di database. Tuttavia, mentre in quest'ultimo i dati possono essere inseriti, modificati e cancellati, in un *ledger* è possibile solo l'aggiunta di nuove informazioni. Si è già accennato, infatti, a come la combinazione di meccanismi quali la decentralizzazione, la crittografia e il protocollo di consenso rendano immutabili i dati registrati nella blockchain. Inoltre, un *ledger* non può neppure essere paragonato ad un database al quale sono stati imposti determinati vincoli alle operazioni attuabili. Blockchain e database, infatti, soddisfano problematiche differenti. In particolare, la prima risponde alla necessità di fiducia all'interno di una comunità in cui le parti sono fra loro sconosciute e «non "fidate"»[117]. Un database, invece, presuppone un sistema di accesso controllato e la gestione da parte di soggetti noti e affidabili.

Il *ledger* digitale che implementa la blockchain, come si è visto, è formato da una struttura di blocchi concatenati fra loro. Ognuno di essi è costituito da un codice informatico contenente qualche tipo di informazione. Per assicurare la sequenzialità dei blocchi aggiunti alla catena, ognuno di essi contiene, oltre ai dati da registrare, una prova matematica generata tramite la crittografia. Quest'ultima fa sì che i blocchi così connessi siano «*tamper proof*»[118], a prova di manomissione. La struttura a blocchi concatenati è comune fra le diverse implementazioni della blockchain, mentre, a seconda dello scopo di progettazione, può variare il design dei blocchi.

Si è parlato di una prova matematica crittografata che garantisce la consequenzialità nella connessione dei blocchi. Tale prova è costituita da una funzione crittografica di *hash*, una specie di impronta digitale di un file che ne certifica l'identità. L'*hashing* viene utilizzato per «mappare dati di dimensioni arbitrarie in

[117] *Ivi*, posizione 646.

[118] *V*. GO-Science, *Block chain technology*, in "YouTube", 19 gennaio 2016 (https://youtu.be/4sm5LNqL5j0, consultato il 6 agosto 2020).

dati di dimensioni fisse»[119]. In sostanza, l'input della funzione di *hash* può essere qualsiasi file digitale, mentre l'output sarà sempre una stringa alfabetico-numerica di un determinato numero di bit. In particolare, un dato input produce sempre lo stesso *hash* e la minima modifica al file iniziale determina uno sconvolgimento del risultato in uscita. Inoltre, la funzione di *hash* è unidirezionale, ovvero, a livello computazionale è molto facile ottenere l'output da un dato input, mentre l'operazione inversa è pressoché impossibile, a meno che non si provino tutte le possibili combinazioni (metodo *brute-force*)[120].

Si è quindi visto come, una volta calcolato l'*hash* di un dato file, qualora quest'ultimo subisse delle modifiche, il relativo *hash* acquisirebbe un aspetto completamente differente. Pertanto, disponendo dell'*hash* originale di un insieme di dati, è possibile verificare l'autenticità di un determinato file calcolandone l'*hash* e confrontandolo con quello che si sa essere accertato. Se i due *hash* non dovessero corrispondere si è consapevoli che il file di cui si dispone deve aver subito delle modifiche. Il vantaggio di una prova matematica ottenuta dal confronto tra *hash* è che è molto più rapida della comparazione di interi file[121].

La funzione di *hash* viene usata consecutivamente nel sistema della blockchain al fine di ottenere agilmente una stringa di dati di lunghezza definita che esprima in modo univoco l'intero stato della blockchain in un determinato momento. Quando un nuovo blocco viene aggiunto alla catena, infatti, il suo *hash* viene calcolato avendo come input della funzione le informazioni che si vogliono registrare, alcuni metadati dell'operazione e l'*hash* del blocco precedente. Tale meccanismo fa sì che, qualora qualcuno cercasse di modificare le informazioni di un qualsiasi blocco nel libro mastro, cambierebbe anche il relativo *hash* e così anche quelli dei blocchi successivi.

---

[119] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 670.

[120] *Ivi*, posizione 680.

[121] *Ivi*, posizione 696.

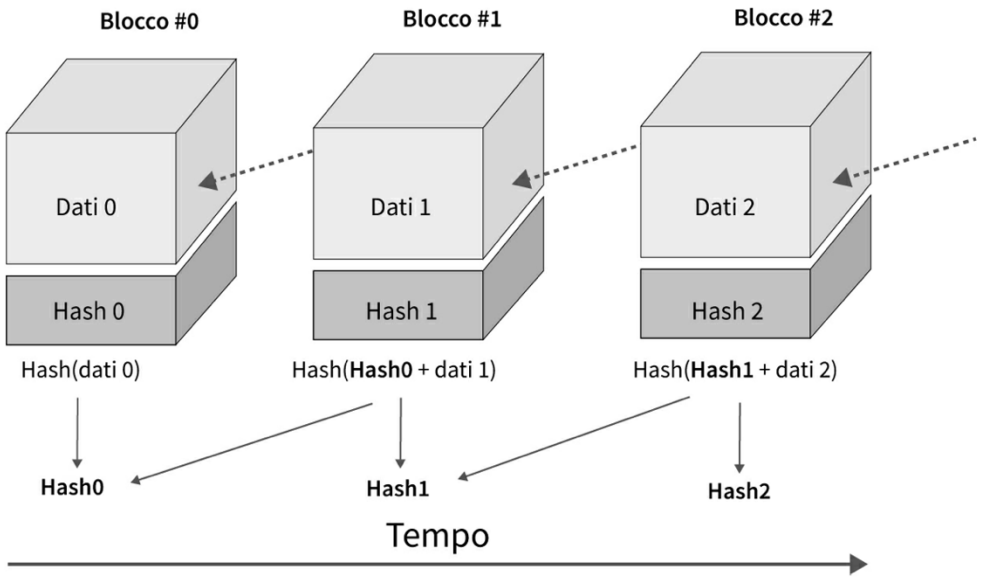

Figura 3: Concatenazione di blocchi in una blockchain, in Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 704.

La valutazione della regolarità di una blockchain non richiede quindi l'analisi dell'intero sistema, ma solo la consultazione dell'*hash* dell'ultimo blocco aggiunto.

Si è già accennato a come la gestione dell'autorità all'interno della blockchain possa essere completamente decentrata o tendere alla centralizzazione. In particolare, a seconda della posizione di un determinato sistema all'interno di tale spettro, esistono tre alternative: blockchain pubblica, ad autorizzazione o privata. Nel primo caso la tecnologia si definisce *permissionless* e rappresenta il modello maggiormente in uso, nonché quello a cui si fa tipicamente riferimento quando si parla di blockchain. Si tratta della classica tecnologia strutturalmente distribuita e completamente decentralizzata dal punto di vista dell'autorità. Un simile sistema comporta che chiunque possa partecipare al network, dal quale non si può neppure essere esclusi. La blockchain *permissionless* è, inoltre, neutrale, ovvero non discrimina né per origine, né per destinazione e nemmeno per contenuto. La decentralizzazione assoluta dell'autorità comporta anche che ad ogni nodo della rete spettino «uguali diritti e responsabilità»[122], in particolare, ogni

[122] *Ivi*, posizione 829.

membro può indagare e verificare qualsiasi transazione all'interno del network. L'esigenza di limitare la decentralizzazione dell'autorità all'interno di una blockchain sorge in determinati contesti nei quali è più importante un controllo degli accessi al sistema. In questi casi si ha solitamente la presenza di una o più terze parti *trusted* (fidate) in cui la comunità pone la propria fiducia per la selezione e l'identificazione dei partecipanti al network[123]. A venire controllato, in particolare, può essere sia l'accesso alla blockchain, sia la possibilità di partecipazione al processo di validazione del consenso. Si avrà quindi un sistema completamente privato (*permissioned* o *fully private*) nel caso in cui l'accesso alla rete sia limitato e la verifica delle transazioni venga affidata esclusivamente ad un gruppo ristretto di soggetti riconosciuti preselezionati. La blockchain potrà, invece, definirsi ibrida o consortium nel caso in cui, rispettivamente, l'accesso sia libero, ma la partecipazione al processo di validazione ristretta oppure l'ammissione limitata, ma la verifica delle transazioni distribuita fra un gruppo di soggetti in possesso di determinati prerequisiti[124].

3) Le transazioni all'interno di una blockchain

«Una transazione (valida) è l'unità elementare di informazione che viene scritta sulla blockchain»[125]. Il compimento di una transazione produce un cambio di stato nel sistema e rappresenta quindi la particella fondamentale di tutto il processo fin qui esposto. Al fine di descrivere lo svolgimento di una transazione all'interno della blockchain è, tuttavia, primario specificare il funzionamento di alcuni componenti essenziali del sistema.

---

[123] *V.* Roberto Garavaglia, *Tutto su Blockchain*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2018, posizione 2275.

[124] *Ivi*, posizione 2312.

[125] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 1038.

3.1) Crittografia e criptazione

Innanzitutto, si è visto come la crittografia svolga una funzione fondamentale all'interno del processo di registrazione di nuove informazioni. Tale meccanismo ricopre un ruolo importante anche nelle operazioni di transazione di *asset* digitali. In primo luogo, la crittografia si definisce come «lo studio delle tecniche di comunicazione sicura in un ambiente ostile»[126]. In questo caso, una struttura distribuita e in cui l'autorità è decentralizzata fra un insieme di individui ignoti può essere considerata un ambiente ostile. In particolare, all'interno della blockchain occupa un posto di particolare rilievo la crittografia asimmetrica. Come spiegano G. Chiap, J. Ranalli e R. Bianchi nel testo *Blockchain. Tecnologia e applicazioni per il business*, tale sistema implica l'utilizzo di una coppia di chiavi matematicamente collegate tra loro. Una chiave è un numero molto grande, solitamente espresso nel sistema esadecimale. Nella crittografia asimmetrica sono previste una chiave privata, generata casualmente, ed una pubblica, calcolata dalla prima. Le chiavi private sono concepite in modo tale da rendere praticamente infattibile crearne due uguali, benché sia matematicamente possibile. Inoltre, mentre generare una chiave pubblica da una privata è un'operazione semplice, il processo inverso è computazionalmente quasi impossibile[127].

La criptazione è un processo di codifica delle informazioni tale da permettere solo ai soggetti autorizzati di accedere ai dati originali. In particolare, viene utilizzata per occultare un messaggio in modo che, se intercettato, non possa essere letto da persone non legittimate. Un'informazione può essere criptata utilizzando l'algoritmo a chiave pubblica, il che permette - appunto - che un messaggio venga trasmesso attraverso un canale non sicuro, mantenendo comunque la segretezza del contenuto. In questo caso viene impiegata la chiave pubblica del destinatario dell'informazione per criptarla prima di trasmetterla. Di conseguenza, solo il soggetto in possesso della chiave privata da cui è stata generata quella pubblica

[126] *Ivi,* posizione 864.

[127] Si specifica "quasi impossibile", perché quando si entrerà nell'era del *quantum computing* la potenza computazionale sarà tale da consentire di scardinare tale meccanismo. Il che pone un nuovo serio problema, in prospettiva, al modello della blockchain dal punto di vista della sicurezza.

utilizzata per la criptazione sarà in grado di decodificare il messaggio. Tale soggetto coincide con il destinatario della trasmissione, supponendo ovviamente che la sua chiave privata non gli sia stata rubata o non l'abbia perduta.

L'algoritmo a chiave pubblica pone, tuttavia, un problema. Il fatto che un messaggio criptato rimanga segreto a chi lo intercetta a meno che non sia in possesso della corretta chiave privata per decifrarlo, non impedisce che l'informazione possa essere manomessa. In questo contesto interviene la tecnica dell'*hashing*, che, come si è visto, permette di individuare se sia intervenuta una modifica all'insieme di dati in questione. Per questo motivo, criptazione e *hashing* vengono spesso combinati. È bene sottolineare, tuttavia, che, benché possano sembrare tecniche simili, rispondono a finalità diverse. La criptazione viene impiegata per garantire la confidenzialità dei dati su cui si applica. Tuttavia, un messaggio criptato con l'algoritmo a chiave pubblica può sempre essere decifrato dalla chiave privata corrispondente. La funzione di *hashing*, invece, è irreversibile in quanto unidirezionale[128].

3.2) Firma digitale

Un altro elemento di cui è opportuno spiegare il funzionamento prima di procedere ad approfondire il sistema delle transazioni in una blockchain è quello delle firme digitali. Queste ultime sono un meccanismo per dimostrare l'identità di qualcuno, evitando che debba essere presente fisicamente. La firma digitale prevede una combinazione della crittografia a chiave pubblica e dell'*hashing*. Il messaggio che si vuole trasmettere viene inizialmente sottoposto alla funzione di *hashing*. La stringa risultante e l'informazione originale vengono insieme firmate digitalmente con la chiave privata del mittente. Una volta ricevuto l'intero "pacchetto", il destinatario lo decripta con la chiave pubblica del mittente, calcola l'*hash* del messaggio così ottenuto e lo confronta con quello integrato nell'insieme trasmesso. Tale successione di tecniche garantisce al sistema determinate proprietà:

[128] *Ivi,* posizione 907.

- l'autenticazione, grazie alla firma digitale attraverso la chiave privata del mittente, che solo lui può avere;
- l'integrità, permessa dall'*hashing*;
- il non ripudio, poiché se qualcuno firma un messaggio attraverso la firma digitale non può negare di averlo fatto[129].

3.3) Indirizzi e *wallet*

L'ultimo elemento di cui è importante conoscere il funzionamento al fine di comprendere il sistema delle transazioni è rappresentato dagli indirizzi. Questi ultimi costituiscono gli equivalenti dei profili utente, in quanto rappresentano degli identificatori che individuano la destinazione di una transazione. Gli indirizzi, quindi, non contengono criptovalute, sono solo dei riferimenti utilizzati per trasferire *asset* digitali. Nella blockchain, infatti, la moneta non esiste come concetto fisico, ma esclusivamente come voce contabile. Pertanto, la "proprietà" di un indirizzo corrisponde al saldo finale calcolato dalla somma di tutte le transazioni che lo coinvolgono. Dal punto di vista tecnico, un indirizzo è il risultato dell'applicazione di tecniche quali la crittografia a chiave pubblica e l'*hashing*. Inizialmente si genera la chiave privata da un numero casuale. Da essa viene matematicamente derivata la corrispondente chiave pubblica. Infine, a quest'ultima vengono applicati diversi tipi di funzioni di *hashing* il cui esito è l'indirizzo. Per gestire gli indirizzi all'interno della blockchain sono stati introdotti i *wallet*, specie di portafogli digitali in cui vengono memorizzate le chiavi pubbliche e private di un dato indirizzo. Il wallet spesso fornisce anche un'interfaccia per verificare il saldo contabile degli indirizzi posseduti da un utente e agevolare la firma delle transazioni[130].

3.4) Transazioni

Si è già visto come una transazione comporti un cambio di stato della blockchain. In un sistema decentralizzato, mancando un'autorità centrale, per determinare lo

[129] *Ivi*, posizione 915-921.
[130] *Ivi*, posizione 921-989.

stato del sistema - ovvero quali transazioni sono avvenute e in quale ordine - è necessario raggiungere il consenso dei partecipanti. Una data transazione risulta valida e interviene quindi a modificare lo stato della blockchain se riceve il consenso della rete. Altrimenti viene considerata invalida. Una transazione, una volta accettata diviene immutabile, ovvero non può essere eliminata, annullata, né modificata.

Per effettuare una transazione all'interno di una blockchain è innanzitutto necessario dimostrare di disporre dell'oggetto che si vuole trasferire. Le firme digitali rendono possibile tale attestazione. Gli *asset* di una blockchain, infatti, non sono collegati ad una persona ma ad un dato indirizzo. Di conseguenza, possedere le chiavi private di un dato indirizzo significa avere accesso agli *asset* ad esso connessi. Pertanto, nel momento di una transazione, il mittente la firma con la propria chiave privata e la successiva applicazione della funzione di *hashing* ne garantisce l'integrità. Una volta creata, la transazione viene propagata ai nodi limitrofi responsabili di verificarne la validità e, in tal caso, di propagarla ulteriormente nel sistema. Ogni transazione, infatti, deve subire questo processo di verifica per poter essere inclusa in un blocco e quindi registrata in modo immutabile nella blockchain[131].

4) Consenso e *mining*

Una blockchain, come si ha già approfondito, insiste su un network di nodi pari fra loro. Ciò implica che non esista un partecipante più o meno importante di un altro e conseguentemente ciascun membro «ha lo stesso diritto di inserire o fare inserire un'informazione sulla blockchain»[132]. In questo contesto per raggiungere un accordo su ciò che avviene ed è considerato valido all'interno del sistema è necessario implementare un meccanismo di consenso.

---

[131] Ivi, 1038-1109.

[132] Julian Hosp, *Blockchain 2.0: spiegata semplicemente - ben oltre il bitcoin*, Kindle ed., 2019, posizione 1067.

«Il consenso è un accordo generale tra i membri di un dato gruppo (in questo caso i nodi della blockchain), ognuno dei quali ha una parte del potere decisionale. In una blockchain il consenso è un accordo su ciò che è accaduto, e detiene l'unica possibile verità sullo stato attuale della blockchain»[133].

Come si avrà modo di approfondire, la blockchain implementa un sistema che, per incentivare tutti i membri a raggiungere l'accordo su un dato stato, impiega matematica, economia e teoria dei giochi. Il processo del consenso per la validazione delle transizioni e l'aggiunta di nuovi blocchi alla catena viene chiamato *mining*, mentre gli attori che vi partecipano sono i *miner*. È importante specificare che quello del consenso è un processo continuo e non discreto, ovvero non si verifica la situazione per cui un istante prima non vi è consenso e nell'istante dopo viene raggiunto, ma si tratta di un procedimento perpetuo. Approfondendo i compiti che gli attori che partecipano al *mining* devono svolgere emerge che:

- un *miner*, assieme ai nodi, si occupa di verificare che le transazioni siano valide e, in tal caso, di propagarle al resto della rete;
- sempre insieme agli altri nodi, ad un *miner* spetta anche controllare la validità dei nuovi blocchi e diffondere al resto del network quelli legittimi;
- infine, un *miner* sceglie le transazioni, le ordina e le aggrega in un dato blocco[134].

Il coinvolgimento dei nodi nel controllo della validità e nella propagazione di transazioni e blocchi è funzionale alla sicurezza del sistema, per garantire un controllo sul lavoro dei *miner*. Inoltre, per incentivare i questi ultimi a partecipare efficientemente al processo è previsto un meccanismo di ricompensa. In particolare, gran parte delle blockchain prevede l'inclusione, all'interno di una transazione, di una certa commissione, la quale corrisponde al costo necessario per portare a termine l'operazione.

Infine, si procederà ora a descrivere l'algoritmo maggiormente impiegato nel contesto delle blockchain per la creazione consensuale di un nuovo blocco: il

[133] Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 1150.

[134] *Ivi*, posizione 1192.

Proof of Work. Tale meccanismo è costituito da un protocollo impiegato per raggiungere un accordo «distribuito nel quale il potere di voto si basa sulla potenza computazionale»[135]. Innanzitutto, la creazione di un nuovo blocco presuppone che un *miner* scelga un numero limitato di transazioni validate da una *transactional pool* (vasca delle transazioni) e le raggruppi, appunto, in un blocco denominato candidato. Quest'ultimo deve poi ottenere la validazione consensuale da parte degli altri nodi del network per essere aggiunto alla catena. In particolare, nel caso in cui tale procedimento di *mining* si basi sull'algoritmo del Proof of Work, i nodi che vi partecipano devono concorrere per risolvere un problema matematico complesso. La soluzione consiste nell'individuazione - appunto - di una Proof of Work, una prova di lavoro, valida. Quest'ultima è rappresentata da un numero computazionalmente difficile da individuare, ma facilmente verificabile. Si tratta di un procedimento casuale a bassa probabilità che prevede un metodo *brute-force*, ossia la prova di tutte le possibili combinazioni. Il primo *miner* che risolve tale problema matematico riscuote la ricompensa. Successivamente il blocco così creato viene propagato nella rete, affinché gli altri nodi ne appurino la validità. Grazie alle caratteristiche dell'algoritmo del Proof of Work, la prova di lavoro risulta molto difficile da trovare, ma è facile poi, per gli altri nodi, verificarne la correttezza. Se il blocco in questione risulta valido, i nodi che lo hanno esaminato lo inoltrano a quelli vicini e, in seguito, il blocco viene aggiunto alla blockchain, altrimenti viene ignorato[136].

Il Proof of Work è solo uno degli algoritmi impiegati nella blockchain, poiché quest'ultima rappresenta una tecnologia particolarmente complessa. Si è proceduto fin qui a spiegarne il funzionamento di base a partire dalla struttura implementata su un *ledger* decentralizzato, passando poi a descrivere i meccanismi di sicurezza del sistema e, infine, al processo di creazione e validazione di nuove transazioni e blocchi - gli elementi costitutivi della blockchain. Non ci si soffermerà ad approfondire altri dettagli di tale tecnologia, in quanto non funzionali a

[135] *Ivi,* posizione 1237.
[136] *Ibid.*

sostegno della tesi discussa in questo elaborato. Per concludere l'analisi portata avanti in questo capitolo, nel prossimo paragrafo si provvederà a descrivere la caratteristica che maggiormente supporta la sicurezza di un database distribuito come quello implementato nella blockchain: l'immutabilità.

5) Immutabilità nella blockchain

Si è già evidenziato come la blockchain differisca da un normale database per l'impossibilità di modificare, annullare o cancellare un'informazione registrata nel sistema. Nel precedente paragrafo è stato descritto il processo di creazione, validazione e registrazione di una transazione all'interno della blockchain. Ora è giunto il momento di chiarire quali siano i meccanismi che consentono l'immutabilità di un'informazione una volta inserita nel *ledger* decentralizzato.

Innanzitutto, è importante specificare che tale proprietà non è garantita, come potrebbe sembrare, dalla funzione di *hashing*. Quest'ultima, infatti, assicura solamente l'integrità della blockchain, permettendo di individuare, come si è visto, eventuali modifiche apportate ai blocchi. «L'*hashing* rende ogni manomissione della blockchain evidente, ma non rende la blockchain a prova di manomissione»[137]. Per riuscire ad apportare efficacemente una modifica al sistema è necessario convincere il network che lo stato della catena manomessa è/sia quello corretto. L'elemento che garantisce l'inalterabilità della blockchain, quindi, è il protocollo di consenso fra i nodi della rete.

In particolare, le caratteristiche del *ledger* di essere distribuito e pubblico implicano che ogni nodo del network possieda e visualizzi una copia identica del registro. Ciò rende la blockchain particolarmente difficile da violare (è bene specificare, infatti, che nulla è assolutamente tutelato dagli attacchi informatici). Ad esempio, in un network composto da mille nodi, per alterare un'informazione salvata nel registro, non è sufficiente hackerare e modificare il *ledger* in possesso di un singolo nodo. La decentralizzazione e il protocollo del consenso, infatti, fanno

[137] *Ivi*, posizione 1545.

sì che sia necessaria l'alterazione contemporanea di almeno il 50% + 1 dei partecipanti alla rete e che tale modifica venga effettuata in modo identico su tutte le copie del registro. Solo in questo modo, infatti, la maggior parte dei nodi che implementano la blockchain potrebbero concordare sullo stato del sistema che comprende la manomissione[138].

Si è quindi visto come l'immutabilità e la sicurezza delle informazioni all'interno della blockchain siano una caratteristica costitutiva del sistema. Si avrà modo di riscontrare come tali proprietà rappresentino alcuni degli elementi che hanno permesso di definire la tecnologia in esame come disruptiva. Nel prossimo capitolo, infatti, si provvederà ad affrontare il tema centrale di questa tesi, ovvero come un sistema decentralizzato, basato su protocolli e su una tecnologia quale quella della blockchain, possa apportare diversi benefici per la risoluzione delle maggiori difficoltà affrontate dalle odierne piattaforme di social networking.

[138] *V*. GO-Science, *Block chain technology*, in "YouTube", 19 gennaio 2016 (https://youtu.be/4sm5LNqL5j0, consultato il 6 agosto 2020).

CAPITOLO 3 - IL RISPETTO DELL'UTENTE

Nel primo capitolo di questo elaborato si è evidenziato come le piattaforme centralizzate godano di determinate caratteristiche che ne hanno comportato un iniziale vantaggio sui paralleli servizi decentralizzati. Tuttavia, dall'analisi svolta, è emerso come, ad oggi, la prevalenza di tali piattaforme sia messa in discussione da una serie di difficoltà conseguite dall'espansione dei sistemi centralizzati. Riassumendo le criticità evidenziate, si ricorda come la centralizzazione comporti una minaccia per la privacy degli utenti delle piattaforme, la difficoltà di bilanciamento tra la libertà di espressione e la necessità di moderazione del discorso online, un pericolo per la persistenza dei dati personali, la discussione delle posizioni monopoliste occupate dalle realtà in questione, l'instabilità del relativo modello di business e, infine, la preoccupazione per l'influenza dei sistemi di social networking nel dibattito pubblico. In questo capitolo si procederà ad approfondire alcune fra queste tematiche che maggiormente costituiscono una minaccia per determinati diritti fondamentali degli individui.

In vista di tale analisi si vuole specificare, tuttavia, come l'accesso ai servizi veicolati attraverso Internet sia oggi considerato una condizione per il godimento di dati diritti umani. La rete, infatti, rappresenta un veicolo essenziale per la comunicazione, l'apprendimento e la partecipazione alla vita sociale, politica ed economica di miliardi di persone[139]. I servizi di social networking, in particolare, svolgono un ruolo importante nello sviluppo relazionale degli individui, nonché nel loro processo informativo. Internet ha permesso l'accesso universale alla conoscenza digitale e le piattaforme ne incrementano l'usabilità, fornendo determinate funzionalità che agevolano la fruizione di tale sapere[140]. Eppure, il valore che queste realtà garantiscono è condizionato da un costo sistemico. Come riporta

[139] *V.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 5.

[140] *V.* Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 1.

Amnesty International nel report *Surveillance Gianst: How the Business Model of Google and Facebook threatens Human Rights*, infatti, le compagnie che offrono tali servizi insistono su un modello di business basato sulla sorveglianza dei soggetti online. Tale sistema pone gli utenti di fronte ad un compromesso inconsapevole: per poter godere dei diritti e delle libertà garantiti dalla realtà online, le persone devono sottostare ad un meccanismo che alimenta la violazione di altre prerogative fondamentali. Fra queste ultime rientrano la privacy, la libertà di espressione e di pensiero, il diritto all'uguaglianza e alla non-discriminazione, al controllo sui propri dati personali, nonché la capacità di plasmare la propria identità all'interno di una sfera privata. Si procederà ad approfondire, dunque, nei prossimi paragrafi come questi principi siano minacciati dal *business model* delle piattaforme centralizzate. Nella sezione seguente, in particolare, si specificherà in cosa consiste e da dove deriva tale potere di sorveglianza[141].

1) Il business della sorveglianza

L'esperienza online è per sé stessa caratterizzata da un insieme di tracce, di dati che gli utenti producono nel corso di qualsiasi attività in rete. Si tratta di una conseguenza della convergenza digitale, ovvero di quel processo che ha comportato la progressiva conversione di qualsiasi informazione possibile dai diversi formati analogici all'univoco sistema in bit[142]. Inizialmente, i dati creati come sottoprodotto dell'offerta di un servizio online sono stati considerati un rifiuto. Solo in seguito realtà quali Google e Facebook hanno colto il potenziale di tale risorsa come fonte di inedite informazioni e ne hanno fatto la base per il loro modello di business. Grazie allo sviluppo tecnologico che ha permesso un aumento delle capacità di immagazzinamento dei dati, alla parallela riduzione dei costi di tali sistemi e alla crescente dislocazione online di diversi aspetti della vita delle persone,

---

[141] *V.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 5-6.

[142] Juan Carlos De Martin, La rivoluzione digitale, in "Treccani Web Tv" (https://www.treccani.it/magazine/webtv/videos/Int_Juan_Carlos_De_Martin_rivoluzione_digitale.html, consultato il 31 ottobre 2020).

il volume delle informazioni immagazzinate nei depositi di poche, grandi aziende è cresciuto esponenzialmente[143]. Ciò ha offerto immense possibilità di monetizzazione ai soggetti che hanno saputo cogliere il valore di quel capitale. Contemporaneamente, tuttavia, ha creato un circolo vizioso per il quale tali realtà sono portate a voler accrescere sempre di più la propria base di dati[144].

Come si è già accennato nel primo capitolo di questo elaborato, infatti, i servizi offerti dalle grandi piattaforme sono nominalmente gratuiti, ma l'utente che ne fruisce paga tali funzionalità - spesso inconsapevolmente - cedendo le proprie informazioni personali prodotte nell'esperienza online. Tale materiale, se aggregato e analizzato attraverso potenti algoritmi di profilazione, è in grado di svelare interessi, pensieri, identità e impensabili dettagli intimi su qualsiasi individuo, nonché di predirne preferenze e comportamenti. Il business dei grandi colossi del web si basa sulla vendita di questo complesso di informazioni a chi desidera rivolgersi a target definiti di persone, quindi, principalmente agli inserzionisti pubblicitari. Si ritiene importante specificare, comunque, che questa risorsa cattura fortemente l'interesse anche di altri svariati attori, dalle agenzie di sicurezza nazionale alle compagnie assicurative. In ogni caso, il business dei dati si trova, ad oggi, nelle mani di pochi, giganti soggetti. Fra questi, in particolare, emergono i ruoli ricoperti da Facebook e Google, i quali detengono il controllo sui canali primari attraverso cui la maggior parte della popolazione accede e interagisce con Internet. Per questo motivo si parla di duopolio del mercato dell'advertising online, nonché del più grande ecosistema dei dati. In molti contesti, infatti, le due piattaforme in questione rappresentano l'opzione principale per la fruizione del web e il loro utilizzo risulta necessario per la partecipazione alla vita sociale moderna[145].

---

[143] *V.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 12.

[144] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[145] *V.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, pp. 8-12.

In aggiunta, tali colossi sono costantemente alla ricerca di soluzioni per espandere ulteriormente la propria area di influenza e per poter raccogliere quantità di dati maggiori. Per questo motivo le piattaforme online appaiono sempre più come conglomerati che accorpano un'ampia varietà di servizi, prodotti e filiali. Inoltre, il modello di business della sorveglianza incentiva la "*datafication*", ovvero la conversione in dati di sempre nuovi aspetti della realtà. In questo senso si stanno diffondendo enormemente le tecnologie dell'Internet of Things, che cospargono il mondo fisico di sensori digitali. Allo stesso modo, gli spazi pubblici diventano una nuova fonte per l'estrazione di dati con l'implementazione delle *smart cities*. Infine, l'espansione dei colossi digitali avviene anche a livello geografico, attraverso l'investimento nello sviluppo tecnologico delle aree più arretrate[146].

All'interno delle piattaforme e, in particolare, dei social network gli utenti hanno la sensazione di avere il controllo sui propri dati, di conoscere quali sono le informazioni che forniscono, con chi le condividono e di poterle eventualmente revocare[147]. Tuttavia, la raccolta dei dati va ben oltre quelli consapevolmente e intenzionalmente provveduti, come i dati anagrafici, i recapiti o la posizione. Sistemi quali Google e Facebook sono in grado di tracciare qualsiasi attività durante la navigazione online dei propri utenti e tale possibilità di rilevamento è oggi straordinariamente incrementata dall'utilizzo degli smartphone, quali mezzo primario di connessione. Inoltre, ad aumentare ulteriormente le informazioni ottenibili dalle grandi piattaforme contribuisce la raccolta dei metadati, i quali costituiscono delle informazioni sui dati stessi, come la marca temporale di un determinato contenuto o i record di posizione. Come riconosciuto dall'Alto Commissariato delle Nazioni Unite per i Diritti Umani, i metadati «possono fornire una visione del comportamento, delle relazioni sociali, delle preferenze personali e dell'identità di un individuo che va oltre anche quella ottenuta dall'accesso al contenuto stesso

[146] *Ivi*, pp. 13-14.

[147] *Cfr.* Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, Tim Berners-Lee, *Decentralization: The future of online social networking*, in *W3C Workshop on the Future of Social Networking Position Papers*, vol. II, gennaio 2009, pp. 2-7.

di una comunicazione»[148]. Infine, l'enorme quantità di dati a disposizione di piattaforme come Facebook o Google permette di svolgere analisi più complesse rispetto ai dati relativi ad un singolo individuo, consentendo di delineare modelli comportamentali su scala potenzialmente mondiale.

L'insieme della raccolta dei dati, della loro aggregazione e di sviluppate tecniche di analisi permette, quindi, l'accesso ad un capitale di conoscenze sugli utenti inedito. Sofisticati modelli algoritmici consentono alle piattaforme di dedurre persino informazioni sensibili, di cui alcune rientrano fra le caratteristiche protette dalla legge sui diritti umani. Tali sistemi possono acquisire la conoscenza di stati d'animo, etnia, orientamento sessuale, opinioni politiche, vulnerabilità, identità sessuale e tratti della personalità della maggior parte degli individui che usufruisce dei loro servizi. Tutto ciò contrasta con il fatto che la protezione dei dati personali è ritenuta un elemento di fondamentale importanza per il godimento del diritto alla privacy e quest'ultimo, a sua volta, tutela un'area personale di libera costruzione ed espressione della propria identità. Si avrà modo di vedere, inoltre, come una simile invadenza della vita privata degli utenti minacci la loro stessa capacità di sviluppare e manifestare pensieri senza interferenze o costrizioni. In aggiunta, il modello di business in questione, per una serie di effetti correlati, mette in pericolo anche la sussistenza di altri diritti, come quello all'uguaglianza e alla non discriminazione o la libertà di opinione[149].

A questo proposito, la legge internazionale per i diritti umani afferma che gli stessi diritti che vengono garantiti alle persone offline devono essere protetti anche in rete e gli Stati dovrebbero agevolare un «ambiente online favorevole»[150] per il godimento di tali prerogative. Inoltre, le aziende stesse hanno la responsabilità di proteggere i diritti umani, indipendentemente dalla capacità o dalla volontà

[148] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 16.
[149] *Ivi,* pp.5-16.
[150] I*vi,* p. 17.

di uno Stato di adempiere ai propri suddetti obblighi in relazione alla materia in questione[151].

Per questo motivo, nei prossimi paragrafi si procederà ad approfondire come e in che misura le grandi piattaforme centralizzate minacciano il godimento di determinati diritti, con particolare attenzione ai servizi di social networking. Per ogni questione analizzata, inoltre, verranno evidenziati i benefici che la decentralizzazione potrebbe apportare per la protezione di tali prerogative, nonché per lo sviluppo di un ambiente online più affine agli interessi degli utenti e favorevole alla creazione di contenuti e di un discorso di qualità.

2) La tutela della privacy

In questo paragrafo sarà posta particolare attenzione al rispetto della privacy, in merito al quale la legge internazionale per i diritti umani stabilisce chiaramente che tale prerogativa deve essere garantita «contro interferenze arbitrarie "sia che provengano da autorità statali sia da persone fisiche o giuridiche"[152]». Tale affermazione tutela quindi la privacy anche da violazioni ad opera di società, come possono essere quelle che reggono le piattaforme centralizzate. Tuttavia, come si è già evidenziato, il modello di business della sorveglianza - così definito da Amnesty International nel report citato - pone diversi ostacoli alla garanzia di tale diritto, al punto da risultarvi quasi incompatibile.

2.1) Il concetto di privacy

Innanzitutto, è importante definire la nozione di privacy, in quanto termine il cui significato evolve costantemente in risposta ai cambiamenti della società e alle necessità che ne derivano. Uno dei primi scritti sul concetto di privacy, nonché uno dei più importanti, è il saggio intitolato *The Right to Privacy*, scritto da Samuel

---

[151] *Ibid.*

[152] Comitato per i Diritti Umani delle Nazioni Unite, *General Comment No. 16*, HRI/GEN/1/Rev.9 (Vol. I), para 1, 1988, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 19.

Warren e Louis Brandeis nel 1890. La tesi sostenuta dai due autori prevede che l'ambito coperto dalla legge sulla privacy debba comprendere un contesto più ampio della protezione fisica della propria casa o della propria proprietà concreta. Per Warren e Brandeis, infatti, la privacy identifica in primo luogo il diritto ad essere lasciati soli. Una simile deduzione deriva dall'introduzione - ai tempi - di particolari innovazioni, quali la fotografia e i giornali ad ampia diffusione, che producono effetti pubblicitari. In relazione a ciò, i due autori descrivono il concetto di privacy informativa, come area da tutelare da una possibile invasione della vita privata degli individui a causa dell'ampia divulgazione pubblica di informazioni personali. Secondo Warren e Brandeis, infatti, il contesto mediatico ed informativo a loro contemporaneo rende necessario il riconoscimento normativo di un diritto alla privacy che includa la prerogativa delle persone ad avere il controllo sulla condivisione dei propri pensieri, sentimenti ed emozioni[153].

In merito all'evoluzione del concetto di privacy parallelamente ai cambiamenti sociali, alla fine del '900 il Comitato delle Nazioni Unite per i Diritti Umani riconosce che tale tutela include la regolamentazione della raccolta e della conservazione «di informazioni personali su computer, banche dati e altri dispositivi, da parte di autorità pubbliche, privati o enti»[154]. Il diritto viene quindi aggiornato per coprire un nuovo contesto di utilizzo dei dati personali, quello destinato a diventare il mercato dei Big Data.

Successivamente, nel 2018 l'Alto Commissariato delle Nazioni Unite per i Diritti Umani definisce la privacy come «la presunzione che gli individui dovrebbero avere un'area di sviluppo, interazione e libertà autonomi, una "sfera privata" […] libera dall'ingerenza dello Stato e dall'intervento eccessivo e non richiesto di altri individui indesiderati»[155]. Tale definizione, che riprende il pensiero di Warren

---

[153] Cfr. Leila Bahri, Barbara Carminati, Elena Ferrari, *Decentralized privacy preserving services for Online Social Networks*, in "Online Social Networks and Media", 6 (2018), pp. 18-25.

[154] Comitato per i Diritti Umani delle Nazioni Unite, *General Comment No. 16: Article 17*, HRI/GEN/1/Rev.9 (Vol. I), 1988, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 19.

[155] Alto Commissariato delle Nazioni Unite per i Diritti Umani, *The right to privacy in the digital age*, A/HRC/39/29, para. 5, 3 agosto 2018, in Amnesty International, *Surveillance Giants: How the*

e Brandeis, racchiude tre concetti correlati, i quali delineano i tre diversi ambiti di copertura del diritto alla privacy: la libertà da intrusioni nella propria vita privata, la facoltà di controllare le informazioni su sé stessi e il diritto ad avere uno spazio in cui esprimere liberamente la propria identità. Nel prossimo sotto-paragrafo si procederà, pertanto, ad evidenziare come ciascuno dei tre contesti citati venga compromesso dal modello di business delle piattaforme centralizzate, andando a minare l'essenza stessa della privacy[156].

2.2) La minaccia del business della sorveglianza

Per quanto riguarda il diritto a non subire intrusioni nella propria vita privata, l'Alto Commissariato delle Nazioni Unite per i Diritti Umani ha specificato che la privacy non viene intaccata solamente attraverso l'esaminazione o l'utilizzo delle informazioni personali di un individuo. Per interferire con tale diritto, infatti, è sufficiente anche semplicemente produrre e raccogliere dati «relativi all'identità, alla famiglia o alla vita di una persona, […] poiché attraverso questi passaggi un individuo perde un certo controllo sulle informazioni che potrebbero mettere a rischio la sua privacy»[157]. Conseguentemente a questa premessa risulta evidente come la quantità di dati raccolti da grandi piattaforme quali Facebook e Google possa scontrarsi con quanto affermato dalla suddetta istituzione delle Nazioni Unite. I colossi del business della sorveglianza, infatti, hanno oggi la capacità di accumulare un volume di informazioni sulle persone e sulle attività umane precedentemente impensabile. Inoltre, gli algoritmi, le tecniche di analisi e i vari meccanismi di elaborazione dei dati sono in grado di estrarre da tale risorsa informazioni così intime e dettagliate da poter potenzialmente conoscere qualsiasi cosa sui propri utenti[158].

Business Model of Google and Facebook threatens Human Rights, Londra, Amnesty International Ltd, 2019, p. 19.

[156] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 19.

[157] Consiglio per i Diritti Umani delle Nazioni Unite, *The right to privacy in the digital age*, A/HRC/39/29, para. 7, 2018.

[158] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 20.

Tuttavia, la legge internazionale per i diritti umani chiarisce esplicitamente che l'interferenza con il diritto alla privacy di un individuo è consentita solo se né arbitraria, né illegale. L'interpretazione di tale presupposto, in particolare, individua tre principi per i quali è ammessa la violazione della prerogativa in questione. Si tratta delle condizioni di «legalità, necessità e proporzionalità»[159]. Come sostiene Amnesty International nel report precedentemente citato, l'attività delle piattaforme centralizzate, con la raccolta indiscriminata e l'analisi incondizionata dei dati dei relativi utenti, risulta evidentemente non necessaria, né conforme, nonché ancor meno ammissibile in relazione al diritto alla privacy.

Per quanto riguarda il secondo componente del principio in questione, esso prevede che gli individui abbiano la facoltà di mantenere il controllo sulle proprie informazioni personali, altrimenti detta diritto all'autodeterminazione informativa. Quest'ultimo implica che le persone possano decidere come e quando i propri dati personali vengano condivisi con terzi. In particolare, questo secondo ambito di copertura del diritto alla privacy ha rappresentato la base per l'affermazione della *data protection*, materia che ha acquisito sempre più importanza proprio con la diffusione del business della sorveglianza e la crescita spropositata delle piattaforme che lo alimentano. Anche nel caso di questo secondo componente del complessivo diritto alla privacy, appare, quindi, evidente come l'attività dei colossi dei Big Data sia in diretto conflitto con l'ambito tutelato[160].

Infine, il terzo elemento che compone la prerogativa in esame prevede che l'individuo abbia diritto alla creazione e alla protezione di uno spazio all'interno del quale plasmare ed esprimere la propria identità. Tale principio fa riferimento alla consapevolezza che la nostra percezione dell'identità è dinamica e la sua costruzione subisce influenze sociali. È facile osservare, infatti, come l'individuo tenda a mostrare un aspetto diverso di sé stesso a seconda del contesto in cui si trova. Ad esempio, qualcuno potrà presentarsi come più responsabile all'interno dell'ambiente di lavoro e allo stesso tempo essere maggiormente spontaneo con un

[159] *Ibid.*
[160] *Ibid.*

gruppo di amici o di persone fidate. Ciascuna di queste sfaccettature è, inoltre, in continua evoluzione, fintantoché al soggetto è permesso di mantenere distinti e riservati i propri diversi aspetti dell'identità. È in questa dimensione che interviene la privacy, al fine di garantire all'individuo l'autonomia, la libertà e la capacità per poter determinare la propria identità. La presenza di una costante sorveglianza, al contrario, tende a far uniformare l'individualità delle persone, per l'impossibilità di variare i propri lati differenti. In questo senso, la privacy agevola anche la diversità culturale, poiché l'esistenza di stratificazioni dell'identità costituisce la base per la salvaguardia dei gruppi minoritari all'interno di una cultura dominante[161]. Il business invadente delle piattaforme centralizzate contribuisce, invece, a restringere lo spazio necessario all'individuo per autonomamente determinarsi. La sorveglianza e l'interferenza con la sfera privata delle persone da parte di attori commerciali e governativi origina un processo che rende «gli individui e le comunità fissi, trasparenti e prevedibili»[162]. In aggiunta, le attività di targeting e profilazione costituiscono per sé stesse dei procedimenti che deducono e delineano le caratteristiche di un dato utente, fossilizzando così la personalità di un soggetto davanti al mondo esterno. Ciò, pertanto, contribuisce ulteriormente alla limitazione del diritto all'autodeterminazione personale.

In conclusione, si è discusso come la sorveglianza esercitata su una scala come quella delle grandi piattaforme centralizzate interferisca in ogni aspetto possibile del concetto di privacy. Non si tratta quindi solo di un'intrusione nella vita privata degli utenti, ma l'invadenza è tale da andare a comprimere lo stesso spazio di autodeterminazione dell'identità di un individuo, compromettendo persino la diversità culturale. Pertanto, si procederà ora ad accennare i tentativi di assunzione di responsabilità da parte dei soggetti in questione, nonché ad evidenziarne le reazioni scettiche da parte del pubblico. Contestualmente verranno introdotti un

[161] *Ivi*, p. 22.

[162] Julie E. Cohen, *What Privacy is For*, in "Harvard Law Review", 126 (2013), in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 22.

esempio dell'inaffidabilità della custodia dei dati personali ad opera delle piattaforme centralizzate ed un recente intervento volto a sostenere la *data protection*.

2.3) Lo scandalo e la speranza

Negli ultimi anni i rappresentanti dei colossi della sorveglianza come Google e Facebook hanno più volte riconosciuto l'importanza del diritto alla privacy, come tutela di uno spazio privato fondamentale per gli individui. Il fondatore e CEO di Facebook Mark Zuckerberg, ad esempio, ha annunciato nel 2019 che la sua piattaforma si sarebbe evoluta verso una maggiore garanzia di tale diritto fondamentale, attraverso una generale conversione dei propri servizi in funzionalità orientate ad un'interazione più fidata tra le persone. Contemporaneamente Google ha rivelato che avrebbe messo in atto maggiori restrizioni sulla condivisione dei dati con gli inserzionisti attraverso il proprio sistema di aste pubblicitarie[163]. Questi sono solo alcuni esempi delle diverse enunciazioni delle maggiori piattaforme centralizzate a favore di un recupero della privacy. Tuttavia, sebbene tali ammissioni siano per sé stesse positive, in quanto rivelano la consapevolezza dell'importanza del tema in questione, altre voci si sono mostrate scettiche in merito alle reali intenzioni di questi soggetti. Ciò che alimenta la diffidenza, in particolare, è il fatto che il modello di business di tali colossi si basi sulla sorveglianza e quindi sulla proprietà, l'elaborazione e la vendita dei dati degli utenti. Inoltre, attività quali il targeting e la profilazione sono funzionali all'offerta stessa dei servizi previsti dalle piattaforme in questione. In passato, in aggiunta, si sono verificati diversi casi in cui i colossi del web hanno infranto determinate promesse, hanno aggirato le condizioni impostegli e hanno dato vita a scandali sulla gestione della privacy. A questo proposito si procederà ora ad introdurre l'evento che recentemente ha attirato maggiormente l'attenzione del pubblico, nonché delle autorità di regolamentazione, sul tema.

[163] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 22.

Si sta facendo riferimento ad una delle più grandi violazioni di dati nella storia del colosso del social networking Facebook. La vicenda ha inizio il 17 marzo 2018 quando due dei maggiori quotidiani rispettivamente del Regno Unito e degli Stati Uniti, The Guardian e The New York Times, rivelano che una società di *data mining* chiamata Cambridge Analytica ha acceduto impropriamente ai profili di più di 50 milioni di utenti del social network di Mark Zuckerberg[164]. L'insieme dei fatti che si andrà a specificare ha costituito un caso mediatico, in particolare per i legami dell'azienda in questione con le elezioni presidenziali degli Stati Uniti nel 2016. Tuttavia, ciò che si vuole evidenziare in questo contesto è la fragilità della *data protection* di una delle più grandi piattaforme al mondo, nonché l'impossibilità di controllo da parte degli utenti sulle proprie informazioni personali all'interno del contesto centralizzato.

La raccolta dei dati degli utenti di Facebook è avvenuta ad opera di *Thisisyourdigitallife*, un'applicazione, sviluppata dall'accademico dell'Università di Cambridge Aleksandr Kogan, che permetteva agli utilizzatori di ottenere un profilo psicologico in base alla propria esperienza online. Una delle possibilità di accesso all'applicazione era attraverso il *Facebook Login*, sistema che consente di iscriversi ad un servizio senza la necessità di creare un apposito profilo con relative credenziali, ma sfruttando i propri account social - in questo caso quello della piattaforma di Mark Zuckerberg. Tale attività ha avuto inizio nel 2014 e, al tempo, la politica di Facebook prevedeva che i servizi a cui una persona accedeva attraverso il *Facebook Login* potessero raccogliere non solo le informazioni personali degli utenti custodite dal social network, ma anche i dati dei relativi amici[165]. In questo modo, attraverso l'iscrizione a *Thisisyourdigitallife* di 270 mila persone, Kogan ha ottenuto informazioni su 50 milioni di profili. Fino a qui, tuttavia, l'attività dell'accademico di Cambridge rispettava i termini del social network di Zuckerberg. La

---

[164] *Cfr.* Emanuele Menietti, *Il caso Cambridge Analytica, spiegato bene*, in "Il Post", 19 marzo 2018 (https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/, consultato il 30 ottobre 2020).

[165] *V.* Carole Cadwalladr, Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, in "The Guardian", 17 marzo 2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, consultato il 31 ottobre 2020).

violazione è avvenuta nel momento in cui Kogan ha condiviso i dati così raccolti con il Gruppo Strategic Communication Laboratories, di cui Cambridge Analytica costituiva il ramo d'azienda deputato all'analisi dei dati[166]. La politica di Facebook, infatti, consentiva esclusivamente la raccolta dei dati del network di amici di un dato profilo con lo scopo di migliorare l'esperienza dell'utente nell'applicazione in questione, mentre ne vietava la vendita e la condivisione con terze parti, in particolare a fini pubblicitari[167]. Al contrario, Cambridge Analytica ha aggiunto l'insieme di informazioni ottenuto al suo complessivo volume di dati impiegato per la profilazione e il targeting a scopo propagandistico. Verrà approfondito, infatti, nei prossimi paragrafi il ruolo svolto da tale società nella campagna presidenziale di Donald Trump nel 2016 e in quella referendaria pro-Brexit.

Ciò che si vuole evidenziare in questo contesto, invece, è l'irresponsabilità dimostrata da una delle più grandi piattaforme centralizzate al mondo. Facebook, infatti, ha innanzitutto peccato dal punto di vista processuale, prevendo un sistema dedicato alla protezione dei dati personali facilmente violabile. Si tratta di un difetto di *privacy by design*, principio la cui importanza è stata evidenziata dalle più recenti normative sul tema. La società di Zuckerberg, inoltre, è colpevole per quanto riguarda il comportamento tenuto successivamente alla violazione. Venuta a conoscenza dell'infrazione, infatti, Facebook non ha provveduto ad informare gli utenti coinvolti. In aggiunta, benché la società abbia imposto a Cambridge Analytica l'eliminazione dei dati in questione, in seguito, non si è preoccupata di accertarsene. Anzi, è emerso successivamente come Facebook fosse informata del fatto che la società di *data mining* aveva mantenuto il possesso delle informazioni[168].

---

[166] V. Casey Newton, *Facebook suspended Donald Trump's data operations team for misusing people's personal information*, in "The Verge", 16 marzo 2018 (https://www.theverge.com/2018/3/16/17132172/facebook-cambridge-analytica-suspended-donald-trump-strategic-communication-laboratories, consultato il 30 ottobre 2020).

[167] *V.* Carole Cadwalladr, Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, in "The Guardian", 17 marzo 2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, consultato il 31 ottobre 2020).

[168] *V.* Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, in "The New York Times", 17 marzo 2018 (https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html, consultato il 29 ottobre 2020).

Solo a marzo del 2018, infatti, la piattaforma si è occupata di rimuovere i profili di Cambridge Analytica e della Strategic Communication Laboratories dal social network. Gli utenti coinvolti, inoltre, sono venuti a conoscenza della vicenda solo in seguito all'indagine mediatica e allo scandalo pubblico[169].

A sostegno della tesi discussa in questo elaborato, i fatti narrati vogliono evidenziare quanto siano elusivi e fragili i termini che dovrebbero proteggere la privacy degli utenti all'interno di sistemi centralizzati. Inoltre, lo scandalo di Cambridge Analytica mostra quanto sia difficile applicare le politiche esistenti e mantenere il controllo sulle informazioni condivise con soggetti terzi. Non si procederà in questo contesto ad approfondire ulteriormente la vicenda in questione, della quale per di più non sono ancora chiari tutti i dettagli e vi sono tuttora indagini in corso. Nei prossimi capoversi si vuole invece introdurre uno spiraglio sulla legislazione delle questioni in analisi, andando a descrivere il nuovo Regolamento europeo per la protezione dei dati personali, altrimenti detto General Data Protection Regulation (GDPR).

Quest'ultimo rappresenta la normativa applicata nel contesto dell'Unione Europea per disciplinare l'utilizzo dei dati personali in tutti i Paesi membri dell'organizzazione e non solo. Il GDPR, infatti, entrato in vigore il 25 maggio 2018, definisce innanzitutto un ambito di applicazione territoriale particolarmente ampio, poiché regola non solo il trattamento di informazioni personali all'interno della Comunità Europea, ma ha effetto altresì sugli «Enti che risiedono al di fuori»[170] di tale territorio. In particolare, sono oggetto del Regolamento anche le società o le imprese che hanno sede all'esterno dell'UE, ma la cui attività è svolta al fine di offrire beni e servizi o per monitorare il comportamento di soggetti stabiliti nei Paesi membri. Tale estensione risponde alle esigenze dello sviluppo tecnologico e in particolare alla natura globale di Internet, in relazione alla quale il

[169] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 33.

[170] Gdpr.net, *General Data Protection Regulation*, in "Gdpr.net" (https://www.gdpr.net, consultato il 20 agosto 2020).

GDPR riconosce l'importanza di tutelare i cittadini della Comunità Europea anche da enti che abbiano sede all'estero[171].

Il Regolamento riporta una specifica definizione di dato personale particolarmente ampia, poiché fa riferimento a «qualsiasi informazione relativa a una persona fisica identificata o identificabile»[172]. Ciò fa sì che rientrino fra i dati tutelati anche quelli anonimizzati, qualora attraverso l'analisi o il confronto con informazioni aggiuntive possano ricondurre ad un determinato soggetto. Analogamente, anche i dati dedotti o previsti sono compresi in tale definizione se collegati ad identificatori univoci o comunque attribuibili a una persona fisica[173].

Lo scopo primario del Regolamento è quello di porre l'utente in una posizione di maggiore consapevolezza e controllo su come le proprie informazioni personali vengano raccolte ed utilizzate. Innanzitutto, il GDPR fissa determinati principi che vincolano il trattamento dei dati. Di particolare rilievo è quello della limitazione delle finalità, secondo il quale la raccolta e l'impiego di informazioni personali sono vincolati ad un'esposizione chiara dello scopo di tali attività e alla specificazione dello stesso nelle informative sulla privacy rivolte agli utenti. Dal momento in cui un soggetto acconsente alla condivisione dei propri dati per una determinata finalità, l'utilizzo degli stessi deve essere limitato ad essa. In aggiunta, il GDPR prevede la possibilità per l'utente di richiedere ed ottenere una copia dei propri dati di cui un determinato ente è in possesso, garantendo così agli individui una maggiore coscienza di quali informazioni le aziende dispongano su di loro[174]. Il nuovo Regolamento europeo per la protezione dei dati personali, inoltre, stabilisce uno standard particolarmente elevato per il consenso al trattamento e lo vincola ai requisiti di libertà, specificità, informazione e inequivocabilità. In particolare, per garantire che il consenso sia prestato liberamente, esso si ritiene privo di

---

[171] Il Post, *Perché in questi giorni siti e app vi perseguitano coi messaggi sulla privacy*, in "Il Post", 28 aprile 2018 (https://www.ilpost.it/2018/04/28/gdpr-guida/, consultato il 3 novembre 2020).

[172] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 21.

[173] *Ibid.*

[174] *V.* Russell Brandom, *Everything you need to know about GDPR*, in "The Verge", 25 maggio 2018 (https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice, consultato il 2 novembre 2020).

una base giuridica valida laddove vi sia uno squilibrio fra i vantaggi ottenuti tramite il trattamento dei dati a favore del responsabile e a sfavore dell'utente. Tuttavia, le grandi piattaforme che si basano sul business della sorveglianza subordinano l'accesso o comunque il pieno utilizzo dei propri prodotti e servizi al fatto che gli utenti forniscano il consenso alla condivisione delle proprie informazioni personali. Ciò nega il requisito di libertà.

Infine, per quanto il GDPR rappresenti un punto di riferimento a livello mondiale per la data *protection* e la regolamentazione della privacy degli utenti, in molti diffidano sulla sua effettiva capacità di disciplinare l'attività di colossi quali quelli del business della sorveglianza. In particolare, infatti, dal punto di vista delle sanzioni applicabili, il Regolamento europeo prevede delle cifre molto più elevate rispetto alle precedenti normative, dal momento che le multe per le violazioni possono arrivare fino al 4% del fatturato globale di un'azienda o comunque al tetto massimo di 20 milioni di dollari. Tuttavia, mentre simili cifre potrebbero determinare il fallimento per un'azienda di medie dimensioni, l'impatto su società come Facebook o Google non sarebbe altrettanto significativo[175].

L'approfondimento fin qui esposto sulla nuova normativa generale per la protezione dei dati personali ha voluto evidenziare la direzione intrapresa dal Regolatore europeo verso una maggiore tutela della privacy dei cittadini della Comunità. Parallelamente, anche altri Paesi, prendendo esempio dalla disciplina del vecchio continente, si stanno muovendo con lo stesso orientamento. Tuttavia, l'introduzione del GDPR evidenzia contemporaneamente le difficoltà di normare il contesto online e, in particolare, l'attività dei colossi del web, le cui dimensioni sono diventate tali da renderli di fatto immuni ad interventi sanzionatori. Per questo motivo, nel prossimo paragrafo si procederà ad introdurre la proposta di un approccio decentralizzato come valida alternativa per affrontare le problematiche in questione.

[175] *Ibid.*

2.4) Approccio decentralizzato alla tutela dei dati

Nel primo capitolo di questo elaborato si è già accennato ai benefici che genericamente un approccio decentralizzato potrebbe apportare ad un servizio online e, in particolare, ad uno di social networking. In questa sede si procederà ad approfondire il tema seguendo innanzitutto la distinzione proposta L. Bahri, B. Carminati e E. Ferrari nell'articolo *Decentralized privacy preserving services for Online Social Networks* fra privacy online e privacy offline. La prima, in particolare, fa riferimento alla capacità di controllo da parte dell'utente sulla condivisione dei propri dati con i propri contatti, ossia la possibilità di scegliere quali informazioni rendere visibili a chi. Tale meccanismo è conosciuto come gestione del controllo degli accessi e comprende, oltre alla capacità di regolazione dell'accesso esterno ai propri contenuti, anche i diversi modi in cui i servizi online possono applicare tale sistema. Con privacy offline, invece, ci si riferisce a quell'area personale dell'individuo che dev'essere tutelata in quanto sede di pensieri, emozioni, comportamenti, interessi e che potrebbe essere violata dalla raccolta e dall'elaborazione dei dati di un utente abilitate dai servizi di socializzazione online[176].

In un servizio centralizzato la privacy online e, in particolare, la gestione del controllo degli accessi sono facoltà tipicamente garantite. Esse costituiscono la dimensione della riservatezza personale più visibile all'utente, poiché quest'ultimo può concretamente riscontrarne le implicazioni. Ad esempio, un soggetto potrebbe trarre giovamento dalla libertà di bloccare la condivisione dei propri contenuti attinenti allo svago con il datore di lavoro. A tale riguardo sono molti e vari i servizi offerti dai social network odierni, dalla possibilità di rendere privato il proprio intero profilo, alla creazione di diverse liste o gruppi di contatti a cui permettere la visione di una singola pubblicazione. I provider di sistemi di social networking hanno posto particolare attenzione allo sviluppo di interfacce e meccanismi per la gestione della privacy online, garantendo un'elevata granularità nella scelta del

[176] Cfr. Leila Bahri, Barbara Carminati, Elena Ferrari, *Decentralized privacy preserving services for Online Social Networks*, in "Online Social Networks and Media", 6 (2018), pp. 18-25.

pubblico per ogni singolo contenuto[177]. Ciò risulta particolarmente agile in un sistema centralizzato, dal momento che l'autorità proprietaria ha l'esclusivo controllo su tutti i dati, le comunicazioni e i canali di accesso. Più complicata è la gestione della privacy online nel contesto decentralizzato, poiché implica la condivisione della responsabilità fra i vari nodi della rete. Per questo motivo acquistano particolare importanza le capacità di coordinamento e di conseguimento del consenso per assicurare uno stato sicuro e univoco del sistema in questione[178].

È in questo scenario che entra in gioco la tecnologia della blockchain, che, come si è visto, implementa un meccanismo del consenso che garantisce l'univocità dello stato del sistema. In particolare, l'innovazione introdotta da Satoshi Nakamoto risponde propriamente all'esigenza di raggiungere l'accordo su un singolo stato della rete all'interno di un contesto non fidato come quello decentralizzato[179]. Non si procederà ora a descrivere nuovamente il funzionamento della tecnologia in questione, in quanto sufficientemente approfondito nel secondo capitolo di questo elaborato. In questa sede si provvederà, piuttosto, ad evidenziare i requisiti di un sistema di gestione del controllo degli accessi - e quindi della privacy online - e l'approccio a tali questioni previsto in un servizio decentralizzato. Innanzitutto, il contesto di un social network si caratterizza per la presenza di enormi quantità di dati, una consistente base di utenti e un controllo degli accessi dinamico ed estremamente variabile. In un simile scenario è richiesto quindi che la gestione della privacy online preveda livelli di specificazione del diritto di accesso a grana fine, per poter riflettere lo spettro di relazioni esistenti fra gli utenti, fra le diverse risorse e fra utenti e risorse. Pertanto, la sfida che i social network decentralizzati devono affrontare è come rispondere a tali requisiti, offrendo politiche di accesso flessibili e granulari, che permettano la combinazione di singoli attributi per i diversi accessi[180].

---

[177] *Ibid.*

[178] *Ibid.*

[179] V. Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019, posizione 1140.

[180] Cfr. Leila Bahri, Barbara Carminati, Elena Ferrari, *Decentralized privacy preserving services for Online Social Networks*, in "Online Social Networks and Media", 6 (2018), pp. 18-25.

In questo contesto, il meccanismo maggiormente impiegato per l'applicazione del controllo degli accessi prevede l'impiego delle tecniche di crittografia. Anche in questo caso si ha già provveduto a specificare il significato di tale pratica nella tesi in discussione e pertanto si rimanda al relativo paragrafo. Il motivo per cui tale tecnica è stata richiamata in questa sede è che permette di limitare l'accesso ad un contenuto esclusivamente a chi è autorizzato. Ciò è consentito attraverso il meccanismo delle chiavi, il quale fa sì che quando un'informazione crittografata viene intercettata, solo chi detiene la proprietà esclusiva della chiave privata in grado di decrittarla può accedervi. La sfida per un servizio di social networking decentralizzato, pertanto, è quella di implementare un sistema efficiente per la gestione delle chiavi. A questo proposito sono diverse le alternative implementate e studiate, dalla proposta di demandare lo scambio delle chiavi di accesso ad un canale esterno al *layer* della blockchain, all'alternativa dell'implementazione di tabelle di *hash* dinamiche[181]. Tuttavia, non attiene allo scopo di questa tesi l'approfondimento di tali tecniche.

Si passerà ora a discutere la questione della tutela della privacy offline in una piattaforma decentralizzata. Si ha già avuto modo di rilevare come dall'elaborazione e dall'analisi dei dati e dei metadati che gli individui producono nella loro esperienza all'interno di una data piattaforma sia possibile ricavare informazioni estremamente dettagliate e intime sulla vita di una persona. Ciò è dovuto dal fatto che gli utenti accedono ai servizi offerti dalle piattaforme gratuitamente, ma in cambio consentono la raccolta e il trattamento dei propri dati. In un contesto decentralizzato, invece, viene a mancare la presenza di un'autorità centrale che accumuli le informazioni personali degli individui e che sia autorizzata ad elaborarle, poiché tutte le attività necessarie per implementare il sistema vengono prese in carico dalla rete di nodi pari fra loro[182]. Si è già spiegato come, per accedere ad un servizio decentralizzato, ad esempio uno di social networking, un utente debba

[181] *Ibid.*

[182] Cfr. Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 351.

scegliere un server fidato sul quale depositare i propri dati[183]. I vari host di un sistema *peer-to-peer* sono poi fra loro indipendenti ed interconnessi e le trasmissioni delle informazioni avvengono solo con il consenso esplicito del soggetto di riferimento[184]. Ciò garantisce che l'utente rimanga in possesso dei propri dati e abbia il controllo sulla condivisione degli stessi, la cui sicurezza, nel momento di una transizione, viene ulteriormente comprovata dalla presenza dei meccanismi di criptazione dei messaggi. Quest'insieme di garanzie fa sì che anche i processi di *data mining*, ovvero l'estrazione massiccia dei dati[185], e le connesse attività di analisi per finalità come la profilazione e il targeting siano ostacolati dalla proprietà delle informazioni a carico dell'utente stesso.

Tuttavia, il deposito dei dati di un soggetto su un unico server comporta evidentemente pericoli per le informazioni, poiché tale host rappresenta un *single point of failure* e pertanto, se soggetto a malfunzionamenti o ad attacchi esterni, determinerebbe la perdita dei dati. Per questo motivo, nella realtà di un social network decentralizzato le informazioni non sono solo archiviate in un'unica posizione, ma sono piuttosto replicate e disperse tra diversi *peer* della rete. La ridondanza, infatti, agevola - se non assicura - la persistenza dei dati in un sistema. Tuttavia, ciò pone nuovamente il problema della fiducia nei confronti dei server destinati ad ospitare le copie dei dati di utente. Qui interviene la crittografia, per secretare le informazioni sia nei nodi di archiviazione che in quelli di replica[186]. All'interno di questo scenario promettenti sviluppi per la protezione dei dati - e conseguentemente della privacy offline - in un sistema decentralizzato di nodi non fidati derivano dall'applicazione della tecnologia della blockchain alla gestione del

---

[183] C*fr. V.* Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, Tim Berners-Lee, *Decentralization: The future of online social networking*, in *W3C Workshop on the Future of Social Networking Position Papers*, vol. II, gennaio 2009, pp. 2-7.

[184] *Cfr.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[185] *Cfr.* Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 357.

[186] *V.* Leila Bahri, Barbara Carminati, Elena Ferrari, *Decentralized privacy preserving services for Online Social Networks*, in "Online Social Networks and Media", 6 (2018), pp. 18-25.

deposito distribuito dei dati. Come si è visto nel secondo capitolo di questo elaborato, infatti, l'innovazione di Satoshi Nakamoto aggrega un insieme di tecniche, fra cui la crittografia e l'hashing, e la struttura a blocchi concatenati per apportare determinate proprietà al sistema. In particolare, interessanti in questo contesto sono due caratteristiche garantite dalla blockchain ad un *ledger* distribuito e ad autorità decentralizzata: la descrizione irrevocabile e incensurabile della proprietà e la salvaguardia dei dati. Della prima si è già discusso in conclusione al secondo capitolo di questo elaborato. Per argomentare la seconda prerogativa basterà ricordare che «una blockchain si basa sulla crittografia, attraverso la quale si può accedere all'elaborazione dei dati solamente tramite la creazione di una *private key* senza ulteriori autenticazioni»[187]. Ciò esclude la necessità di registrarsi ad un dato servizio attraverso l'indirizzo e-mail o altri identificatori, come invece è richiesto nelle normali piattaforme. La blockchain permette quindi di agire in anonimato, impedendo pertanto anche l'eventuale identificazione di utente attuabile attraverso l'aggregazione e l'analisi dei metadati delle transizioni di informazioni. In un contesto decentralizzato che implementa la tecnologia della blockchain, infatti, non è possibile risalire a chi o a che cosa controlli una data *private key*.

Si conclude qui il paragrafo di questo elaborato dedicato alla difficoltà di tutela del diritto alla privacy nell'ambito dei servizi online centralizzati e alla proposta di un approccio decentralizzato per contribuire alla risoluzione di tali problematiche. Nella prossima sezione si provvederà invece ad affrontare un'altra questione che comporta notevoli ostacoli alla gestione centralizzata delle piattaforme, in particolare quelle di social networking. Si sta facendo riferimento al problema della moderazione dei contenuti, fra la pretesa della libertà di espressione e il desiderio di un discorso online di qualità.

[187] Julian Hosp, *Blockchain 2.0: spiegata semplicemente - ben oltre il bitcoin*, Kindle ed., 2019, posizione 1309.

3) La moderazione del discorso online

Introducendo questo elaborato si ha già evidenziato come l'iniziale sentimento delle persone a favore delle piattaforme centralizzate stia attualmente lasciando posto a dubbi e criticità. L'originale progetto della rete come luogo in cui esprimere liberamente il proprio pensiero e sviluppare nuove e creative idee sembra si sia tramutato in una serie di *walled gardens* all'interno dei quali gli utenti si uniformano fra loro. Infatti, «la massa critica derivante dalla loro adozione generalizzata conferisce a tali piattaforme una capacità normativa sul linguaggio che diviene parte integrante del loro potere»[188]. Ne consegue che tali realtà promuovano determinati modelli di comportamento a cui le persone devono conformarsi per poter fruire dei servizi offerti. Ad esempio, un social network come Facebook ha il potere di stabilire i tipi di reazione che gli utenti possono scambiarsi tra loro o di limitare i contenuti accettabili. Inoltre, si è già accennato a come il business della sorveglianza ostacoli lo sviluppo della diversità culturale, comprimendo la privacy quale area di personale sviluppo dell'identità degli individui[189].

3.1) Minaccia alla libertà di espressione

Oltre alle spaventose conseguenze del business della sorveglianza fin qui evidenziate, c'è un altro aspetto che si tiene ad evidenziare. I complessi algoritmi che alimentano i benamati servizi personalizzati delle piattaforme centralizzate rispondono a due precisi obiettivi: l'offerta di advertising targettizzato e la massimizzazione del coinvolgimento degli utenti, il cosiddetto *engagement*. Tuttavia, entrambe le finalità comportano degli effetti collaterali che minacciano la tutela di determinati diritti umani. In particolare, la proposta di annunci e contenuti personalizzati fa sì che i servizi online come Google e Facebook abbiano un'importante influenza sull'esperienza in rete degli individui e sulle informazioni a cui gli utenti

[188] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

[189] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 22.

accedono[190]. Ciò significa che le piattaforme svolgono un ruolo considerevole nel determinare non solo il contenuto che le persone possono creare, ma anche quello che consumano[191]. In questo senso il business della sorveglianza costituisce una minaccia per la libera manifestazione del pensiero, di cui il diritto alla privacy rappresenta un requisito fondamentale. Come sostenuto da Frank La Rue, *Special Rapporteur* delle Nazioni Unite, infatti, «la libertà di espressione è un diritto collettivo, che consente alle persone di cercare e ricevere informazioni come gruppo sociale e di "dare voce alle proprie opinioni collettive"»[192]. I meccanismi di manipolazione e persuasione prodotti dagli algoritmi delle grandi piattaforme, invece, generano un impatto sulle persone - sia singolarmente, che a livello di gruppo - tale da influenzarne l'opinione[193].

In aggiunta, come si è già evidenziato, per la maggior parte degli individui i servizi dei grandi colossi online rappresentano il canale primario, se non l'unico, per accedere ai contenuti in rete. Per di più, le persone utilizzano le piattaforme per la ricerca di notizie sull'attualità, sugli eventi, spesso preferendole ai media tradizionali. L'ascesa dei social a fonte di informazione non riguarda solo - come si potrebbe pensare - le generazioni più giovani di utenti, ma coinvolge tutti i gruppi demografici. Parallelamente a questa tendenza, inoltre, le risorse e i contenuti online sono sempre più concentrati nelle mani di un numero limitato e in calo di soggetti. Si tiene a ribadire, quindi, come questi ultimi acquisiscano una straordinaria autorità su ciò che il pubblico consuma quotidianamente. In particolare, tale influenza si manifesta in due distinti aspetti, ovvero nella padronanza di ciò che viene pubblicato e nel controllo della probabilità di ricezione di tale contenuto. Tutto ciò può comportare rilevanti ostacoli per quanto riguarda la libertà di

---

[190] *Ivi*, p. 29.

[191] *Cfr.* Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 1.

[192] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/14/23, para. 29, 20 aprile 2010, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 31.

[193] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 31.

espressione, nonché quella di informazione, delle persone. I problemi che possono manifestarsi, in particolare, sono di più tipi, dalla censura di determinati materiali su incentivo delle autorità di regolamentazione, all'influenza più discreta, ma non meno importante, dei bias nella cura dei contenuti, ad opera di algoritmi opachi[194]. In questo secondo caso, inoltre, è importante specificare che le piattaforme che dominano l'infosfera online e che sono pertanto responsabili dell'informazione delle persone risultano difficili, se non impossibili, da monitorare e controllare. In aggiunta, in determinati contesti non vengono neanche consapevolmente selezionate dagli utenti per ricoprire tale ruolo, ma rappresentano una scelta forzata. Pertanto, si procederà ora ad analizzare i già citati pericoli che tali colossi comportano per la libertà di espressione degli individui.

Innanzitutto, particolarmente rilevante è il problema della possibile influenza governativa sulla censura di determinati contenuti. La natura centralizzata delle piattaforme, nello specifico, fa sì che esse risultino esposte alle pressioni di governi e autorità che vogliano estendere le proprie regole nazionali alla sfera online. Anche se un dato servizio è offerto sul web, infatti, ciò non esclude che l'azienda che lo implementa sia soggetta alle leggi locali, in particolare nei territori in cui ha delle sedi fisiche. Nel caso le piattaforme non dovessero attenersi a tali regolamenti, potrebbero subire delle ripercussioni finalizzate ad ostacolarne l'attività in determinate giurisdizioni. C. Barabas, N. Narula e E. Zuckerman, nel loro articolo *Defending Internet Freedom through Decentralization: Back to the Future?,* riportano a questo proposito un caso che ha coinvolto Facebook nel 2016. In quell'occasione il social network di Mark Zuckerberg aveva deciso di censurare per gli utenti della Tailandia le pagine satiriche sulla famiglia reale del Paese. La piattaforma, così come altri siti, aveva infatti subito pressioni da parte del governo nazionale affinché si conformasse alla legge che vietava la diffamazione della famiglia reale, bloccando i contenuti ritenuti «"una minaccia per la pace e

[194] *V.* Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, pp. 1, 16.

l'ordine"»[195] della nazione. Tuttavia, decisioni come questa rappresentano una sfida importante per i servizi centralizzati, poiché possono andare a costituire un precedente, che porti poi ad ulteriori richieste da parte delle autorità di regolamentazione nazionale. Dall'altro lato, il rifiuto di un adeguamento alle leggi locali può determinare lo sviluppo di reazioni che ostacolino la libera attività nei territori in questione. Ad esempio, in Cina il governo ha istituito un *firewall* che permette la selezione dei siti visibili agli utenti e propone un ecosistema di servizi alternativi a quelli di piattaforme mondiali come Google e Facebook[196]. È importante specificare, inoltre, che queste situazioni non sono limitate a territori in cui la legge è particolarmente incisiva sulla libertà dei cittadini. Come proposto sempre nell'articolo citato, ad esempio, negli Stati Uniti si sono verificate diverse occasioni in passato nelle quali ai servizi online è stato richiesto di rimuovere determinati contenuti che ritraevano scene di violenza o omicidio ad opera della polizia. In merito a ciò si tiene a ripetere che quello che mette le piattaforme in una simile posizione è il fatto che siano centralizzate e che quindi vi sia una leadership definita che permette ai governi di avere un soggetto a cui rivolgersi. In aggiunta, tali servizi hanno effettivamente la capacità di controllo e di intervento sui contenuti che diffondono e pertanto sono potenzialmente in grado di ottemperare ad eventuali richieste da parte delle autorità di regolamentazione[197].

Un secondo ostacolo determinato dall'attività delle piattaforme centralizzate nei confronti della libertà di espressione ed informazione è relativo ai possibili effetti dei bias incorporati negli algoritmi di selezione dei contenuti. In questo caso quindi non si tratta di una censura direttamente perpetrata, ma di un meccanismo indiretto. In particolare, i sistemi di ottimizzazione del contenuto all'interno di

---

[195] Katrina Pascual, *Thailand Military Government To Pressure Facebook, Line To Censor Content*, in "Tech Times", 3 febbraio 2016, in Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 16.

[196] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 11.

[197] V. Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, pp. 17-18.

servizi come Facebook tendono ad incentivare i materiali virali e più piacevoli per il pubblico, spesso a discapito di informazioni di maggiore apporto divulgativo. Ciò fa sì che ad esempio in un contesto elettorale una forza politica possa sfruttare tale funzionamento degli algoritmi per incentivare l'esposizione degli utenti ai contenuti a proprio sostegno, a discapito dei messaggi delle forze concorrenti e perciò in violazione della disciplina per la propaganda elettorale nei media tradizionali. Si procederà ad approfondire l'influenza delle grandi piattaforme sul discorso pubblico nel paragrafo dedicato. Quello che si vuole evidenziare in questa sede è come stia crescendo la preoccupazione per gli effetti degli algoritmi di personalizzazione all'interno dell'infosfera, con la somministrazione agli utenti di contenuti che confermano e sostengono e loro preferenze e convinzioni, a scapito della copertura degli eventi basata sui fatti[198]. Ciò in particolare ha sollevato l'attenzione sulla manifestazione di pregiudizi involontari nei meccanismi di selezione delle informazioni, i quali indirettamente comportano la censura di altri materiali.

Infine, vi è una terza modalità con cui le grandi piattaforme possono intralciare il pieno godimento per gli utenti del diritto alla libertà di espressione e si tratta dell'abuso del potere di cura dei contenuti. Questo consiste, come si può intuire, nella volontaria censura di informazioni da parte dei servizi stessi per diversi motivi. Ad esempio, C. Barabas, N. Narula e E. Zuckerman riportano l'occasione in cui alcuni anonimi ex-dipendenti di Facebook hanno rivelato che il social network avrebbe sistematicamente fatto rimuovere al suo staff le notizie di stampo conservatore dalla sezione dei contenuti di tendenza, anche se classificati dagli algoritmi come *hot topic*[199]. Non si tratta quindi di una vera e propria eliminazione di tali informazioni dalla piattaforma, ma, nel contesto dell'*information overload* e dell'*attention economy*, l'esclusione dai contenuti di tendenza comporta lo stesso

[198] *Ivi*, p. 19.
[199] *Ivi*, p 21.

risultato[200]. Indipendentemente dal fatto che nel caso citato Facebook abbia sostenuto che non ci fossero prove a sostegno delle accuse ricevute, ciò che è rilevante è che per un utente sarebbe per lo più impossibile individuare eventuali interventi ad opera delle piattaforme. Queste ultime, infatti, non sono soggette ad alcun obbligo di rivelare i meccanismi che assegnano la priorità ai contenuti, anche perché spesso gli algoritmi si ritengono tutelati dalla proprietà intellettuale[201].

Tali sviluppi suscitano crescenti preoccupazioni, poiché la base di utenza delle grandi piattaforme è tale che anche una minima influenza su di essa potrebbe condizionare il risultato di importanti eventi civici quali le elezioni. Storicamente, i principali organi di stampa sono regolamentati da atti governativi che garantiscono il rispetto del principio dell'interesse pubblico. Con la crescente influenza delle fonti di informazione online è opportuno chiedersi se tali regolamenti debbano essere estesi anche a quest'area. In ogni caso è importante evidenziare come, per poter applicare il concetto di responsabilità pubblica alle grandi piattaforme, sia necessario comprendere come queste ultime esercitino il loro potere di cura dei contenuti. La tutela del diritto di libera espressione nel contesto dei servizi centralizzati implica quindi maggiore trasparenza. Tuttavia, quest'ultima non è un concetto facilmente applicabile agli algoritmi, i quali sono costituiti da «pezzi di codice complessi e viventi che si evolvono nel tempo»[202].

Si è visto fin qui come l'attività di cura dei contenuti ad opera delle grandi piattaforme rappresenti una minaccia alla libertà di espressione sotto diversi aspetti. È possibile presupporre, quindi, che si voglia sostenere l'assoluta garanzia di tale diritto all'interno di questi sistemi. Tuttavia, come si procederà ad evidenziare nel prossimo paragrafo, la libertà di espressione comporta anche delle derive patologiche e il potenziale deterioramento della qualità del discorso online.

---

[200] *V.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[201] V. Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 22.

[202] *Ivi*, p. 20.

3.2) Le derive della libera espressione

Si è sostenuto fin qui che le piattaforme debbano essere responsabili del rispetto della libera espressione, al di là delle ripercussioni dei meccanismi algoritmici evidenziate. È importante sottolineare che tale diritto comprende anche conversazioni potenzialmente offensive o disturbanti, come sostenuto dal Comitato per i Diritti Umani delle Nazioni Unite[203]. A questo proposito, la Convenzione Internazionale sui Diritti Civili e Politici prescrive agli Stati di proibire solo «"qualsiasi difesa dell'odio nazionale, razziale o religioso che costituisca incitamento alla discriminazione, all'ostilità o alla violenza"»[204]. In questo modo molte altre forme di espressione discutibili rimangono escluse da una limitazione normativa. Nel contesto delle piattaforme ciò risulta nella promozione e amplificazione di contenuti offensivi, discriminatori o carichi di odio. Si è già visto, infatti, come uno degli obiettivi dell'implementazione di algoritmi di cura e selezione delle informazioni sia l'*engagement*, ovvero l'aggancio dell'utente affinché massimizzi il tempo trascorso fruendo di un dato servizio online. A tale scopo, il tipo di materiale che maggiormente crea coinvolgimento è quello sensazionalista e provocatorio. Come recita un modo di dire inglese, infatti, "*if it bleeds, it leads*", ovvero ciò che sanguina e quindi che crea scandalo, attira. In questo senso, poiché gli algoritmi di raccomandazione sono programmati per agevolare i contenuti maggiormente in grado di agganciare l'utente, le piattaforme possono determinare la creazione di cosiddette «"tane del coniglio"»[205] di materiale tossico per la qualità del discorso online. Ciò conferma quanto sostenuto dal CEO di Twitter Jack Dorsey e già riportato, ovvero che «la centralizzazione […] agevola un meccanismo non virtuoso per il quale si sarebbe portati a "focalizzare l'attenzione su contenuti e

---

[203] *Cfr.* Comitato per i Diritti Umani delle Nazioni Unite, *General Comment No. 34*, Article 19, CCPR/C/GC/43, 2011, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 34.

[204] *Convenzione Internazionale sui Diritti Civili e Politici*, art. 20, 16 dicembre 1966, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 34.

[205] Kevin Roose, *The Making of a YouTube Radical*, in "The New York Times", June 2019, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 34.

conversazioni che generano polemiche e indignazione, piuttosto che conversazioni che informano e promuovono la conoscenza"»[206]. Emblematica in questo senso è una riflessione di Mark Zuckerberg su delle ricerche condotte in merito ai meccanismi che alimentano la piattaforma di Facebook. Secondo il fondatore del più grande social network al mondo, infatti, non importa dove venga tirata la linea di ciò che è consentito: più un contenuto si avvicina a tale linea, più le persone sono mediamente interessate da esso[207]. Indignazione e paura sono infatti due emozioni che determinano un aumento del coinvolgimento degli utenti. Quest'ultimo è perseguito poiché alimenta il business della pubblicità e di conseguenza le entrate delle piattaforme: l'advertising targettizzato, infatti, risulta più efficace affinché gli individui clicchino sugli annunci e la personalizzazione si ottiene dall'analisi dei dati personali prodotti dall'interazione con i servizi online.

Il business della sorveglianza, pertanto, fa sì che i soggetti responsabili della diffusione di informazioni ed idee si basino su meccanismi in contrasto con un ambiente favorevole alla diversità dei media e all'autonomia delle voci. Il sensazionalismo ha sempre caratterizzato il contesto mediatico, tuttavia gli algoritmi di raccomandazione delle piattaforme tendono a privilegiare sistematicamente contenuti estremi che vanno anche oltre il limite tollerato. Mike Masnick, nel suo saggio già citato, riferisce come «alcuni ritengano che queste piattaforme siano diventate pozzi neri di *trolling*, intolleranza e odio»[208]. Queste ultime sono solo alcune delle derive patologiche del web e del meccanismo delle piattaforme centralizzate che alimenta lo sviluppo di contenuti offensivi e sensazionalisti. La rete e, in particolare, i contesti implementati dagli algoritmi di raccomandazione, infatti, risultano contaminati sempre più da comportamenti definiti "abusivi". Si tratta di

---

[206] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[207] *Cfr.* Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement*, in "Facebook", novembre 2018, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 34.

[208] Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

atteggiamenti difficilmente individuabili, poiché estremamente dipendenti dal contesto in cui si manifestano. In ogni caso rientrano in tale definizione numerose categorie di attività, delle quali Masnick nomina le molestie, i discorsi d'odio, le minacce, il *trolling*, i contenuti osceni, il *doxing* e lo spam importuno[209]. Molti di questi termini risultano intuitivi, per questo motivo si procederà ora a precisare il significato solo di alcuni dei comportamenti nominati. In particolare, i discorsi d'odio, altrimenti noti come *hate speech*, si riferiscono all'utilizzo strategico di contenuti o espressioni mirati a «diffondere, propagandare o fomentare l'odio, la discriminazione e la violenza per motivi etnici, nazionali, religiosi, o fondati sull'identità di genere, sull'orientamento sessuale, sulla disabilità, o sulle condizioni personali e sociali»[210]. Il *trolling*, invece, consiste nell'attività di utenti della rete che entrano a far parte di una comunità, un gruppo o semplicemente una conversazione con lo scopo di causare interruzioni, innescare o esacerbare conflitti, provocare gli altri partecipanti al solo fine del proprio divertimento[211]. Il *doxing*, infine, si definisce come «il rilascio pubblico intenzionale su Internet di informazioni personali su un individuo da parte di terzi, spesso con l'intento di umiliare, minacciare, intimidire o punire l'individuo identificato»[212].

Realtà come i social network spesso definiscono delle policy che individuano quali atteggiamenti sono tollerati all'interno di una data piattaforma. Per questo motivo verrà proposto ora l'insieme di regole delineate da Twitter per approcciare quelli che all'interno del social network fondato da Jack Dorsey sono considerati comportamenti abusivi. Innanzitutto, una definizione generale di questi ultimi comprende per Twitter i tentativi di molestare, intimidire o mettere a tacere la voce di qualcun altro. Andando poi nello specifico le regole della piattaforma individuano quattro principali categorie di attività non tollerate: il desiderio o la

---

[209] *Ibid.*

[210] Maria Novella Campagnoli, *Informazione, social network & diritto: Dalle fake news all'hate speech online. Risvolti sociologici, profili giuridici, interventi normativi*, Kindle ed., Milano, Key Editore S.r.l., novembre 2020, posizione 1604.

[211] *Cfr.* Claire Hardaker, *Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions*, in "Journal of Politeness Research", 6 (2010), pp. 215-242.

[212] David M. Douglas, *Doxing: a conceptual analysis*, in "Ethics Inf Technol", 18 (2016), pp. 199-210.

speranza di danneggiare gravemente una persona o un gruppo di persone; proposte sessuali indesiderate; l'impiego di insulti aggressivi allo scopo di molestare o intimidire gli altri; infine, l'incoraggiamento di altri a molestare un individuo o un gruppo di persone. Queste quattro definizioni sono poi ulteriormente puntualizzate da delle descrizioni e da singoli comportamenti ritenuti abusivi nel dettaglio. In particolare, secondo la policy di Twitter, nella prima categoria rientrano i contenuti che esprimono desiderio o speranza di morte, lesioni personali gravi o malattie mortali contro un individuo o un gruppo di persone. Alcuni esempi inclusi in questa tipologia riguardano sperare che qualcuno muoia a causa di una grave malattia, desiderare che una persona cada vittima di un grave incidente o, ancora, affermare che un gruppo di individui meriti gravi lesioni fisiche[213]. La seconda categoria di comportamenti abusivi attiene ad avances sessuali indesiderate e contenuti che oggettivizzano sessualmente un individuo senza il suo consenso. Alcune attività comprese in queste definizioni consistono nell'inviare a qualcuno contenuti multimediali per adulti non richiesti o indesiderati, nel dare origine a discussioni sessuali indesiderate sul corpo di qualcuno, nella sollecitazione di atti sessuali e, in generale, nella creazione di qualsiasi contenuto che sessualizzi un individuo senza il suo consenso[214]. La terza categoria viene specificata come comportamenti eccessivamente aggressivi che prendono di mira un soggetto, inclusi i contenuti che contengono insulti o linguaggio simile. Infine, la quarta tipologia di atteggiamenti non tollerati dalla policy di Twitter riguarda l'incoraggiamento di altre persone a molestare o prendere di mira individui o gruppi specifici con comportamenti offensivi. Quest'ultima definizione si estende anche al contesto offline, poiché specifica che sono compresi non solo gli inviti a prendere di mira le persone con abusi o molestie online, ma anche i comportamenti che sollecitano un'azione offline come molestie fisiche[215].

[213] *Cfr.* Twitter, Abusive behavior, in "Twitter" (https://help.twitter.com/en/rules-and-policies/abusive-behavior, consultato il 5 novembre 2020).
[214] *Ibid.*
[215] *Ibid.*

Non si procederà oltre ad approfondire le molte e varie derive patologiche del web e, in particolare, degli algoritmi di raccomandazione delle piattaforme centralizzate che alimentano lo sviluppo di contenuti abusivi e offensivi online. Si è voluto fin qui specificarle per evidenziare come la libertà di espressione abbia dei limiti, i quali devono attenere al rispetto di altre libertà e prerogative fondamentali dell'individuo. Nel contesto dei servizi centralizzati, infatti, questo particolare tipo di contenuti sensazionalisti suscita spesso nell'utenza la richiesta di interventi di censura da parte dell'autorità di riferimento. Come afferma Mike Masnick, il controllo implica responsabilità ed è quest'ultima che i consumatori dei servizi online pretendono dalle piattaforme[216]. Tuttavia, si è già discusso come le attività di censura comportino a loro volta delle difficoltà e soprattutto delle implicazioni che minacciano il pieno godimento del diritto alla libertà di espressione da parte degli utenti. Per questo motivo, nel prossimo paragrafo si procederà ad evidenziare come le piattaforme centralizzate si trovino paralizzate nella ricerca di un compromesso fra queste due diverse ed opposte esigenze degli individui che fruiscono del loro servizio. Inoltre, verrà proposto un approccio risolutivo di tale *impasse* che prevede niente meno che la decentralizzazione.

3.3) La ricerca di un compromesso

Sono state fin qui affrontate due particolari questioni fra loro opposte che pongono le piattaforme centralizzate in una situazione di *impass*. Nello specifico, si è evidenziato come, da un lato, il business della sorveglianza e gli algoritmi che lo sostengono alimentino un contesto all'interno dei servizi online che pone a rischio il godimento della libertà di espressione da parte degli utenti. Dall'altro lato, si è discusso come quest'ultima prerogativa, se non opportunamente limitata, possa determinare lo sviluppo di comportamenti lesivi dell'individuo sotto altri punti di

[216] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

vista. Le grandi piattaforme centralizzate devono quindi affrontare oggi la necessità dell'individuazione di un compromesso fra queste due forze opposte.

In particolare, la prima questione, come si è visto, deriva dalla capacità d'intervento dei servizi online centralizzati sui contenuti prodotti dai propri utenti. Tale possibilità genera crescente preoccupazione nei confronti dei provider delle piattaforme per quanto riguarda la loro responsabilità nella raccomandazione, nel controllo e nell'eventuale blocco delle informazioni. In questo contesto, le scelte di moderazione operate dai colossi del web sono costantemente oggetto di critiche. In primo luogo, infatti, risultano sicuramente scontenti gli utenti il cui contenuto viene censurato o bloccato. Parallelamente, anche i soggetti interessati a fruire o condividere quel materiale possono manifestare dispiacere o frustrazione. Fra i timori e le accuse rivolte ai responsabili delle piattaforme, ad esempio, ricorre il sospetto che gli interventi sui contenuti siano influenzati dal pregiudizio politico[217].

Contemporaneamente, da più parti si invoca la necessità di una maggiore proattività nella cura e nel controllo delle informazioni condivise all'interno delle grandi piattaforme, in particolare per quanto riguarda i comportamenti abusivi. Sia gli utenti, sia le autorità di regolamentazione, infatti, sono consapevoli della nocività di tale tipologia di contenuti. La difficoltà sta nell'individuare una conclusione unanime su quali atteggiamenti rientrino effettivamente in tale definizione. Come si è visto, sono numerose e differenti le categorie di comportamenti e attività che comportano la minaccia, la molestia, l'intimidazione o altri atti che turbino o violino l'individualità delle persone. In aggiunta, uno stesso atteggiamento può assumere un significato e un livello di tolleranza completamente diverso in relazione al contesto in cui si manifesta. Ad esempio, offese e volgarità possono trasformarsi in beffeggiamenti ironici in una conversazione colloquiale. O, ancora, un dato comportamento può essere percepito in modo differente a seconda del destinatario della comunicazione. Come spiega Mike Masnick, per esempio, il tentativo di una

[217] *Ibid.*

persona di esprimere un'opinione con forza può essere visto come una molestia da un determinato individuo[218]. Ad eccezione dei contenuti che sono normativamente riconosciuti come non tutelati dalla libertà di espressione, infatti, qualsiasi informazione o messaggio necessita di un'interpretazione e un'analisi del contesto per valutarne la tollerabilità. Tuttavia, «lasciare che ogni piattaforma giudichi tali cose è un compito impossibile, specialmente quando si tratta di centinaia di milioni di contenuti al giorno»[219].

Tutto ciò, quindi, pone i responsabili dei servizi online centralizzati in una posizione particolarmente scomoda, poiché qualsiasi decisione di moderazione determina lo scontento di qualcuno. Gli algoritmi o, in generale, i meccanismi di classificazione sono soggetti a due tipologie di errore: il falso positivo e il falso negativo[220]. Per quanto riguarda il sistema di controllo e selezione dei contenuti all'interno di una piattaforma, il primo consiste nel classificare come illecita e rimuovere un'informazione ritenuta invece tollerabile da molti utenti, che risulteranno pertanto infastiditi da tale intervento. Il caso del falso negativo, d'altra parte, comporta che non venga censurato un contenuto che disturba una grande quantità di persone[221].

In un simile contesto è importante specificare, quindi, che per approcciare tale situazione in modo da scontentare il minor numero possibile di soggetti, le piattaforme centralizzate sono costrette ad intervenire sempre di più per ottimizzare i loro sistemi di moderazione. Questi ultimi, in particolare, sono attivati da due insiemi di "attori", gli algoritmi da un lato e squadre di addetti umani dall'altro. Per questo motivo i responsabili dei servizi online seguitano ad investire consistentemente nello sviluppo di soluzioni tecnologiche per la classificazione dei contenuti e ad assumere migliaia di impiegati che approccino il problema da un punto

---

[218] *Ibid.*

[219] *Ibid.*

[220] Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, p. 25.

[221] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

di vista "umano". Gli algoritmi, infatti, per quanto ben sviluppati, non sono in grado di individuare elementi caratteristici della comunicazione interpersonale, come l'ironia, la satira o l'iperbole, che dipendono dal contesto o dall'intento degli interlocutori. Contemporaneamente, tuttavia, anche per i moderatori umani risulta complesso considerare il contesto di una conversazione, in parte perché tendenzialmente non hanno accesso all'insieme dei messaggi per una questione di privacy, in parte perché il tempo richiesto da un'analisi antropica di ogni situazione non è conveniente in termini di efficienza[222].

Come sostiene Barbara Calderini nel suo articolo *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, quindi, «l'approccio tradizionale alla moderazione finirebbe inevitabilmente per creare delle diseconomie di scala»[223]. Lo stesso Jack Dorsey nell'annunciare l'interesse di Twitter in un progetto decentralizzato ha rivelato che «"i social network crescono e con l'incremento della partecipazione aumenta anche l'esigenza di far fronte a fake news ed hate speech, ci si trova così a dover impegnare ingenti risorse economiche e umane in uno sforzo che prevede investimenti con ritorni limitati"»[224].

3.4) Decentralizzazione della responsabilità

Anche in questo contesto si propone un approccio alla problematica evidenziata che prevede la decentralizzazione. Come si ha già più volte avuto modo di spiegare, infatti, quest'ultima modifica il concetto di *service provider*, poiché viene a mancare la figura dell'unico soggetto responsabile, alla quale si sostituisce una rete di nodi pari fra loro, i quali condividono il compito di garantire le funzionalità

[222] *Ibid.*

[223] Barbara Calderini, op. cit., in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[224] Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106) in Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

necessarie per azionare il sistema[225]. In una piattaforma decentralizzata, quindi, anche la competenza della moderazione del contenuto viene trasferita dal centro alla periferia della rete, ovvero ai suoi singoli componenti. Invece di avere un unico soggetto proprietario che stabilisce le regole di ciò che è ammesso e ciò che non lo è all'interno del suo *walled garden*, ogni utente può decidere a cosa accedere in base ai propri interessi e alla propria sensibilità. Tuttavia, poiché è auspicabile che i singoli individui non intendano esercitare manualmente e personalmente la selezione delle informazioni, il contesto decentralizzato fa sì che soggetti agenti come terze parti possano farsene carico sviluppando filtri, interfacce o altri sistemi che rispecchino le diverse preferenze e i livelli di tolleranza dell'utenza[226].

Per rendere più comprensibile lo scenario delineato si provvederà ora a riportare un esempio proposto da Mike Masnick nel suo saggio già citato. La posta elettronica, infatti, insiste su un sistema simile, nel senso che è implementata da protocolli aperti, come SMTP, POP3 e IMAP. Questi garantiscono un elevato grado di flessibilità, perché, ad esempio, permettono ad un utente che ha un indirizzo Gmail - il servizio di posta elettronica di Google - di accedervi attraverso l'interfaccia di Outlook - il corrispettivo di Microsoft - o viceversa. Oppure, ancora, è possibile creare nuove interfacce partendo da quella di Gmail stessa, ad esempio mediante un'estensione di Chrome[227].

Ciò che si vuole evidenziare è che un simile sistema garantisce numerosi vantaggi dal punto di vista del consumatore. Innanzitutto, grazie ai software *open-source*, ai protocolli comunicativi e alla distribuzione del database - che si è visto essere gli elementi costitutivi di un servizio decentralizzato[228] - chiunque è

---

[225] *Cfr*. Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 351.

[226] *Cfr.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[227] *Ibid.*

[228] V. Marvin Ammori, *The Coming Decentralized Decade*, in "Morning Consult", 6 gennaio 2020 (https://morningconsult.com/opinions/the-coming-decentralized-decade/, consultato il 14 giugno 2020).

potenzialmente in grado di sviluppare una propria interfaccia o dei filtri personalizzati per accedere al comune corpus di dati condiviso fra i nodi della rete e mantenuto al sicuro grazie alla crittografia e a tecnologie come la blockchain. Dal punto di vista della questione della moderazione dei contenuti, ciò fa sì che gli utenti possano impiegare i software che preferiscono in base alla propria sensibilità e ai propri interessi. In un simile contesto, quindi, viene a mancare il soggetto responsabile di errori falsi positivi o falsi negativi nella classificazione delle informazioni, perché non vi è limite alla libertà di espressione, ma piuttosto una moltitudine potenzialmente illimitata di filtri che riflettano i diversi livelli di tolleranza degli individui.

Inoltre, tale architettura permette di evitare anche il meccanismo del *lock-in*, poiché i dati di un singolo soggetto non sono vincolati alla piattaforma in cui vengono generati, ma sono decentralizzati e cambiando interfaccia si modifica solo l'intermediario tecnologico con cui vi si accede[229]. Ciò rappresenta la base per un ecosistema ad alta competizione, grazie anche alla riduzione dei costi di innovazione garantita dalla possibilità di intervenire su strumenti *open-source* e aggiungere o modificare funzionalità senza dover ricostruire l'intera esperienza di una data piattaforma[230]. La varietà dei servizi offerti e l'annientamento dei costi di passaggio da un'implementazione ad un'altra, quindi, fanno sì che l'utente sia libero di preferire continuamente un nuovo intermediario tecnologico. Ciò, a sua volta, determina che le terze parti che implementano tali funzionalità siano incentivate a offrire il miglior servizio possibile - più aggiornato, meglio performante e *user-friendly* - in modo da ottenere il favore degli utenti, affinché non scelgano implementazioni concorrenti. Nel contesto centralizzato, al contrario, il passaggio da una piattaforma ad un'altra comporta ingenti costi per gli individui, come si è visto,

[229] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[230] *Cfr.* Marvin Ammori, *The Coming Decentralized Decade*, in "Morning Consult", 6 gennaio 2020 (https://morningconsult.com/opinions/the-coming-decentralized-decade/, consultato il 14 giugno 2020).

poiché determina la perdita di tutti i dati, compresa la rete di contatti instaurati. Si crea così un effetto di *lock-in*, che, a sua volta, fa sì che i servizi accentrati non debbano costantemente cercare di conquistare gli utenti offrendo loro servizi che meglio rispondano alle loro esigenze. Inoltre, la posizione di monopolio delle grandi piattaforme nel mercato di riferimento determina pressoché l'annullamento delle dinamiche competitive[231].

La decentralizzazione incentiva l'innovazione e la competizione anche per quanto riguarda lo sviluppo di implementazioni dei servizi esistenti. Nel contesto delle grandi piattaforme, infatti, soggetti come Twitter e Facebook hanno la tendenza ad escludere dai propri ecosistemi le applicazioni di terze parti a seconda dei cambiamenti che introducono ai propri prodotti. Al contrario, con la decentralizzazione, appunto, risulta incentivato il mercato dei servizi aggiuntivi, grazie alla minore dipendenza da un'unica piattaforma che potrebbe improvvisamente rimuoverli[232].

Riportando il focus sulla questione della moderazione dei contenuti, in un contesto decentralizzato come quello appena delineato ogni utente ha la possibilità di scegliere o persino sviluppare la propria interfaccia per approcciare l'intero corpus di contenuti distribuito nella rete. Il che significa che non vi sono più le grandi piattaforme centralizzate a svolgere il ruolo di unico arbitro del sistema, capace di determinare cosa è ammesso e cosa no, o persino a chi è concesso di esprimersi[233]. La piena libertà di parola garantita da un simile meccanismo può far sorgere preoccupazioni per quanto riguarda la moderazione di contenuti sensazionalisti, offensivi e abusivi. Tuttavia, come si è già detto, nel contesto decentralizzato la responsabilità e l'autorità delle scelte viene demandata alla periferia della rete, ovvero agli utenti[234]. Ciò fa sì che, grazie alla grande varietà di implementazioni offerte

---

[231] *V.* Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[232] *Ibid.*

[233] *Ibid.*

[234] V. Nathaniel Popper, *Twitter and Facebook Want to Shift Power to Users. Or Do They?*, in "The New York Times", 18 dicembre 2019 (https://www.nytimes.com/2019/12/18/technology/facebook-twitter-bitcoin-blockchain.html, consultato il 17 agosto 2020).

per interfacciare i contenuti, siano gli individui stessi a scegliere quelle che più rispecchiano la propria sensibilità e la propria tolleranza nei confronti dei diversi discorsi, senza censurare completamente qualcuno o che siano altri soggetti a scegliere per loro. Conseguentemente, se gli utenti optano per interfacce e filtri che tendono ad escludere contenuti importuni, la potenza e l'impatto di questi ultimi risultano automaticamente più limitati e confinati al pubblico che li tollera. In ogni caso, si tratta di un approccio democratico alla libertà di informazione e a quella di espressione, attraverso il quale nessuno viene pienamente silenziato e non risulta neppure violata la sensibilità delle persone grazie all'auto-moderazione delle informazioni con cui ci si interfaccia. In aggiunta, si è visto come nei sistemi centralizzati lo sviluppo di contenuti sensazionalisti sia alimentato dagli algoritmi di raccomandazione che agevolano i discorsi che più fanno presa sulla gente. Con la decentralizzazione, invece, viene a mancare anche questo meccanismo, poiché il mercato dei filtri consente una maggiore granularità nella selezione dei contenuti. «Piuttosto che il sistema centralizzato di oggi, dove tutte le voci sono più o meno uguali (o completamente bandite), in un mondo incentrato sui protocolli le opinioni radicali sarebbero semplicemente meno propense a raggiungere l'attenzione generale»[235].

Infine, vi è un'ultima caratteristica del contesto decentralizzato che può contribuire alla qualità del discorso online, senza necessità di moderazione o di censura accentrata dei contenuti. Si tratta della possibilità di remunerare in criptovalute gli utenti, nei cosiddetti *social incentivized*[236]. In particolare, i recenti progressi nella tecnologia della blockchain e dei ledger distribuiti rendono possibile l'eventualità di ricompensare i soggetti che all'interno di un servizio decentralizzato - ad esempio un social network - si occupano della creazione e della

[235] Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[236] *Cfr.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

raccomandazione di contenuti di alta qualità[237]. Ciò è permesso dallo sviluppo dei sistemi che implementano criptovalute o *token*, i quali possono essere assegnati come retribuzione - appunto - sia per i creatori di contenuti, come incentivo alla produzione di informazioni valevoli e veritiere, sia per gli elaboratori di interfacce, filtri e altri *tool* funzionali all'implementazione dell'architettura, affinché sviluppino sistemi performanti[238]. In questo modo si costruisce un modello di business che non favorisce i pochi e accentrati soggetti a capo delle piattaforme che traggono profitto dall'acquisizione dei dati dei propri utenti. Bensì si crea un sistema che riconosce ai produttori di contenuti il loro lavoro, andando anche a tutelare la proprietà intellettuale grazie al meccanismo di controllo delle transizioni e della condivisione delle informazioni[239].

4) Le piattaforme sociali nel dibattito pubblico

Si è visto fin qui come la centralizzazione alimenti il business della sorveglianza, il quale, a sua volta, rappresenta una minaccia per il pieno godimento degli utenti dei propri diritti alla privacy e alla libera espressione. Si è discusso, inoltre, come il sistema di algoritmi implementato dalle grandi piattaforme favorisca lo sviluppo di contenuti sensazionalisti e abusivi. A tutto ciò si è risposto proponendo un approccio basato sulla decentralizzazione, la quale, come si ha argomentato, rappresenta un'alternativa dal punto di vista tecnologico per contribuire ad affrontare i problemi evidenziati. Rimane da approfondire un'ultima grande questione che genera preoccupazione per quanto riguarda l'attività delle piattaforme centralizzate: la loro influenza nel dibattito pubblico.

---

[237] *Cfr.* Chao Li, Balaji Palanisamy, *Incentivized Blockchain-based Social Media Platforms: A Case Study of Steemit*, in *The 10th ACM Conference. Atti del convegno*, giugno 2019, pp. 145-154.

[238] Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

[239] *V.* Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, Krzysztof Rzadca, *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010, p. 358.

Come si ha già accennato, infatti, i colossi dei servizi online ricoprono un importante ruolo in quanto spazio di discorso pubblico. Sistemi come i social network aumentano la capacità di ogni individuo di ottenere informazioni, di sviluppare rapporti sociali e, in generale, rappresentano un mezzo fondamentale attraverso cui le persone esprimono il proprio pensiero. In questo senso le piattaforme costituiscono dei veri e propri attori all'interno della scena pubblica e politica. Per questo motivo suscitano particolari preoccupazioni gli effetti dei meccanismi e degli algoritmi che selezionano e raccomandano le informazioni fruite dagli utenti all'interno di questi sistemi.

4.1) Persuasione e manipolazione nella comunicazione politica

A questo proposito si procederà ora a riproporre il caso di Cambridge Analytica. Nella sezione di questo elaborato dedicata alla privacy si ha introdotto lo scandalo che ha coinvolto la società in questione e Facebook in una delle più grandi violazioni di dati nella storia del colosso del social networking fondato da Mark Zuckerberg. In tale contesto si ha voluto evidenziare l'ambiguità e la vulnerabilità dei termini delle policy che dovrebbero attenere alla protezione dei dati personali degli utenti all'interno delle piattaforme centralizzate. Inoltre, si ha posto attenzione al rischio di violazioni comportato dal commercio dei dati e, in particolare, alla difficoltà di mantenimento del controllo sulle informazioni condivise con soggetti terzi da parte dei servizi a cui vengono cedute e affidate. In questa sede, invece, si provvederà ad approfondire le circostanze al cui interno la violazione ha avuto luogo e a seguito delle quali la vicenda è stata comunemente definita come "scandalo".

Innanzitutto, si ha già accennato al fatto che Cambridge Analytica fosse una società di *data mining*, il che significa che si occupava di estrarre dati personali degli utenti dai social network, da applicazioni o altri servizi centralizzati, per poi farli elaborare da modelli e algoritmi di profilazione. Si tratta di un approccio simile a quello della psicometria, «il campo della psicologia che si occupa di

misurare abilità, comportamenti e più in generale le caratteristiche della personalità»[240]. In particolare, quest'ultima viene quantificata dalla psicologia attraverso un sistema di 5 tratti caratteriali: l'apertura a nuove esperienze, la consapevolezza, l'estroversione, la piacevolezza e la nevrosi. Nel 2012 un gruppo di scienziati dell'Università di Cambridge e della Stanford University ha avviato uno studio con l'obiettivo di individuare una relazione tra tali caratteristiche e le reazioni apposte dagli utenti ai contenuti all'interno dei social network. Una volta trovato il meccanismo di collegamento tra questi due elementi, gli scienziati sono stati in grado di costruire un algoritmo capace di dedurre la personalità di un individuo dai suoi "Mi piace" su Facebook[241]. Inoltre, uno studio successivo del 2014, condotto dallo stesso gruppo di ricercatori e guidato da Michal Kosinski, ha quantificato la conoscenza di una persona ottenibile dall'analisi di un certo numero di preferenze indicate da essa sui social. Sarebbero, infatti, sufficienti 70 "Like" applicati su Facebook da un utente per sapere più cose di tale individuo rispetto ai suoi amici. Con 150 reazioni si raggiungerebbe la conoscenza di un genitore e con 300 quella di un coniuge. Infine, una quantità ancora maggiore di "Mi piace" permetterebbe di comprendere i dettagli sulla personalità di un dato individuo meglio di quanto possibile al soggetto stesso[242]. Lo scopo di tali studi era capire come applicare queste informazioni agli annunci pubblicitari. Successivamente, i ricercatori hanno così sperimentato la pubblicazione sui social network di inserzioni mirate in base ai tratti caratteriali degli utenti.

Prima di proseguire con il collegamento tra le questioni descritte e le attività di Cambridge Analytica, si vuole aprire una parentesi sull'influenza di tali capacità di analisi e personalizzazione sull'individualità delle persone. In particolare, la raccomandazione dei contenuti e la targetizzazione della pubblicità attraverso l'applicazione di algoritmi comportano che le piattaforme come Google e Facebook

---

[240] Emanuele Menietti, *Il caso Cambridge Analytica, spiegato bene*, in "Il Post", 19 marzo 2018 (https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/, consultato il 30 ottobre 2020).

[241] *Cfr.* Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, p. 16.

[242] *Cfr.* Emanuele Menietti, *Il caso Cambridge Analytica, spiegato bene*, in "Il Post", 19 marzo 2018 (https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/, consultato il 30 ottobre 2020).

giochino un ruolo particolarmente rilevante nel dare forma all'esperienza degli individui online. In aggiunta, gli algoritmi rispondono allo scopo di trovare il miglior modo per spingere le persone verso particolari risultati, in base all'analisi delle loro caratteristiche personali. L'insieme di questi fattori fa sì che si possano influenzare e modificare i pensieri e le opinioni degli individui a tal punto da alterarne la capacità di compiere scelte autonome. In questo senso il tecno-sociologo Zeynep Tufecki descrive le piattaforme come «"architetture di persuasione"»[243], in quanto sistemi capaci di manipolare e influenzare i propri utenti. Questo complesso di meccanismi, come si è già visto, pone quindi a rischio i diritti alla libertà di pensiero, coscienza e religione, nonché le libertà di opinione e di espressione degli individui. Inoltre, il mercato dei dati fa sì che simili prerogative fondamentali della persona possano essere violate anche da altri attori che indirettamente accedono a tali modelli. Mentre, da un lato, la legge internazionale sui diritti umani sancisce che le libertà in questione sono protette incondizionatamente, dall'altro lato «"l'intersezione tra tecnologia e *content curation* solleva nuove domande sui tipi di coercizione o incentivo che possono essere considerati un'interferenza con il diritto di formare un'opinione"»[244], come spiegato dallo Special Rapporteur delle Nazioni Unite. Si vuole sottolineare ancora una volta, quindi, come la persuasione algoritmica possa essere applicata in modo granulare, inconscio e personalizzato a tal punto da esercitare effetti significativi sull'autonomia cognitiva degli individui e sul loro diritto a formare la propria opinione e a prendere decisioni indipendenti[245].

Il contesto più evidente in cui può essere fatto cattivo uso delle capacità di profilazione e targetizzazione degli utenti da parte delle grandi piattaforme è quello della comunicazione politica. A questo proposito, il caso che recentemente ha

---

[243] Zeynep Tufekci, *We're building a dystopia just to make people click on ads*, in "TEDGlobal", settembre 2017, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 30.

[244] David Kaye, *Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression report to the UN General Assembly*, A/73/348, para. 24, 29 agosto 2018, in Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 30.

[245] *Cfr.* Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 30.

suscitato maggiore scalpore è proprio lo scandalo che ha coinvolto Facebook e Cambridge Analytica. Nella sezione di questo elaborato dedicata alla privacy si è già provveduto a spiegare come la società di *data mining* in questione fosse riuscita a venire illegalmente in possesso dei dati di milioni di utenti del noto social network. Si procederà ora ad analizzare l'utilizzo che di tali informazioni è stato fatto. In particolare, Cambridge Analytica stessa vantava come propria abilità quella di poter influenzare gruppi targettizzati della popolazione attraverso la creazione di profili di personalità straordinariamente dettagliati e la successiva personalizzazione dei messaggi politici sulla base di tali modelli[246]. La costruzione di questi ultimi, ovviamente, era subordinata al possesso di enormi quantità di dati, che la società otteneva dall'attività di *mining* o acquistandoli dai *data broker* - aziende che raccolgono e comprano informazioni personali per poi aggregarle e creare profili sugli utenti il più possibile completi, che in seguito vengono rivenduti[247]. L'acquisizione illecita dei dati degli utenti di Facebook, pertanto, ha permesso a Cambridge Analytica di aggiungere al proprio database ulteriori rilevanti informazioni.

L'insieme di dati così raccolti e la creazione di profili psicometrici da essi ottenuta sono stati in seguito applicati dalla società di *data mining* in due contesti di comunicazione politica particolarmente rilevanti: la campagna elettorale di Donald Trump per le presidenziali del 2016 e quella referendaria a favore della Brexit. Nel primo caso, in particolare, Cambridge Analytica era legata al futuro presidente degli Stati Uniti attraverso importanti rapporti con alcuni dei suoi più stretti collaboratori. Fondatore della società di *data mining* era Robert Mercer, miliardario imprenditore di stampo conservatore e, inoltre, finanziatore del sito d'informazione di estrema destra *Breitbart News*, diretto da Steve Bannon. Quest'ultimo era il manager della campagna elettorale di Donald Trump e precedentemente era stato vicepresidente di Cambridge Analytica stessa. Conseguentemente a tale insieme di contatti, nel 2016 alla società fu affidata la gestione della raccolta dati per la

[246] *Ivi,* p. 32.
[247] *V.* Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, p. 13.

campagna elettorale[248]. Per quanto riguarda, invece, il referendum britannico, secondo l'inchiesta condotta nel maggio 2017 da *The Guardian*, il comitato del *Leave* - il gruppo a favore della Brexit - sarebbe stato in contatto con Cambridge Analytica attraverso figure quali Robert Mercer, Steve Bannon e lo stesso Trump. Il contributo della società alla campagna referendaria avrebbe riguardato la raccolta dei dati e delle informazioni sugli utenti, per condurre una propaganda microtargettizzata e condizionare l'opinione degli elettori a favore dell'uscita del Regno Unito dall'Unione Europea. Ulteriori particolari di entrambe le vicende sono stati analizzati e ipotizzati da molti, al punto che le indagini per stabilire definitivamente il flusso degli eventi sono tuttora in corso. Nelle parole di Emanuele Minietti, autore dell'articolo *Il caso Cambridge Analytica, spiegato bene*: «In tutta questa vicenda al momento ci sono moltissimo fumo e indizi che qualcosa sia effettivamente bruciato, ma nessuno ha ancora trovato l'arrosto»[249]. Tuttavia, l'insieme dei fatti ha posto l'attenzione su delle questioni fondamentali.

Innanzitutto, è importante evidenziare come la percezione della propaganda politica mirata da parte delle persone sia viziata da un'asimmetria. Ogni individuo, infatti, è convinto di compiere le proprie scelte autonomamente e di essere immune alla manipolazione. Allo stesso tempo, comunque, le persone sono ormai relativamente consapevoli che gli annunci e i contenuti letti sui social network hanno la capacità di fare leva sui gusti e sulle emozioni degli utenti. Ogni individuo però è portato a pensare che tali tecniche di persuasione e manipolazione facciano breccia solo sugli altri, poiché è naturale non ritenere sé stessi ingenui. Gli studi e gli esperimenti, tuttavia, rivelano che per quanto un soggetto possa reputarsi immune alla manipolazione emotiva, è probabile che non lo sia[250]. In particolare, la sfera emozionale risulta essere una tipica scorciatoia cognitiva impiegata dagli elettori nelle

---

[248] V. Marco Lo Conte, *Chi è e cosa fa Cambridge Analytica, la società che ha inguaiato Facebook*, in "Il Sole 24 ore", 20 marzo 2018 (https://www.ilsole24ore.com/art/chi-e-e-cosa-fa-cambridge-analytica-societa-che-ha-inguaiato-facebook-AETt4mJE?refresh_ce=1, consultato il 31 ottobre 2020).

[249] Emanuele Menietti, *Il caso Cambridge Analytica, spiegato bene*, in "Il Post", 19 marzo 2018 (https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/, consultato il 30 ottobre 2020).

[250] Cfr. Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, p. 17.

scelte di voto. Secondo le neuroscienze, infatti, i messaggi razionali hanno molte meno possibilità di attivare i circuiti neurali che presiedono al comportamento di voto. Al contrario, le comunicazioni più efficaci sono proprio quelle che ad elementi cognitivi associano contenuti che suscitano speranza, paura, rabbia o disprezzo[251].

In aggiunta, oltre alla manipolazione emotiva, influisce sulla capacità di scelta degli individui anche il loro isolamento all'interno di esperienze altamente personalizzate della rete, confezionate su misura sulla base di deduzioni e profili ricavati algoritmicamente. In particolare, il micro-targeting dei messaggi ostacola la libera espressione delle persone confinandole in una visione del mondo curata e «inospitale per il discorso politico pluralistico»[252]. Ciò rimanda alla già accennata questione delle bolle dei filtri. Eli Pariser introduce questo concetto nel suo testo omonimo ed espone come il sistema degli algoritmi che alimentano le piattaforme centralizzate costruisca delle bolle invisibili, all'interno delle quali gli utenti fruiscono di un universo di informazioni specifico per ciascuno di loro[253]. Tuttavia, all'interno di una simile esperienza personalizzata, la sfera pubblica, ovvero il contesto in cui vengono individuati i problemi comuni per cercare di risolverli, perde rilevanza[254]. In particolare, Dean Eckles, teorico della profilazione a fini pubblicitari, definisce l'ambiente all'interno del quale un utente è immerso nella sua esperienza online come "mondo amico". Gli algoritmi delle grandi piattaforme sono programmati per favorire i contenuti che ricevono più "Mi Piace", più "Like", ovvero le notizie più piacevoli. Come spiega Eli Pariser, è difficile che la propria visione del mondo venga scossa da ciò a cui si accede attraverso un *news feed* personalizzato. Ciò che spaventa è che fra gli effetti collaterali del "mondo amico" vi è la scomparsa dei problemi di maggiore interesse pubblico. Questo si verifica poiché generalmente, «le questioni complesse che non hanno una rapida

---

[251] V. Marco Caciotto, *Il Nuovo Marketing Politico, Vincere le elezioni e governare al tempo della politica veloce*, Bologna, Società editrice Il Mulino, 2019, p. 150.

[252] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 31.

[253] *Cfr.* Eli Pariser, *Il Filtro*, Milano, il Saggiatore S.p.A., 2012, pp. 14-15.

[254] *Ivi,* p. 119.

evoluzione e non ci coinvolgono personalmente, cioè quelle veramente importanti, non entrano nella bolla»[255]. Di conseguenza, i filtri personalizzati ostacolano la capacità di apprendimento delle persone, poiché da un lato la bolla dei filtri le circonda di messaggi già familiari, dall'altro rimuove dal loro ambiente informativo gli stimoli che inducono il desiderio di imparare. Il ricercatore Travis Proulx introduce il concetto di "minacce al senso", come «quei fenomeni che ci turbano e ci confondono alimentando il nostro desiderio di capire e di acquisire nuove idee»[256]. La personalizzazione, invece, espone gli individui ad un "ignoto vicino", che, come si è già visto, non ne destabilizza gli schemi preesistenti stimolando la nascita di domande e curiosità, ma soddisfa in modo superficiale la personale necessità di apprendere assopendola.

Per concludere, è difficile stabilire quanto le tecniche di targetizzazione e profilazione possano incidere all'interno della comunicazione politica, ad esempio in una campagna elettorale o referendaria. Ciò che si è voluto evidenziare attraverso l'analisi delle vicende che hanno coinvolto Facebook e Cambridge Analytica è quanto possano essere pericolosi i sistemi di elaborazione dei dati applicati a immense quantità di informazioni quali quelle estraibili dalle piattaforme centralizzate e poi impiegati in un ambito delicato come quello del dibattito pubblico. L'utilizzo delle tecniche di micro-targeting, inoltre, è particolarmente problematico a causa della mancanza di trasparenza e controllo sulle informazioni che vengono mostrate e su chi le trasmette. «Ciò lascia aperta la possibilità per le campagne di utilizzare annunci politici "oscuri", in cui le persone ricevono messaggi altamente personalizzati che sono visibili solo a loro e dove potrebbe non essere chiaro quale organizzazione o individuo ci sia dietro - o quali informazioni vedano e ricevano le altre persone»[257]. Questi meccanismi suscitano diverse preoccupazioni per quanto riguarda la proliferazione di *fake news* o titoli clickbait che confermano le preferenze e le convinzioni politiche preesistenti degli elettori a scapito

[255] *Ivi,* p. 122.
[256] *Ivi*, p. 74.
[257] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019, p. 32.

della copertura basata sui fatti di attualità[258]. Ad esempio, un *whistleblower* (ovvero un informatore) sul caso di Cambridge Analytica ha affermato che la società avrebbe adottato spesso la tattica di diffondere articoli basati su falsità per manovrare il voto degli elettori americani. In ogni caso, è importante specificare che l'impatto di questo insieme di meccanismi - almeno per ora - risulta molto ridotto. Come spiega Hannah Fry nel suo testo *Hello World, Essere umani nell'era delle macchine*, «non siamo bersagli così indifesi, siamo molto bravi a ignorare la pubblicità o a dare la nostra interpretazione personale alla propaganda»[259]. Tuttavia, se una campagna personalizzata riesce ad influenzare anche solo una frazione minima dei suoi destinatari, in un'elezione un'influenza così marginale potrebbe essere sufficiente a capovolgerne il risultato[260]. Ciò in particolare è evidente nel contesto contemporaneo caratterizzato da un'elevata polarizzazione. Nel prossimo paragrafo, infatti, si avrà modo di approfondire gli effetti delle piattaforme e dei loro algoritmi di personalizzazione sull'instabile realtà attuale.

4.2) The Social Dilemma

A questo proposito ha attirato particolare attenzione un documentario recentemente diffuso da Netflix, *The Social Dilemma*[261]. Quest'ultimo «esplora la diffusione negli anni recenti dei social network e i danni che hanno provocato alla società, citando fra i tanti effetti il commercio dei dati, l'irrobustimento del cosiddetto capitalismo di sorveglianza, lo sfruttamento dei profili personali per scopi personali, la diffusione di fake news e teorie della cospirazione, e non ultimo le conseguenze sulla salute mentale in particolare degli utenti più giovani»[262]. Quella fornita nel documentario è stata ritenuta da molti una visione distorta e

---

[258] Cfr. Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 19.

[259] Hannah Fry, *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019, pp. 17-18.

[260] *Ibid.*

[261] *The Social Dilemma* (Jeff Orlowski, 2020).

[262] Paolo Armelli, *Facebook risponde alle critiche di The Social Dilemma*, in "Wired.it", 6 ottobre 2020 (https://www.wired.it/play/televisione/2020/10/06/facebook-risponde-critiche-social-dilemma/, consultato il 10 ottobre 2020).

sensazionalista del reale fenomeno rappresentato dai social media, al punto che il filmato viene definito come docudrama. Tuttavia, l'attenzione attirata da *The Social Dilemma* e il dibattito generatosi in seguito alla sua diffusione ne determinano il merito, ovvero l'aver approfondito tematiche di cruciale importanza[263].

Innanzitutto, il documentario affronta la questione della dipendenza dai social network e dallo smartphone in generale. Come già più volte ripetuto, infatti, uno degli obiettivi delle piattaforme centralizzate è quello di massimizzare l'*engagement* degli utenti per alimentare il business della sorveglianza e il mercato dei dati. Nel contesto dell'*information overload* le compagnie che sviluppano social media competono fra loro per catturare la limitata attenzione delle persone e perciò sono costantemente alla ricerca di nuovi espedienti per rendere l'esperienza all'interno dei propri *walled gardens* sempre più coinvolgente[264]. Come spiega il documentario, il meccanismo che alimenta tutte le funzionalità e i servizi adottati dalle piattaforme centralizzate è il cosiddetto "sistema di rinforzo intermittente positivo" illustrato da Tristan Harris, ex software designer di Google e fondatore del Center for Human Technology. Non si procederà in questa sede ad approfondire come funzioni tale meccanismo in quanto non pertinente a sostegno della tesi in discussione. Ciò che si vuole esplicitare, piuttosto, è che attraverso tale sistema si stimola il cervello umano a produrre dopamina, un neurotrasmettitore alla base della motivazione. Questa sostanza crea dipendenza, poiché provoca una sensazione di piacere. Di conseguenza l'individuo è sollecitato a ricreare la situazione che ha determinato lo sviluppo della dopamina. Nel contesto delle piattaforme centralizzate, quindi, «i social network […] sfruttano la capacità del nostro cervello di generare all'improvviso delle scariche di piacere per tenerci inchiodati e passare quanto più tempo possibile sulle applicazioni»[265].

---

[263] V. Andrea Daniele Signorelli, *Dopamina e ricompense: come uno smartphone hackera il nostro cervello*, in "Wired.it", 24 settembre 2020 (https://www.wired.it/attualita/tech/2020/09/24/social-dilemma-dopamina-effetto-smartphone-cervello/, consultato il 10 ottobre 2020).

[264] *Ibid.*

[265] *Ibid.*

Tuttavia, la tematica affrontata dal *The Social Dilemma* che è di maggiore interesse per questa sezione dell'elaborato in discussione è quella degli effetti della personalizzazione dei contenuti sulla frammentazione della società. In particolare, Rashida Richardson, professoressa della New York University School of Law, spiega nel documentario come gli individui online abbiano a che fare con sistemi diversi di informazioni, che si è visto essere una conseguenza della bolla dei filtri. Quando su larga scala le persone sono esposte ognuna a contenuti differenti e raccomandati, man mano, non risultano più in grado di fronteggiare o persino fruire di informazioni che contraddicono la visione del mondo che si sono create. Ciò implica che gli utenti smettono di essere individui oggettivi e costruttivi, conclude Richardson. Inoltre, se ogni persona accede ad un insieme informativo diverso, è come se fosse esposta ad una personale versione della realtà. Ne risulta, prosegue il documentario, che la personalizzazione elimina la necessità di trovare un compromesso fra modi di vedere diversi, di venirsi incontro, e persino di interagire. L'esistenza stessa di una società si basa su una comprensione comune della realtà[266]. Le piattaforme, al contrario alimentano la frammentazione e la polarizzazione, esponendo le persone ad una dieta mediatica che prevede informazioni che non consentono di scoprire visioni alternative a quella che si ha già[267].

Inoltre, l'avvento della rete e dei social media sembra aver portato alla disinformazione, piuttosto che alla promessa originaria di un accesso incondizionato a un corpus della conoscenza mondiale. Infatti, la comparsa della figura del consumatore-produttore ha innanzitutto minato il rapporto fra fonti di informazione e fruitori. Se ognuno può esprimere e diffondere un proprio messaggio agilmente, si riduce il valore della competenza e diminuisce la fiducia negli esperti[268]. In aggiunta, gli algoritmi di raccomandazione del contenuto alimentano la produzione di notizie false, le quali suscitano maggiore scalpore e sono quindi in grado di trattenere gli utenti ingaggiati più a lungo. *The Social Dilemma*, infatti, rivela che

[266] *V. The Social Dilemma* (Jeff Orlowski, 2020).

[267] *Cfr*. Enrico Pedemonte, *Piattaforme digitali: la dittatura vorace che piace*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 2, Iss. 3, 2017, pp. 9-14.

[268] *Ibid.*

secondo le statistiche le fake news si diffondono 6 volte più velocemente delle informazioni vere.

Si vuole aprire in questo contesto una piccola parentesi sui meccanismi cognitivi che intervengono nel momento in cui un individuo acquisisce una nuova informazione. Innanzitutto, vi è una prima fase di compressione dei dati, ovvero nel momento in cui si è esposti a stimoli esterni questi vengono ridotti a concetti che ne colgono il senso, i cosiddetti schemi. Questi ultimi permettono alle persone di approcciarsi al mondo come se non fosse sempre completamente nuovo. Successivamente, una volta acquisito uno schema, l'individuo è propenso a rafforzarlo. Ciò avviene poiché le idee vengono organizzate nella mente secondo collegamenti reticolari e gerarchici. Conseguentemente, se un concetto dovesse mutare troppo velocemente, potrebbe determinare l'alterazione o addirittura la rimozione di altre idee e così via fino a causare il crollo dell'intero sistema. Nel momento in cui un individuo apprende nuove informazioni, quindi, deve attuare un'operazione di bilanciamento fra il processo di assimilazione e quello di adattamento. Il primo consiste nell'adeguamento dei dati recepiti dalla realtà alla propria struttura cognitiva; il secondo si verifica quando sono gli schemi ad essere adattati agli impulsi esterni[269]. Tuttavia, la resistenza all'apprendimento di nuovi concetti è tendenzialmente molto forte, per questo motivo si fa difficoltà ad imparare e accettare qualcosa non strettamente connesso alle proprie convinzioni personali o alla propria visione del mondo. In particolare, intervengono determinati *bias*, delle scorciatoie cognitive, che portano l'individuo a rafforzare le sue credenze preesistenti:

- Innanzitutto, l'essere umano è costituzionalmente soggetto al pregiudizio di conferma, ovvero il processo attraverso cui, nella ricerca di nuove informazioni, si tende a privilegiare i dati che confortano ciò in cui già si crede.
- Parallelamente, l'effetto "ritorno di fiamma" è il meccanismo che interviene nel momento in cui si è esposti a prove che contraddicono le proprie convinzioni. Quando qualcuno o qualcosa tenta di modificare e correggere gli

[269] *V.* Eli Pariser, *Il Filtro*, Milano, il Saggiatore S.p.A., 2012, pp. 70-73.

schemi mentali di un'altra persona, infatti, quest'ultima sarà soggetta ad un "ritorno di fiamma" che rafforza i suoi giudizi preesistenti, invece di indebolirli.

- Si ha poi il ragionamento regolato, secondo il quale, non solo nella ricerca di nuove informazioni si privilegiano quelle a sé affini, ma, in aggiunta, si tende ad esaminare più severamente le idee che mettono in discussione i propri preconcetti.
- L'assimilazione partigiana rappresenta, invece, la tendenza delle persone ad interpretare e recepire i nuovi dati in modo che si accordino con le proprie opinioni.
- L'effetto dei media ostili interviene nel momento in cui un soggetto esposto ad una data notizia la giudica particolarmente faziosa solo per la sua provenienza da un dato media. In particolare, questo *bias* consiste nel ritenere che i mezzi di informazione siano prevenuti contro il proprio punto di vista. Ciò può portare due persone che sono state in contatto con uno stesso contenuto a trarne interpretazioni diametralmente opposte.
- La polarizzazione di gruppo è il processo che si verifica quando un individuo si trova a discutere all'interno di un gruppo. Se i membri di quest'ultimo condividono le opinioni di tale persona, questa tenderà ad assumere posizioni ancora più convinte. Se un soggetto si inserisce in una conversazione con un'idea poco chiara sull'argomento in discussione, verrà influenzato dalle convinzioni del gruppo. Infine, è stato riscontrato che quando un individuo deve rapportarsi con punti di vista diversi dal proprio, risulta in difficoltà nell'intraprendere una discussione significativa.
- Pericolose per il dibattito politico sono poi le voci terroristiche o *rumor bomb*, definite come slogan strategici pensati appositamente per minare una discussione valida giocando sull'incertezza e la paura del pubblico. La ripetizione di una voce terroristica, anche se fatta per smontarla, ne causa l'esplosione, ovvero un attecchimento ancor più profondo nella mente delle persone.

- La trasparenza della smentita, poi, è quel fenomeno per cui, quando si nega una storia, al tempo stesso la si diffonde. Ciò avviene poiché le persone lavorano sulle informazioni in modo cumulativo, ossia un elemento nuovo si aggiunge ad uno vecchio, non lo cancella.
- Infine, vi è l'effetto Cliff Clavin, definito così da Craig Silverman, autore del testo *Bugie, bugie virali e giornalismo*. Tale fenomeno si verifica nel momento in cui le persone cercano di smentire o correggere dei *wishful rumors*. Facendo ciò, i cosiddetti *debunkers* vengono spesso criticati per aver rovinato quella comunemente ritenuta come una bella storia ed ottengono così un effetto contrario a quello desiderato[270].

Si ha voluto fin qui approfondire i meccanismi cognitivi che intervengono nella fase di apprendimento di nuove informazioni da parte di un individuo, per evidenziare come l'intelletto umano sia tendenzialmente portato alla conservazione delle proprie strutture mentali. Ciò si ricollega alla questione della personalizzazione dei contenuti all'interno delle piattaforme centralizzate, poiché in tale contesto i fenomeni descritti risultano ulteriormente rafforzati. In questo modo funziona anche il sistema dei "Consigliati", spiega The Social Dilemma. L'obiettivo consiste nell'individuazione di una "tana del coniglio", ovvero di un contenuto in grado di agganciare l'utente e trascinarlo all'interno di un tunnel di collegamenti, all'interno del quale l'individuo risulta esposto ad informazioni simili e affini fra loro. In un simile spazio diviene difficile anche distinguere cosa sia vero e cosa no[271].

L'insieme di questi fenomeni rinchiude l'individuo all'interno in un insieme informativo personalizzato, come si è visto. Ciò deriva dal generale cambiamento dell'infosfera, all'interno della quale l'aumento nella quantità e nella varietà di canali e fonti di informazione ha determinato parallelamente una maggiore offerta di contenuti di nicchia e faziosi. Tali sviluppi nell'ambiente d'informazione pubblica e, in particolare, politica hanno creato strutture di opportunità per l'esposizione

[270] Cfr. Craig Silverman, *Bugie, bugie virali e giornalismo*, in "Il Post", Columbia Journalism School.

[271] *V. The Social Dilemma* (Jeff Orlowski, 2020).

selettiva alle notizie, basata sulle attitudini e le opinioni politiche preesistenti. Ciò sta portando a una sempre maggiore polarizzazione dell'opinione pubblica, che, a sua volta determina una minore condivisione dei fatti, l'estremismo e la mancanza di rispetto nei confronti di persone con punti di vista diversi dal proprio. Allo stesso tempo, tutto contribuisce ad indebolire la coesione sociale e a mettere alla prova le istituzioni e le pratiche democratiche fondamentali[272]. Per concludere si vuole proporre una citazione di Eli Pariser, il quale osserva che:

> La personalizzazione è al tempo stesso la causa e l'effetto del processo di frammentazione […]. La bolla dei filtri non ci piacerebbe tanto se non facesse appello al nostro desiderio postmaterialista di massima autoespressione. Ma una volta che ci siamo dentro, l'adattamento del flusso di informazioni alla nostra identità può portare alla graduale scomparsa dell'esperienza comune e frammentare eccessivamente il discorso politico[273].

4.3) Trasparenza e autodeterminazione dell'ambiente informativo

Nelle sezioni di questo elaborato dedicate alla privacy e alla necessità di un compromesso fra la libertà di espressione e la moderazione dei contenuti si ha avuto modo di approfondire come tali questioni rappresentino dei punti deboli per quanto riguarda il modello di business basato sulla sorveglia. Per entrambe le problematiche, inoltre, si ha proposto un approccio alternativo basato sulla decentralizzazione della responsabilità all'interno di piattaforme basate su un'architettura distribuita. In questa sede si avrà modo di vedere come la decentralizzazione possa fornire un valido apporto anche alla questione dell'impatto dei servizi online - in particolare di quelli di social networking - sulla qualità del discorso pubblico e politico.

Si ha già illustrato come l'essenza dei problemi causati dalla centralizzazione al dibattito online, all'ambiente informativo delle persone, ad alcune libertà

---

[272] *Cfr.* Peter Van Aelst, Jesper Strömbäck, Toril Aalberg, Frank Esser, Claes de Vreese, Jörg Matthes, David Hopmann, Susana Salgado, Nicolas Hubé, Agnieszka Stępińska, Stylianos Papathanassopoulos, Rosa Berganza, Guido Legnante, Carsten Reinemann, Tamir Sheafer, James Stanyer, *Political communication in a high-choice media environment: a challenge for democracy?*, in "Annals of the International Communication Association", Vol. 41, N. 1, 2017, pp. 3-27.

[273] Eli Pariser, *Il Filtro*, Milano, il Saggiatore S.p.A., 2012, p. 129.

fondamentali dell'individuo e, in generale, al benessere della sfera pubblica risieda nel sistema di algoritmi su cui si basa lo stesso business della sorveglianza. Si ha, inoltre, preso in esame i diversi effetti negativi prodotti dai meccanismi di targetizzazione e personalizzazione che implementano sia la raccomandazione dei contenuti all'interno delle piattaforme, sia la somministrazione degli annunci pubblicitari. A questo proposito, Jonathan Zittrain, professore di Diritto Internazionale presso la Harvard Law School, sostiene che l'assunzione di responsabilità da parte dei servizi centralizzati dovrebbe essere incentivata dalla presenza di standard etici nella progettazione degli algoritmi e dalla loro trasparenza. Quest'ultima, in particolare, permetterebbe agli utenti di scegliere consapevolmente la piattaforma a cui affidarsi, in base alla relativa politica di raccomandazione dei contenuti e, in generale, al rispetto degli interessi dei consumatori. La competizione fra servizi risultante da una simile concorrenza fungerebbe da protezione nei confronti delle persone, poiché, per accaparrarseli, i diversi sistemi dovrebbero puntare a fornire la migliore esperienza[274]. Tuttavia, prosegue Zittrain, una tale prospettiva richiede interoperabilità tra le piattaforme e minori costi di trasferimento, al fine di rendere praticabile per gli utenti lasciare un dato servizio centralizzato e unirsi ad un altro. Per questo motivo, gli autori del saggio *Defending Internet Freedom through Decentralization: Back to the Future?* affermano che: «Se la concorrenza sarà mai un percorso significativo verso la risoluzione di questi problemi, dobbiamo sviluppare metodi pratici per ridurre i costi di passaggio tra diversi fornitori di servizi»[275].

Nel contesto di questo elaborato la soluzione a tale difficoltà sembra ovvia: la decentralizzazione. Si ha già avuto modo di approfondire, infatti, come la portabilità dei dati da un servizio ad un altro rappresenti una delle peculiarità di un sistema a struttura distribuita. O meglio, all'interno di una rete costruita da nodi

---

[274] *V.* Jonathan Zittrain in Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 20.

[275] Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017, p. 21.

pari fra loro, si è visto come gli utenti rimangano in controllo dei propri dati, i quali sono condivisi fra i vari host della rete, invece di essere rinchiusi nei server proprietari di un unico soggetto. Le persone possono poi scegliere l'interfaccia, i filtri e qualsiasi altro *tool* preferiscano per accedere al complessivo corpus di contenuti. Inoltre, la decentralizzazione non garantisce solo una notevole riduzione dei costi di transizione da un servizio ad un altro, ma risponde anche al requisito di trasparenza, poiché è implementata da protocolli e software *open source*, pubblici e aperti. Come afferma Mike Masnick, infatti, la chiave risiede nell'assicurarsi «che le "regole" non siano solo condivisibili, ma completamente trasparenti e sotto il controllo di qualsiasi utente finale»[276].

Ciò, come si è visto, offre innanzitutto una valida alternativa per affrontare la questione dei contenuti abusivi. Può preoccupare, infatti, che l'assenza di autorità in grado di controllare ed intervenire nei confronti dei comportamenti fastidiosi possa portare ad un'incondizionata proliferazione di tali atteggiamenti. Inoltre, lo sviluppo di interfacce concorrenti che rispecchiano diversi interessi a primo impatto sembra possa sfociare nella generazione di "pozzi neri" della rete, nei quali si aggrega tutto il contenuto nocivo e viene amplificato come in una bolla dei filtri. Tuttavia, la decentralizzazione contribuirebbe, al contrario, ad isolare i comportamenti abusivi, poiché i relativi messaggi avrebbero meno probabilità di entrare nelle implementazioni e nei servizi utilizzati dalla maggior parte delle persone. Conseguentemente, i contenuti offensivi e fastidiosi rimarrebbero confinati all'interno di "angoli oscuri" e, allo stesso tempo, la loro capacità di infettare il resto della rete e di reclutare utenti affini sarebbe notevolmente limitata.

Per quanto riguarda il capitalismo della sorveglianza, basato sul mercato dell'advertising, la decentralizzazione offre la possibilità di creare modelli di business alternativi. In particolare, in tale contesto, essendo i dati e la condivisione degli stessi nelle mani degli utenti, la raccolta di informazioni personali non

[276] Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

sarebbe facilmente praticabile, né utile. Per questo motivo si prospetta l'implementazione di meccanismi per gli annunci che escludano la profilazione. A questo proposito Masnick propone alcune alternative. Innanzitutto, una prima opzione potrebbe prevedere un sistema di advertising che richieda una quantità limitata di dati e che si focalizzi, piuttosto, sulla correlazione con interessi, preferenze e passioni. Il promotore dell'approccio "*Protocols, Not Platforms*" riporta a questo proposito l'esempio del modello pubblicitario originario di Google, il quale non poggiava sul micro-targeting, ma piuttosto proponeva gli annunci in base alla conoscenza del contesto delle ricerche online degli utenti in quel momento specifico[277]. Un'altra proposta di Masnick è quella del ritorno al tradizionale advertising di marca, in cui sono inserzionisti a cercare le proprie comunità di consumatori di riferimento. La proliferazione di interfacce che corrispondo a diversi interessi all'interno del contesto decentralizzato potrebbe favorire un simile modello pubblicitario. Infine, la terza alternativa di Masnick si basa sul controllo dei dati nelle mani dei relativi utenti. Tale proposta prevede lo sviluppo di un sistema ad asta inversa, secondo il quale potrebbero essere gli stessi consumatori ad offrire la condivisione delle proprie informazioni personali in cambio dell'accesso alle offerte di determinati inserzionisti.

Per quanto riguarda la monetizzazione in generale dei sistemi decentralizzati si ha già più volte fatto riferimento al meccanismo basato su criptovalute e *token*. Tali *asset* potrebbero, infatti, essere impiegati sia per sostenere l'implementazione e l'aggiornamento dell'architettura, sia per remunerare i creatori di contenuti e gli sviluppatori di servizi vari. Tali questioni sono già state approfondite in precedenza; quello che si vuole evidenziare in questo contesto, piuttosto, è che non è neppure detto «che alla base dello sviluppo di una rete sociale decentralizzata debba necessariamente esserci il profitto, o almeno quel tipo di (super) profitto che caratterizza la fase di sviluppo attuale»[278]. Anzi, gli autori di studi sul tema concordano sul fatto che la decentralizzazione sia maggiormente legata «all'affermazione di un modello di sviluppo globale più equilibrato e sostenibile»[279]. La collaborazione con gli utenti, la valorizzazione della loro creatività,

[277] *Ibid.*

[278] Guido Vetere, *L'impossibile necessità delle piattaforme sociali decentralizzate*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 3, Iss. 1, 2018, pp. 41-50.

[279] *Ibid.*

della loro capacità di innovazione e, soprattutto, dei loro interessi sembrano essere la chiave per il successo delle piattaforme sociali decentralizzate.

PROSPETTIVE E CONCLUSIONI

Nei capitoli del presente elaborato si ha proposto la decentralizzazione come approccio alternativo per le maggiori difficoltà affrontate dalle piattaforme sociali centralizzate che monopolizzano il web. Si ha approfondito come si presenta dal punto di vista tecnico un'architettura decentralizzata per i sistemi online. Sono state evidenziate le proprietà che l'implementazione di un servizio di social networking sulla tecnologia della blockchain comporta. In seguito, si ha proceduto ad analizzare i benefici che tale implementazione apporta alla questione della privacy, alla necessità di moderazione dei contenuti, alle libertà fondamentali di espressione ed opinione e, infine, alla qualità del discorso pubblico online. Tuttavia, per quanto riguarda la decentralizzazione si ha sempre ragionato a livello teorico, prospettando degli scenari che ad oggi esistono, ma sono limitati ad un'utenza di appassionati e professionisti. Per questo motivo si procederà ora ad analizzare il caso che ha dato spunto all'elaborato sviluppato: l'annuncio da parte del CEO di Twitter della fondazione di un gruppo di ricerca orientato allo sviluppo di un protocollo decentralizzato per il social networking.

a) Dalla teoria alla pratica

Quando si ha iniziato a parlare di decentralizzazione, con l'introduzione dei Bitcoin e della loro tecnologia, la blockchain, i maggiori esponenti dei settori finanziari e tecnologici si sono opposti a tale implementazione, ritenendola una minaccia per i loro affari. Il motivo di tale resistenza risulta intuitivo per entrambi i contesti. Per quanto riguarda l'ambito economico, infatti, una struttura decentralizzata che permette la disintermediazione delle transazioni di beni rappresenta un palese rischio per soggetti quali gli istituti finanziari. In relazione, invece, al contesto delle Big Tech, le caratteristiche di una simile tecnologia sono essenzialmente opposte al modello di business basato sul mercato dei dati. Anzi, la decentralizzazione, inizialmente, era vista come lo strumento stesso che avrebbe messo

alla prova il potere delle piattaforme centralizzate[280]. Tuttavia, con un colpo di scena, proprio queste ultime hanno dimostrato interesse per tali sviluppi tecnologici, asserendo che avrebbero potuto costituire la chiave per la risoluzione di determinati loro problemi. Ad oggi, quindi, il concetto di rete decentralizzata diffuso grazie all'intuizione di Satoshi Nakamoto sembra imporsi come elemento disruptivo non solo nell'ambito delle criptovalute, ma anche in molti altri settori[281].

Nel contesto dei giganti del business della sorveglianza, uno dei primi ad aver palesato la propria attenzione per i progressi tecnologici in questione è stato Mark Zuckerberg, fondatore e amministratore delegato di Facebook. Il 4 gennaio 2018 ha infatti pubblicato un post sul proprio social network, affermando che la decentralizzazione potrebbe contribuire a riportare «il potere nelle mani delle persone»[282], obiettivo che rientra nella *mission* stessa del colosso.

Mark Zuckerberg
4 gennaio 2018 ·

•••

For example, one of the most interesting questions in technology right now is about centralization vs decentralization. A lot of us got into technology because we believe it can be a decentralizing force that puts more power in people's hands. (The first four words of Facebook's mission have always been "give people the power".) Back in the 1990s and 2000s, most people believed technology would be a decentralizing force.

But today, many people have lost faith in that promise. With the rise of a small number of big tech companies — and governments using technology to watch their citizens — many people now believe technology only centralizes power rather than decentralizes it.

There are important counter-trends to this --like encryption and cryptocurrency -- that take power from centralized systems and put it back into people's hands. But they come with the risk of being harder to control. I'm interested to go deeper and study the positive and negative aspects of these technologies, and how best to use them in our services.

This will be a serious year of self-improvement and I'm looking forward to learning from working to fix our issues together.

---

[280] Cfr. Nathaniel Popper, *What is the Blockchain? Explaining the Tech Behind Cryptocurrencies*, in "The New York Times", 27 giugno 2018 (https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-information.html?action=click&module=RelatedLinks&pgtype=Article, consultato il 6 agosto 2020).

[281] *V.* Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[282] Mark Zuckerberg, in "Facebook", 4 gennaio 2018 (https://www.facebook.com/zuck/posts/10104380170714571?pnref=story, consultato il 10 agosto 2020).

A febbraio 2019, inoltre, Zuckerberg ha dichiarato in un'intervista con Jonathan Zittrain che Facebook stava ragionando su come implementare il *login* al social network attraverso la blockchain, il che garantirebbe agli utenti il potere di concedere l'accesso ai propri dati alle app di terze parti senza l'intermediazione della piattaforma[283]. Nel maggio 2018, infatti, Facebook ha dato il via ad un team di ricerca dedicato allo studio dei modi in cui la tecnologia introdotta da Nakamoto potrebbe fornire un apporto al servizio di social networking. Da questo punto di vista un meccanismo di autenticazione decentralizzato che sostituisca Facebook Connect consentirebbe agli utenti non solo di poter decidere con quali software e applicazioni condividere i propri dati, ma anche in quale misura. Ciò rappresenterebbe un'importante svolta per gli sviluppatori dei servizi che ad ora necessitano dell'intermediazione della piattaforma, poiché non sarebbero più soggetti ad eventuali impedimenti da parte di quest'ultima e potrebbero contribuire ad elaborare una varietà di funzionalità accessorie[284].

Inoltre, Facebook ha investito anche nella creazione di una propria criptovaluta, Libra. La società ne ha annunciato la nascita nel giugno 2019. In seguito, tuttavia, il progetto ha subito dei rallentamenti a causa dell'opposizione da parte delle autorità finanziarie. Negli ultimi mesi, quindi, il colosso ha lavorato per rendere Libra più in linea con le preoccupazioni dei regolatori, i cui timori riguardano il fatto che l'*asset* virtuale possa «interferire con le valute nazionali e le politiche monetarie dei singoli Paesi»[285].

Vi è un altro soggetto la cui attenzione nei confronti della decentralizzazione risulta particolarmente interessante per quanto riguarda questo elaborato. Si tratta infatti di Twitter, il cui CEO, Jack Dorsey, l'11 dicembre 2019 ha rivelato la fondazione di un gruppo di ricerca indipendente, con lo scopo di sviluppare

---

[283]Cfr. Mark Zuckerberg, in "Facebook", 20 febbraio 2019 (https://www.facebook.com/zuck/videos/10106612617413491, consultato il 25 ottobre 2020).

[284] V. Shannon Liao, *Mark Zuckerberg is 'potentially interested' in putting Facebook login on the blockchain*, in "The Verge", 20 febbraio 2019 (https://www.theverge.com/2019/2/20/18233338/facebook-login-blockchain-mark-zuckerberg, consultato il 25 ottobre 2020).

[285] Staff, *Libra 2.0, la criptovaluta di Facebook cambia strategia*, in "Forbes.it", 18 aprile 2020 (https://forbes.it/2020/04/18/libra-la-criptovaluta-di-facebook-cambia-strategia/, consultato il 5 novembre 2020).

uno standard aperto e decentralizzato per i social media, di cui Twitter stesso diventerebbe *client*. Il fondatore del social network ha in seguito evidenziato le motivazioni che avrebbero portato a una tale direzione, facendo riferimento ad alcune difficoltà che attualmente ostacolano le piattaforme proprietarie. Innanzitutto, secondo Dorsey «è improbabile che l'applicazione centralizzata della politica globale per affrontare le informazioni abusive e ingannevoli si sviluppi nel lungo termine senza gravare troppo sulle persone»[286]. In secondo luogo, il fondatore di Twitter si è mostrato preoccupato per il fatto che il valore dei social media si stia spostando dall'*hosting* dei contenuti alla loro raccomandazione, permessa da algoritmi proprietari unilateralmente imposti. Successivamente, come già riportato, Dorsey ha sostenuto che i meccanismi che implementano le piattaforme portano a concentrare l'attenzione su contenuti e conversazioni che scatenano polemiche e indignazione, piuttosto che dialoghi che informano e promuovono la conoscenza. Infine, l'informatico ha spiegato che l'approccio decentralizzato sarebbe ora agevolato dall'introduzione di nuove tecnologie come la blockchain. Quest'ultima in particolare costituirebbe una soluzione agevole per l'*hosting*, la governance e persino la monetizzazione dei contenuti[287].

Il fondatore di Twitter ha anche citato due esperti che avrebbero ispirato il progetto e sollevato le motivazioni condivise da Dorsey. Questi sono Stephen Wolfram, autore di un articolo pubblicato sul suo blog dal titolo *Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms*, e Mike Masnick, al cui approccio ci si ha spesso fatto riferimento in questo elaborato.

Inoltre, Dorsey ha elencato i benefici che la decentralizzazione apporterebbe per Twitter, facendo riferimento all'opportunità di accedere e contribuire ad un corpus molto più ampio di conversazioni pubbliche, alla possibilità di concentrare gli sforzi sulla creazione di algoritmi di raccomandazione aperti che

[286] Cfr. Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).
[287] *Ibid.*

promuovano una conversazione sana e, infine, allo stimolo ad essere molto più innovativi rispetto al passato[288].

Il CEO ha concluso il *tweetstorm* con i riferimenti a Blue Sky, specificando l'importanza che la ricerca dello «standard decentralizzato solido, scalabile e applicabile ai social media» venga portata avanti «in modo trasparente e allo scoperto, non sotto il possesso di una singola società privata, promuovendo i principi aperti e decentralizzati di Internet»[289]. L'unica direzione indicata da Twitter, ha precisato Dorsey, è che il team individui un protocollo esistente da sostenere e aiutare nello sviluppo oppure, in mancanza di ciò, che ne crei uno da zero[290].

Come illustrato da Barbara Calderini nel suo articolo precedentemente citato, il progetto di Twitter non è nuovo né sul piano teorico, né su quello pratico. Dal primo punto di vista, infatti, risale al 2009 il paper *Decentralization: The future of online social networking*, in cui gli autori, fra cui lo stesso Tim Berners-Lee, propongono un primo approccio alla questione. Come si è visto, inoltre, nel giugno 2016 Internet Archive ha ospitato il primo vertice Web Decentralizzato, durante il quale Brewster Kahle, un altro pioniere del web, ha annunciato il progetto *Locking the Web Open*. Alla base di quest'ultimo vi è l'idea - appunto - di un ritorno alla rete degli anni '90, «quando gli utenti pubblicavano contenuti direttamente in modo decentralizzato e intuitivo, senza la necessità di intermediari aziendali e del loro approccio ambizioso»[291]. Per quanto riguarda il punto di vista pratico, Calderini evidenzia come attualmente esistano già diversi social network decentralizzati, fra i quali cita *Diaspora*, fondato già nel 2010, *Steemit* e *Mind*s, due noti *social incentivized*, *Mastodon*, di fatto una versione decentralizzata di Twitter, *Golos*, *DTube*, ispirato a YouTube, e, infine, *Sola*, sistema che «sfrutta l'architettura dei nodi e a differenza delle principali piattaforme di oggi, non si basa sui concetti di *follower* ma utilizza algoritmi di AI in combinata con le

---

[288] *Ibid.*
[289] *Ibid.*
[290] *Ibid.*
[291] Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Decentralized Social Networks Sound Great. Too Bad They'll Never Work*, in "Wired", 9 agosto 2017 (https://www.wired.com/story/decentralized-social-networks-sound-great-too-bad-theyll-never-work/, consultato il 20 agosto 2020).

reazioni degli utenti per diffondere informazioni»[292]. Successivamente, l'autrice specifica come l'idea non sia nuova neanche per Twitter stesso, per il quale uno standard decentralizzato rappresenterebbe un ritorno alle origini. Fino al 2012, infatti, il social network costituiva di fatto un «parco giochi del design»[293] per i suoi sviluppatori. Lo stesso Dorsey fa riferimento a ciò nei suoi tweet su Bluesky, spiegando come, tuttavia, la piattaforma abbia in seguito preso la strada della centralizzazione, «per una serie di ragioni, tutte ragionevoli all'epoca»[294].

I maggiori colossi dell'hi-tech, inoltre, collaborano già ad un progetto che si propone di sviluppare dei sistemi interoperabili che consentano agli utenti di trasferire i propri dati da un servizio ad un altro. Si chiama *Data Transfer Project*, è stato lanciato nel luglio 2018 e ne fanno parte società come Apple, Google, Microsoft, Facebook e Twitter. Il lavoro si basa sull'idea di rendere compatibili fra loro i diversi *tool* elaborati dalle varie piattaforme per permettere alle persone di scaricare le loro informazioni personali dal servizio online ad un proprio hard disk[295].

Le diverse proposte delineate evidenziano come la decentralizzazione possa effettivamente rappresentare la direzione futura delle grandi piattaforme. Tuttavia, queste ultime non hanno fatto i conti con la comunità decentralizzata già esistente, che non ha accolto favorevolmente l'annuncio di Dorsey. Si è già accennato, infatti, a come le caratteristiche e i principi della decentralizzazione siano essenzialmente opposti al business delle piattaforme basato sulla sorveglianza e sul mercato dei dati. In una struttura distribuita ad autorità condivisa, innanzitutto, le informazioni personali degli utenti rimangono sotto il controllo degli stessi. In secondo luogo, non vi è un unico provider dei servizi che

---

[292] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[293] *Ibid.*

[294] Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).

[295] Cfr. Russell Brandom, *Apple joins Google, Facebook, and Twitter in data-sharing project*, in "The Verge", 30 luglio 2019 (https://www.theverge.com/2019/7/30/20746868/apple-data-transfer-project-google-microsoft-twitter, consultato il 6 novembre 2020).

determina tutte le soluzioni del sistema e implementa algoritmi di raccomandazione dei contenuti unilateralmente determinati. Per questi motivi, gli intenti delle piattaforme centralizzate hanno suscitato scetticismo e perplessità da parte di molti esperti. Le accuse maggiori vanno dal sospetto che i colossi come Twitter e Facebook vogliano solo momentaneamente distrarre l'attenzione dalla loro difficoltà nell'affrontare i problemi che li ostacolano, al timore che la strada della decentralizzazione rappresenti una soluzione per scaricare sugli utenti la responsabilità delle piattaforme di questioni come la privacy e la moderazione dei contenuti[296]. Inoltre, diversi esponenti della comunità decentralizzata hanno rimproverato a Twitter di volersi espandere in un nuovo settore con il solo scopo di colonizzarlo, di plasmarlo a proprio favore. Il fondatore di Mastodon, Eugen Rochko, ha evidenziato il cosiddetto "*Embrace, Extend, Extinguish problem*", che delinea la strategia secondo la quale «una grande azienda adotta un protocollo aperto, diventa il suo più grande operatore e poi ne modifica il sistema per chiudere fuori gli altri»[297]. Allo stesso modo, Sean Tilley, *community manager* del primo network decentralizzato, *Diaspora*, sostiene che l'interpretazione pessimistica della situazione sia che Twitter non voglia solo entrare in Activity Pub - noto standard decentralizzato -, ma intenda controllarlo[298].

Al contrario, le probabilità di successo di Bluesky sarebbero molto più alte se il team di ricerca lavorasse con la comunità decentralizzata esistente, invece che contro di essa, spiegano diversi esperti. Ad esempio, Darius Kazemi, co-fondatore di *Feel Train* e collaboratore in molti progetti che promuovono la

[296] V. Nathaniel Popper, *Twitter and Facebook Want to Shift Power to Users. Or Do They?*, in "The New York Times", 18 dicembre 2019 (https://www.nytimes.com/2019/12/18/technology/facebook-twitter-bitcoin-blockchain.html, consultato il 17 agosto 2020).

[297] Adi Robertson, *Twitter wants to decentralize, but decentralized social network creators don't trust it*, in "The Verge", 12 dicembre 2019 (https://www.theverge.com/2019/12/12/21012553/twitter-bluesky-decentralized-social-network-developers-reaction-mastodon-activitypub, consultato il 5 agosto 2020).

[298] *Ibid.*

decentralizzazione del web, ha affermato che «Twitter potrebbe aiutare circa il 1.000 percento in più semplicemente finanziando selezionati progetti già esistenti»[299].

Come già accennato, un servizio decentralizzato simile a Twitter esiste già e si chiama Mastodon. Si tratta di una piattaforma di *microblogging*, composta da server gestiti individualmente o comunitariamente e liberamente collegati tra loro attraverso un sistema chiamato "*Fediverse*"[300]. È stato creato da Eugen Rochko nel 2016 e ai tempi, racconta il suo fondatore, era stato etichettato come un clone di Twitter, ma decentralizzato. «"Ora, sembra che Twitter stia creando un clone di Mastodon"»[301], ha ironicamente osservato Rochko, rivelando che la sua reazione nei confronti dell'annuncio di Jack Dorsey è stata mista. Da un lato, infatti, il giovane informatico si è mostrato deluso dal fatto che il lavoro svolto dagli sviluppatori di Mastodon non sia stato riconosciuto e che Twitter abbia addirittura sottovalutato l'impegno richiesto dall'elaborazione di uno standard decentralizzato, dedicandoci un team molto ridotto[302]. Dall'altro lato, Rochko ha ammesso che l'intera comunità decentralizzata potrebbe guadagnare dall'investimento della piattaforma nel settore e, infine, ha specificato che «l'adozione di ActivityPub da parte di Twitter sarebbe una buona cosa e una vittoria per il web»[303].

Si ritiene importante chiarire, infine, in cosa consiste ActivityPub e perché diversi esperti di decentralizzazione vi facciano riferimento come realtà a cui Bluesky potrebbe contribuire. ActivityPub, innanzitutto, è un *protocollo open*

---

[299] Darius Kazemi in Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[300] Cfr. Adi Robertson, *Twitter is funding research into a decentralized version of its platform*, in "The Verge", 11 dicembre 2019 (https://www.theverge.com/2019/12/11/21010856/twitter-jack-dorsey-bluesky-decentralized-social-network-research-moderation, consultato il 5 agosto 2020).

[301] Eugen Rochko in Maya Shwayder, *Hey @Jack Dorsey, decentralizing Twitter won't solve hate speech problems*, in "Digitaltrends", 11 dicembre 2019 (https://www.digitaltrends.com/social-media/jack-dorsey-decentralizing-twitter-wont-solve-your-hate-speech-problems/, consultato il 5 agosto 2020).

[302] *Ibid.*

[303] Eugen Rochko in Adi Robertson, *Twitter wants to decentralize, but decentralized social network creators don't trust it*, in "The Verge", 12 dicembre 2019 (https://www.theverge.com/2019/12/12/21012553/twitter-bluesky-decentralized-social-network-developers-reaction-mastodon-activitypub, consultato il 5 agosto 2020).

source decentralizzato per il social networking, realizzato dal *W3C Social Web Working Group*. Quest'ultimo era un gruppo di sviluppatori, scioltosi nel febbraio 2018, che aveva l'obiettivo di «definire delle specifiche tecniche standard e delle API con cui facilitare l'accesso alle funzionalità di social networking nell'ambito del progetto per la Open Web Platform ideato dal W3C»[304]. Il protocollo partorito da tale gruppo di ricerca si basa sul formato per i dati ActivityStreams 2.0. Lo standard prevede una API *client-server* per la creazione, l'aggiornamento e l'eliminazione dei contenuti, e una API federata *server-to-server* per la consegna delle notifiche e del contenuto. Di fatto, ActivityPub fornisce due *layer*: un *server to server federation protocol*, che permette la condivisione decentralizzata di informazioni tra siti web; e un *client to server protocol*, il quale consente agli utenti (che siano reali, bot o altri processi automatizzati) di comunicare con ActivityPub tramite il proprio account sui server, direttamente da smartphone, PC o attraverso delle applicazioni web. All'interno di ActivityPub un utente è rappresentato come un "attore" che corrisponde ad un account sui server. Ogni attore dispone di una *inbox* e una *outbox*, attraverso cui, rispettivamente, riceve e invia messaggi agli altri utenti[305].

ActivityPub implementa, ad esempio, la piattaforma di Mastodon, il cui fondatore, a proposito della possibilità che Twitter possa contribuire a tale protocollo con l'intenzione di acquisirne il controllo, conclude che lo standard sarebbe in grado di sopravvivere ad un simile tentativo di acquisizione. ActivityPub, infatti, è stato sviluppato in parte proprio in risposta ai fallimenti delle grandi piattaforme centralizzate e molte persone si sono iscritte al protocollo specificatamente perché non gradivano l'ampia scala, le funzionalità e le politiche di servizi come Twitter[306].

---

[304] Claudio Davide Ferrara, *ActivityPub: decentralized social networking protocol*, in "Html.it", 29 giugno 2018 (https://www.html.it/29/06/2018/activitypub-il-decentralized-social-networking-protocol/, consultato il 7 agosto 2020).

[305] *Cfr.* W3C Social Web Working Group, *ActivityPub, W3C Recommendation*, in "W3.org", 23 gennaio 2018 (https://www.w3.org/TR/activitypub/, consultato il 6 agosto 2020).

[306] Cfr. Adi Robertson, *Twitter wants to decentralize, but decentralized social network creators don't trust it*, in "The Verge", 12 dicembre 2019

Rimane da chiedersi, quindi, se il divario fra le piattaforme centralizzate e la comunità decentralizzata rimarrà sempre tale o vi sono possibilità di collaborazione, in grado di trarre il meglio da entrambi contesti.

b) Verso un futuro ibrido

Si è introdotto il presente elaborato dipingendo il contesto del web attuale come un panorama monopolizzato da grandi piattaforme il cui business rappresenta una minaccia per gli utenti sotto diversi punti di vista. Nonostante l'iniziale vantaggio che ha determinato l'affermazione dei servizi centralizzati a scapito di quelli decentralizzati, infatti, il successo dei primi ha in seguito prodotto degli effetti collaterali. Fra questi si è evidenziata, innanzitutto, la questione della privacy, messa a repentaglio dal business della sorveglianza, che mira ad estrarre quante più informazioni possibili sugli individui dalla loro esperienza online. Si è visto, inoltre, come il mercato dei dati rappresenti un pericolo per la *data protection*, proponendo il caso di Cambridge Analytica, società entrata illegalmente in possesso delle informazioni di milioni di utenti di Facebook, ignari che i propri dati fossero stati violati. Si ha mostrato in seguito la situazione di *impasse* in cui si trovano le piattaforme centralizzate per quanto riguarda la loro responsabilità del discorso online. Da un lato, infatti, i colossi del web sono costantemente impegnati nello sviluppo di algoritmi e nell'assunzione di impiegati con lo scopo di vigilare sui contenuti pubblicati all'interno dei propri *walled gardens*, per limitare l'impatto dei comportamenti abusivi. Dall'altro lato, tuttavia, gli utenti si aspettano dai servizi online anche la garanzia della libertà di espressione, poiché le piattaforme sono ormai concepite come spazi di discorso pubblico. Infine, come terza problematica causata dalla centralizzazione si è esaminata l'influenza di tali sistemi sul dibattito pubblico e politico, evidenziando come la raccomandazione micro-targettizzata dei contenuti rappresenti una minaccia per lo sviluppo autonomo del

(https://www.theverge.com/2019/12/12/21012553/twitter-bluesky-decentralized-social-network-developers-reaction-mastodon-activitypub, consultato il 5 agosto 2020).

pensiero, per il confronto libero e civile delle opinioni e, in generale, per la salvaguardia di diversi principi democratici.

Per ognuna delle problematiche esposte, sono stati approfonditi i benefici apportati da un approccio decentralizzato a tali questioni. Dopo un'analisi dei dettagli tecnici di una simile soluzione, infatti, si è proceduto a chiarire come le proprietà che caratterizzano i sistemi decentralizzati possano contribuire a riportare la realtà online al progetto originario di un contesto libero, aperto, democratico e creativo.

Tuttavia, si vuole precisare che nel presente elaborato ci si è volutamente concentrati sugli aspetti positivi della decentralizzazione. Ciò non significa che tale prospettiva tecnologica non riscontri difficoltà o non presenti delle controindicazioni. Dal punto di vista tecnico, innanzitutto, sono svariati gli elementi mancanti per poter garantire una fruibilità paragonabile a quella delle piattaforme centralizzate. Inoltre, anche la decentralizzazione pone degli ostacoli per quanto riguarda la privacy o la gestione dei comportamenti abusivi. Tuttavia, l'elemento che maggiormente complica l'affermazione di tali servizi è la concorrenza dei loro corrispettivi centralizzati. Si è visto, infatti, come già esistano sistemi decentralizzati, i quali però rimangono delle realtà di nicchia, popolate da esperti o appassionati. La vera difficoltà per i servizi in questione è quindi quella di riuscire ad attirare l'attenzione *mainstream*, sia degli utenti, sia degli sviluppatori[307]. Per fare ciò, tuttavia, devono scontrarsi con i monopoli delle grandi piattaforme, le quali, come si è visto, rappresentano di fatto l'accesso primario per le persone all'infosfera e catturano la maggior parte del traffico online. Inoltre, dal punto di vista economico i servizi centralizzati sono avvantaggiati grazie al modello di business basato sul mercato dei dati e sulla pubblicità. La disponibilità di fondi accentrati, come già discusso, permette di implementare e aggiornare costantemente l'infrastruttura tecnologica, la quale giova anche dell'economia di scala.

[307] *Cfr.* Nathaniel Popper, *Twitter and Facebook Want to Shift Power to Users. Or Do They?*, in "The New York Times", 18 dicembre 2019 (https://www.nytimes.com/2019/12/18/technology/facebook-twitter-bitcoin-blockchain.html, consultato il 17 agosto 2020).

Grazie alla loro dimensione, infatti, le grandi piattaforme sono economicamente agevolate nell'acquisto di risorse in blocco.

A ciò si aggiunge un «problema di cultura sociale»[308], come spiega Barbara Calderini. Il digitale, ad oggi, non è più solo uno strumento tecnologico, ma costituisce un'esperienza, un ambiente vissuto quotidianamente dagli individui, in un intreccio costante con il contesto offline. Reale e virtuale stanno diventando ormai indissolubili, l'uno ridefinisce le regole e i confini dell'altro. All'interno di tale ambiente, le piattaforme costituiscono dei servizi irrinunciabili, rappresentano l'anello che congiunge i due mondi, soprattutto attraverso la loro disponibilità su mobile. E dentro a ciascuno di questi sistemi ogni individuo costruisce faticosamente il proprio giardino, lavorando alla propria rete di contatti, producendo accuratamente contenuti e, in generale, creando il proprio *social environment*. A causa della non-portabilità dei dati, entrano così in gioco il meccanismo del *lock-in* e il *network effect*: le piattaforme imprigionano gli utenti trattenendo i loro dati e, soprattutto, la loro rete di relazioni. È difficile che un individuo lasci la realtà che si è costruito all'interno di un sistema centralizzato, per fruire di un nuovo servizio solo per ragioni ideologiche, come la condivisione dei principi della decentralizzazione. Ciò si spiega, a maggior ragione, considerando il fatto che le piattaforme hanno perfezionato le loro interfacce nel tempo, sulla base dei feedback di milioni di utenti, mentre i sistemi decentralizzati sono spesso difficili da utilizzare per i nuovi fruitori[309]. L'insieme di questi elementi crea, quindi, la ricetta perfetta per il consolidamento dei servizi centralizzati.

Risulta spontaneo chiedersi come, in un simile contesto, la decentralizzazione possa affermarsi e portare i benefici esposti in questo elaborato. Tuttavia, in questa sede si vuole specificare che lo scopo della tesi in questione non era quello di sostenere che le piattaforme strutturalmente distribuite e ad autorità

---

[308] Barbara Calderini, *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

[309] *V.* Chelsea Barabas, Neha Narula, Ethan Zuckerman, *Decentralized Social Networks Sound Great. Too Bad They'll Never Work*, in "Wired", 9 agosto 2017 (https://www.wired.com/story/decentralized-social-networks-sound-great-too-bad-theyll-never-work/, consultato il 20 agosto 2020).

condivisa rappresentino una soluzione migliore e definitiva ai tradizionali servizi. Il proposito era piuttosto quello di evidenziare come l'ispirazione alla logica decentralizzata possa offrire delle alternative per affrontare efficacemente questioni sempre più rilevanti. Nel concreto, attualmente, la prospettiva che si ritiene più percorribile è che le grandi piattaforme centralizzate guardino ai principi della decentralizzazione e individuino delle soluzioni da poter adottare. Un sistema ibrido, ad esempio, potrebbe combinare la moderazione accentrata dei contenuti - per limitare l'impatto dei comportamenti abusivi - e un meccanismo decentralizzato per la portabilità dei dati. In questo modo, si farebbe un primo passo verso una maggior tutela della privacy e una migliore *data protection*. Inoltre, grazie alla possibilità di esportare le proprie informazioni personali gli utenti sarebbero liberi di fare affidamento alla piattaforma che preferiscono, incentivando così i diversi servizi a perseguire il bene dei propri consumatori per guadagnarne il favore. In un simile contesto si incentiverebbe la competizione tra sistemi, la quale rappresenta la chiave per l'*empowerment* degli individui attraverso la loro riconquista del potere di scelta.

Si vuole infine riconoscere il merito di iniziative come Bluesky. Anche se, infatti, come ammesso dallo stesso Jack Dorsey, «ci vorranno molti anni per sviluppare uno standard decentralizzato valido, scalabile e utilizzabile per i social media che apra la strada per risolvere le sfide sopra elencate»[310], l'interesse dimostrato da una grande piattaforma come Twitter nei confronti di tale contesto rappresenta l'incentivo ad interrogarsi su come potrebbe configurarsi una rete non monopolizzata da grandi *walled gardens*[311].

[310] Jack Dorsey, in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).

[311] *V.* Adi Robertson, *Twitter is funding research into a decentralized version of its platform*, in "The Verge", 11 dicembre 2019 (https://www.theverge.com/2019/12/11/21010856/twitter-jack-dorsey-bluesky-decentralized-social-network-research-moderation, consultato il 5 agosto 2020).

BIBLIOGRAFIA

Aalberg T., Berganza R., de Vreese C., Esser F., Hopmann D., Hubé N., Legnante G., Matthes J., Papathanassopoulos S., Reinemann C., Salgado S., Sheafer T., Stanyer J., Stępińska A., Strömbäck J., Van Aelst P., *Political communication in a high-choice media environment: a challenge for democracy?*, in "Annals of the International Communication Association", Vol. 41, 1 (2017), pp. 3-27.

Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook threatens Human Rights*, Londra, Amnesty International Ltd, 2019.

Bahri L., Carminati B., Ferrari E., *Decentralized privacy preserving services for Online Social Networks*, in "Online Social Networks and Media", 6 (2018), pp. 18-25.

Barabas C., Narula N., Zuckerman E., *Defending Internet Freedom through Decentralization: Back to the Future?*, The Center for Civic Media & The Digital Currency Initiative - MIT Media Lab, Agosto 2017.

Berners-Lee T., *L'architettura del nuovo Web*, Milano, Giangiacomo Feltrinelli Editore, marzo 2001.

Berners-Lee T., Liccardi I., Lu K., Seneviratne O., Yeung C. A., *Decentralization: The future of online social networking*, in *W3C Workshop on the Future of Social Networking Position Papers*, Vol. II, gennaio 2009, pp. 2-7.

Bianchi R., Chiap G., Ranalli J., *Blockchain. Tecnologia e applicazioni per il business*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2019.

Bortoli S., Bouquet P., Palpanas., *Social networking: Power to the people*, in *Papers presented in W3C Workshop on the Future of Social Networking Position*, Barcellona, gennaio 2009.

Boyd D. M., Ellison N. B., *Social Network Sites: Definition, History, and Scholarship*, in "Journal of Computer-Mediated Communication", 13 (2008), pp. 210-230.

Buchegger S., Datta A., Rzadca K., Strufe T., Vu L., *Decentralized Online Social Networks*, in Borko Furth (ed.) *Handbook of Social Network Technologies and Applications*, Springer, 2010.

Caciotto M., *Il Nuovo Marketing Politico, Vincere le elezioni e governare al tempo della politica veloce*, Bologna, Società editrice Il Mulino, 2019.

Campagnoli M. N., *Informazione, social network & diritto: Dalle fake news all'hate speech online. Risvolti sociologici, profili giuridici, interventi normativi*, Kindle ed., Milano, Key Editore S.r.l., novembre 2020.

Codeluppi V., *Mi metto in vetrina*, Milano, Mimesis Edizioni, 2015.

Consiglio per i Diritti Umani delle Nazioni Unite, *The right to privacy in the digital age*, A/HRC/39/29, para. 7, 2018.

Conti M., Guidi B., Passarella A., Ricci L., *Managing social contents in Decentralized Online Social Networks: A survey*, in "Online Social Networks and Media", 7 (2018), pp. 12-29.

Douglas D. M., *Doxing: a conceptual analysis*, in "Ethics Inf Technol", 18 (2016), pp. 199-210.

Fry H., *Hello World: Essere umani nell'era delle macchine*, ed. digitale, Torino, Bollati Boringhieri, 2019.

Garavaglia R., *Tutto su Blockchain*, Kindle ed., Milano, Ulrico Hoepli Editore S.p.A., 2018.

Guidi B., *When Blockchain meets Online Social Networks*, in "Pervasive and Mobile Computing", 62 (2020), pp. 101-131.

Hardaker C., *Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions*, in "Journal of Politeness Research", 6 (2010), pp. 215-242.

Hosp J., *Blockchain 2.0: spiegata semplicemente - ben oltre il bitcoin*, Kindle ed., 2019.

Kurose J. F., Ross K. W., *Reti di calcolatori e Internet*, 7a ed., Milano-Torino, Pearson Italia, 2017.

Li C., Palanisamy B., *Incentivized Blockchain-based Social Media Platforms: A Case Study of Steemit*, in *The 10th ACM Conference*, giugno 2019, pp. 145-154.

Marinelli A., *Internet e World Wide Web*, in *Scienza e tecnica, Istituto dell'Enciclopedia italiana*, Roma, 2008, pp. 339-349.

Pariser E., *Il Filtro*, Milano, il Saggiatore S.p.A., 2012.

Pedemonte E., *Piattaforme digitali: la dittatura vorace che piace*, in "DigitCult, Scientific Journal on Digital Cultures", Vol. 2, Iss. 3, 2017, pp. 9-14.

Silverman C., *Bugie, bugie virali e giornalismo*, in “Il Post”, Columbia Journalism School.

Talia D., *La Società Calcolabile e i Big Data*, Soveria Mannelli, Rubbettino Editore, 2018.

Vetere G., *L’impossibile necessità delle piattaforme sociali decentralizzate*, in “DigitCult, Scientific Journal on Digital Cultures”, Vol. 3, Iss. 1, 2018, pp. 41-50.

SITOGRAFIA

Ammori M., *The Coming Decentralized Decade*, in "Morning Consult", 6 gennaio 2020 (https://morningconsult.com/opinions/the-coming-decentralized-decade/, consultato il 14 giugno 2020).

Armelli P., *Facebook risponde alle critiche di The Social Dilemma*, in "Wired.it", 6 ottobre 2020 (https://www.wired.it/play/televisione/2020/10/06/facebook-risponde-critiche-social-dilemma/, consultato il 10 ottobre 2020).

Barabas C., Narula N., Zuckerman E., *Decentralized Social Networks Sound Great. Too Bad They'll Never Work*, in "Wired", 9 agosto 2017 (https://www.wired.com/story/decentralized-social-networks-sound-great-too-bad-theyll-never-work/, consultato il 20 agosto 2020).

Bell E., *Facebook's moderation is of public interest. It should be public knowledge*, in "Columbia Journalism Review", 23 marzo 2017 (https://www.cjr.org/tow_center/facebook-moderation-guardian.php, consultato il 23 settembre 2020).

Berners-Lee T., *Information Management: A Proposal*, in "CERN Document Server", marzo 1989 (https://cds.cern.ch/record/369245/files/dd-89-001.pdf, consultato il 5 agosto 2020).

Brandom R., *Everything you need to know about GDPR*, in "The Verge", 25 maggio 2018 (https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice, consultato il 2 novembre 2020).

Brandom R., *Apple joins Google, Facebook, and Twitter in data-sharing project*, in "The Verge", 30 luglio 2019 (https://www.theverge.com/2019/7/30/20746868/apple-data-transfer-project-google-microsoft-twitter, consultato il 6 novembre 2020).

Cadwalladr C., Graham-Harrison E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, in "The Guardian", 17 marzo 2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, consultato il 31 ottobre 2020).

Calderini B., *I social e il web decentralizzato: che c'è di vero dietro l'utopia*, in "Agenda Digitale", 13 gennaio 2020 (https://www.agendadigitale.eu/cultura-digitale/i-social-e-il-web-decentralizzato-che-ce-di-vero-dietro-lutopia/, consultato il 15 maggio 2020).

Cambridge Dictionary, *Disruptive*, in "Cambridge Dictionary" (https://dictionary.cambridge.org/it/dizionario/inglese/disruptive, consultato il 28 ottobre 2020).

Data Center Knowledge, *Google Data Center FAQ*, in "DataCenter Knowledge", 17 marzo 2017 (https://www.datacenterknowledge.com/archives/2017/03/16/google-data-center-faq, consultato il 3 ottobre 2020).

De Martin J. C., La rivoluzione digitale, in "Treccani Web Tv" (https://www.treccani.it/magazine/webtv/videos/Int_Juan_Carlos_De_Martin_rivoluzione_digitale.html, consultato il 31 ottobre 2020).

Dorsey J., in "Twitter", 11 dicembre 2019 (https://twitter.com/jack/status/1204766078468911106, consultato il 20 aprile 2020).

Eagar M., *What is the difference between decentralized and distributed systems?*, in “Econova”, 4 novembre 2017 (https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462, consultato il 20 aprile 2020).

Ferrara C. D., *ActivityPub: decentralized social networking protocol*, in “Html.it”, 29 giugno 2018 (https://www.html.it/29/06/2018/activitypub-il-decentralized-social-networking-protocol/, consultato il 7 agosto 2020).

Gdpr.net, *General Data Protection Regulation*, in “Gdpr.net” (https://www.gdpr.net, consultato il 20 agosto 2020).

GO-Science, *Block chain technology*, in “YouTube”, 19 gennaio 2016 (https://youtu.be/4sm5LNqL5j0, consultato il 6 agosto 2020).

Hern A., *How social media filter bubbles and algorithms influence the election*, in “The Guardian”, 22 maggio 2017 (https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles, consultato il 10 ottobre 2020).

Il Post, *Perché in questi giorni siti e app vi perseguitano coi messaggi sulla privacy*, in “Il Post”, 28 aprile 2018 (https://www.ilpost.it/2018/04/28/gdpr-guida/, consultato il 3 novembre 2020).

Kahle B., *Locking the Web Open: A Call for a Decentralized Web*, in “Brewster Kahle's Blog”, 11 agosto 2015 (http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/, consultato il 20 agosto 2020).

Liao S., *Mark Zuckerberg is ‘potentially interested’ in putting Facebook login on the blockchain*, in “The Verge”, 20 febbraio 2019

(https://www.theverge.com/2019/2/20/18233338/facebook-login-blockchain-mark-zuckerberg, consultato il 25 ottobre 2020).

Lo Conte M., *Chi è e cosa fa Cambridge Analytica, la società che ha inguaiato Facebook*, in "Il Sole 24 ore", 20 marzo 2018 (https://www.il-sole24ore.com/art/chi-e-e-cosa-fa-cambridge-analytica-societa-che-ha-inguaiato-facebook-AETt4mJE?refresh_ce=1, consultato il 31 ottobre 2020).

Masnick M., *Protocols, Not Platforms: A Technological Approach to Free Speech*, in "First Amendment Institute at Columbia University", 21 agosto 2019, (https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, consultato il 15 aprile 2020).

Menietti E., *Il caso Cambridge Analytica, spiegato bene*, in "Il Post", 19 marzo 2018 (https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/, consultato il 30 ottobre 2020).

Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, in "Bitcoin.org", 31 ottobre 2008 (https://bitcoin.org/bitcoin.pdf, consultato il 28 ottobre 2020).

Newton C., *Facebook suspended Donald Trump's data operations team for misusing people's personal information*, in "The Verge", 16 marzo 2018 (https://www.theverge.com/2018/3/16/17132172/facebook-cambridge-analytica-suspended-donald-trump-strategic-communication-laboratories, consultato il 30 ottobre 2020).

Popper N., *What is the Blockchain? Explaining the Tech Behind Cryptocurrencies*, in "The New York Times", 27 giugno 2018 (https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-

information.html?action=click&module=RelatedLinks&pgtype=Article, consultato il 6 agosto 2020).

Popper N., *Twitter and Facebook Want to Shift Power to Users. Or Do They?*, in "The New York Times", 18 dicembre 2019 (https://www.nytimes.com/2019/12/18/technology/facebook-twitter-bitcoin-blockchain.html, consultato il 17 agosto 2020).

Robertson A., *Twitter is funding research into a decentralized version of its platform*, in "The Verge", 11 dicembre 2019 (https://www.theverge.com/2019/12/11/21010856/twitter-jack-dorsey-bluesky-decentralized-social-network-research-moderation, consultato il 5 agosto 2020).

Robertson A., *Twitter wants to decentralize, but decentralized social network creators don't trust it*, in "The Verge", 12 dicembre 2019 (https://www.theverge.com/2019/12/12/21012553/twitter-bluesky-decentralized-social-network-developers-reaction-mastodon-activitypub, consultato il 5 agosto 2020).

Rosenberg M., Nicholas Confessore, Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, in "The New York Times", 17 marzo 2018 (https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html, consultato il 29 ottobre 2020).

Shwayder M., *Hey @Jack Dorsey, decentralizing Twitter won't solve hate speech problems*, in "Digitaltrends", 11 dicembre 2019 (https://www.digitaltrends.com/social-media/jack-dorsey-decentralizing-twitter-wont-solve-your-hate-speech-problems/, consultato il 5 agosto 2020).

Signorelli A. D., *Storia di internet e del world wide web*, in "Wired.it", 11 marzo 2019 (https://www.wired.it/internet/web/2019/03/11/internet-world-wide-web-storia/?refresh_ce=, consultato il 6 agosto 2020).

Signorelli A. D., *Dopamina e ricompense: come uno smartphone hackera il nostro cervello*, in "Wired.it", 24 settembre 2020 (https://www.wired.it/attualita/tech/2020/09/24/social-dilemma-dopamina-effetto-smartphone-cervello/, consultato il 10 ottobre 2020).

Staff, *Libra 2.0, la criptovaluta di Facebook cambia strategia*, in "Forbes.it", 18 aprile 2020 (https://forbes.it/2020/04/18/libra-la-criptovaluta-di-facebook-cambia-strategia/, consultato il 5 novembre 2020).

Terenzio C., *How Walled Gardens Like Facebook Are Cannibalizing Media Publishers*, in "Forbes", 6 giugno 2018 (https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/06/how-walled-gardens-like-facebook-are-cannibalizing-media-publishers/#5703c6f65101, consultato il 15 settembre 2020).

The Economist, *Everywhere and nowhere,* in "The Economist, Business", 19 marzo 2008 (https://www.economist.com/business/2008/03/19/everywhere-and-nowhere, consultato il 15 settembre 2020).

The Economist, *Everybody wants to rule the world*, in "The Economist", 27 novembre 2014 (https://www.economist.com/briefing/2014/11/27/everybody-wants-to-rule-the-world, consultato il 3 ottobre 2020).

Twitter, Abusive behavior, in "Twitter" (https://help.twitter.com/en/rules-and-policies/abusive-behavior, consultato il 5 novembre 2020).

W3C Social Web Working Group, *ActivityPub, W3C Recommendation*, in "W3.org", 23 gennaio 2018 (https://www.w3.org/TR/activitypub/, consultato il 6 agosto 2020).

We Are Social, *Digital 2020*, in "wearesocial.com" (https://wearesocial.com/digital-2020, consultato il 5 agosto 2020).

Wikipedia, *Vendor lock-in*, in "Wikipedia", 21 ago 2020 (https://it.wikipedia.org/wiki/Vendor_lock-in#cite_note-ITIL_p157-1, consultato il 15 settembre 2020).

Wikipedia, *Platform Economy*, in "Wikipedia", 26 novembre 2020 (https://en.wikipedia.org/wiki/Platform_economy#The_platform_business_model, consultato il 26 novembre 2020).

WordPress, *Democratize Publishing*, in "WordPress.org" (https://wordpress.org/about/, consultato il 15 ottobre 2020).

Zuckerberg M., in "Facebook", 4 gennaio 2018 (https://www.facebook.com/zuck/posts/10104380170714571?pnref=story, consultato il 10 agosto 2020).

Zuckerberg M., in "Facebook", 20 febbraio 2019 (https://www.facebook.com/zuck/videos/10106612617413491, consultato il 25 ottobre 2020).

FILMOGRAFIA

The Social Dilemma (Jeff Orlowski, 2020).