



**Politecnico  
di Torino**

# **POLITECNICO DI TORINO**

Corso di Laurea in Ingegneria Gestionale

A.A. 2020/2021

Sessione di Laurea Dicembre 2021

## **L' Economia dei dati** *The data Economy*

Relatore:

Prof. Carlo Cambini

Candidato:

Matteo Tenna

---

*Com'è definita l'identità?*  
*In passato si diceva: "Io sono quello che dico di essere".*  
*Oggi, siamo quello che Google dice che siamo.*  
*Siamo sempre meno persone, sempre più profili.*

*(Stefano Rodotà)*

---

---

# SOMMARIO

<b>INTRODUZIONE .....</b>	<b>1</b>
<b>CAPITOLO 1 .....</b>	<b>4</b>
<b>IL PROCESSO DI DIGITALIZZAZIONE E L'AVVENTO DEI BIG DATA .....</b>	<b>4</b>
1.1 Dati e Big Data .....	5
1.2 La persona come fonte di dati.....	9
1.3 Le caratteristiche dei big data .....	12
1.3.1 Il volume .....	13
1.3.2 La varietà.....	16
1.3.3 La velocità.....	18
1.3.4 La veridicità .....	21
1.3.5 La valenza .....	21
1.3.6 La visualizzazione.....	22
1.3.7 Il valore .....	22
1.4 Limiti dei big data.....	23
1.5 La catena del valore nell'ecosistema big data .....	24
<b>CAPITOLO 2 .....</b>	<b>30</b>
<b>UNO SGUARDO ALLA NORMATIVA EUROPEA ED EXTRA EUROPEA SUL TRATTAMENTO DEI DATI PERSONALI.....</b>	<b>30</b>
2.1 Il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali .....	33
2.2 Come siamo arrivati al GDPR? .....	36

---

2.3	Le caratteristiche principali del DGPR.....	39
2.4	Le conseguenze del GDPR in tema di concorrenza.....	45
2.5	La convenzione 108 e la convenzione 108+.....	48
<b>CAPITOLO 3 .....</b>		<b>54</b>
<b>REGOLAMENTI EUROPEI PER IL MERCATO DIGITALE:</b>		
<b>DSA E DMA .....</b>		<b>54</b>
3.1	Digital Services Act (DSA) .....	58
3.2	Digital Markets Act (DMA) .....	69
<b>CAPITOLO 4 .....</b>		<b>77</b>
<b>INCHIESTA ANTITRUST:</b>		
<b>IL CASO GOOGLE - FITBIT .....</b>		<b>77</b>
4.1	La storia di Google e il concetto di monopolio .....	78
4.2	Accordo Google – Fitbit: rischi e preoccupazioni.....	83
4.3	Gli impegni di Google .....	87
<b>CONCLUSIONI .....</b>		<b>91</b>
<b>BIBLIOGRAFIA .....</b>		<b>95</b>

# INTRODUZIONE

*“Dati uguale potere. È il potere di raccogliere informazioni sulle persone, costruire inferenze attraverso quelle informazioni e trasformarle in fonte di valore, sotto forma di profitti commerciali oppure in termini di capacità di condizionamento dei comportamenti altrui. È un potere nelle mani di una cerchia relativamente ristretta.”<sup>1</sup> (Giovanni Buttarelli)*

L’economia dei dati rappresenta, al giorno d’oggi, uno dei settori che sta avanzando sempre più velocemente nel suo sviluppo; infatti, grazie alla sempre maggiore informatizzazione dei sistemi e all’incremento della digitalizzazione, essa è diventata fondamentale nel sistema economico attuale.

Il presente lavoro di ricerca vuole proporre un’analisi attuale del fenomeno dell’economia dei dati, il quale sta continuando ad evolversi seguendo lo sviluppo sempre più repentino dell’informatizzazione digitale. L’analisi parte dall’esplorazione del fenomeno della digitalizzazione, iniziato nel XXI secolo, il quale ha necessariamente portato alla produzione di molte informazioni legate agli utenti. Tali informazioni, con il susseguirsi degli anni, sono aumentate sia in numero che in complessità e hanno rappresentato una nuova forma di business: si è arrivati così all’avvento dei *Big Data*.

---

<sup>1</sup> C. D’Cunha, *Idee di Giovanni Buttarelli, trascritte da Christian D’Cunha*, in *Privacy 2030. Una nuova visione per l’Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, URL: <https://www.garanteprivacy.it/documents/10160/0/Privacy+2030+-+Un+manifesto+per+il+nostro+futuro+-+Volume.pdf/8a243e2f-53e9-8dfa-a3be-0e80347499d3?version=2.1> p. 12.

Caratterizzati da molteplici proprietà, tra le quali le famose 7 V (volume, varietà, velocità, veridicità, valenza, visualizzazione e valore), essi seguono un preciso iter che conduce all'estrazione del loro valore, divenuto al giorno d'oggi talmente prezioso che viene paragonato al petrolio. Nonostante i molti vantaggi e una vasta eterogeneità di opportunità che scaturiscono dall'utilizzo dei *Big Data*, esso implica anche alcune conseguenze negative, come sottolineato anche da Giovanni Buttarelli, magistrato italiano nominato Garante Europeo per la Protezione dei Dati tra il 2014 e il 2019: *“Ci stiamo accorgendo delle esternalità legate al trattamento massivo di dati e alla connettività pervasiva. Connettere tutto ha un costo per la società e per l'ambiente, ma anche per le persone”*<sup>2</sup>

Dopo aver analizzato il processo di elaborazione dei *big data* e di estrazione del loro valore, si prosegue con la presentazione di un excursus storico normativo sulle principali disposizioni grazie alle quali oggi si è potuti arrivare a due importanti normative che vengono applicate sia in campo europeo che extra europeo: in Europa, il GDPR e la Convenzione 108 e 108+, valida per tutti i Paesi che intendono aderirvi, sia che appartengano all'UE sia che non vi appartengano. Tali documenti mirano ad ampliare il concetto di protezione dei dati e a tutelare i diritti dei consumatori e degli utenti online, mettendo in atto disposizioni volte alla salvaguardia delle informazioni degli individui alle quali conformarsi, al fine di non incorrere in sanzioni, spesso molto onerose.

In seguito, vengono analizzati altri due importanti documenti molto recenti nati in ambito europeo, il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA) che hanno lo scopo di regolamentare il mercato digitale. Nel primo vengono definiti e disciplinati le responsabilità e gli obblighi ai quali si dovranno attenere gli intermediari digitali, cioè le società che dirigono i *social network* o le piattaforme nate per condividere informazioni o, ancora, *store* e

---

<sup>2</sup> Ibidem

## INTRODUZIONE

---

*app store*. Nel secondo, invece, vengono definiti i comportamenti e gli obblighi delle *big tech*, denominate anche *gatekeeper*: aziende che hanno assunto una notevole rilevanza nel mercato digitale europeo e mondiale.

La ricerca si conclude con l'analisi di un caso molto recente, avvenuto tra la fine del 2019 e il 2021, che riguarda l'acquisizione dell'azienda di *smartwatch* Fitbit da parte di Google. Vengono messe a confronto le preoccupazioni dei *competitors* e dell'autorità antitrust europea con le motivazioni e le dichiarazioni della *big tech*, concludendo poi con gli accordi e gli impegni che il colosso statunitense ha dichiarato di mantenere in seguito alla fusione con Fitbit, avvenuta nel gennaio del 2021.

# CAPITOLO 1

## IL PROCESSO DI DIGITALIZZAZIONE E L'AVVENTO DEI BIG DATA

Il XXI secolo rappresenta il periodo in cui si può definire l'inizio del processo di digitalizzazione dei sistemi: in ambito aziendale, per esempio, l'introduzione di innovative tecnologie negli uffici e la trasformazione dei documenti cartacei in PDF ha permesso di ottimizzare, semplificare, accelerare e rendere più agili tutte le attività.

Molti altri aspetti della vita quotidiana vengono interessati da questa trasformazione: un esempio può essere rappresentato dal “nuovo” mercato online. Il processo di digitalizzazione dei consumi e del mercato porta anche le aziende a stare al passo con i tempi e, quindi, a digitalizzare anch'esse i loro processi. In tal senso, quindi, si può parlare anche di una profonda trasformazione culturale.

Esattamente come le aziende private, ugualmente la Pubblica Amministrazione è stata travolta dalla digitalizzazione dei processi attraverso un aumento dell'utilizzo della componente informatica: si può quindi affermare che la digitalizzazione sia realmente un fenomeno trasversale, che tocca moltissimi aspetti della vita di tutti i giorni.

L'adozione in massa da parte dei consumatori di servizi digitali, delle istituzioni e delle imprese si è rivelata essere una chiave di volta che ha

trasformato l'economia mondiale. La ricerca online di informazioni, di intrattenimenti, di acquisti e le esigenze comunicative stanno rendendo sempre più indispensabili i servizi online, che ormai hanno quasi definitivamente sostituito quelli tradizionali.

Tali ricerche interconnesse creano un'enorme quantità di informazioni digitali, chiamate dati: le parole si trasformano in dati, la posizione geografica si trasforma in dati, le interazioni sociali si trasformano in dati, anche le cose, se connesse in rete, diventano dati. Si parla addirittura di impronte informatiche, così come si legge nel Big Data Interim Report dell'ente AGCOM del giugno 2018:

*“L'utilizzo crescente di internet da parte degli individui, in particolare tramite i dispositivi mobili, è una sorgente inesauribile di dati; le tracce vengono lasciate in rete in ogni momento - online footprint -, quando ci si sposta da un luogo a un altro, quando si condividono le foto o i commenti, quando si effettuano i pagamenti, quando si pratica attività sportiva, ecc”<sup>1</sup>*

### 1.1 DATI E BIG DATA

Sin da quando sono stati formati, i dati digitali hanno occupato un posto rilevante per le attività sociali ed economiche, specialmente attraverso la loro analisi, dalla quale si possono estrarre diverse informazioni. Un passo avanti, rispetto agli anni passati, nei quali venivano offerte soltanto delle rappresentazioni analogiche delle esigenze sociali, è stato compiuto proprio dalle imprese, dalle istituzioni e dagli individui che hanno stimolato e aumentato

---

<sup>1</sup> AGCOM (2018), *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*. URL: <https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>

la propria competenza nell'analizzare la realtà attraverso i dati, offrendo una rappresentazione di scelte ed eventi sociali nati già in digitale.

Proprio per la complessità e il gran numero di dati che sono stati prodotti durante il processo di digitalizzazione e che vengono tuttora prodotti, piuttosto che utilizzare il semplice termine "dati", si preferisce far riferimento ad un concetto più complesso, utilizzando il termine big data. Attraverso quest'ultimo, infatti, ci si riferisce alla grande quantità di dati presenti nei sistemi digitali di oggi che necessitano di nuovi e più performanti processori ed algoritmi per la loro analisi, dal momento che derivano da una molteplicità di fonti diverse.

Una definizione interessante che permette di capire questo concetto e questa differenza è stata data da De Mauro, quando afferma che i big data rappresentano

*“il patrimonio informativo caratterizzato da un volume, una velocità e una varietà così elevati da richiedere tecnologie e metodi analitici specifici per la sua trasformazione in valore”<sup>2</sup>*

Grazie a questa definizione la differenza tra dati e big data è chiara e netta; ciò che li contraddistingue è la presenza, nei big data, delle cosiddette 4V, nate con il progresso tecnologico: il volume dei dati raccolti, la varietà dei dati elaborati, la velocità con la quale vengono raccolti, analizzati e archiviati e il valore delle informazioni ricavate da essi.

L'analisi dei big data può avere funzioni differenti: per le aziende private, essa può incrementare l'innovazione e i servizi e migliorare la pubblicità offerta, creando modelli di business personalizzati in base alle

---

<sup>2</sup> De Mauro A., Greco M. e Grimaldi M. (2016), *Una definizione formale dei Big Data basata sulle sue caratteristiche essenziali*, Recensione della Biblioteca 65(3), pp. 122-135

preferenze dei clienti. Anche la Pubblica Amministrazione utilizza l'analisi dei big data per migliorare i servizi offerti ai cittadini, rendendoli più efficaci.

Si può affermare che i big data siano i protagonisti di un'economia *data-driven*: in questo nuovo tipo di economia, infatti, tutti gli ambiti, sia privati che pubblici, sono stati influenzati dalla raccolta e dall'analisi dei dati; questo fattore ha permesso di offrire servizi innovativi, rendere migliori quelli preesistenti e di rispondere più conformemente alle esigenze dei cittadini e dei consumatori, proponendo servizi e prodotti ad hoc in base alle loro richieste.

L'importanza della raccolta e dell'analisi dei big data la si deve principalmente a due tendenze: il progresso tecnologico e lo sviluppo di nuove tecniche analitiche. Mentre grazie al primo, si sono ridotti i costi della raccolta e dell'uso dei dati in continua produzione, il secondo ha reso possibile un'elaborazione sempre più specifica e accurata dei dati, fattore che ne permette l'aumento di valore, in ambito economico e sociale.

Nel mondo della digitalizzazione si possono trovare diversi protagonisti che giocano diversi ruoli all'interno dell'ecosistema dei big data:

- i fornitori di dati: sono i soggetti che creano e generano i dati;
- i fornitori della strumentazione tecnologica: si tratta delle diverse piattaforme online che raccolgono e gestiscono i dati;
- gli utenti: coloro che trasformano i big data in valore aggiunto;
- i *data brokers*: rappresentano delle organizzazioni che vendono ad altre organizzazioni i dati raccolti da una molteplicità di fonti pubbliche e private;
- le imprese e le organizzazioni di ricerca, che sviluppano nuovi algoritmi e tecnologie per l'analisi dei dati;

- gli enti pubblici, che migliorano l'offerta dei prodotti e dei servizi per l'aumento del benessere della cittadinanza.

Un'altra componente che sta crescendo con il fenomeno dei big data è quello dei *data center*: sistemi che cercano di venire incontro alla necessità di raccolta, conservazione e analisi dei dati in un periodo in cui i big data continuano ad aumentare in quantità e dimensione.

Per poter comprendere meglio le argomentazioni presentate in questa ricerca, però, è necessario approfondire maggiormente il concetto e le definizioni che sono state date ai big data; l'economista Antonio Nicita e il ricercatore Marco Delmastro hanno provato a dare una panoramica di definizioni per poter spiegare meglio il concetto di big data, nel loro lavoro di ricerca intitolato "Big Data – Come stanno cambiando il nostro mondo".

Un ventennio fa i big data erano stati definiti dalla società Gartner come

*“asset informativi ad alto volume, alta velocità e alta varietà che richiedono nuove forme di lavorazione ed elaborazione delle informazioni che permettono di migliorare le decisioni, intuire scoperte e ottimizzare i processi”*<sup>3</sup>

mentre, più recentemente, l'Unione Europea ha proposto una definizione più istituzionale definendo i big data come

*“grandi quantità di tipi diversi di dati prodotti da varie fonti, fra cui persone, macchine e sensori”*<sup>4</sup>

La prima definizione permette di analizzare i fattori che caratterizzano i big data (velocità, varietà e volume) e di comprendere quale profondo legame

---

<sup>3</sup> Nicita, Delmastro, *Big Data – Come trasformano l'economia e la politica*, p.7

<sup>4</sup> Ibidem

ci sia tra i big data di per sé e il processo di aggregazione e di lavorazione che li accompagna costantemente, cioè gli algoritmi.

La seconda definizione, invece, lascia intendere l'ampiezza del carattere di disomogeneità che caratterizza i big data: le immagini satellitari, i dati ambientali, le fotografie digitali, i dati GPS o l'indirizzo IP di una data connessione Internet. Sono compresi anche i dati più "strutturati" legati alla persona: dalle generalità, dagli estremi bancari, dai segni particolari, dai dati sanitari e lavorativi ai *social network*, alla cronologia delle ricerche e degli acquisti online. Oltre a questo tipo di dati, ve ne sono anche di meno strutturati, cioè dei dati lasciati in rete in modo più impersonale e più dovuto alla casualità: le immagini delle telecamere di sicurezza della città o dei locali e i dati sulla nostra posizione registrata dimenticando il GPS attivo possono esserne due esempi.

Tutta questa serie di dati viene prodotta quotidianamente, minuto per minuto, da ogni singolo individuo nel mondo.

### 1.2 LA PERSONA COME FONTE DI DATI

La connessione in rete di ogni individuo comporta la produzione, consapevole e inconsapevole, di dati. Tali dati possono essere informazioni personali (nome, cognome, età, indirizzo, estremi bancari etc.), informazioni che riguardano le attività di una persona (acquisti online, cronologia delle ricerche etc.) o, ancora, informazioni che, in base alla loro analisi possono essere ricollegate all'individuo stesso. Tutta questa serie di informazioni, unite e processate insieme, forma l'impronta digitale (*online footprint*) di ogni persona.

Vista la grande quantità di informazioni rilasciate ogni giorno da ciascun individuo, è comprensibile chiedersi se queste informazioni siano tutelate o meno. Una delle principali difficoltà nella tutela di questi dati sta proprio nel riconoscere a priori quali siano ritenuti dati personali e quali invece no, dal

momento che informazioni apparentemente poco importanti come la cronologia delle ricerche, se processate e incrociate ad altri dati, possano comunque rivelare informazioni personali del soggetto stesso.

Risulta molto difficile, se non addirittura impossibile, cercare di rallentare questo fenomeno, poiché sia lo sviluppo tecnologico sia la facile fruibilità di devices e strumenti sono in continua crescita: sia in ambito lavorativo che in ambito privato l'utilizzo di uno smartphone o di un tablet o di un personal computer collegati ad internet è diventato quasi indispensabile. È proprio a causa della diffusione dell'uso di internet nella popolazione mondiale che risulta così complesso applicare l'approccio tradizionale all'analisi delle informazioni personali di un individuo.

Oltre a questo, va tenuto presente che un determinato dato potrebbe fungere la funzione di dato personale per alcuni operatori, mentre per altri potrebbe perdere questa caratteristica: potrebbe essere il sempre più frequente caso di una fotografia scattata dalle telecamere di sorveglianza di un supermercato o di una banca. Per un poliziotto, essa potrebbe rivelarsi un dato molto importante al fine di riconoscere un qualche soggetto ricercato, mentre per un giornalista potrebbe semplicemente fungere come fonte da allegare al proprio articolo di giornale. Questo semplice esempio fa comprendere che molto sull'analisi dei dati dipende non solo da chi li produce, ma soprattutto da chi li processa e li analizza.

È necessario, ora, per cercare di comprendere meglio da cosa sia generata la complessità del fenomeno dei big data, elencare e procedere con l'approfondimento dei principali ambiti che fungono da sorgente di dati da parte dell'individuo:

- Attività online: a partire dalla semplice connessione del proprio dispositivo alla rete internet fino a tutte le attività che possono essere svolte in rete. Queste azioni generano una miriade di dati

che, analizzata e processata, può fornire molte informazioni sull'utente. Per esempio, la semplice connessione di un dispositivo alla rete internet fornisce informazioni di dati geografici legate all'indirizzo IP necessario per poter entrare in rete. Informazioni legate alle preferenze o alle abitudini dell'utente, invece, possono essere ricavate dall'utilizzo dei motori di ricerca, dalla visualizzazione di video, dai giochi online, dagli acquisti o dalla lettura di giornali online.

- Casella e-mail e utilizzo della posta elettronica: strumento usato principalmente per comunicare in ambito lavorativo e non solo, produce tutta una serie di dati legati a testi, immagini e contatti che possono essere raccolti e utilizzati.
- *Social network*: grandi quantità di dati vengono prodotti ogni minuto sui *social network*, piattaforme digitali sulle quali ogni utente può scrivere messaggi personali (posts), condividere fotografie e video, creare gruppi ed eventi, commentare e taggare altri utenti. Tutte queste azioni, specialmente negli ultimi anni, sono diventate naturali per gli utenti dei *social*; tuttavia, minima risulta la consapevolezza digitale che vi è dietro a queste semplici azioni e alla quantità di dati che esse producono.
- Mobilità e spostamenti: tutti i dispositivi permettono la propria localizzazione, se richiesta. Gli LBS (*Located Based Services*) rappresentano un'altra importante fonte di dati, in particolare geografici, che permettono di avere informazioni sulle abitudini e sulle preferenze degli individui.
- Sistemi di sensori: riconoscimento facciale, accelerometro, giroscopio, GPS, sensore di luminosità, lettore delle impronte digitali e facciali sono solo alcuni dei sensori che sono presenti

quotidianamente nelle vite di tutti gli individui, o nei luoghi pubblici (come, per esempio, i sistemi di videosorveglianza) o nei dispositivi mobili che ognuno possiede.

Un individuo non sempre diventa fonte di dati in modo consapevole: la parte dei dati raccolti più rilevante è rappresentata dai *passive data*, cioè dai dati che vengono raccolti senza esplicito consenso da parte dell'utente e che, passivamente, divengono la principale fonte di informazioni.

Ogni persona, o meglio, ogni utente rappresenta un grande valore nel mondo digitale proprio per la grande quantità e varietà di dati che produce, in modo consapevole o meno; due sono le ragioni del valore di questi dati: la prima, proprio perché essi consentono di profilare la domanda individuale dell'utente di servizi e prodotti, permettendo una personalizzazione sempre maggiore della pubblicità e del commercio e aumentando la possibilità di vendita. In secondo luogo, perché, con la produzione di dati sempre diversi e nuovi, gli algoritmi che li analizzano, migliorano e contribuiscono alla stima di una domanda media di consumi di prodotti e servizi. Quindi, da questo si desume che il valore dei dati accresca con il loro volume e la loro varietà.

### 1.3 LE CARATTERISTICHE DEI BIG DATA

Riprendendo la definizione fornita da Gartner<sup>5</sup>, si può evincere che le caratteristiche principali dei big data siano volume, velocità, varietà alle quali vanno aggiunte veridicità e valore. La gestione simultanea di queste caratteristiche ha permesso l'invenzione e la produzione di sempre più nuove e innovative *analytics* (tecniche di analisi dei dati), molto diverse da quelle tradizionali adottate fino ad oggi; da queste ha origine il valore prodotto dai big data, che risulta essere utile “*sia per la risoluzione di problemi specifici sia per*

---

<sup>5</sup> Ibidem

*l'identificazione di nuove opportunità commerciali e di nuove modalità di definizione di politiche pubbliche*"<sup>6</sup>.

### 1.3.1 Il volume

Il volume è senza dubbio la caratteristica più direttamente collegabile ai big data, dal momento che si riferisce esplicitamente alla dimensione del fenomeno, cioè alla quantità di dati raccolti finora, che formano la *datasphere*.

Nonostante numerosi siano stati i tentativi di quantificare il volume dei big data e le statistiche<sup>7</sup>, risulta realmente difficile misurare tale caratteristica poiché le statistiche e le ricerche riportano cifre e stime molto diverse tra loro; tuttavia, tutte riportano un dato in comune: la dinamica di crescita esponenziale di questo fenomeno, uno sviluppo continuo che non dà segni di rallentamento e che, si stima, possa crescere nei prossimi anni. Questa costante crescita ha portato anche al cambiamento dell'unità di misura di questa caratteristica: se, in passato, era stato identificato l'*exabyte* come metro quantificatore del fenomeno, oggi bisogna preferire e far riferimento allo *zettabyte* (1000 *exabyte*), dal momento che il primo è risultato essere non più idoneo per la misurazione del volume dei big data. Nella tabella di seguito vengono elencate le unità di misura dell'informazione (vedere Tabella 1 - Le misure dell'informazione).

Per facilitare la comprensione della quantità di 1 ZB si può pensare ad una capacità di archiviazione pari a più di 36.000 anni di video in HD (in termini di durata). L'*International Data Corporation* prevede che, nel 2025, nel mondo ci saranno circa 163 ZB di dati, portato principalmente dall'aumento di consumo di video online e dal numero sempre maggiore di sensori e di sistemi di sensori

---

<sup>6</sup> Nicita, Delmastro, *Big Data – Come trasformano l'economia e la politica*, p.27

<sup>7</sup> Un esempio può essere il progetto pionieristico iniziato nel 2000, nel quale gli economisti P. Lyman e H. Varian si posero il problema di quantificare l'informazione prodotta nel mondo, con riferimento in particolare alla produzione di informazione originale; cfr. URL: <http://www2.sims.berkeley.edu/research/projects/how-much-info>

in rapporto all'*Internet of Things* (IoT), grazie all'arrivo delle nuove connessioni 5G.

Altro aspetto che desta interesse è il valore opzionale di un dato: ogni dato, infatti, può essere utilizzato e analizzato più volte nel tempo. Il valore dei dati, quindi, diventa superiore rispetto a quello che aveva durante il suo primo utilizzo, infatti, numerosi progetti di molte grandi piattaforme online stanno lavorando proprio sul plurimo utilizzo dei dati.

Unità e simbolo	Dimensione	In termini pratici ...
Bit (b)	1 o 0	L'unità di misura elementare dell'informazione, diminutivo di " <i>binary digit</i> " che viene rappresentata alternativamente con le cifre 0 e 1, in quanto corrisponde a una scelta tra due alternative egualmente possibili.
Byte (B)	8 bits	L'informazione utile a creare un singolo carattere nel codice del computer; è l'unità di base di calcolo.
Kilobyte (KB)	1.000 o $2^{10}$ bytes	Una pagina di testo equivale a 2KB. 100KB misurano una immagine fotografica in bassa risoluzione.
Megabyte (MB)	1.000 KB o $2^{20}$ bytes	Un file MP3 di un brano musicale "tipo" è pari a 4MB. 100MB equivalgono ad una pila di libri pari ad un metro.
Gigabyte (GB)	1.000 MB o $2^{30}$ bytes	Un film della durata di circa due ore può essere compresso in 1-2GB. Un testo di 1GB contiene all'incirca 1 miliardo di caratteri, ovvero circa 4.500 libri di 200 pagine o 240.000 caratteri.

## IL PROCESSO DI DIGITALIZZAZIONE E L'AVVENTO DEI BIG DATA

---

Unità e simbolo	Dimensione	In termini pratici ...
Terabyte (TB)	1.000 GB o $2^{40}$ bytes	<p>1TB equivale a 262.144 file MP3 (con una durata media di 4MB). 1TB equivale a circa 4.580.000 libri di 200 pagine. Tutti i libri catalogati nella <i>America Library of Congress</i> ammontano a 15TB. Tutti i <i>tweet</i> inviati prima del 2013 equivalgono ad un file di testo di 18.5TB; per stampare un testo simile (ad una velocità di 15 pagine formato A4 per minuto) ci vorrebbero 1200 anni.</p>
Petabyte (PB)	1.000 TB o $2^{50}$ bytes	<p>1PB corrisponde a circa 4.691.000.000 libri da 200 pagine. La NSA (<i>National Security Agency</i>) analizza circa l'1,6% del traffico internet globale, circa 30PB al giorno. Volendo ascoltare 30PB di musica senza soluzione di continuità, ci vorrebbero più di 60.000 anni.</p>
Exabyte (EB)	1.000 PB o $2^{60}$ bytes	<p>1EB di dati corrisponde ad una capacità di immagazzinamento dei dati corrispondente a 33.554.432 di <i>iPhone 5</i> con una memoria di 32GB. Nel 2018, il volume mensile del traffico dati tramite telefonia mobile si stima ammonti a 1EB; se questo ammontare di dati fosse conservato in smartphone <i>iPhone 5</i> da 32 GB, sarebbe necessario formare una pila di <i>iPhone 5</i> alta 239 l'Empire State Building.</p>
Zettabyte (ZB)	1.000 EB o $2^{70}$ bytes	<p>1ZB corrisponde a 281.474.977.500.000 file MP3 della grandezza media di 4MB, ovvero 250.000.000.000 di DVD da 4,38GB.</p>
Yottabyte (YB)	1.000 ZB o $2^{80}$ bytes	<p>Il contenuto di codice genetico appartenente ad una singola persona può essere immagazzinato in meno di 1,5GB; ciò implica che 1YB può contenere il genoma di 800 trilioni di individui, ovvero 100.000 volte circa la popolazione del pianeta.</p>

*Tabella 1 - Le misure dell'informazione<sup>8</sup>*

---

<sup>8</sup> Fonte: Elaborazione dell'Autorità su dati *Economist*, URL: [www.computerhope.com](http://www.computerhope.com), Cisco e Emmanuel Letouzé

A quest'ultimo punto si può legare il concetto di *data driven economy* che rende chiaro il ruolo sempre più centrale che ha nelle decisioni economiche e sociali l'utilizzo primario e secondario dei dati. Questo è stato possibile grazie alle dinamiche, per esempio, delle piattaforme *social*, sulle quali qualsiasi parola, attività, *like*, reazione, fotografia, documenti o video caricati ogni minuto da milioni di utenti vengono tracciati e trasformati in dati.

L'aumento continuo del volume dei dati, però, porta anche delle problematiche organizzative che necessitano di soluzioni sempre nuove: i dati, infatti, affinché acquistino valore, devono essere archiviati e conservati e questo richiede un costo proporzionale alla loro crescita. Oltre a questo, non bisogna dimenticare che anche l'analisi e la misurazione del valore dei dati ha un costo, che comprende la ricerca e il mantenimento di algoritmi sempre più innovativi e di figure professionali in continua formazione che sappiano gestirne la complessità.

### 1.3.2 La varietà

Una delle altre caratteristiche dei big data è la varietà, intesa come *"eterogeneità nelle fonti sorgenti dei dati, nei formati, con cui vengono acquisite le informazioni (tradizionali / strutturati e, soprattutto, non strutturati) e nella rappresentazione e analisi (anche semantica) dei dati immagazzinati"*<sup>9</sup>.

Come ben sappiamo, quando si parla di big data si fa riferimento non solo ad un grande numero di dati, ma anche ad una vasta eterogeneità riguardo la loro natura: nel mondo big data, infatti, non si parla soltanto di dati strutturati (come poteva essere in ambito di small data), ma anche di dati non strutturati e, cioè, di dati che non possono essere organizzati attraverso precisi schemi, ma

---

<sup>9</sup> AGCOM (2018), *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*. URL: <https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>

che, al contrario, per essere analizzati e creare valore, richiedono *softwares* e tecniche sempre più complesse e specifiche. Questa rappresenta una delle differenze tra small data e big data: quando si parla di small data ci si riferisce a dati prettamente strutturati, organizzati, cioè, secondo particolari strutture di righe e colonne che ne facilitano l'ordinamento e l'elaborazione sulla base di *database* relazionali come RDBMS, fogli di calcolo, *datawarehouse*, *Customer Relationship Management System*, ecc. che ne permettono l'estrazione del valore in modo più agevole e con tecniche consolidate. Oggi è ampiamente riconosciuto che la maggior parte dei dati prodotti (circa l'80%) sia di natura non strutturata.

Questo fattore comporta, di conseguenza, una difficoltà sempre maggiore nella gestione dell'eterogeneità dei dati, per tutti gli enti che si trovano a doverli gestire; diversamente da quanto accade, per esempio, con la problematica del volume dei dati che interessa soltanto alcune aziende o imprese. Queste ultime, infatti, devono essere in grado di gestire sia la possibilità di associare i dati in modi sempre differenti (per ricavarne sempre più valore) sia la diversità di sorgenti dalle quali derivano.

Oltre ai dati strutturati e non strutturati, ne esistono anche di un terzo tipo: i dati semi-strutturati. Questa tipologia comprende e-mail, HTML, RDF, *Electronic Data Interchange*, documenti CSV, XML e JSON. Le e-mail, per esempio, rientrano in questa categoria perché parte dei loro dati possono essere categorizzati e inseriti in schemi ben precisi (data di invio, data di ricezione, mittente, destinatario, oggetto etc.), mentre un'altra parte, come il testo o gli allegati, non rientrano in nessuna struttura perché di diversa natura (si pensi alle varie tipologie di allegati).

### 1.3.3 La velocità

Oltre al volume e alla varietà, a caratterizzare i big data c'è anche la velocità che è legata “*alla alta frequenza con cui i dati circolano da un punto di origine a uno di raccolta*”<sup>10</sup>, cioè ai tempi impiegati per alimentare le banche dati. Anche se la velocità dipende in modo particolare dal progresso tecnologico che va sempre più migliorando i tempi di raccolta dei dati in tempi reali, essa non consiste soltanto in questo. La velocità non comprende soltanto il processo di raccolta dei dati, ma riguarda anche il bisogno di processare nel modo più rapido possibile i dati al fine di ricavarne informazioni, sulla base delle quali prendere delle decisioni anche addirittura in tempo reale (*real time action*). Questo aspetto rappresenta un'altra fonte di valore per i dati, dal momento che la rapidità con la quale vengono processati consente di accedere a maggiori opportunità di business per le aziende che riescono ad anticipare le azioni dei *competitors* nel medesimo mercato.

Jeff Bezos, fondatore di Amazon, sostiene fortemente quanto conti la velocità nel business<sup>11</sup> e spiega quanto potrebbe essere rischioso e quanto potrebbe costare all'azienda attendere di avere il 90% dell'informazione, senza accontentarsi del 70%. Quest'attesa di un'informazione sempre più perfetta o precisa causerebbe sicuramente dei ritardi decisionali che porterebbero l'azienda a perdere diverse occasioni di business.

Nell'atto pratico, comunque, è difficile che tutte le aziende possiedano *softwares* sempre più all'avanguardia per raccogliere, gestire, trattare in modo proficuo e archiviare i dati raccolti: per questo motivo, infatti, esse si affidano ad enti esterni specializzati in questo tipo di servizio e che possiedono i *data*

---

<sup>10</sup> Ibidem

<sup>11</sup> Anita Balakrishnan (2017), *Bezos shareholder letter: Don't let the world push you into becoming a 'Day 2' company*. URL: [www.cnbc.com](http://www.cnbc.com)

center, edifici o strutture che accolgono al loro interno le apparecchiature di elaborazione dei dati di una o più organizzazioni.

Ora risulta interessante analizzare come la velocità abbia caratterizzato la produzione di big data nell'anno 2021 rispetto all'anno 2020. Di seguito, due riepiloghi illustrati su cosa avviene su internet in 60 secondi in tutto il mondo.



Figura 1 - Cosa avviene su Internet in 60 secondi (anno 2020)<sup>12</sup>

<sup>12</sup> Internet Usage is growing, URL: <https://ec.europa.eu/newsroom/rtd/items/713444/en>



Figura 2 - Cosa avviene su Internet in 60 secondi (anno 2021)<sup>13</sup>

Osservando queste due figure (Figura 1 e Figura 2) si possono notare alcuni aspetti molto interessanti: innanzitutto esse mostrano una valida sintesi di come le tre principali caratteristiche dei big data (volume, varietà e velocità) operino in modo sinergico. In secondo luogo, un altro aspetto interessante è rappresentato dal fatto che in tutti gli ambiti si riscontra un aumento di dati; aumento che continua ad essere in costante crescita. In confronto all'anno 2020, infatti, non si sono registrati cali, ma, al contrario, gli aumenti più significativi si possono osservare nei *download* di TikTok, nei dispositivi Amazon Echo spediti e nelle *views* di Twitch.

<sup>13</sup> Ibidem

### 1.3.4 La veridicità

La qualità e l'integrità dei dati compongono la veridicità, altra importante caratteristica che contraddistingue i big data. Questo aspetto risulta essere fondamentale nelle fasi di raccolta e di analisi dei dati, dal momento che è proprio da questo che dipendono analisi utili e affidabili.

La veridicità riguarda gli aspetti qualitativi dei dati e la fiducia che in essi si può riporre<sup>14</sup>; se un'azienda si ritrova a lavorare con dati *fake*, sicuramente le decisioni di business che prenderà potrebbero rivelarsi non del tutto proficue poiché i dati sulle quali sono state pensate e attuate quelle stesse decisioni, si sono rivelati essere non del tutto vicini alla realtà. La veridicità potrebbe compromettere seriamente la correttezza dei risultati delle analisi dei dati raccolti, causando anche diverse potenziali perdite all'azienda.

Riconosciuta e famosa online, e non solo, infatti, è divenuta la concezione secondo cui un dato errato risulta peggiore del fatto di non avere nessun dato (*bad data is worse than no data*): questo ha spinto numerose aziende ed enti di raccolta e gestione dei dati ad avviare procedure di *preprocessing*, al fine di analizzare criticamente i dati raccolti, eliminando quelli non veri o non integri.

### 1.3.5 La valenza

La valenza riguarda la possibilità e la capacità di un dato di legarsi e di creare collegamenti, diretti o indiretti, con altri dati: tanto un dato è connesso con altri, più grande sarà la sua valenza. Questa caratteristica cresce nel tempo, dal momento che i collegamenti tra dati divengono sempre maggiori, specialmente quando un dato viene analizzato più volte e da esso si ricavano sempre più informazioni.

---

<sup>14</sup> M. White, (2012), *Digital workplaces: Vision and reality*, Business Information Review, 29(4) pp. 205–214.

### 1.3.6 La visualizzazione

Con questo termine si fa riferimento all'attività di sintesi e di estrazione delle informazioni essenziali che caratterizzano un dato, in modo da riuscire ad elaborare informazioni sintetiche provenienti da una grande quantità di dati.

Per portare in atto questa attività, numerose piattaforme online propongono gli infografici, complessi schemi grafici, i quali, senza ridurre il valore informativo di un dato, riescono però a sintetizzarne le informazioni.

La difficoltà principale che riguarda la visualizzazione è proprio la complessità di tale attività, perché risulta parecchio complicato riuscire a proporre argomentazioni, storie e informazioni in modo essenziale, senza alterarne il valore.

### 1.3.7 Il valore

Legato a quest'ultima caratteristica vi è l'importanza stessa dei big data: essi, infatti, rappresentano un'ottima risorsa per molti aspetti economici di oggi proprio perché dalle informazioni dei dati si può estrarre un valore, non solo a livello economico o di business, ma anche a livello di benessere collettivo della società odierna.

Le nuove tecniche di analisi, sempre più sofisticate, permettono infatti di rendere migliore le prestazioni, nate da un più preciso processo decisionale, e di migliorare l'efficienza e la qualità dei servizi o dei prodotti offerti, rendendoli sempre più innovativi e personalizzati<sup>15</sup>.

Per capire quanto sia alta l'importanza del valore dei dati per le aziende basti notare una pratica assai diffusa nell'universo digitale di oggi: molte

---

<sup>15</sup> AGCOM, AGCM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2020), *Indagine conoscitiva sui BigData*. URL: <https://www.agcom.it/documents/10179/17633816/Documento+generico+10-02-2020+1581346981452/39c08bbe-1c02-43dc-bb8e-6d1cc9ec0fcf?version=1.0>

imprese, infatti, sono anche disposte ad offrire gratuitamente al consumatore alcuni dei loro servizi in cambio del suo consenso alla raccolta e all'utilizzo dei dati che egli stesso produce in quel momento, magari proprio usufruendo di quello stesso servizio.

### 1.4 LIMITI DEI BIG DATA

Nonostante diversi siano gli aspetti positivi legati al mondo dei big data e al loro utilizzo, ci sono anche diversi rischi nati come conseguenza della complessità di questo fenomeno. Principalmente i rischi legati alla raccolta e all'utilizzo dei big data sono tre e si possono riassumere in: privacy dei dati, sicurezza dei dati e discriminazione dei dati.<sup>16</sup>

Uno di questi è rappresentato proprio dalla raccolta sempre più pervasiva di informazioni legate alle preferenze o alle abitudini delle persone; queste informazioni, poi analizzate, hanno permesso di creare sempre più modelli di proposte personalizzate e innovative. Mentre da un certo punto di vista questo potrebbe rappresentare un aspetto positivo, specialmente per le aziende, esso diviene complesso quando si fa riferimento al concetto di tutela della privacy. Come sappiamo, il valore dei big data non è legato soltanto alla raccolta di grandi quantità di informazioni qualitativamente valide, ma anche e soprattutto alla possibilità successiva di supportare o permettere, in qualunque momento, processi decisionali sempre diversi: proporzionalmente, infatti, più aumenta il volume dei dati, più esso si trasforma in conoscenza.

Per quanto riguarda la sicurezza dei dati, con il continuo aumento del volume dei dati e dei dispositivi connessi, una parte dei dati raccolti viene esposta a potenziali violazioni di sicurezza; questo fatto, purtroppo, deve fare i

---

<sup>16</sup> Per approfondimenti si veda 3. *Massive Big Data Problems Everyone Should Know About*, (2017), URL: <https://www.forbes.com/sites/bernardmarr/2017/06/15/3-massive-big-data-problems-everyone-should-know-about/>

conti anche con il numero insufficiente di professionisti sempre più aggiornati nel settore di protezione dei dati digitali nelle aziende: non tutte le aziende ne hanno.

Il terzo aspetto critico riguarda la discriminazione delle persone: conosciute tutte le informazioni dei consumatori, sarà necessariamente indispensabile per le aziende procedere con determinate decisioni su prodotti o servizi per soddisfare il maggior numero di consumatori, piuttosto che su altre scelte che invece soddisferebbero un numero minore di consumatori. In questo caso i big data diventano uno strumento per l'inclusione, o piuttosto, per l'esclusione?<sup>17</sup>

Infine, un'ulteriore criticità legata a quell'aspetto è anche rappresentata dal fatto che l'ecosistema dei big data sia composto da un livello di interconnessione tra i vari soggetti che vi partecipano tale da rendere difficile l'individuazione di singoli mercati ben definiti. Questa complessità, frutto di queste dinamiche, contribuisce a creare un contesto in cui le diverse parti del sistema risultano spesso in stretta relazione tra loro. In tale contesto sono più facilitate ad operare poche grandi imprese multinazionali, caratterizzate da un più alto livello di integrazione in tutte le fasi dell'ecosistema, accanto ad una vasta quantità di piccole imprese specializzate.

### 1.5 LA CATENA DEL VALORE NELL'ECOSISTEMA BIG DATA

Quando si parla della catena di valore nell'ecosistema big data si fa riferimento ad un preciso schema, denominato anche *data science process*, che permette di chiarire quali siano gli step necessari per l'estrazione del valore dei

---

<sup>17</sup> Federal Trade Commission Report (2016), *BIG DATA – A Tool for Inclusion or Exclusion? Understanding the issues*, URL: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

dati. Si può assumere che questa catena del valore rappresenti il vero e proprio ciclo di vita di un dato<sup>18</sup>, poiché dopo la fase di raccolta si susseguono tutta una serie di fasi interconnesse e interdipendenti, le quali contribuiscono ad aumentarne il valore. Di seguito, nella Figura 3, vengono elencate le fasi che caratterizzano la catena del valore nei big data<sup>19</sup>.

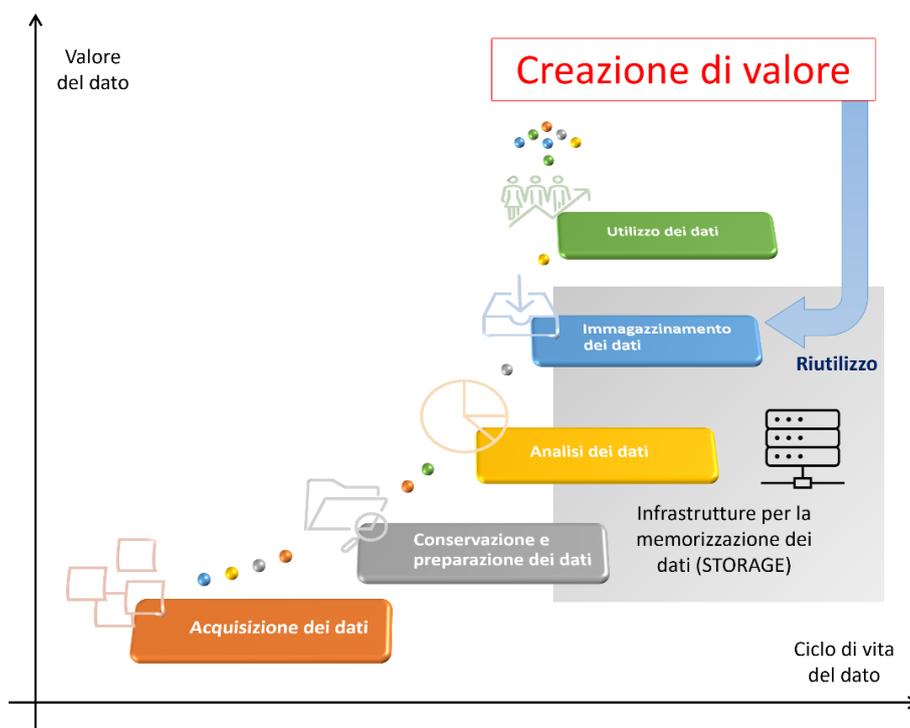


Figura 3 - Valore e ciclo di vita del dato

Il primo momento nella catena del valore dei big data è rappresentato dall'acquisizione dei dati, che comprende non solo l'individuazione del dato stesso, ma anche la sua aggregazione con altri dati. In altri termini, quindi, in questa fase il dato passa da una fonte ad un sistema di smistamento di dati. Dal momento che, per garantire una bassa latenza e per eseguire correttamente

<sup>18</sup> Ibidem

<sup>19</sup> Per ulteriori approfondimenti, si consulti il Report *European Data Market* redatto a cura della IDC e Open Evidence per conto della Commissione Europea, febbraio 2017, URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2017:0495:FIN:IT:PDF>

questa fase è necessario soddisfare dei requisiti minimi, spesso essa necessita di considerevoli sforzi finanziari per gli investimenti infrastrutturali indispensabili: infatti, l'acquisizione dei dati avviene attraverso diversi strumenti come gli applicativi di condivisione, le API di coloro che forniscono i dati originati sui *social network*, o ancora, gli strumenti di *web scraping* ed ETL (*Extract/Transform/Load*). Tuttavia, oggi, si è diffusa una pratica piuttosto comune, agevolata dal progresso tecnologico e dalla nascita di altre strumentazioni che permettono il tracciamento delle scelte e delle abitudini dei consumatori: si tratta della *over collection*<sup>20</sup>, attività che prevede la raccolta di dati in volume e varietà maggiori di quelli necessari per le finalità dichiarate. Questa *over collection* è stata resa possibile grazie a tre tipologie diverse di tracciamento, presenti sul web:

- *Cookie* → “I cookie (“biscotto” in inglese) sono dei piccoli file di testo necessari affinché il server del sito web che li ha installati possa ottenere informazioni sulla specifica attività che l'utente compie su quelle pagine web. Che si è collegato a quel sito e che cosa vi ha fatto. Ogni volta che quel dispositivo si ricollega al sito gli rimanda il cookie e così è possibile riconoscere e tracciare l'attività a distanza di tempo”<sup>21</sup>.
- *Tracking pixels* → o *web beacons*, immagini a volte invisibili, contenute in e-mail o pagine internet che, vengono richieste nel momento in cui il motore di ricerca riceve l'invio per scaricare il sito o l'e-mail. In quel momento la richiesta arriva al proprietario

---

<sup>20</sup> Dal report *Big data and Privacy: A Technological Perspective* a cura del “President's Council of Advisors on Science and Technology, (2014)

<sup>21</sup> *Cookie: cosa sono, come funzionano e come proteggerli*, (2020), URL: <https://www.agendadigitale.eu/infrastrutture/tutto-quello-che-dobbiamo-sapere-sui-cookie-per-la-privacy-da-utenti-o-gestori/>

dell'immagine o del *pixel* che può tracciare l'evento, le informazioni di base e l'indirizzo IP del visitatore.

- *Browser fingerprinting* → grazie alla configurazione del browser di un utente (sistema operativo, *plugin*, fuso orario, risoluzione dello schermo, fonti utilizzati etc.) questa tecnica permette di identificarlo e di raccogliere tutto quell'insieme di dati.

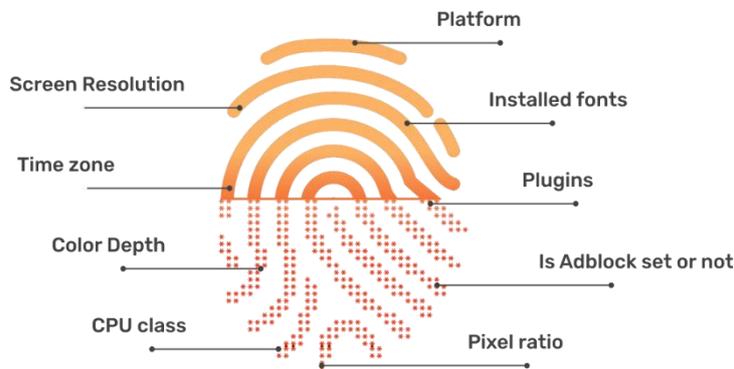


Figura 4 - Browser fingerprinting<sup>22</sup>

All'acquisizione succede una seconda fase di elaborazione, cioè la preparazione del dato e la sua conservazione per gli utilizzi che l'azienda o l'ente vorrà farne; è proprio in questa fase che ogni singolo dato inizia a tramutarsi in informazione. Non è un processo così semplice, dal momento che, come riporta il report dell'AGCOM,

*“affinché i dati grezzi (raw data) si trasformino in informazione, [...] diventa necessario possedere le strumentazioni e le competenze che consentano di affrontare i problemi connessi alla varietà dei dati e, quindi, generare i presupposti affinché diversi tipi di dati possano interloquire tra loro, spesso in tempo reale. Si tratta di implementare quelle infrastrutture (in termini principalmente di dotazione di capacità*

---

<sup>22</sup> *Understanding Canvas Fingerprinting*, (2021), URL: <https://gologin.com/what-is-canvas-fingerprinting>

*elaborativa e software) grazie alle quali si garantisce sia una facile scalabilità dei dati, sia una loro corretta conservazione.”<sup>23</sup>*

La fase successiva porta alla trasformazione dell'informazione del dato in conoscenza dell'evento, del fenomeno o dell'attitudine ricercata: questa fase è composta dall'esplorazione, dalla trasformazione e dalla modellazione e prende il nome di analisi dei dati. Proprio in questa fase vengono sintetizzate le informazioni per riuscire a scovare anche quelle più indirette e, nello stesso tempo, si cerca di mettere in luce quelle più rilevanti.

La memorizzazione dei dati e il loro immagazzinamento rappresentano lo step successivo: per poterlo eseguire al meglio bisogna far fronte alla problematica dell'aumento del volume dei dati, che in un modo o nell'altro, influenza la velocità e l'efficienza con le quali si accede ai dati, compromettendo potenzialmente i processi decisionali delle imprese. Proprio per questo motivo, molte aziende hanno optato per la scelta dei *database* distribuiti: memorie di massa di diversi computer che compongono la rete di un'organizzazione con diversi centri di archiviazione. Concentrare tutta la memorizzazione delle informazioni in un solo centro (detto nodo) può essere controproducente per l'organizzazione stessa: in termini pratici, dal momento che potrebbero innescarsi problemi di congestione per l'eccessivo flusso di informazioni e, in secondo luogo, ma non meno importante, in termini di sicurezza, poiché centralizzare tutti i dati in un solo nodo renderebbe più vulnerabile tutto il sistema.

Tuttavia, anche se le informazioni sono localizzate tra loro in luoghi lontani fisicamente, risulta necessaria un'integrazione di tipo logico tra i diversi archivi perché, per garantire l'efficacia di un sistema di *database* distribuiti, bisogna attuare una corretta gestione degli stessi. In questo modo, diventa

---

<sup>23</sup> AGCOM (2018), *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*. URL: <https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>

possibile permettere a tutti gli utenti del suddetto sistema di *database* distribuiti accedere a tutte le informazioni necessarie e costantemente aggiornate, qualunque sia la loro posizione geografica.

L'ultima fase, denominata utilizzo dei dati, è il risultato della lavorazione dei big data attraverso le fasi precedenti e rappresenta il momento in cui il dato, "*da semplice conoscenza, si trasforma in visione dei fatti*"<sup>24</sup>, per essere utilizzato per compiere decisioni, quindi, come supporto dei processi decisionali. Questo aspetto si traduce semplicemente nel trovare un accostamento tra le informazioni ricavate ed elaborate e le azioni e scelte intraprese dalle aziende: alcuni esempi possono essere l'organizzazione del personale, l'ideazione di nuovi servizi, la fabbricazione di nuovi prodotti, la riduzione dei costi di produzione; insomma, tutto ciò che potrebbe comportare un miglioramento dell'offerta e degli indici di performance verso i consumatori.

Un esempio pratico di questa dinamica lo si può trovare prendendo in considerazione il funzionamento dei browser: più ricerche vengono effettuate attraverso questi motori, maggiori saranno i livelli di miglioramento dei motori di ricerca e, quindi, la precisione e l'attinenza delle ricerche stesse. Tale miglioramento del servizio porterà poi un maggior numero di persone ad utilizzare quello stesso browser.

In ambito aziendale, invece, un'altra finalità di utilizzo e di riutilizzo dei dati la si può ritrovare nel creare e sfruttare nuove possibilità di business grazie all'offerta di prodotti e servizi sempre più recenti.

Questo aspetto, però, non riguarda soltanto le aziende e le imprese private, ma anche gli enti pubblici negli ambiti dell'offerta di nuovi servizi, nel diverso utilizzo delle risorse e nel miglioramento dei servizi già presenti.

---

<sup>24</sup> Ibidem

## CAPITOLO 2

### UNO SGUARDO ALLA NORMATIVA EUROPEA ED EXTRA EUROPEA SUL TRATTAMENTO DEI DATI PERSONALI

Dall'avvento del fenomeno della digitalizzazione, dalla nascita dei *social networks* fino ad arrivare al continuo incremento dell'*Internet of Things*, la pervasività della rete ha messo al centro dell'odierno sistema economico i dati personali e, la loro analisi, attraverso *software* sempre più innovativi, rappresenta il motore delle principali decisioni prese in ambito economico e, sempre più spesso, anche politico<sup>1</sup>.

Questo è stato reso possibile dal fatto che, oggi, i confini della cosiddetta privacy sono molto confusi e, non sempre, le aziende, le piattaforme, i motori di ricerca o altri enti riescono a proteggere in modo sicuro e adeguato la mole di dati che raccolgono e utilizzano, non importa quanto famose o importanti essi siano.

Uno dei primi esempi di questo tipo di situazione lo si può ritrovare nel 2011, nel caso che ha visto come vittima informatica la multinazionale giapponese Sony, alla quale sono stati rubati, per mano degli hacker, i dati personali (informazioni anagrafiche, di contatto, di residenza, bancarie etc.) di

---

<sup>1</sup> Per approfondimenti si veda Rodotà S. (2009), *Data Protection as a Fundamental Right*. In: Gutwirth S., Pouillet Y., De Hert P., de Terwangne C., Nouwt S. (eds) *Reinventing Data Protection?*, Springer, Dordrecht, p. 82, «any changes affecting data protection impact on the degree of democracy we all can experience»

77 milioni di individui<sup>2</sup>. La questione ha raggiunto un ulteriore livello di gravità, poiché la società nipponica non ha avvisato subito i proprietari dei dati, ma questo è avvenuto soltanto sette giorni dopo. Di esempi come questo se ne possono trovare molti nel corso degli ultimi anni e, purtroppo, sono dovuti ad una mancanza di normativa sulla protezione dei dati su scala mondiale.

Tali situazioni hanno portato ad una rivalutazione dei concetti di riservatezza e di privacy, i quali, inizialmente erano considerati soltanto dal punto di vista individuale e personale, mentre, ora, hanno assunto anche la natura di una questione a livello collettivo<sup>3</sup>.

Il diritto alla protezione dei dati, la *Data protection*, è uno strumento essenziale al fine di permettere lo sviluppo libero e incondizionato della personalità individuale<sup>4</sup> e la sua tutela risulta, specialmente oggi, fondamentale.

Nonostante ciò, però, come accennato precedentemente, non esiste una normativa per la protezione dei dati condivisa e sottoscritta da tutti i Paesi a livello mondiale: parecchie difficoltà nel raggiungerla sono rappresentate dalla contrapposizione tra il diritto alla privacy e il diritto di espressione oppure dal diritto alla privacy e la sicurezza nazionale.

Tuttavia, al fine di contrastare l'eccessiva invadenza delle attività di sfruttamento dei dati, i regolatori della privacy di diverse giurisdizioni hanno provato a proteggere le scelte personali dei consumatori attraverso la richiesta

---

<sup>2</sup> Keith Stuart and Charles Arthur, 27 aprile 2011, *PlayStation Network hack: why it took Sony seven days to tell the world*, The Guardian, URL:

<https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony>

<sup>3</sup> S. Zuboff, novembre 2019, *Molte sfaccettature di un solo diamante*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, URL:

<https://www.garanteprivacy.it/documents/10160/0/Privacy+2030+-+Un+manifesto+per+il+nostro+futuro+-+Volume.pdf/8a243e2f-53e9-8dfa-a3be-0e80347499d3?version=2.1>, p. 47.

<sup>4</sup> S. Calzolaio, (2017), *Protezione dei dati personali*, Utet, Torino, cit., p. 603; C. D'Cunha, *Idee di Giovanni Buttarelli, trascritte da Christian D'Cunha*, cit., *passim*

alle aziende di ottenere il cosiddetto consenso informato da parte dell'utente sulla raccolta e sull'utilizzo dei propri dati, imponendo sanzioni pecuniarie alle imprese che non vogliono applicarlo. Sebbene questo consenso informato esista, non sempre esso è del tutto volontario: è quasi diventata abituale la situazione in cui il consumatore, per ottenere il servizio desiderato, si trova a cedere i propri dati pur di usufruirne. Questo tipo di atteggiamento è reso possibile dal potere di mercato delle aziende stesse che attuano politiche sulla privacy a dir poco "abusanti" nei confronti degli utenti. Come specificato da Yassine Lefouili e da Ying Lei Toh nella loro ricerca, *"un modo per prevenire pratiche abusive sui dati da parte delle grandi aziende tecnologiche è attraverso restrizioni normative sui modi in cui queste aziende raccolgono e utilizzano i dati dei consumatori"*<sup>5</sup>.

A riguardo, è importante sottolineare che l'Unione Europea, nonostante le diverse difficoltà sorte a causa dell'a-territorialità di Internet, ha provveduto alla proposta e all'applicazione di un regolamento valido nei territori di tutti gli Stati membri, mostrandosi molto attenta alla protezione dei dati dei cittadini europei.

Oltre a questo, sul livello internazionale, sempre grazie alla stessa Unione Europea, è stato raggiunto un regolamento che rappresenta un utile strumento legale per la protezione degli individui in tema di trattamento automatizzato dei dati personali: la Convenzione di Strasburgo del 1981, detta più comunemente, Convenzione 108 del Consiglio d'Europa, vincolante giuridicamente per tutti gli Stati firmatari (anche non membri dell'UE) che vi aderiscono. Il testo di questa convenzione ha subito un protocollo di modifica nel 2018 con lo scopo di modernizzarlo, introducendo innovazioni rilevanti riguardo i diversi principi da rispettare e riguardo il tema giuridico, prendendo infine il nome di Convenzione 108+.

---

<sup>5</sup> Yassine Lefouili e Ying Lei Toh, (2019), *Privacy Regulation and Quality Investment*

## 2.1 IL DIRITTO AL RISPETTO DELLA VITA PRIVATA E IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

Generalmente, quando si utilizza il termine privacy si fa riferimento non solo alle questioni che riguardano la vita privata di un individuo, ma anche a tutto ciò che può essere considerato un'informazione personale che lo riguarda. Il termine privacy, quindi, ha assunto un significato più generico rispetto a quello che rappresenta in realtà. Tuttavia, se si fa riferimento ad argomentazioni in materia di diritti, risulta funzionale e doveroso utilizzare la terminologia corretta, in base alle definizioni precise di ogni espressione. Infatti, il diritto al rispetto alla vita privata e il diritto alla protezione dei dati personali sono due diritti differenti, anche se connessi. Il primo è stato sancito nel 1948 a livello mondiale nella Dichiarazione Universale dei Diritti dell'uomo (UDHR) e, in seguito, nel 1950 anche nella Dichiarazione Europea dei Diritti dell'Uomo (CEDU)<sup>6</sup>, nella quale, attraverso l'articolo 8 si evince che:

*“Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.”<sup>7</sup>*

Con l'avvento della digitalizzazione e lo sviluppo dei sistemi informatici, a causa della nascita di nuovi rischi per la tutela del diritto al rispetto della vita privata, è stato necessario ridefinire la nuova situazione introducendo

---

<sup>6</sup> FRA e Consiglio d'Europa, (2018), *Manuale sul diritto europeo in materia di protezione dei dati*, p.20

<sup>7</sup> Council of Europe, (1950), *European Convention on Human Rights*, p.11

un nuovo concetto, quello di autodeterminazione informativa<sup>8</sup>, grazie al quale si è arrivati alla nascita di normative che prevedono anche la protezione dei dati personali.

Il primo esempio di normativa volta a tutelare i dati personali degli individui la si ritrova intorno al 1970, in Germania, nello stato dell'Assia; qualche anno dopo, la Svezia ha mosso un passo in più verso una legge nazionale per la protezione dei dati personali, sancita nel 1973: è stato il primo Paese al mondo ad applicare una normativa a livello nazionale riguardo questo ambito. Soltanto tra gli anni '80 -'90 anche altri Paesi europei, come Francia, Regno Unito, Germania e Paesi Bassi hanno seguito l'esempio della Svezia, adottando anch'essi una normativa nazionale in merito.

Nel corso degli anni il concetto di protezione dei dati si è consolidato grazie a diversi strumenti utilizzati a livello europeo in ambito informatico e oggi esso non coincide con il diritto al rispetto della vita privata, poiché, nell'ordinamento giuridico europeo, è diventato esso stesso un diritto: il diritto alla protezione dei dati.

Appare funzionale, quindi, analizzare e determinare le principali analogie e differenze tra questi due diritti: entrambi, infatti, hanno l'obiettivo di tutelare l'autonomia e la dignità dell'individuo, permettendogli di poter esprimere la propria personalità, il proprio pensiero e di formarsi un'opinione sulle varie situazioni. Entrambi i diritti permettono, quindi, di esercitare le libertà fondamentali dell'essere umano (di espressione, di associazione, di religione etc.).

Le differenze principali riguardano, invece, la loro formulazione e il loro ambito: mentre il diritto al rispetto della vita privata prevede un chiaro divieto di intromissione nelle questioni personali di un individuo, il diritto alla

---

<sup>8</sup> Corte EDU, (2017), *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, n. 931/13, 27 giugno 2017, punto 137

protezione dei dati prevede un insieme di controlli applicati al fine di proteggere l'individuo tutte le volte che vengono raccolte, utilizzate ed elaborate delle informazioni, dei dati che lo riguardano. Queste azioni vengono generalmente accomunate con il termine "trattamento", processo che viene regolarizzato secondo specifici criteri enunciati nell'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea:

- "1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
- 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*
- 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."*<sup>9</sup>

In questo articolo vengono sottolineate, infatti, le finalità e le modalità attraverso le quali agire il trattamento dei dati degli individui: è sempre necessario il consenso dello stesso e devono esserci degli scopi specifici e determinati, oltre che mantenere valido il principio di lealtà nell'utilizzo dei dati.

Il diritto alla protezione dei dati si esercita in tutti i momenti e in tutte le situazioni in cui vengono raccolti, analizzati, elaborati e archiviati dei dati personali: il suo ambito, quindi, è molto più ampio di quello del diritto al rispetto della vita privata, anzi si può affermare che il primo potrebbe comprendere il secondo. La protezione dei dati, infatti, raccoglie il trattamento e tutte le

---

<sup>9</sup> Consiglio Europeo e Commissione Europea, (2000), *Carta dei diritti fondamentali dell'Unione Europea*, art.8

tipologie di dati, a prescindere dal fatto che siano legati alla sfera del privato o meno.

Il diritto al rispetto della vita privata si esercita in tutte quelle situazioni che presentano informazioni legate alla sfera intima di un individuo, informazioni sensibili e riservate, che potrebbero compromettere l'immagine dell'individuo stesso nei confronti del gruppo sociale in cui vive, influenzando il suo stile di vita e i comportamenti attuati dagli altri individui nei suoi confronti.

## 2.2 COME SIAMO ARRIVATI AL GDPR?

Per arrivare a parlare del Regolamento Generale sulla Protezione dei Dati (GDPR)<sup>10</sup>, è indispensabile comprendere il contesto sociale e normativo che lo ha preceduto e che lo ha prodotto.

Dal punto di vista storico bisogna partire dagli anni che vanno dal termine del secondo conflitto mondiale e a quelli della Guerra Fredda, durante i quali si sentiva il bisogno di proteggere la sfera privata degli individui dallo Stato. A tal fine vengono redatti due documenti che contengono due norme che si pongono lo scopo di tutelare la riservatezza dei cittadini:

- L'articolo 8 della CEDU<sup>11</sup> (riportato in precedenza) che sancisce il diritto al rispetto della propria vita privata;
- L'articolo 2 della Costituzione italiana<sup>12</sup>, la quale sancisce il rispetto dei diritti fondamentali dell'uomo sottolineando che

---

<sup>10</sup> General Data Protection Regulation - Regolamento EU-GDPR 2016/679

<sup>11</sup> Pubblicato nel 1950

<sup>12</sup> In vigore dal 1947

l'individuo è al centro rispetto allo Stato e che la Repubblica ha il dovere di riconoscerli e di tutelarli.

Trent'anni dopo, proprio nella Germania ancora divisa dal muro di Berlino e a contatto con un'Unione Sovietica che controllava completamente i suoi cittadini, per timore del pericolo di una dittatura, viene sancita dallo stato federale dell'Assia la prima legge per la protezione dei dati personali.

Nel 1981, a motivo del veloce diffondersi dei sistemi informatici di massa e del rapido sviluppo della digitalizzazione, il Consiglio d'Europa elabora e pubblica il più grande documento in ambito europeo in tema di protezione dei dati, la famosa Convenzione 108, nata per tutelare i dati degli individui. In questo documento vengono anche spiegati la definizione di dato personale e il suo legame intrinseco con la libertà individuale, la quale va tutelata da tutte le tipologie di controllo alle quali viene sottoposta; infine viene anche spiegato cosa sia il trattamento attraverso la gestione automatizzata dei dati e il diritto che ogni individuo ha di conoscere la procedura di analisi dei propri dati e chi la elabora.

Con la nascita della Comunità Europea (CE) nel 1993<sup>13</sup> si è poi arrivati alla costituzione di un'area di libera circolazione delle persone e delle merci: nel 1995 è entrata in vigore la Convenzione di Schengen. Con la nascita di un mercato unico europeo, quindi, era anche lecito un libero scambio di dati a livello europeo: tale situazione rappresentò una questione da prendere in considerazione, dal momento che mancavano delle normative nazionali che regolamentassero questo libero scambio di dati e il quadro normativo dei diversi Stati membri era molto disomogeneo. Per ovviare a questa situazione, la Comunità Europea adotta la Direttiva 95/46 nella quale vengono specificate delle disposizioni a livello indicativo riguardanti le finalità da raggiungere, ma

---

<sup>13</sup> Trattato di Maastricht

## UNO SGUARDO ALLA NORMATIVA EUROPEA ED EXTRA EUROPEA SUL TRATTAMENTO DEI DATI PERSONALI

lasciando ad ogni Paese una libera interpretazione e la possibilità di emanare leggi nel rispetto delle indicazioni della direttiva stessa.

Nel 2007 si giunge poi al Trattato di Lisbona, che ha come finalità quella di porre gli obiettivi dell'Unione Europea; uno tra questi è proprio il rispetto dei diritti umani. Tale trattato permette, quindi, alla Carta di Nizza<sup>14</sup> del 2001 di ottenere valore giuridico, dal momento che rappresenta il documento chiave in tema di diritti dell'uomo nell'Unione Europea. Tra i diritti elencati nella Carta dei diritti dell'uomo, come già espresso in precedenza, all'articolo 8 si trova il riferimento alla tutela dei dati personali. È proprio grazie a questo fatto che il GDPR, che verrà emanato nel 2016, assumerà la sua validità giuridica.

Di seguito viene riportata uno schema riassuntivo delle principali normative, elencate dal punto di vista cronologico, volte alla tutela del diritto al rispetto della vita privata e alla tutela del diritto alla protezione dei dati personali.

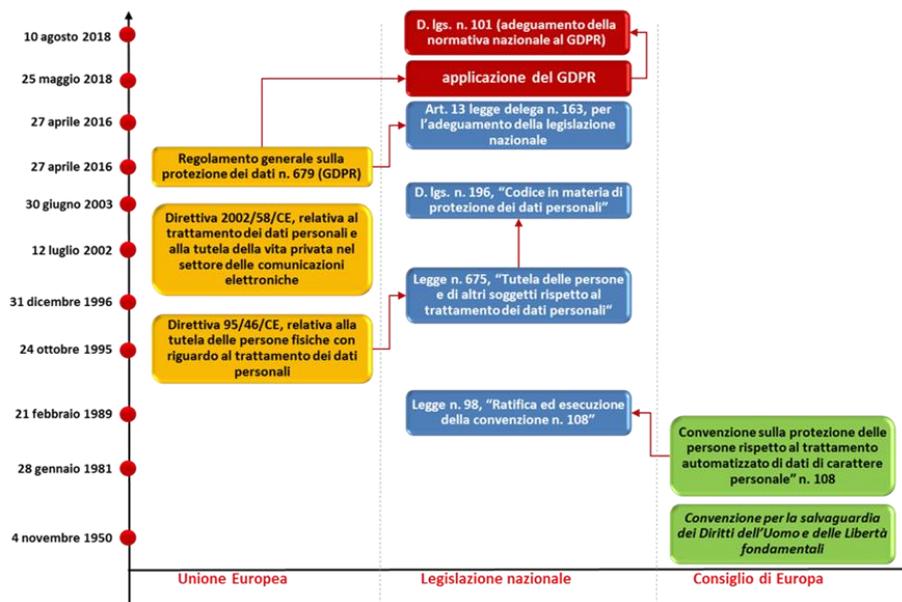


Figura 5 - I principali step verso il GDPR

<sup>14</sup> Carta dei diritti fondamentali dell'Unione Europea

## 2.3 LE CARATTERISTICHE PRINCIPALI DEL DGPR

Entrato in vigore nel maggio 2016, ma attuato soltanto a partire dal maggio 2018, il Regolamento Generale per la Protezione dei Dati<sup>15</sup> nasce con lo scopo di rafforzare e consolidare la protezione dei dati personali, e sostituisce la direttiva 95/46. Attraverso questo regolamento, infatti, vengono fornite a tutti gli Stati membri delle direttive da integrare a quelle già presenti nel Paese. In Italia, per esempio, il GDPR è stato integrato alla già presente normativa del Codice Privacy<sup>16</sup>, il quale è stato novellato e adattato al Regolamento europeo nell'anno 2018.

Il GDPR regola il trattamento dei dati personali degli individui residenti nel territorio dell'Unione Europea e interessa non solo le aziende o gli enti europei, ma anche quelli appartenenti ad altri Paesi extra UE. Proprio questa rappresenta una notevole differenza rispetto alla Direttiva 95/46 e la si ritrova nell'articolo 3, riportato di seguito:

*“Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione”<sup>17</sup>.*

La motivazione legata a questo aspetto del regolamento è dovuta principalmente a due fattori:

---

<sup>15</sup> General Data Protection Regulation – Regolamento EU-GDPR 2016/679

<sup>16</sup> Decreto Legislativo 30 giugno 2003, n196

<sup>17</sup> *Regolamento Generale Sulla Protezione Dei Dati, GDPR*, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. URL: <https://www.garanteprivacy.it/il-testo-del-regolamento>

- il rischio che i dati dei cittadini europei vengano raccolti e analizzati secondo procedure regolamentate da normative meno restrittive e più facilmente aggirabili;
- a causa della disparità di rigidità tra normative di Paesi extra UE, il rischio che le imprese europee possano trovarsi in svantaggio rispetto alle aziende estere concorrenti<sup>18</sup>.

Nell'articolo 4 vengono poi elencati e definiti quali sono i principali soggetti e argomenti che il regolamento affronta; viene data una definizione di dato personale, di trattamento, di profilazione, di limitazione di trattamento di archivio e di altri concetti. I soggetti che vengono descritti sono i principali attori del regolamento, detentori di diritti e doveri:

- *data subject*: la persona alla quale si riferiscono i dati, cioè l'interessato al trattamento. In questo regolamento viene sottolineata l'importanza di questa figura, dal momento che il suo consenso diviene condizione indispensabile per avviare la raccolta e il trattamento dei suoi dati. Tale consenso, inoltre, deve possedere determinate caratteristiche (non attraverso caselle preselezionate, per esempio): esso, infatti, deve essere necessariamente sotto forma di affermazione;
- *data controller*: l'ente (una persona, un'azienda, un servizio o un'autorità) che determina gli scopi, le modalità e gli strumenti necessari per il trattamento dei dati, cioè il titolare del trattamento stesso;

---

<sup>18</sup> Lucarelli S, Musolino E., Rocchi G., Ciacciarelli S., Laniado D., Espelt R., Senabre E., Morell M., Bria F, (2017), *Economic and regulatory analysis of data platforms and value creation models of the on demand economy*, DECODE, Project n. 732546

- *data processor*: l'ente (una persona, un'azienda, un servizio o un'autorità) che elabora i dati per conto del *data controller*; si tratta in questo caso del responsabile del trattamento.

Nell'articolo 5 vengono spiegati quali sono i sette principi cardine sui quali si basa tutto il regolamento riguardo la protezione dei dati<sup>19</sup>. Viene infatti esplicitato che i dati sono:

- *“trattati in modo lecito, corretto e trasparente nei confronti dell'interessato”*<sup>20</sup>, tale principio fa riferimento ai concetti di liceità, correttezza e trasparenza. Un dato viene trattato in modo lecito quando viene chiesto e viene data all'interessato la possibilità di dare il proprio consenso informato per il trattamento. La trasparenza riguarda invece un obbligo da parte del titolare o del responsabile del trattamento nel dare all'interessato tutte le informazioni riguardo il trattamento (identità del titolare, finalità, diritti del *data subject*), in modo che esse siano chiari.
- *“raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità”*<sup>21</sup>: in questo punto, sottoscritto come limitazione delle finalità, viene esplicitato che le finalità per la raccolta e il trattamento dei dati devono essere precisate, chiare e regolari.

---

<sup>19</sup> *Regolamento Generale Sulla Protezione Dei Dati*, GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Art.5. URL: <https://www.garanteprivacy.it/il-testo-del-regolamento>

<sup>20</sup> Ibidem

<sup>21</sup> Ibidem

- *“adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”*<sup>22</sup>: questo principio fa riferimento alla cosiddetta minimizzazione dei dati, che prevede che i dati raccolti siano adatti agli scopi dichiarati;
- *“esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati”*<sup>23</sup>: è il principio che riguarda l’esattezza dei dati e il loro eventuale aggiornamento;
- *“conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati...”*<sup>24</sup>: è il principio denominato limitazione della conservazione ed impone che i dati siano mantenuti in modo che, per il periodo di conservazione previsto dalle finalità, possano essere ritrovati dai soggetti ai quali si riferiscono;
- *“trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali”*: secondo il principio di integrità e riservatezza, i dati devono essere protetti da diversi fattori con sistemi di sicurezza adeguati;
- *“il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo”*<sup>25</sup>: l’ultimo principio in

---

<sup>22</sup> Ibidem

<sup>23</sup> Ibidem

<sup>24</sup> Ibidem

<sup>25</sup> Ibidem

elenco fa riferimento alla responsabilizzazione, secondo il quale il titolare del trattamento è responsabile dell'osservanza delle direttive precedenti e deve anche dimostrarne il rispetto.

Una delle caratteristiche più interessanti di questo regolamento è rappresentato dall'art.17 che difende il rinomato diritto alla cancellazione o all'oblio: *“L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali...”*<sup>26</sup>. Questo diritto prevede la cancellazione dei propri dati, se richiesto, in forma rafforzata; con ciò si intende che i titolari dei dati, nel caso in cui abbiano reso pubblici i dati dell'utente, devono informare anche gli altri titolari che utilizzano quegli stessi dati della richiesta di cancellazione in qualunque caso (anche se si trovano in link, in copie o in riproduzioni)<sup>27</sup>.

Un altro aspetto che merita essere approfondito è quello che riguarda l'articolo 20 del GDPR, il quale espone il diritto, da parte dell'interessato, alla portabilità dei dati<sup>28</sup>. Tale diritto permette al soggetto di ottenere, previa richiesta scritta, i propri dati da parte del titolare del trattamento; questi dati devono essere consegnati all'individuo in formato *“strutturato, di uso comune e leggibile da dispositivo automatico”*<sup>29</sup> e possono essere trasmessi ad un altro ente, senza impedimenti o ostacoli. Grazie a questo diritto per gli individui è possibile scegliere anche altri fornitori di servizi, evitando così che si formino fenomeni di *lock in*, cioè di blocco all'interno di un servizio. Questo diritto

---

<sup>26</sup> *Regolamento Generale Sulla Protezione Dei Dati*, GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Art.17 URL: <https://www.garantepriacy.it/il-testo-del-regolamento>

<sup>27</sup> Per approfondimenti si veda: *Diritto all'oblio*, URL: <https://www.garantepriacy.it/regolamentoue/oblio>

<sup>28</sup> *Regolamento Generale Sulla Protezione Dei Dati*, GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Art.17 URL: <https://www.garantepriacy.it/il-testo-del-regolamento>

<sup>29</sup> Ibidem

contribuisce, quindi, ad aumentare il controllo che un soggetto ha sulle proprie informazioni e stimola l'economia digitale, favorendo il libero spostamento dei dati. Inoltre, esso, attraverso la circolazione dei dati da un servizio ad un altro, accresce la concorrenza tra aziende, contribuisce all'innovazione e alla nascita di nuovi servizi. Grazie a questo articolo, infatti, il soggetto può direttamente chiedere al vecchio ente di trasmettere i propri dati al nuovo gestore con la finalità del cambio del servizio desiderato, senza dover provvedere egli stesso al rinvio di tutte le proprie informazioni necessarie.

Un aspetto interessante di questo diritto è che, secondo alcune interpretazioni, esso risulti non del tutto completo<sup>30</sup>: infatti, nonostante nel comma 2 si chiarisca che non devono esserci impedimenti da parte del primo titolare, ciò non implica nessun tipo di obbligo per questi ultimi di utilizzare strutture di trattamento dei dati compatibili tecnicamente con quelli di altri enti. A questo si lega anche il fatto che il GDPR non si esprime in merito al formato dei dati da fornire per mettere in atto tale diritto: l'eterogeneità dei settori e delle aziende rende complesso trovare formati idonei e condivisi.

Un altro argomento sul quale il Regolamento vuole porre l'accento è l'aumento della responsabilità del titolare e del responsabile del trattamento: in questo senso si parla proprio di responsabilità congiunta. Secondo questo principio, infatti, i titolari del trattamento non possono sottrarsi dalla responsabilità per le violazioni in tema di protezione dei dati che si possono verificare durante la collaborazione con i responsabili del trattamento. Nell'articolo 13 viene specificato che il titolare del trattamento ha l'obbligo di informare l'utente riguardo al passaggio dei suoi dati verso fornitori terzi (i responsabili del trattamento) e può essere responsabile con lui di eventuali violazioni del Regolamento. Se questo dovesse capitare, sono previste sanzioni molto dure nei confronti di coloro che violano tali norme: nell'articolo 83 si

---

<sup>30</sup> Giampiero Uricchio, (2019), *Diritto alla portabilità dei dati: diritto incompleto*, URL: [www.altalex.com](http://www.altalex.com)

specifica che “*In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.00 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*”<sup>31</sup>.

## 2.4 LE CONSEGUENZE DEL GDPR IN TEMA DI CONCORRENZA

Il quadro normativo europeo sembra assicurare ai cittadini e alle imprese europee una maggiore protezione dei dati rispetto agli altri Paesi; tuttavia, sorgono spontanee la riflessione e il dubbio sul fatto che tale regolamento influisca anche sull'aspetto economico e sulla concorrenza in ambito aziendale.

Le aziende, per rispettare il Regolamento, devono offrire un quadro chiaro sulla loro politica di raccolta e conservazione dei dati, giustificando per quali finalità tengono in archiviazione i dati raccolti per diversi periodi di tempo; oltre a questo, esse sono obbligate a cancellare tali dati se non servono più per gli scopi dichiarati inizialmente. Quindi deve aumentare la trasparenza riguardo il trattamento e l'informazione rivolta ai consumatori, affinché essi stessi possano controllare e decidere in merito al trattamento dei propri dati<sup>32</sup>.

Riguardo quest'ultimo punto, ben esplicitato nel Considerando 32, si pone un esempio di richiesta di consenso di utilizzo di *cookie* post GDPR utilizzato in Gran Bretagna (Figura 6) messa a confronto con una richiesta di consenso di *cookie policy* degli USA (Figura 7): il primo mette in risalto i riferimenti legislativi, specificando quali *cookie* vengono elaborati e per quali finalità, offrendo all'individuo la possibilità di non aderirvi. Per quanto riguarda

---

<sup>31</sup> *Regolamento Generale Sulla Protezione Dei Dati*, GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Art.83 – par.5 URL: <https://www.garanteprivacy.it/il-testo-del-regolamento>

<sup>32</sup> G. Aridor, Yeon-koo Che, T.Salz, (2020), *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, p.7

## UNO SGUARDO ALLA NORMATIVA EUROPEA ED EXTRA EUROPEA SUL TRATTAMENTO DEI DATI PERSONALI

---

la Figura 7, invece, i consumatori vengono direttamente indirizzati ad usufruire dei mezzi privacy basati sul browser, i quali controllano i *cookie* del sito stesso; inoltre, non presenta nessuna opzione esplicita per rifiutare la raccolta dei dati.

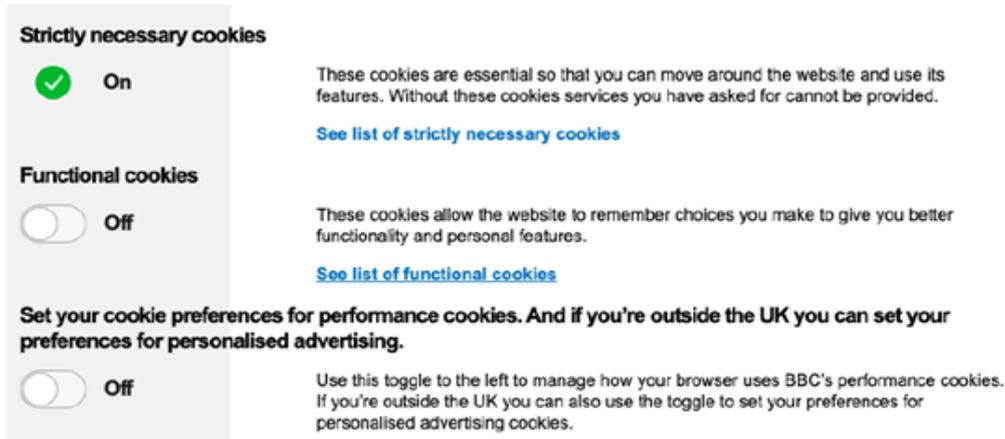


Figura 6 - Dialogo di consenso post GDPR (GB)

### 3. How Do I Manage Cookies?

You can change your Cookie settings above by opting out of all Cookies.

You may refuse or accept Cookies from the Site or any other website at any time by activating settings on your browser. Most browsers automatically accept Cookies, but you can usually modify your browser setting to decline Cookies if you prefer. If you choose to decline Cookies, you may not be able to sign in or use other interactive features of our Site that depend on Cookies. Information about the procedure to follow in order to enable or disable Cookies can be found at:

[Chrome](#)  
[Safari](#)  
[Safari Mobile \(iPhone and iPads\)](#)  
[Firefox](#)  
[Microsoft Edge](#)

For more information about other commonly used browsers, please refer to <http://www.allaboutcookies.org/manage-cookies/>.

Please be aware that if Cookies are disabled, not all features of the Site may operate as intended.

Figura 7 - Opt-out standard (USA)

Il requisito del consenso viene descritto con molta attenzione nel Regolamento ed è uno dei pilastri del documento: per questo motivo, i rischi per il mancato rispetto della normativa possono arrivare fino a 20 milioni di euro di sanzioni o il 4% delle vendite annuali globali dell'anno finanziario precedente.

Queste sanzioni hanno l'obiettivo di rappresentare un forte incentivo per le aziende a rispettare il Regolamento stesso<sup>33</sup>.

Oltre al rischio di contravvenzioni, sia che si tratti di imprese europee, sia che si tratti di imprese straniere, il GDPR impone indistintamente ingenti costi, i quali, il più delle volte si rivelano essere fissi, legati all'adattamento delle proprie strumentazioni e delle proprie procedure alla normativa vigente; questo, senza dubbio, rappresenta un termine di svantaggio per le imprese minori, che ne perdono sul campo della concorrenza.

Alcuni esempi di quanto questi costi possano rappresentare per un'azienda, li si possono ritrovare negli USA, dove, al fine di conformarsi al rispetto del GDPR, il 68% aziende statunitensi deve affrontare spese che variano tra 1 milione e 10 milioni di dollari<sup>34</sup>.

O ancora nello stesso continente europeo, nel Regno Unito la spesa media per la medesima finalità corrisponde a 1,7 milioni di sterline. Per questi motivi l'OECD sottolinea quanto le spese per adattarsi al regolamento siano importanti<sup>35</sup>.

I risultati di questi sondaggi e di queste ricerche destano molte preoccupazioni riguardo al fatto che il Regolamento Generale sulla Protezione dei Dati possa favorire e permettere lo stabilirsi, in maniera fissa, delle aziende più grandi e che si occupano di una vasta eterogeneità di servizi, grazie alla

---

<sup>33</sup> G. Aridor, Yeon-koo Che, T.Salz, (2020), *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, p.8

<sup>34</sup> PwC, (2017), *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017*, According to PwC Survey, URL: <https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-pressrelease.html>

<sup>35</sup> OECD, (2020), *Consumer Data Rights and Competition*, JT03461266, URL: <http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm>

quale è più facile ottenere consensi e permessi per il trattamento dei dati da parte dei consumatori<sup>36</sup>.

## 2.5 LA CONVENZIONE 108 E LA CONVENZIONE 108+

Nel 1976 si sente il bisogno di formare un Comitato di esperti riguardo la protezione dei dati, al fine di comporre un documento normativo per la tutela della privacy. Tra il 1976 e il 1979 si adoperava per arrivare a questo documento e nel '78 questo comitato prende il nome di *Project Group on Data Protection*

---

<sup>36</sup> Per ulteriori approfondimenti sul tema, si propongono:

- GDPR E GLI EFFETTI NEGATIVI SUL CAPITALE A RISCHIO, Jia, Jian, Ginger Zhe Jin, and Liad Wagman. (2018) *The short-run effects of GDPR on technology venture investment*. National Bureau of Economic Research.
- GDPR E IMPATTO ECONOMICO SUI SITI WEB: Goldberg, Samuel, Garrett Johnson, and Scott Shriver (2019). *Regulating Privacy Online: the Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes*. Available at SSRN 3421731.
- GDPR E IMPATTO SUI CONTRATTI DI CONNESSIONE AD INTERNET: Zhuo, Ran, Bradley Huffaker, Shane Greenstein, et al. (2019) *The Impact of the General Data Protection Regulation on Internet Interconnection*. National Bureau of Economic Research.
- CAMBIAMENTI NELLA CONCENTRAZIONE DI MERCATO DEI FORNITORI DI TECNOLOGIA WEB DOPO IL GDPR: Johnson, Garrett, and Scott Shriver (2019) *Privacy & market concentration: Intended & unintended consequences of the GDPR*. Available at SSRN.
- SITI WEB CHE SI SONO AGGIORNATI NELLA RICHIESTA DI CONSENSO AI COOKIE: Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. (2018) *We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*. arXiv preprint arXiv:1808.05096.
- ETEROGENEITÀ NELL'ATTUAZIONE DEL GDPR TRA I SITI WEB CHE HA PORTATO A DIFFERENZE SIGNIFICATIVE PER IL FATTO CHE I CONSUMATORI ABBIANO DATO IL PROPRIO CONSENSO ALLA RACCOLTA DATI: Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (2019), *(Un) informed Consent: Studying GDPR Consent Notices in the Field*. 973–990, ACM

(CJ-PD); dopo aver iniziato la collaborazione<sup>37</sup> con l'OCSE<sup>38</sup> a motivo del principio di non limitazione dello scambio di dati oltre frontiera e dello sviluppo economico.

Si arriva, così, a stilare un documento che possa essere riconosciuto non solo dai Paesi membri dell'Unione Europea, ma anche da Stati extra-UE: proprio per questo motivo, spiegato chiaramente nell'articolo 23<sup>39</sup>, tale documento prenderà semplicemente il nome di Convenzione (e non Convenzione Europea). Esempi concreti dell'applicazione di questo articolo li si possono trovare nel 2013, quando l'Uruguay decide di aderirvi, oppure nel 2016 quando vi aderiscono Senegal e Mauritius.

La stesura della versione finale del testo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale<sup>40</sup> viene redatta e pubblicata nel 1980 e firmata a Strasburgo nel 1981.

*"Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»).*<sup>41</sup>

---

<sup>37</sup> J. Michael, (1994), *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, Dartmouth/UNESCO, Aldershot, p. 33

<sup>38</sup> Organizzazione per la Cooperazione e lo Sviluppo Economico

<sup>39</sup> Articolo dedicato all'adesione di Stati non membri

<sup>40</sup> Convention for the Protection of Individuals with regard to automatic Processing of Personal Data

<sup>41</sup> Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art.1

Nel primo articolo della Convenzione viene spiegato chiaramente quale sia la sua finalità: il rispetto delle libertà e dei diritti fondamentali per ogni individuo, in particolare quello legato alla vita privata, messo in relazione con il trattamento dei dati personali.

Nell'ambito dei provvedimenti presi su questo argomento, questa Convenzione risulta fondamentale per tre motivi:

- si parla per la prima volta, in ambito internazionale, di protezione dei dati (*data protection*);
- si crea un legame formale tra la protezione dei dati e il rispetto dei diritti fondamentali degli individui;
- si forma un collegamento tra il diritto alla privacy e la protezione dei dati personali; la protezione dei dati, quindi, viene regolamentata per favorire la protezione della vita privata.

Non si parla, però, solo di protezione dei dati, ma anche di scambio libero di dati oltre frontiera: questo aspetto viene approfondito nell'art.12 che spiega che *“una Parte non può, al solo fine della protezione della vita privata, proibire o sottoporre a una autorizzazione speciale i flussi attraverso i confini di dati a carattere personale destinati al territorio di un'altra Parte.”*<sup>42</sup>

Attraverso questo articolo, infatti, viene sottolineata l'importanza che può assumere il flusso dei dati in ambito internazionale e che esso non può essere ostacolato dalla protezione della privacy. Continuando la lettura dell'articolo, però, si comprende meglio come questo possa avvenire tenendo presente il presupposto implicito che i Paesi interessati dallo scambio, diano la garanzia di un alto livello di protezione dei dati.

---

<sup>42</sup> Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art.12

Lo scambio dei dati risulta così importante perché fondamentalmente connesso al concetto di libero mercato e di libera espressione<sup>43</sup> e perché permette la libera circolazione delle informazioni, aspetto considerato come valore imprescindibile per lo sviluppo sociale ed economico.

L'ambito di applicazione della Convenzione risulta davvero ampio, anche se riguarda soltanto alle *“collezioni automatizzate di dati a carattere personale e all'elaborazione automatica di tali dati nei settori pubblico e privato”*<sup>44</sup>. Anche se viene specificato l'ambito di applicazione, però, non vengono chiarite, al fine di applicare la normativa, la forma sotto la quale i dati vengono raccolti ed elaborati: può trattarsi di tracciamenti GPS, oppure di immagini, di filmati o altro ancora<sup>45</sup>. Si chiarisce, invece, la natura dei dati personali, intesi come *“ogni informazione relativa ad una persona fisica identificata o identificabile (persona interessata).”*<sup>46</sup>

Oltre a questo, negli articoli successivi (art.5-6-7-8) vengono elencati e spiegati i principi fondamentali per la protezione dei dati e le disposizioni ad essi riferite:

- “qualità dei dati”;
- “categorie speciali di dati”;
- “sicurezza dei dati”;
- “ulteriori garanzie per la persona interessata”.<sup>47</sup>

---

<sup>43</sup> CEDU, art.10 par.1

<sup>44</sup> Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art. 3

<sup>45</sup> M. Fumagalli Meraviglia, (2016), *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, p. 1 ss., spec. pp. 3-4.

<sup>46</sup> Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art. 2

<sup>47</sup> Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art. 5-6-7-8

In questa parte della Convenzione viene sottolineato che la raccolta e l'elaborazione dei dati devono svolgersi soltanto con l'ausilio normativo che ne autorizza il trattamento automatizzato; gli scopi dell'utilizzo dei dati devono essere legittimi e le informazioni non devono essere trattenute oltre il tempo utile per raggiungere gli scopi prestabiliti. La qualità dei dati da utilizzare si traduce nel fatto che essi siano corretti, pertinenti e non eccessivi agli obiettivi prefissati. Nella Convenzione viene specificato il divieto di utilizzo di dati sensibili (razza, opinioni politiche, salute etc.) se non a motivo di garanzie giuridiche; stabilisce, inoltre, il diritto dell'individuo interessato a richiedere e ottenere i dati raccolti su sé stesso e, se errati, a chiederne la modifica.

Con il termine Convenzione 108+ si fa riferimento, invece, al protocollo di modifica, attuato nel maggio 2018<sup>48</sup>, di questo documento con lo scopo di modernizzarla per inserirla meglio nel quadro giuridico contemporaneo.

Proprio per queste motivazioni, di seguito ecco elencate le principali modifiche apportate<sup>49</sup>:

- obbligo di comunicare le violazioni dei dati (*data breach*);
- rafforzamento del principio di minimizzazione dei dati;
- rafforzamento del principio di trasparenza dell'elaborazione;
- introduzione del principio di *privacy by design* (maggiori tutele nell'ambito dei trattamenti algoritmici);

---

<sup>48</sup> Comunicato ufficiale: *Enhancing data protection globally: Council of Europe updates its landmark convention*, (2018), URL: [https://search.coe.int/directorate\\_of\\_communications/Pages/result\\_details.aspx?ObjectId=09000016808ac976](https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976)

<sup>49</sup> *Convenzione 108 del Consiglio d'Europa*, (2018), URL: <https://protezionedatipersonali.it/convenzione-108-consiglio-europa>

- ampliamento della tipologia di trattamenti considerati: la Convenzione 108+ analizza tutti i tipi di trattamenti (come anche quelli derivanti dalla difesa e dalla sicurezza nazionale, a differenza del GDPR), tranne quelli riguardanti l'esercizio di attività domestiche e personali.

Interessante risulta il fatto che tale protocollo di modifica ha permesso alla Convenzione 108+ di avvicinare il proprio regime a quello del GDPR (Regolamento Generale sulla Protezione dei Dati), il quale, però, nonostante i molti parallelismi, risulta essere molto più incisivo poiché direttamente applicabile.

## CAPITOLO 3

### REGOLAMENTI EUROPEI PER IL MERCATO DIGITALE: DSA E DMA

Le informazioni, che possono essere di tipo personali e non personali, hanno diverse modalità di circolazione ed appropriazione: nel panorama giuridico europeo, nonostante le informazioni personali siano inserite nel contesto dei diritti fondamentali, ne avviene la circolazione e l'uso al fine economico.

Seppur i dati rappresentino un asset strategico e rilevante dal punto di vista economico, la crescente concentrazione delle informazioni avviene principalmente per pochi soggetti, pubblici e privati: sono poche le aziende che possono investire in strutture tecnologiche scalabili, che possono finanziare attività di sviluppo e ricerca riuscendo a detenere la gestione di queste informazioni, che devono essere raccolte ed analizzate quotidianamente. Questi soggetti, che riescono ad aumentare la concentrazione del potere sull'informazione con la sola gestione dei *database* di cui dispongono, assumono il ruolo di *gatekeeper*: piattaforme che dominano il mercato.

Raccogliere e utilizzare i dati consente di accedere a nuove opportunità di crescita economica. Questo viene reso possibile sia mediante l'analisi delle esigenze e delle attese delle persone, sia offrendo nuovi prodotti o nuove soluzioni. L'introduzione di servizi digitali sempre più evoluti, oltre a portare vantaggi innovativi agli utenti che decidono di utilizzarli, ha offerto nuove

opportunità commerciali che hanno effetti sia sul mercato interno, sia sul mercato estero, che ne risulta più agevolato.

Quando gli utenti decidono di fornire i propri dati personali per ricevere e fruire di servizi offerti a titolo gratuito, le informazioni personali acquisiscono valore economico trasformandosi in una moneta dell'economia digitale, anche se la natura di questi servizi gratuiti non consente di definire un preciso valore economico dei dati acquisiti. Gli aspetti costo-beneficio riguardanti la divulgazione e la protezione dei dati sono tuttora oggetto di studio.

Di seguito, (Figura 8) si riporta una tabella esplicativa<sup>1</sup>, contestualizzata nel dicembre del 2019, che presenta i principali servizi, suddivisi per categoria, offerti agli utenti. Le *big tech* acquisiscono un vasto ammontare di dati individuali attraverso il gran numero di utenti e il loro tempo speso nell'utilizzo degli applicativi offerti.

---

<sup>1</sup> Fonte: AGCOM (2019), *Osservatorio sulle piattaforme online del 12/2019*, URL: [https://www.agcom.it/documentazione/documento?p\\_p\\_auth=fLw7zRht&p\\_p\\_id=101\\_INSTANCE\\_FnOw5IVOIXoE&p\\_p\\_lifecycle=0&p\\_p\\_col\\_id=column-1&p\\_p\\_col\\_count=1&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_struts\\_action=%2Fasset\\_publisher%2Fview\\_content&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_assetEntryId=17328706&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_type=document](https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5IVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5IVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5IVOIXoE_assetEntryId=17328706&_101_INSTANCE_FnOw5IVOIXoE_type=document)

	Google	amazon	Apple	facebook	Microsoft	NETFLIX
SEARCH	G				Bing	
SOCIAL NETWORK				f @	in	
INSTANT MESSAGING	☺ ☻		☺	☺ ~	S	
EMAIL	M		✉		o	
MAPPE	📍 🗺		📍		Bing maps	
ASSISTENZA VOCALE	🗣	alexa	🗣		🗣	
APP STORE	▶	amazon appstore	A		🛒	
INTRATTENIMENTO	YouTube	prime video twitch	tv		mixer	N
SALUTE	❤		❤			
PAGAMENTI	G Pay	amazon pay	Apple Pay		Microsoft Wallet	
ANALYTICS	📊	aws		📧	Microsoft	

Figura 8 - Servizi offerti e dati sugli utenti

Con l'evoluzione tecnologica sempre più repentina e con la diffusione dei big data, il controllo delle informazioni soffre di limitazioni: considerando che i mercati e la loro natura mostrano interesse ai dati personali, si stanno diffondendo problematiche economiche legate alla loro protezione.

Sta diventando, quindi, sempre più necessario rivedere i criteri fino ad ora utilizzati dalle autorità Antitrust, ripensando a nuove modalità per focalizzare l'attenzione sulla protezione dei dati.

Negli ultimi anni, le autorità europee ed americane hanno cambiato l'atteggiamento verso le *big tech* e, in generale, anche l'approccio nei confronti delle violazioni all'interno del mercato digitale.

Per trovare un orientamento nell'odierna situazione di incertezza normativa riguardante il mercato digitale e per limitare il potere delle *big tech*, la Commissione Europea ha proposto una specifica strategia digitale, composta da due iniziative legislative: il *Digital Services Act* (DSA) ed il *Digital Markets*

*Act* (DMA), al fine di iniziare a comporre un quadro normativo per consentire alle autorità di intervenire in difesa dei cittadini contro i comportamenti abusivi online, con la possibilità di emettere sanzioni efficaci.

Viene costituito un insieme di regole applicabili in tutta la Comunità, creando uno spazio digitale più affidabile. Il DSA ed il DMA hanno due obiettivi principali: in primo luogo, creare uno spazio digitale in cui per tutti gli utenti vengano tutelati i diritti fondamentali, e, in secondo luogo, definire parità di condizioni per promuovere innovazione e competitività a livello globale.

Nel DSA vengono definiti obblighi e responsabilità cui si dovranno sottoporre gli intermediari digitali: ad esempio *social network*, piattaforme per condividere informazioni, *store online*, *app store*, etc. Alle società verrà richiesto di assumersi maggiore responsabilità nella gestione dei contenuti che sono inseriti sulle piattaforme online e, inoltre, di attrezzarsi con degli strumenti che consentano un rapido intervento nella rimozione di materiale definito “illegale”, come, ad esempio, contenuti che trasmettano incitamento alla violenza, all’odio, al terrorismo, alla vendita di prodotti illegali o contraffatti. In caso di inadempienza, il rischio è quello di subire delle sanzioni pari al 6% del fatturato annuo. Oltre a ciò, al fine di garantire una certa trasparenza, ad esempio, potrà essere richiesto alle società di condividere sia con gli utenti, sia con le autorità, il funzionamento dell’algoritmo che indicizza il prodotto.

Nel DMA, invece, verranno definiti i comportamenti delle aziende che, nel tempo, hanno acquisito una rilevanza importante: saranno descritti gli obblighi che porteranno a ridurre i comportamenti sleali, a cui i *gatekeepers* dovranno adempiere. Infatti, queste grandi piattaforme sono spazi digitali con un ruolo sistemico nel mercato interno e si identificano come “colli di bottiglia” tra imprese e consumatori per differenti servizi digitali. Nel caso di violazione delle regole di concorrenza, potranno essere applicate sanzioni fino al 10% dei ricavi globali di queste aziende. E poi, in caso di comportamento recidivo,

l'Unione Europea può agire con rimedi straordinari imponendo l'obbligo di cessione di asset aziendali al fine di separare strutturalmente le attività.

### 3.1 DIGITAL SERVICES ACT (DSA)

A seguito dell'emissione della "Direttiva e-commerce" 2000/31/CE<sup>2</sup>, si è riscontrato l'emergere di nuovi servizi digitali innovativi che hanno conseguenze sullo stile di vita delle persone, condizionandone e trasformandone gli atteggiamenti quotidiani nella comunicazione, nell'uso delle piattaforme online, negli acquisti, contribuendo sempre più alle trasformazioni sociali ed economiche nell'Unione Europea e nel mondo. Inoltre, l'espansione e l'evoluzione di questo atteggiamento a livello globale, è diventato fonte di rischio sia per gli utilizzatori dei servizi, sia per la società nel suo insieme.

La Commissione Europea si è impegnata a lavorare sull'aggiornamento delle norme che definiscono le responsabilità e gli obblighi dei soggetti che forniscono servizi digitali, in particolare per chi mette a disposizione le piattaforme online. L'obiettivo di questo impegno europeo sta nel promuovere l'innovazione, la crescita e la competitività nei mercati online, non perdendo di vista la sicurezza dei consumatori e la protezione dei loro diritti fondamentali, disponendo di uno scenario chiaro ed efficace in ambito di trasparenza e responsabilità delle piattaforme digitali.

Una delle misure chiave in ambito digitale è la proposta di legge sui servizi digitali (*Digital Services Act, DSA*)<sup>3</sup> che viene presentata

---

<sup>2</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1), URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2000%3A178%3ATOC>

<sup>3</sup> Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE della Commissione Europea del 15/12/2020, URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0825&from=IT>

simultaneamente alla “legge dei mercati digitali” con la volontà di identificare le responsabilità dei soggetti che forniscono servizi di informazione, definendo meglio il controllo sulle politiche del contenuto delle piattaforme stesse, introducendo dei precetti volti a garantire all’interno dei mercati equità e contendibilità.

La proposta in esame, si aggiunge ai contenuti nella Direttiva 2000/31/CE sul commercio elettronico: rimangono validi i principi fondamentali sui quali nasce la direttiva vigente, mentre alcune specifiche norme dovranno essere aggiornate in relazione agli intermediari ed alle piattaforme online, incrementandone il livello di trasparenza e di *accountability* degli intermediari stessi. Ad esempio, alcuni punti come gli articoli 12-15 della direttiva sul commercio elettronico che disciplinano la responsabilità dei provider intermediari, sono stati sostituiti con il presente regolamento, che li riproduce mantenendo il quadro dell’esenzione della responsabilità per i fornitori di servizi intermediari.

In questa proposta si evidenzia un cambio di paradigma: la direttiva e-commerce aveva lo scopo primario di tutelare i consumatori, solo successivamente sono derivati altri regolamenti, come ad esempio il Codice dei Consumatori italiano. Il punto principale era la “categoria economica” dei consumatori che compravano beni di consumo e servizi online.

Il DSA, invece, ha l’obiettivo di tutelare i diritti fondamentali di tutti i soggetti che oggi “vivono in un mondo digitale”, come si può evincere da una parte del testo dell’introduzione riportato di seguito:

*“La proposta introduce importanti garanzie per consentire ai cittadini di esprimersi liberamente, rafforzando nel contempo il ruolo degli utenti nell’ambiente online nonché l’esercizio di altri diritti fondamentali come*

*il diritto a un mezzo di ricorso efficace e alla non discriminazione, i diritti dei minori e la protezione dei dati personali e della vita privata online.”<sup>4</sup>*

I soggetti cui si rivolge il DSA sono i cittadini e la collettività in generale: esso si applica a chiunque voglia offrire servizi digitali nell’Unione Europea, incluse anche le piattaforme che offrono servizi intermediari come ad esempio *hosting, social networks, marketplaces*.

Tale proposta è stata presentata dalla Commissione UE il 15 dicembre 2020 e ora seguirà l’iter legislativo. Si tratta di un percorso che va a completare quanto avviato con il GDPR. In particolare, si prendono in considerazione i principali problemi rilevati:

- maggiore esposizione dei cittadini ai rischi online, con particolare attenzione ai danni che possono provocare attività illecite e alla violazione dei diritti fondamentali degli individui;
- carenza di coordinamento ed efficacia della struttura di *governance* sulle piattaforme online a livello di UE. L’attuale direttiva sul commercio elettronico viene applicato in modalità differenti e non lineari dagli Stati membri;
- considerato che, inizialmente, la regolazione dei servizi digitali è stata affrontata a livello nazionale, si presenta la necessità di fronteggiare il vantaggio competitivo per i soggetti già esistenti di dimensioni molto grandi.

Con il periodo della pandemia Covid-19, si è evinto sia il valore e l’importanza dei servizi digitali, sia le relative vulnerabilità in termini di affidabilità e sicurezza. In linea generale, l’obiettivo che la Commissione vuole intraprendere è quello di trovare una soluzione efficace nell’affrontare questi

---

<sup>4</sup> Ibidem

problemi cercando di garantire il funzionamento del mercato unico per la fornitura dei servizi online a livello dell'UE.

Nella proposta del DSA si evidenziano i seguenti obiettivi prefissati:

- garantire la sicurezza degli utenti per l'accesso ai dati personali trattati dai fornitori dei servizi in caso di attività illegali, come ad esempio, disinformazione e pubblicità ingannevole, vendita di prodotti contraffatti e pericolosi, contenuti d'odio;
- definire il perimetro di responsabilità previsto dalla direttiva sul commercio elettronico rispetto ai servizi digitali, con specifica attenzione agli intermediari come *social media*, motori di ricerca, *cloud storage providers*;
- rivedere il ruolo dei *gatekeeper* e le relative problematiche delle piattaforme digitali, rivalutando i concetti "potere *gatekeeper*" e "potere di mercato";
- individuare un quadro di cooperazione amministrativa, al fine di consentire ai regolatori di agire in modo più efficaci al fine di garantire l'applicazione delle norme all'interno degli Stati membri, in modo coerente.

La proposta di regolamento definisce le modalità alle quali le piattaforme online devono attenersi per poter beneficiare dell'esenzione dalla responsabilità rispetto ai contenuti ospitati. Un esempio, l'articolo 5 relativo ai fornitori di servizi di *hosting* descrive il tipo di prestazione ed il relativo perimetro di responsabilità dell'intermediario:

*"Nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle*

*informazioni memorizzate su richiesta di un destinatario del servizio, a condizione che detto prestatore:*

*a) non sia effettivamente a conoscenza delle attività o dei contenuti illegali e, per quanto attiene a domande risarcitorie, non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti;*

*oppure*

*b) non appena viene a conoscenza di tali attività o contenuti illegali o diviene consapevole di tali fatti o circostanze, agisca immediatamente per rimuovere i contenuti illegali o per disabilitare l'accesso agli stessi.”<sup>5</sup>*

Per il prestatore del servizio è necessario prevedere sia delle procedure che consentano la gestione dei contenuti illegali sia delle modalità che rispondano alle eventuali contestazioni che potrebbero insorgere a seguito delle decisioni di moderazione del contenuto applicate dalle piattaforme.

È previsto un sistema di “*Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro*”<sup>6</sup> che considera sia la dimensione dell’operatore digitale, sia la categoria di servizi di intermediazione che gestisce. In particolare, i soggetti che offrono servizi digitali, sono soggetti ad una distribuzione delle responsabilità e dei doveri di diligenza bilanciata e proporzionata, proprio perché le informazioni fornite dal destinatario del servizio sono trattate in modo automatico.

---

<sup>5</sup> *Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE della Commissione Europea del 15/12/2020, Art. 5. URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0825&from=IT>*

<sup>6</sup> *Ibidem, Capo III*

Nel caso delle piattaforme online che prevedono di memorizzare e di diffondere al pubblico le informazioni, è possibile rimuovere i contenuti forniti e pubblicati dai destinatari, ritenuti illegali oppure incompatibili dalle condizioni generali del prestatore del servizio. Come riportato nell'articolo 17, si presenta l'obbligo di prevedere un "*sistema interno di gestione dei reclami*"<sup>7</sup>, per far fronte alla gestione dei casi di contestazione circa l'applicazione dei termini e delle condizioni del servizio. Nello specifico, l'utente deve poter accedere ad un sistema che consenta di notificare un reclamo circa una decisione adottata dalla piattaforma online nei suoi confronti.

La piattaforma online deve fornire al destinatario del servizio le informazioni necessarie per illustrargli le motivazioni per le quali determinati contenuti sono reputati illegali o incompatibili con le condizioni generali in essere:

- "a) le decisioni di rimuovere le informazioni o disabilitare l'accesso alle stesse;*
- b) le decisioni di sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari;*
- c) le decisioni di sospendere o cessare l'account dei destinatari."*<sup>8</sup>

Alcune altre misure interessanti sempre in riferimento alla tutela dei diritti fondamentali dei cittadini, riguardano obblighi di trasparenza e valutazione dei rischi.

Un esempio di obbligo per le piattaforme è descritto nell'articolo 24, in tema di trasparenza della pubblicità digitale:

---

<sup>7</sup> Ibidem, Art. 17

<sup>8</sup> Ibidem, Art. 17

*“Le piattaforme online che visualizzano pubblicità sulle loro interfacce online provvedono affinché i destinatari del servizio siano in grado di identificare in modo chiaro e non ambiguo e in tempo reale, per ogni singolo messaggio pubblicitario mostrato a ogni singolo destinatario:*

- a) la natura pubblicitaria delle informazioni visualizzate;*
- b) la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità;*
- c) informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità.”<sup>9</sup>*

Questo riguarda principalmente le piattaforme online che mostrano pubblicità durante la navigazione su web, ma non si applica alle microimprese. All’utente deve essere evidente che il banner o la comunicazione visualizzata corrisponda ad una forma di *advertising* e deve essere possibile identificare l’identità dei committenti. Le piattaforme devono conoscere quali sono i destinatari di quella pubblicità: non si tratta di una *banner policy* ma serve a mappare ogni singolo *advertisement* mediante una sorta di etichetta.

Nella sezione 4 del capo III vengono descritti gli *“Obblighi supplementari a carico delle piattaforme online di dimensioni molto grandi per la gestione dei rischi sistemici”<sup>10</sup>*. Per le piattaforme molto grandi, identificate per numero di destinatari attivi/mensili nell’Unione in media pari o superiori a 45 milioni, c’è l’obbligo di prevedere misure adatte per ridurre i rischi sistemici relativi al funzionamento e all’utilizzo del servizio offerto.

---

<sup>9</sup> Ibidem, Art. 24

<sup>10</sup> Ibidem, Capo III, sez. 4

Negli articoli 26, 27, 29 e 30 vengono riportate ulteriori misure di trasparenza per piattaforme definite molto grandi, come Facebook, che vanno oltre al concetto di sito web.

Ad esempio, nell'articolo 26, "*Valutazione del rischio*"<sup>11</sup> e nell'articolo 27 "*Attenuazione dei rischi*"<sup>12</sup> si affronta il discorso dei rischi sistemici che hanno la possibilità e la potenzialità di affliggere tutta la comunità, tutti i cittadini della Comunità Europea.

La Commissione, per limitare questi rischi adotta diverse misure che impongono a queste piattaforme di identificare, analizzare e valutare questi rischi sistemici che derivano dall'utilizzo stesso di queste piattaforme. Tra i rischi sistemici, ci sono 3 categorie descritte nei punti a), b), c) dell'articolo 26:

- disseminazione di contenuti illegali;
- rischi per diritti fondamentali (privacy, libertà espressione);
- sfruttamento e manipolazione dei servizi (salute, sicurezza, processi elettorali);

Nell'articolo 29, dove si parla di sistemi di raccomandazione, viene riportato:

*“Le piattaforme online di dimensioni molto grandi che si avvalgono di sistemi di raccomandazione specificano nelle loro condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione che possano avere messo a disposizione dei*

---

<sup>11</sup> Ibidem, Art. 26

<sup>12</sup> Ibidem, Art. 27

*destinatari del servizio per consentire loro di modificare o influenzare tali parametri principali ...”<sup>13</sup>*

I *recommender system* sono sistemi automatizzati per fare quello che molti definiscono “personalizzazione dei contenuti”. È necessario descrivere quali sono i parametri usati per generare questi suggerimenti di contenuti e quali sono le istruzioni per disattivare o modificare questi parametri sulla volontà dell’utente.

Tra le modalità più funzionali per settare i parametri di questi suggerimenti deve esserci almeno un’opzione che non si basi sulla profilazione degli utenti: l’utente può scegliere di non essere profilato. Le modifiche delle preferenze devono avvenire in tempo reale.

Nell’articolo 30 vengono descritti ulteriori obblighi di trasparenza riguardo l’*advertising*, i quali vanno ad integrare quelli già presentati nell’articolo 24:

*“Le piattaforme online che visualizzano pubblicità sulle loro interfacce online provvedono affinché i destinatari del servizio siano in grado di identificare in modo chiaro e non ambiguo e in tempo reale, per ogni singolo messaggio pubblicitario mostrato a ogni singolo destinatario:*

- a) la natura pubblicitaria delle informazioni visualizzate;*
- b) la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità;*
- c) informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità.”<sup>14</sup>*

---

<sup>13</sup> Ibidem, Art. 29

<sup>14</sup> Ibidem, Art. 24

Le piattaforme dovranno creare un archivio contenente le informazioni sulle attività di *advertising* eseguita sulle informazioni; questa cronologia dovrà durare almeno un anno e dovrà poter essere consultabile da parte degli utenti in un registro specifico. Come riportato nel punto 2 dell'articolo 30, oltre a poter visionare quali sono gli *advertising* visualizzati, dovranno essere rese disponibili le informazioni sui soggetti che hanno consultato, il periodo in cui l'advertisement è stato visualizzato, le modalità di visualizzazione, i parametri utilizzati per identificare il target di riferimento ed altre informazioni numeriche come il numero di destinatari<sup>15</sup>. Questo è importante perché si torna al concetto di profilazione ed è necessario conoscere i parametri utilizzati da queste piattaforme per profilare gli atteggiamenti commerciali, in ambito sociale e politico.

Quello che traspare dal DSA è che queste grandi piattaforme giocano un ruolo fondamentale nell'ecosistema digitale e che contribuiscono a creare rischi significativi sia a livello individuale che collettivo. L'*online advertisement* può contribuire alla diffusione di disinformazione di massa, come ad esempio le cosiddette *fake news*, oppure i rischi di discriminazione e di manipolazione del pubblico.

Ad esempio, esistono algoritmi che consentono di destinare le informazioni ad un pubblico differente, con l'utilizzo di particolari *data set* che portano dietro una serie di *gender bias*: agli uomini vengono mostrati posti di lavoro per opportunità di consulenza giuridico, mentre alle donne annunci di infermieristica, educazione.

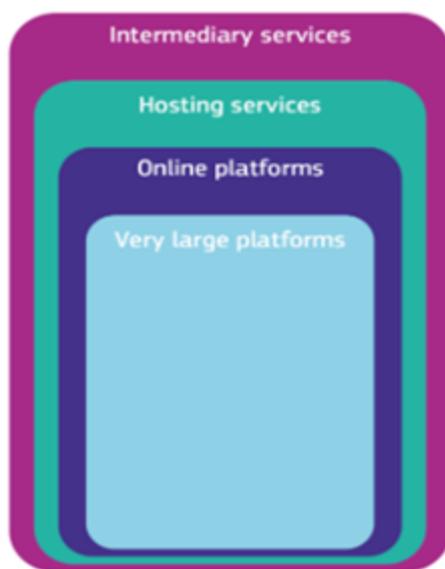
In generale, comunque, il DSA si rivolge a destinatari differenti, meglio differenziati dal ruolo, dalla dimensione e dall'impatto che hanno all'interno dell'ecosistema online. *“I fornitori di servizi di intermediazione offrono infrastrutture di rete: fornitori di accesso a Internet, registrazione di nomi di*

---

<sup>15</sup> Ibidem, Art. 30

*dominio. Al loro interno si distinguono i servizi di hosting, quali servizi cloud e web hosting, tra cui anche: le piattaforme online che riuniscono venditori e consumatori come mercati online, app store, piattaforme di economia collaborativa e piattaforme di social media. La nuova disciplina stabilisce norme specifiche per le piattaforme molto grandi, che prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni, tenuto conto dei rischi peculiari che pongono tali tipologie di piattaforme.”<sup>16</sup>*

Per illustrare meglio la platea dei soggetti identificati nella nuova normativa, nonché destinatari degli obblighi differenziati previsti, si riporta uno schema semplificato (Figura 9).



*Figura 9 - Schema dei principali destinatari del DSA (Fonte: Commissione Europea)*

---

<sup>16</sup> *The Digital Services Act: ensuring a safe and accountable online environment*, URL: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en)

### 3.2 DIGITAL MARKETS ACT (DMA)

Il *Digital Markets Act*, DMA<sup>17</sup> è la proposta di regolamento sui mercati digitali che è stata presentata insieme al DSA precedentemente descritto. Essa è orientata principalmente ad utenti di tipo business e ha l'obiettivo di garantire un mercato unico e competitivo per i servizi digitali. Tuttavia, si parte dal presupposto che in Europa si contino numerose piattaforme, ma sono poche quelle che riescono ad affermarsi come strutture fondamentali dell'economia digitale, con la funzione di intermediario per le transazioni che avvengono tra consumatori ed imprese: un esempio valido può essere Amazon, che fattura miliardi annualmente.

Tali piattaforme riescono quindi a detenere una certa importanza grazie alle dimensioni che hanno raggiunto, ricoprendo quindi la funzione di *gatekeeper*: si tratta di aziende dette *big tech* che rappresentano il principale punto di accesso dei clienti.

Questo è possibile poiché:

- detengono un impatto significativo sul mercato interno;
- gestiscono uno o più importanti nodi commerciali;
- godono di una posizione radicata e durevole nelle loro posizioni.

Lo stato di *gatekeeper* si presume quando:

- la piattaforma realizza un fatturato annuo pari o superiore a 6,5 miliardi negli ultimi 3 esercizi finanziari;

---

<sup>17</sup> Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVO A MERCATI EQUI E CONTENDIBILI NEL SETTORE DIGITALE della Commissione Europea del 15/12/2020, URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0842&from=en>

- il valore di mercato dell'impresa è di almeno 65 miliardi di euro nell'ultimo esercizio finanziario e fornisce un servizio di piattaforma almeno in tre Stati membri;
- qualora fornisca un servizio di piattaforma principale con più di 45 milioni di utenti finali attivi mensilmente stabiliti o ubicati nell'Unione e più di 10.000 utenti commerciali attivi all'anno.

Di seguito (Figura 10) si propone un breve schema riassuntivo delle principali *big tech* dell'anno 2019 con le principali attività e servizi offerti<sup>18</sup>.



Figura 10 - Le principali big tech e i servizi offerti

Questo aspetto è molto importante perché va a correggere il problema del Regolamento UE 2019/1150, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online e che agiva molto sui termini e condizioni: nel caso dei *gatekeepers*, infatti, non riesce più a

<sup>18</sup> Fonte: AGCOM (2019), *Osservatorio sulle piattaforme online del 12/2019*, URL: [https://www.agcom.it/documentazione/documento?p\\_p\\_auth=fLw7zRht&p\\_p\\_id=101\\_INSTANCE\\_FnOw5IVOIXoE&p\\_p\\_lifecycle=0&p\\_p\\_col\\_id=column-1&p\\_p\\_col\\_count=1&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_struts\\_action=%2Fasset\\_publisher%2Fview\\_content&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_assetEntryId=17328706&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_type=document](https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5IVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5IVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5IVOIXoE_assetEntryId=17328706&_101_INSTANCE_FnOw5IVOIXoE_type=document)

disciplinare in maniera corretta il rapporto tra utente ed utente business nei confronti di questi colossi. Si rende necessaria la nascita di regole che possano agire ex-ante.

Si riportano alcuni esempi di situazioni in cui le *big tech* attuano atteggiamenti volti a favorire le proprie piattaforme, a discapito degli altri utenti commerciali:

- Google è sottoposta ad accertamenti sia in Usa, sia in Europa: si ritiene che gestisca i propri servizi favoreggiandoli all'interno delle classifiche;
- Amazon è oggetto di studio poiché si presume che utilizzi gli utenti commerciali con la finalità di competere con gli stessi;
- Amazon e Apple sono indagate perché si presume che non consentano agli utenti di tipo business la possibilità di rendere disponibili gli stessi prodotti a prezzi e condizioni differenti da quelle proposte all'interno della piattaforma<sup>19</sup>.

La Commissione Europea, all'interno del Documento di Lavoro dei Servizi della Commissione (Sintesi Della Relazione Sulla Valutazione d'impatto)<sup>20</sup>, evidenzia che:

*“La comparsa di tali piattaforme che fungono da gatekeeper è stata accompagnata da tre problemi principali:*

---

<sup>19</sup> *Usa e Ue contro le Big Tech, ma così rischiamo un “feudalesimo digitale”*, (2020), URL: <https://www.agendadigitale.eu/cultura-digitale/usa-e-ue-contro-le-big-tech-ma-cosi-rischiamo-un-feudalesimo-digitale/>

<sup>20</sup> *Documento Di Lavoro Dei Servizi Della Commissione Sintesi Della Relazione Sulla Valutazione D'impatto*, Commissione Europea, del 15/12/2020 URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020SC0364>

- i) *debole contendibilità dei mercati delle piattaforme e debole concorrenza su tali mercati;*
- ii) *pratiche commerciali sleali nei confronti degli utenti commerciali;*
- iii) *regolamentazione e vigilanza frammentati per quanto riguarda gli operatori commerciali attivi in tali mercati.*<sup>21</sup>

L'esistenza di problematiche di questa tipologia può portare alla nascita di distorsioni all'interno del mercato senza disporre di alcun sistema di regolazione: infatti, all'interno del settore digitale, la presenza di piattaforme di grandi dimensioni può generare e accrescere la presenza di barriere all'ingresso nei mercati digitali, generando delle situazioni di squilibrio dei poteri contrattuali.

Per le piattaforme online definite di grandi dimensioni, che mediante i parametri quantitativi come fatturato dell'impresa o capitalizzazione media, oppure con il numero di utenti che accedono al servizio, il regolamento enuncia una serie di obblighi e di divieti a cui i *gatekeeper* devono sottostare.

Nell'articolo 5 vengono elencati gli "*obblighi dei gatekeeper*"<sup>22</sup> che devono essere osservati per ogni servizio di piattaforma:

- astenersi dal combinare i dati personali provenienti dai servizi della piattaforma principale con i dati personali di qualsiasi altro servizio offerto dal *gatekeeper* stesso (salvo consenso);

---

<sup>21</sup> Documento Di Lavoro Dei Servizi Della Commissione Sintesi Della Relazione Sulla Valutazione D'impatto del 15/12/2020, Commissione Europea, pag.1 URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020SC0364>

<sup>22</sup> Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVO A MERCATI EQUI E CONTENDIBILI NEL SETTORE DIGITALE della Commissione Europea, del 15/12/2020. Art.5. URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0842&from=en>

- consentire agli utenti commerciali di offrire gli stessi prodotti o servizi (già venduti tramite il *gatekeeper*) anche per mezzo di servizi online di terzi a prezzi o condizioni diversi da quelli offerti tramite il *gatekeeper*;
- astenersi dall'impedire o limitare gli utenti aziendali dal sollevare questioni con qualsiasi autorità pubblica pertinente in relazione a qualsiasi pratica di *gatekeeper*;
- consentire ai propri utenti aziendali di accedere ai dati che generano durante l'utilizzo della piattaforma del *gatekeeper*;
- fornire alle aziende che fanno pubblicità sulla propria piattaforma gli strumenti e le informazioni necessarie agli inserzionisti;
- consentire ai propri utenti aziendali di promuovere la propria offerta e concludere contratti con i propri clienti al di fuori della piattaforma dei *gatekeeper*.

Nell'articolo 6 vengono elencati gli “*obblighi dei gatekeeper che potranno essere oggetto di ulteriori specifiche*”<sup>23</sup>, che corrispondono sostanzialmente ai divieti imposti ai *gatekeeper*:

- trattare i servizi ed i prodotti offerti dal *gatekeeper* stesso in modo più favorevole nella classificazione rispetto a servizi o prodotti simili offerti da terze parti sulla piattaforma del *gatekeeper*;
- impedire ai consumatori di collegarsi ad aziende al di fuori delle loro piattaforme;

---

<sup>23</sup> Ibidem, Art. 6

- impedire agli utenti di disinstallare qualsiasi *software* o *app* preinstallate se lo desiderano.

Sono già previsti inoltre sistemi di aggiornamento dei parametri per stabilire nuove limitazioni o obblighi da imporre ai *gatekeepers* al fine di correggere eventuali pratiche sleali oppure atteggiamenti che limitano la contendibilità dei servizi<sup>24</sup>.

Come argomentato all'interno del Capo IV, la proposta definisce le procedure per poter attuare indagini di mercato<sup>25</sup> per analizzare se i parametri sono ancora attuali o stanno diventando obsoleti. Nello specifico, l'indagine può essere avviata per differenti finalità:

- “*Indagine di mercato per la designazione di gatekeeper*”<sup>26</sup>: l'intenzione della norma è quella di poter disporre degli strumenti per seguire l'evoluzione dei mercati digitali, con la possibilità, ad esempio, di indicare un fornitore di servizi come *gatekeeper*. Inoltre, nell'articolo 33 è previsto che, nel caso in cui tre o più Stati lo richiedano, la Commissione Europea valuti, entro un termine di quattro mesi, l'avvio della suddetta indagine.<sup>27</sup>
- “*Indagine di mercato su un'inosservanza sistematica*”<sup>28</sup>: nel caso in cui, a seguito dell'indagine di mercato svolta, si dimostri che un fornitore di servizi abbia sistematicamente violato gli obblighi descritti negli articoli precedenti, possono essere attuate, entro dodici mesi dall'avvio dell'indagine, misure

---

<sup>24</sup> Ibidem, Art. 10

<sup>25</sup> Ibidem, Art. 14

<sup>26</sup> Ibidem, Art. 15

<sup>27</sup> Ibidem, Art. 33

<sup>28</sup> Ibidem, Art. 16

sanzionatorie proporzionali alla violazione commessa. Sono previsti due tipologie di rimedi proporzionali all'infrazione commessa: comportamentale o strutturale. Nel caso in cui non fosse possibile applicare o non esistesse un rimedio comportamentale, può essere attuato un rimedio strutturale.<sup>29</sup>

- *“Indagine di mercato su nuovi servizi e nuove pratiche”*<sup>30</sup>: a fronte di un'indagine di mercato, la Commissione può valutare se è necessario aggiungere un servizio all'elenco dei servizi di piattaforma di base, stabiliti nel regolamento, oppure può valutare se alcune pratiche possono essere ritenute sleali o possono in qualche modo influenzare la contendibilità dei mercati.

Nel Capo V della proposta, vengono attribuiti alla Commissione Europea i *“poteri di indagine, di esecuzione e di monitoraggio”*<sup>31</sup> che consentono di intervenire nel caso in cui si voglia procedere con l'apertura di procedimenti finalizzati all'applicazione di decisioni specifiche.<sup>32</sup> Ad esempio, la Commissione può intervenire con audizioni e raccolta di informazioni relative all'oggetto dell'indagine, con il potere di *“effettuare accertamenti in loco nei locali di un'impresa o associazione di imprese”*<sup>33</sup> oppure richiedendo l'accesso agli algoritmi ed alle banche dati, nonché chiarimenti ed approfondimenti in merito.

Infine, nel caso di inadempimento degli obblighi presentati nel regolamento o, nel caso di atteggiamenti scorretti da parte del *gatekeeper*, sono

---

<sup>29</sup> Ibidem, Art. 16

<sup>30</sup> Ibidem, Art. 17

<sup>31</sup> Ibidem, Capo V

<sup>32</sup> Ibidem, Art. 18

<sup>33</sup> Ibidem, Art. 20

definite anche le modalità per l'accertamento delle violazioni, seguite poi dalle indicazioni sulle sanzioni previste. Risulta essere una norma severa in quanto sono previste sanzioni fino al 10% del fatturato totale in caso di violazione degli obblighi/divieti.<sup>34</sup>

Il DMA potrebbe essere il primo tassello di una disciplina nuova che vede le *big tech* in prima linea rispetto le aziende ordinarie: per la prima volta viene riconosciuto uno status diverso tra le prime, ad esempio Google, e le seconde, ad esempio il piccolo imprenditore su web.

---

<sup>34</sup> Ibidem, Art. 26

## CAPITOLO 4

### INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

Nel novembre 2019<sup>1</sup> ha iniziato a diffondersi la notizia che il colosso delle ricerche Google avesse intenzione di acquistare per 2,1 milioni di dollari Fitbit, la nota società californiana produttrice dei famosi *sportwatch* che raccolgono le informazioni sulle abitudini sportive degli utenti.

Una delle reazioni più significative a questa notizia è stata quella dell'Unione Europea, la quale, insieme ad altri enti regolatori, ha mosso un'indagine dell'Antitrust per monitorare le finalità di questa fusione.

Nonostante questo, l'azienda statunitense ha ribadito che il suo obiettivo è, e rimane, quello di organizzare le informazioni e i dati di tutto il mondo al fine di renderli utili e accessibili a tutti. Risulta evidente dalle sue decisioni e dal suo percorso negli ultimi decenni che sarebbe più corretto usare il termine "monetizzare le informazioni" più che semplicemente organizzarle.

Diversi sono i motivi per i quali questa situazione ha destato importanti preoccupazioni riguardanti un possibile involuppo della piattaforma, estensione di potere monopolistico e sfruttamento dei consumatori.

---

<sup>1</sup> *Google compra gli orologi FitBit resi famosi da Obama: il titolo vola del 47%* (2019), URL: <https://www.ilsole24ore.com/art/google-compra-orologi-fitbit-resi-famosi-obama-titolo-vola-47per cento-ACmhF7v>

## 4.1 LA STORIA DI GOOGLE E IL CONCETTO DI MONOPOLIO

Nonostante sia il motore di ricerca più usato al mondo, anche Google ha una sua storia. Nato nel 1998 dal progetto di due studenti venticinquenni dell'università di Stanford, Larry Page e Sergey Brin, presentava fin da subito un metodo innovativo per trovare risultati più pertinenti rispetto ai concorrenti contemporanei. Lo scopo dei due ragazzi nel formare questo sistema era quello di aiutare gli utenti di internet a trovare più facilmente le informazioni cercate.

La differenza sostanziale stava nell'algoritmo attuato per trovare i risultati desiderati: gli altri motori di ricerca, al fine di collegare e porre i siti web nei loro *database*, si limitavano a contare le ricorrenze nei testi delle pagine dei termini digitati dagli utenti. Invece, il sistema di ricerca di Google si basava sulla verifica e sul contare le ripetizioni dei termini e i collegamenti che provenivano da altri siti e che portavano ad una specifica pagina web. La strategia che stava alla base di questo algoritmo era semplice: se un sito è riportato o citato da tanti altri siti, allora contiene informazioni che possono essere cercate più spesso, ergo è giusto porlo tra i primi risultati della ricerca. Tale metodo, denominato *Page Rank*, non si limita a contare i link di collegamento, ma valuta anche la qualità delle informazioni da essi contenute e la rilevanza dei siti dai quali arrivano i link.

Un altro vantaggio di Google rispetto agli altri motori di ricerca è stato rappresentato dalla cosiddetta pubblicità contestuale o mirata: inserzioni pubblicitarie contestualizzate alla ricerca su un lato della pagina consultata, con annessi link di collegamento ai siti di aziende che pubblicizzano un prodotto da loro venduto. Questo metodo ha concesso a Google la libertà di imporre ai propri inserzionisti di pagare un "tot per click" più alto rispetto al prezzo che pagherebbero per inserire la medesima pubblicità su siti o portali che trattano di altro. Questo spiega come gli annunci pubblicitari sui motori di ricerca siano

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

diventati un'importante fonte di potere economico: basti pensare che, soltanto nel primo quadrimestre del 2021, l'utile maturato dalla *big tech* statunitense per la pubblicità online ammonta a 17,93 miliardi di dollari (in salita del 162% rispetto al 2020) e il ricavo a 55,31 miliardi di dollari (in crescita del 34% rispetto al 2020)<sup>2</sup>.

Oggi Google non è più soltanto un motore di ricerca: offre risultati veloci e pertinenti, sì, ma è diventato anche un innovatore di servizi offerti agli utenti e anche un innovatore di business. La *big tech* statunitense, infatti, nel corso degli anni si è rinnovata sempre di più al fine di differenziare la sua offerta rispetto ai suoi *competitors* digitali e rispetto ai prodotti tradizionali offerti dal web. Questo suo sviluppo sempre più repentino, la porta a trovare resistenze e denunce da parte dei suoi concorrenti e da organi come quelli dell'Antitrust; la complessità sta appunto nel comprendere se le decisioni di Google siano effettivamente mosse da intenti e condotte anti-competitive o se siano da interpretare come conseguenza diretta della sua crescita e della sua eccellenza digitale.

Un esempio delle offerte innovative proposte dal colosso statunitense è sicuramente rappresentato dalla famosa *Suite*, recentemente rinominata *Workspace*, che offre “gratuitamente” un pacchetto completo di diversi servizi all'utente: una funzionale casella di posta elettronica (Gmail), uno spazio per condividere contenuti e lavori online (Google Drive), la possibilità di comporre documenti online a più mani e a distanza (Google Documenti), organizzare delle chiamate o dei meetings a distanza con il supporto video (Google Meet) e molto altro. Sebbene tutto questo pacchetto possa essere acquisito e utilizzato senza alcun costo in denaro, in realtà per attivarlo rimane necessario l'accettazione dei termini e delle condizioni d'uso, documento che permette alla *big tech* di

---

<sup>2</sup> Google, trimestre da record. La pubblicità online fa volare utile e ricavi. (2021), URL: [https://www.repubblica.it/economia/2021/04/28/news/google\\_trimestre\\_da\\_record\\_volano\\_utili\\_e\\_ricavi-298443548/](https://www.repubblica.it/economia/2021/04/28/news/google_trimestre_da_record_volano_utili_e_ricavi-298443548/)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

raccogliere, analizzare e utilizzare i dati di ogni utente per le finalità dell'azienda: si tratta di dati demografici, interessi, posizione per indirizzare meglio la vendita di annunci pubblicitari.

Oltre a questo, il colosso statunitense, nel corso di 20 anni, ha acquistato circa 140 società in tutto il mondo con la sola finalità di far crescere sempre di più il proprio potere in ambito digitale. Tra le sue più importanti acquisizioni si ricordano quella di Motorola Mobility (2011), di Nest (2014), di DoubleClick (2007), YouTube (2006), Waze (2013) e Postini (2007)<sup>3</sup>.

La storia delle sue acquisizioni segue un intento ben preciso: nonostante essa abbia sempre espresso che la sua missione fosse quella di “*organizzare le informazioni del mondo e renderle universalmente accessibili e utili*”<sup>4</sup>, i fatti sembrano dimostrare altro. Valorizzare e proteggere la mole di dati che raccoglie costantemente e permetterne la monetizzazione attraverso applicazioni in continuo sviluppo sembrerebbe essere il suo scopo principale.<sup>5</sup> Un esempio può essere quello in riferimento a YouTube o a Search, i quali, una volta acquisiti e offerti in modo gratuito agli utenti al fine di essere monetizzati vendendo pubblicità agli inserzionisti. Una situazione simile è avvenuta anche con Android, che, dopo essere stato acquisito, è stato concesso gratuitamente agli sviluppatori di smartphone con lo scopo di far diventare Google il motore di ricerca predefinito sul dispositivo mobile.

Le acquisizioni di Doubleclick e AdMob hanno permesso che il colosso statunitense ottenesse l'attuale monopolio in ambito di intermediazione pubblicitaria; inoltre, anche grazie alle altre acquisizioni minori di altre agenzie di concorrenza, Google è riuscito a facilitare il proprio lavoro di raccolta,

---

<sup>3</sup> *Le dieci acquisizioni di Google più pagate*. (2014), URL: <https://www.wired.it/internet/web/2014/01/17/10-acquisizioni-google-piu-pagate/>

<sup>4</sup> URL: <https://about.google/>

<sup>5</sup> *Google/Fitbit will monetise health data and harm consumers*, (2020), URL: [https://cepr.org/active/publications/policy\\_insights/viewpi.php?pino=107](https://cepr.org/active/publications/policy_insights/viewpi.php?pino=107)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

analisi, sfruttamento e archiviazione dei dati. Con la forma “involucro della piattaforma”<sup>6</sup> ci si riferisce proprio a questo: concedere convenienza agli utenti, mentre si soffoca la concorrenza.

Il monopolio digitale di Google e la conseguente monetizzazione dei dati comporta diversi fattori: l’accesso ad un pubblico sempre più vasto consente alla *big tech* di imporre prezzi pubblicitari più alti<sup>7</sup>; inoltre il controllo all’accesso ai dati appena raccolti e non visualizzati da altri enti, permette all’azienda statunitense di organizzarli dal punto di vista demografico, degli interessi e dei luoghi e di metterli all’asta al miglior offerente.

Il monopolio attuato da Google è, per molti aspetti, differente da un monopolio tradizionale: esso, infatti, non produce soltanto un mercato ordinario, ma, essendo presente in tutti i settori del mercato stesso, agisce come ente discriminatore. Infatti, attraverso la personalizzazione della pubblicità e attraverso il consenso di offerte di prodotto mirate, è in grado di danneggiare o favorire i consumatori stessi e i suoi *competitors*<sup>8</sup>.

In conclusione, si presenta uno schema riassuntivo delle principali caratteristiche del colosso statunitense registrate nell’anno 2016<sup>9</sup> (Figura 11).

---

<sup>6</sup> Eisenmann, T., G. Parker and M. Van Alstyne (2011), *Platform Envelopment*, Strategic Management Journal 32(12): pp. 1270–1285

<sup>7</sup> CMA (2020), *Online Platforms and Digital Advertising*, Market Study Final Report, 3 July

<sup>8</sup> *Google/Fitbit will monetise health data and harm consumers*, (2020), URL: [https://cepr.org/active/publications/policy\\_insights/viewpi.php?pino=107](https://cepr.org/active/publications/policy_insights/viewpi.php?pino=107)

<sup>9</sup> Fonte: *Tutti i numeri di Google, l’alfabeto del web*. (2016), URL: [https://www.repubblica.it/economia/2016/02/02/news/infografica\\_google\\_scheda-132560083/](https://www.repubblica.it/economia/2016/02/02/news/infografica_google_scheda-132560083/)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

### GOOGLE LA SCHEDA

**40.000**

I nuovi posti di lavoro che il gigante ha creato in meno di un ventennio. Sono dislocati in **70 uffici** sparsi tra oltre **40 Paesi** nel mondo: dalla *Thailandia* all'*Uganda*, dall'*Ucraina* al *Senegal*



**74,9 mld**

La società ha debuttato in Borsa nel 2004: da allora non ha mai smesso di macinare utili e aumentare i ricavi. Lo scorso anno ha incassato **74,9 miliardi di dollari** (oltre 16 miliardi gli utili) alla fine del 2013 erano 55,5 miliardi una progressione del 35% in 24 mesi. Contemporaneamente i ricavi dalle attività diverse da Google sono passati a 12 a 448 milioni di dollari.

**523 mld**

Di pari passo vanno le quotazioni del titolo, dai **50 dollari** del debutto ai **770** degli ultimi giorni che sono valsi ad **Alphabet** il titolo di società a maggior capitalizzazione del mondo: **523 miliardi di dollari**, più di Apple, ma anche di un Paese come la Svezia. Se arrivasse a 700 miliardi di euro potrebbe ambire ad avere un posto del G20, magari sostituendo l'Arabia Saudita in difficoltà con il calo del prezzo del petrolio.



**+160 acquisizioni**

Nel 2004 nasce il servizio di posta **Gmail**, sviluppato all'interno, e viene rilevata la società di cartografia digitale Keyhol da cui nel 2005 vengono lanciati **Google Maps** e **Google Earth**. Nel 2006, invece, viene acquisito **YouTube**, il sito di condivisione di video online: attualmente sul sito vengono caricate 60 ore di video al minuto: l'operazione costa 1,65 miliardi di dollari



**12,5 mld**

L'anno dopo arriva viene annunciato **Android**, una piattaforma aperta per dispositivi mobili, e l'Open Handset Alliance. Nel 2011 Google ha comprato per 12,5 miliardi **Motorola** soprattutto per mettere le mani su brevetti dell'azienda e sviluppare uno smartphone targato Mountain View: nel 2014 la società, però, viene ceduta a Lenovo anche se gran parte delle patenti restano a Google.

**40**

Sono i prodotti di Google: dal Wallet al traduttore, ma i campi di ricerca della società si estendono a 360 gradi. Dalla **robotica** alle automobili con lo scopo di arrivare al primo veicolo al mondo senza conducente.



Figura 11 - I numeri di Google nel 2016

## 4.2 ACCORDO GOOGLE – FITBIT: RISCHI E PREOCCUPAZIONI

Come anticipato precedentemente, è stata aperta un'inchiesta antitrust da parte della Commissione Europea per approfondire la questione che riguarda la proposta di acquisizione di Fitbit da parte di Google. Una delle principali preoccupazioni è dichiarata da Margrethe Vestager, responsabile alla Concorrenza che afferma *“preoccupa l'accesso a una nuova mole di dati sensibili.”*<sup>10</sup>

Anche il Garante della privacy, Antonello Soro, afferma: *“Un potere nelle mani di pochi soggetti che incide negativamente sulla tenuta delle democrazie nel pianeta.”*<sup>11</sup>

Nello specifico, l'oggetto dell'approfondimento riguarda l'intento di comprendere se questa acquisizione, potenzialmente, possa accrescere la posizione di Google rispetto ad altri player sul mercato della pubblicità online. Considerando che l'azienda statunitense dispone già di una vasta mole di dati, l'acquisizione di una nuova tipologia di informazioni sensibili riguardanti lo stato di salute degli utenti potrebbe portare a due condizioni: da una parte all'opportunità di utilizzare questi dati con la finalità di personalizzare gli annunci pubblicitari mostrati agli utenti, dall'altra potrebbe portare al rischio di distorsione della concorrenza.

Fitbit, azienda nata nel 2007, si è sempre concentrata nella ricerca di nuovi dispositivi che utilizzano sensori e tecnologia senza fili, come ad esempio gli *smartwatch*: questi nuovi dispositivi, che rientrano nel settore del fitness e

---

<sup>10</sup> Google-Fitbit, *Antitrust Ue apre dossier sull'acquisizione*, (2020), URL: [https://www.repubblica.it/economia/2020/08/04/news/google-fitbit\\_antitrust\\_ue\\_apre\\_dossier\\_sull\\_acquisizione-263727760/](https://www.repubblica.it/economia/2020/08/04/news/google-fitbit_antitrust_ue_apre_dossier_sull_acquisizione-263727760/)

<sup>11</sup> Google: Soro, *con acquisizione Fitbit pericolosa concentrazione di dati*, (2019), URL: [https://www.agi.it/economia/google\\_fitbit-6466269/news/2019-11-01/](https://www.agi.it/economia/google_fitbit-6466269/news/2019-11-01/)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

della salute, stanno prendendo sempre più valenza; risultano essere un prodotto indossabile che potrebbe potenzialmente modificare il concetto di attività fisica da parte degli utenti.

Considerato la tipologia e l'obiettivo principale di Fitbit e visto l'interesse di Google nell'acquisirla, molti sono i dubbi e le domande che ci si può porre e molti gli aspetti non definiti su cui si attendono aggiornamenti.

Google non dispone di un dipartimento o di un'azienda che produce dispositivi: in passato, nel 2018, c'è stato il tentativo di addentrarsi nel mercato degli indossabili con l'avvio del progetto *Wear OS* by Google (prima chiamata *Android Wear*), "*sistema operativo dedicato ai dispositivi indossabili*"<sup>12</sup>, ma non ha riscontrato un grande impatto. Al contrario Fitbit potrebbe fornire a Google una base di utenti più solida su cui lavorare per futuri device indossabili, probabilmente più integrati ad Android. Questo porta a pensare che si venga a creare una più solida partnership per poter contrastare la già presente soluzione nel mondo Apple, iPhone-iWatch.

Quindi, riguardo la questione dell'hardware non stupisce questo interesse per Fitbit da parte di Google che si trova tra i primi *Top 5 Wrist-Worn Wearables Companies by Shipment Volume*<sup>13</sup>. Infatti, osservando il market share degli *wearables* nel 2020 (Figura 12), si può evincere che per il 24% del mercato è ricoperto da Huawei, al primo posto, seguito da Xiaomi con i MiBand per il 20,4%, e da Apple per il 17,1%. Fitbit ricopre il 7,3%, mentre Garmin il 4,5%.

---

<sup>12</sup> *Wear Os By Google, Tutto Sul Sistema Operativo Per Dispositivi Indossabili*, Tuttoandroid, URL: <https://www.tuttoandroid.net/tag/wear-os-by-google/#funzioni>

<sup>13</sup> Fonte: *IDC Worldwide Quarterly Wearable Device Tracker*, URL: [https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC\\_P31315](https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC_P31315)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

Top 5 Wrist-Worn Wearables Companies by Shipment Volume, Market Share, and Year-Over-Year Growth, Q2 2020 (shipments in millions)					
Company	2Q20 Shipments	2Q20 Market Share	2Q19 Shipments	2Q19 Market Share	Year-Over-Year Growth
1. Huawei	8.1	24.0%	5.5	15.7%	45.8%
2. Xiaomi	6.9	20.4%	5.9	16.8%	16.6%
3. Apple	5.8	17.1%	5.1	14.4%	13.7%
4. Fitbit	2.5	7.3%	3.5	9.8%	-29.3%
5. Garmin	1.5	4.5%	1.7	4.7%	-8.5%
Others	9.0	26.7%	13.6	38.6%	-34.0%
<b>TOTAL</b>	<b>33.7</b>	<b>100.0%</b>	<b>35.3</b>	<b>100.0%</b>	<b>-4.4%</b>

Source: IDC Worldwide Quarterly Wearable Device Tracker, August 2020

Figura 12 - Riepilogo dei principali produttori di Wearables più venduti, Agosto 2020

Dal punto di vista dei dati, si vuole imporre come una azienda che abbia un portafoglio clienti molto attento alla propria salute. Sulla *home page* viene riportata qual è la missione principale: si pone l'obiettivo di ispirare gli utenti ad una vita più attiva e salutare, progettando prodotti ed esperienze per consentire loro di raggiungere qualsiasi tipo di obiettivo orientato al fitness e alla salute.

*“To empower and inspire you to live a healthier, more active life. We design products and experiences that fit seamlessly into your life so you can achieve your health and fitness goals, whatever they may be.”<sup>14</sup>*

Per cui l'accesso alle informazioni degli utenti potrebbe poter consentire la generazione di report e statistiche sullo stato di salute: questi sono dati molto importanti anche per Google, soprattutto per la collezione dei dati in campo *healthcare*.

<sup>14</sup> URL: <https://www.fitbit.com/global/us/about-us>

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

Riguardo il *software* non si conoscono ancora nel dettaglio gli intenti di Google in seguito all'acquisizione. Rimane il dubbio se rimarrà in uso il sistema proprietario Fitbit OS oppure se si opterà per il sistema Ware OS.<sup>15</sup>

*“Il Financial Times riferisce che i commissari dell’UE hanno inviato questionari di 60 pagine ai rivali di Google e Fitbit, chiedendo loro di valutare in che modo l’acquisizione influirà sullo spazio sanitario digitale; se svantaggerà le app di tracciamento del fitness ospitate nel Play Store di Google; e come Google potrebbe utilizzare i dati per profilare gli utenti per le sue attività di ricerca e pubblicità.”<sup>16</sup>*

I regolatori vogliono capire se tale fusione possa portare svantaggi alle applicazioni e ai dispositivi concorrenti per il monitoraggio dei parametri di fitness e salute presenti sul mercato, e se Google abbia l'obiettivo di utilizzare i dati catturati dai device per profilare gli utenti per le sue attività di ricerca e pubblicità.

Non è solo la Comunità Europea ad essere allarmata: anche la commissione australiana, per la concorrenza e per i consumatori, ha annunciato le proprie preoccupazioni.

In linea generale si teme che Google possa rafforzare la posizione dominante in questo settore, utilizzando i set di dati sanitari di Fitbit (salute, posizioni geografiche, etc.), aumentando le barriere di ingresso dei potenziali concorrenti.

Di fatto, l'accordo con Fitbit riguarda i dispositivi, non le informazioni: tale acquisizione non farà altro che aumentare la concorrenza, in un mercato già ben strutturato. Risulta difficile sostenere che l'accordo tra Fitbit e Google arrivi

---

<sup>15</sup>Google sta lavorando a un Fitbit con Wear OS, (2021)

URL: <https://global.techradar.com/it-it/news/google-sta-lavorando-a-un-fitbit-con-wear-os>

<sup>16</sup>Acquisti di Fitbit da parte di Google, (2020)

URL: <https://www.imside.it/acquisto-di-fitbit-da-parte-di-google/>

a creare una situazione di monopolio, in quanto, insieme, non detengono particolari quote di mercato degli indossabili.

### 4.3 GLI IMPEGNI DI GOOGLE

Dopo un anno dall'annuncio della volontà di Google di acquisire Fitbit, la Commissione Europea ha dato il suo consenso affinché questo possa avvenire<sup>17</sup>. Tuttavia, si è arrivati a questo consenso dopo un anno di attente analisi dell'Antitrust che ha voluto verificare attentamente le intenzioni del colosso statunitense e valutare se fosse realmente disposto a collaborare al fine di garantire il rispetto e il corretto utilizzo dei nuovi dati che saranno raccolti dopo la fusione.

Tale autorizzazione, però, comporta determinate condizioni che Google dovrà rispettare; esse avranno durata dieci anni e, nel caso in cui lo ritenesse necessario, la Commissione Europea potrà decidere la proroga di queste condizioni per altri dieci anni. Il controllo del rispetto di questi vincoli sarà costante e regolare.

Gli impegni che la *big tech* dovrà rispettare riguarderanno l'utilizzo, la conservazione e lo scambio dei dati, la concorrenza, l'accesso ad essi e le autorizzazioni che riguardano quest'ultimo aspetto. In particolare, le condizioni imposte a Google sono:

- non sfruttare i dati raccolti grazie a Fitbit per finalità commerciali (pubblicità mirate e personalizzate) nell'area commerciale europea;

---

<sup>17</sup> *Ok UE all'acquisizione di Fit Bit con condizioni* (2020), URL: [https://www.ansa.it/europa/notizie/rubriche/altrenews/2020/12/17/ok-ue-allacquisizione-di-fitbit-con-condizioni\\_22a2bb91-e781-4c71-bee2-2127477b07e1.html](https://www.ansa.it/europa/notizie/rubriche/altrenews/2020/12/17/ok-ue-allacquisizione-di-fitbit-con-condizioni_22a2bb91-e781-4c71-bee2-2127477b07e1.html)

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

- conservare i dati raccolti grazie a Fitbit in archivi separati e differenti da quelli utilizzati per la conservazione degli altri dati degli utenti;
- dare la garanzia agli individui di poter scegliere se concedere il consenso o no, lo scambio di dati con gli altri servizi proposti dalla *big tech* (Maps, YouTube, Workspace, Search etc.);
- con l'autorizzazione degli utenti, garantire l'accessibilità gratuita ai dati degli stessi da parte di imprese concorrenti al fine di evitare distorsioni di mercato;
- permettere alle aziende concorrenti di accedere alla piattaforma Android<sup>18</sup>.

Nonostante le condizioni poste, Google non nasconde che le sue finalità, con questa acquisizione, riguardano delle finalità puramente commerciali; la società statunitense, infatti, punta a consolidare la propria posizione nel mercato dei *wearables*, dove il primato è tenuto da Apple per il 33%, Xiaomi per il 13,6% e da Huawei per l'11%<sup>19</sup>.

Un altro aspetto che merita essere approfondito è quello che riguarda le reazioni delle altre aziende del settore a questa decisione della Commissione Europea: numerose le criticità che vedono queste condizioni troppo poco rigide e i dubbi sulla trasparenza del colosso statunitense, il quale, nel 2018, si è già trovato ad essere stato accusato “*di aver violato la fiducia pubblica quando ha trasferito l'unità sanitaria della società di intelligenza artificiale DeepMind,*

---

<sup>18</sup> *L'Europa dà l'ok al matrimonio tra Google e Fitbit, ma a certe condizioni*, (2020), URL: <https://www.wired.it/economia/business/2020/12/18/google-fitbit-acquisizione-europa-condizioni-antitrust/>

<sup>19</sup> *Market share of wearables unit shipments worldwide from 1st quarter 2014 to 2nd quarter 2021, by vendor*, (2021), URL: <https://www.statista.com/statistics/435944/quarterly-wearables-shipments-worldwide-market-share-by-vendor/>

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

*che aveva contratti con il servizio sanitario nazionale britannico per elaborare i dati di 1,6 milioni di pazienti, al controllo di Google Health”<sup>20</sup>.*

Queste argomentazioni si sono sviluppate in seguito ad un questionario inviato a delle imprese di tecnologia sanitaria (Garmin, Samsung e BEUC) se i provvedimenti proposti dal colosso statunitense fossero abbastanza valide da poterli rassicurare in tema di antitrust e privacy. Dalle loro reazioni, sono poi scaturite anche quelle di accademici e associazioni di consumatori<sup>21</sup>.

Google, dal canto suo, dichiara che:

*“Questo accordo ha sempre riguardato i dispositivi, non i dati, e siamo stati chiari sin dall'inizio che proteggeremo la privacy degli utenti Fitbit. Abbiamo lavorato con i regolatori globali su un approccio che salvaguardi le aspettative sulla privacy dei consumatori, inclusa una serie di impegni vincolanti che confermano che i dati sulla salute e sul benessere degli utenti Fitbit non verranno utilizzati per gli annunci Google e questi dati verranno separati dagli altri dati sugli annunci Google. Manterremo inoltre l'accesso alle API Android che consentono a dispositivi come fitness tracker e smartwatch di interagire con gli smartphone Android e continueremo a consentire agli utenti Fitbit di scegliere di connettersi a servizi di terze parti in modo che tu possa ancora sincronizza le tue app di salute e fitness preferite con il tuo account Fitbit.”<sup>22</sup>*

---

<sup>20</sup> I produttori di tecnologia indossabile si oppongono all'accordo Fitbit da 2,1 miliardi di dollari di Google, (2020), URL: <https://www.ft.com/content/d815b103-7d46-4d4e-b3c4-1d40d714b863>

<sup>21</sup> Ibidem

<sup>22</sup> Google completa l'acquisizione di Fit Bit, (2021), URL: <https://blog.google/products/devices-services/fitbit-acquisition/>

## INCHIESTA ANTITRUST: IL CASO GOOGLE - FITBIT

---

Infine, per tutti coloro che mostrano preoccupazioni riguardo questa fusione avvenuta nel gennaio 2021<sup>23</sup>, si spera che davvero gli enti regolatori controlleranno l'operato di Google e che esso stesso li rispetti, come dichiarato dal vicepresidente senior dell'azienda, Rick Osterloh: *“Questi impegni saranno attuati a livello globale in modo che tutti i consumatori possano beneficiarne. Continueremo inoltre a lavorare con le autorità di regolamentazione di tutto il mondo in modo che possano essere certi che stiamo rispettando questi impegni.”*<sup>24</sup>

---

<sup>23</sup> Ibidem

<sup>24</sup> Ibidem

## CONCLUSIONI

*“Abbiamo visto quanto valgono i dati personali: tanto da far nascere nuovi modelli di business e generare profitti enormi per le società che gestiscono i social media. Piattaforme come Facebook hanno affermato con forza di essere «gratuite», e se i consumatori non devono pagare per il servizio la piattaforma non può essere ritenuta colpevole di pratiche anticoncorrenziali. Tuttavia, questo ragionamento si fonda sul presupposto che lo scambio tra i dati personali e accesso alla piattaforma non costituisca una forma di pagamento, quando invece lo è. Ci sono interi mercati che valutano, vendono e danno in licenza dati personali. La falla degli attuali orientamenti antitrust nei confronti delle grandi società tecnologiche è che il valore dei dati dei consumatori non è stato considerato a dovere dalle autorità di controllo. [...] Il valore dei dati ceduti dai consumatori alle principali piattaforme non è bilanciato da benefici corrispondenti.”<sup>1</sup>*

La ricerca condotta, oltre a fornire un approfondimento sul concetto di dato e sulla classificazione delle informazioni, vuole sensibilizzare il lettore sul valore che è necessario attribuire alle informazioni personali condivise dagli utenti online. Ogni giorno, attratte dalla gratuità dei servizi digitali offerti su internet mediante differenti tipologie di architetture, le persone per molte ore fruiscono di una molteplicità di servizi, diffondendo le proprie informazioni, a volte inconsciamente, alle piattaforme che offrono le *utilities* spesso in forma

---

<sup>1</sup> Christopher Wyle (2020), *Il mercato del consenso*. Longanesi, pp. 325-326

## CONCLUSIONI

---

gratuita. In questo modo, il mondo digitale si integra maggiormente con il mondo fisico, aumentandone l'impatto sulla vita delle persone.

Questa tendenza porta spesso a svalutare l'importanza delle informazioni condivise, arrivando a mettere a rischio la privacy, partendo dall'accettare con un *click* un insieme di condizioni, poco chiare all'utente stesso, per poter accedere al servizio offerto delle aziende digitali.

Tutto ciò ha semplificato alle piattaforme l'accesso ai dati degli utenti che sono stati raccolti e classificati al fine di studio, definizione di profili per definire il comportamento degli utenti, generando così un valore importante per le aziende e per il mercato: ad esempio, profilato un utente, si possono generare delle pubblicità dedicate al fine di manipolarne gli atteggiamenti di acquisto.

Risulta quindi sempre più complesso ma anche necessario trovare meccanismi che consentano di regolarne l'uso all'interno dei mercati, considerando i campi di applicazione della legge sulla privacy e la legge antitrust che rispondono a due aree distinte con differenti meccanismi di applicazione ed intervento.

Come riportato, nel dicembre 2020 sono stati presentati dalla Commissione Europea i Regolamenti *Digital Services Act* (DSA) e *Digital Markets Act* (DMA), che descrivono una strategia finalizzata all'equità ed alla competitività del mercato digitale: verso gli utenti, aumentando l'attenzione e garantendone la protezione, verso i fornitori di servizi informativi ed alle piattaforme online di grandi dimensioni, attribuendo più responsabilità.

Come dichiarato dalla vicepresidente della Commissione UE, Margrethe Vestager, nel corso di una videoconferenza organizzata dal Financial Times, queste proposte volte a regolare il mondo digitale e contenere il potere delle *big tech* dovrebbero essere votate in Parlamento UE nella primavera 2022.

## CONCLUSIONI

---

In questo momento ci si trova ancora nella fase della discussione volta ad affinare tali proposte.

A seguito della pubblicazione di queste strategie ci si trova nel periodo della discussione dei contenuti: negli ultimi mesi in particolare, sono giunti in Parlamento UE oltre 3mila emendamenti sia verso il DMA, sia verso il DSA, ora prese in analisi dalla commissione del Mercato interno del parlamento europeo.

I temi contenuti all'interno degli emendamenti volti al DMA mettono in discussione i criteri di soglia di utenti, fatturato e designazione dei *gatekeepers* che verrebbero sottoposti ad una serie di obblighi e divieti a priori. Si rende necessario ridurre al minimo la complessità di applicazione, che risulterebbe inefficace sia per gli utenti, sia per il mercato portando ad un rallentamento dell'innovazione. Sembrano già esserci emendamenti sulla proposta di soglie di fatturato e valore di mercato differenti, in particolare per le *big tech* americane, cosiddette GAFA (Google, Amazon, Facebook e Apple).

Nel DSA, che ha lo scopo di aumentare la sicurezza agli utenti, serve ridurre il rischio che vengano introdotti sistemi finalizzati a burocratizzare i servizi digitali, limitandone la libertà di espressione. Anche in questo caso, tra le divergenze, è rilevante il tema sulla pubblicità personalizzata, i cui divieti potrebbero compromettere la crescita delle PMI; oppure, un altro tema riguarda la rimozione dei contenuti illegali, dove serve prevedere strumenti che possano ripristinare i dati cancellati.

## CONCLUSIONI

---

Tuttavia, nel primo voto al Parlamento UE del 22 novembre 2021, la relazione sul DMA per il mercato interno (IMCO) è stata approvata a larga maggioranza. Il prossimo step sarà quello di avviare i negoziati con il Consiglio dell'UE. Pertanto, la situazione attuale non è ancora del tutto definita, siamo in uno stato di *work in progress*: c'è ancora molto lavoro da svolgere.

La Commissione Europea ha l'ambizione di realizzare una trasformazione digitale entro il 2030, rafforzando la propria sovranità digitale, fissando norme proprie incentrandosi sui dati, sulla tecnologia e sulle infrastrutture, definendo un quadro di specifici diritti e principi digitali la cui finalità è quella di garantire la sicurezza nelle nuove tecnologie ed ecosistemi digitali, assicurando beneficio sia ai cittadini, sia alle imprese.

## BIBLIOGRAFIA

3. *Massive Big Data Problems Everyone Should Know About*, (2017), URL:  
<https://www.forbes.com/sites/bernardmarr/2017/06/15/3-massive-big-data-problems-everyone-should-know-about/>

AGCOM, AGCM e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2020), *Indagine conoscitiva sui BigData*. URL:  
<https://www.agcom.it/documents/10179/17633816/Documento+generico+10-02-2020+1581346981452/39c08bbe-1c02-43dc-bb8e-6d1cc9ec0fcf?version=1.0>

AGCOM (2018), *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*. URL:  
<https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>

AGCOM (2019), *Osservatorio sulle piattaforme online del 12/2019*, URL:  
[https://www.agcom.it/documentazione/documento?p\\_p\\_auth=fLw7zRht&p\\_p\\_id=101\\_INSTANCE\\_FnOw5IVOIXoE&p\\_p\\_lifecycle=0&p\\_p\\_col\\_id=column-1&p\\_p\\_col\\_count=1&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_struts\\_action=%2Fasset\\_publisher%2Fview\\_content&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_assetEntryId=17328706&\\_101\\_INSTANCE\\_FnOw5IVOIXoE\\_type=document](https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5IVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5IVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5IVOIXoE_assetEntryId=17328706&_101_INSTANCE_FnOw5IVOIXoE_type=document)

*Acquisti di Fitbit da parte di Google*, (2020) URL:

<https://www.imside.it/acquisto-di-fitbit-da-parte-di-google/>

Anita Balakrishnan (2017), *Bezos shareholder letter: Don't let the world push you into becoming a 'Day 2' company*. URL: [www.cnbc.com](http://www.cnbc.com)

C. D’Cunha, *Idee di Giovanni Buttarelli, trascritte da Christian D’Cunha*, in *Privacy 2030. Una nuova visione per l’Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, URL:

<https://www.garanteprivacy.it/documents/10160/0/Privacy+2030+-+Un+manifesto+per+il+nostro+futuro+-+Volume.pdf/8a243e2f-53e9-8dfa-a3be-0e80347499d3?version=2.1>

Christopher Wyle (2020), *Il mercato del consenso*. Longanesi, pp. 325-326

CMA (2020), *Online Platforms and Digital Advertising*, Market Study Final Report, 3 July

Commissione Europea (2020), *Documento Di Lavoro Dei Servizi Della Commissione Sintesi Della Relazione Sulla Valutazione D'impatto*. URL:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020SC0364>

Consiglio Europeo e Commissione Europea, (2000), *Carta dei diritti fondamentali dell’Unione Europea*

*Cookie: cosa sono, come funzionano e come proteggerti*, (2020), URL: <https://www.agendadigitale.eu/infrastrutture/tutto-quello-che-dobbiamo-sapere-sui-cookie-per-la-privacy-da-utenti-o-gestori/>

*Convenzione 108 del Consiglio d'Europa*, (2018), URL: <https://protezionedatipersonali.it/convenzione-108-consiglio-europa>

Corte EDU, (2017), *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, n. 931/13, 27 giugno 2017

Council of Europe, (1950), *European Convention on Human Rights*

Council of Europe, (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*

De Mauro A., Greco M. e Grimaldi M. (2016), *Una definizione formale dei Big Data basata sulle sue caratteristiche essenziali*, Recensione della Biblioteca 65(3)

*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)* (OJ L 178, 17.7.2000, p. 1), URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2000%3A178%3ATOC>

*Diritto all'oblio*, URL: <https://www.garanteprivacy.it/regolamentoue/oblio>

Eisenmann, T., G. Parker and M. Van Alstyne (2011), *Platform Envelopment*, Strategic Management Journal 32(12)

Elaborazione dell’Autorità su dati *Economist*, URL: [www.computerhope.com](http://www.computerhope.com), Cisco e Emmanuel Letouzé

*Enhancing data protection globally: Council of Europe updates its landmark convention* (2018) URL:

[https://search.coe.int/directorate\\_of\\_communications/Pages/result\\_details.aspx?ObjectId=09000016808ac976](https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976)

Federal Trade Commission Report (2016), *BIG DATA – A Tool for Inclusion or Exclusion? Understanding the issues*, URL:

<https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

FRA e Consiglio d’Europa, (2018), *Manuale sul diritto europeo in materia di protezione dei dati*

G. Aridor, Yeon-koo Che, T.Salz, (2020), *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*

Giampiero Uricchio, (2019), *Diritto alla portabilità dei dati: diritto incompleto*, URL: [www.altalex.com](http://www.altalex.com)

*Google completa l’acquisizione di Fit Bit*, (2021), URL:

<https://blog.google/products/devices-services/fitbit-acquisition/>

*Google compra gli orologi FitBit resi famosi da Obama: il titolo vola del 47%* (2019), URL: <https://www.ilsole24ore.com/art/google-compra-orologi-fitbit-resi-famosi-obama-titolo-vola-47percento-ACmhF7v>

*Google/Fitbit will monetise health data and harm consumers*, (2020), URL: [https://cepr.org/active/publications/policy\\_insights/viewpi.php?pino=107](https://cepr.org/active/publications/policy_insights/viewpi.php?pino=107)

*Google-Fitbit, Antitrust Ue apre dossier sull'acquisizione*, (2020), URL: [https://www.repubblica.it/economia/2020/08/04/news/google-fitbit\\_antitrust\\_ue\\_apre\\_dossier\\_sull\\_acquisizione-263727760/](https://www.repubblica.it/economia/2020/08/04/news/google-fitbit_antitrust_ue_apre_dossier_sull_acquisizione-263727760/)

*Google: Soro, con acquisizione Fitbit pericolosa concentrazione di dati*, (2019), URL: [https://www.agi.it/economia/google\\_fitbit-6466269/news/2019-11-01/](https://www.agi.it/economia/google_fitbit-6466269/news/2019-11-01/)

*Google sta lavorando a un Fitbit con Wear OS*, (2021), URL: <https://global.techradar.com/it-it/news/google-sta-lavorando-a-un-fitbit-con-wear-os>

*Google, trimestre da record. La pubblicità online fa volare utile e ricavi*. (2021), URL: [https://www.repubblica.it/economia/2021/04/28/news/google\\_trimestre\\_da\\_record\\_volano\\_utile\\_e\\_ricavi-298443548/](https://www.repubblica.it/economia/2021/04/28/news/google_trimestre_da_record_volano_utile_e_ricavi-298443548/)

*I produttori di tecnologia indossabile si oppongono all'accordo Fitbit da 2,1 miliardi di dollari di Google*, (2020), URL: <https://www.ft.com/content/d815b103-7d46-4dbe-b3c4-1d40d714b863>

*IDC ed Open Evidence*, Commissione Europea, (2017), Report *European Data Market*, URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2017:0495:FIN:IT:PDF>

*IDC Worldwide Quarterly Wearable Device Tracker*, URL: [https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC\\_P31315](https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC_P31315)

*Internet Usage is growing*, URL: <https://ec.europa.eu/newsroom/rtd/items/713444/en>

J. Michael, (1994), *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, Dartmouth/UNESCO, Aldershot

Keith Stuart and Charles Arthur, 27 aprile 2011, *PlayStation Network hack: why it took Sony seven days to tell the world*, The Guardian, URL: <https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony>

*L'Europa dà l'ok al matrimonio tra Google e Fitbit, ma a certe condizioni*, (2020), URL: <https://www.wired.it/economia/business/2020/12/18/google-fitbit-acquisizione-europa-condizioni-antitrust/>

*Le dieci acquisizioni di Google più pagate*, (2014), URL: <https://www.wired.it/internet/web/2014/01/17/10-acquisizioni-google-piu-pagate/>

Lucarelli S, Musolino E., Rocchi G., Ciacciarelli S., Laniado D., Espelt R., Senabre E., Morell M., Bria F, (2017), *Economic and regulatory analysis of data platforms and value creation models of the on demand economy*, DECODE, Project n. 732546

M. Fumagalli Meraviglia, (2016), *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*

M. White, (2012), *Digital workplaces: Vision and reality*, Business Information Review, 29(4)

*Market share of wearables unit shipments worldwide from 1st quarter 2014 to 2nd quarter 2021, by vendor*, (2021), URL:  
<https://www.statista.com/statistics/435944/quarterly-wearables-shipments-worldwide-market-share-by-vendor/>

Nicita, Delmastro, *Big Data – Come trasformano l'economia e la politica*

OECD, (2020), *Consumer Data Rights and Competition*, JT03461266, URL:  
<http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm>

*Ok UE all'acquisizione di Fit Bit con condizioni* (2020), URL:  
[https://www.ansa.it/europa/notizie/rubriche/altrenews/2020/12/17/ok-ue-allacquisizione-di-fitbit-con-condizioni\\_22a2bb91-e781-4c71-bee2-2127477b07e1.html](https://www.ansa.it/europa/notizie/rubriche/altrenews/2020/12/17/ok-ue-allacquisizione-di-fitbit-con-condizioni_22a2bb91-e781-4c71-bee2-2127477b07e1.html)

President's Council of Advisors on Science and Technology, (2014), *Big data and Privacy: A Technological Perspective*

*Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVO A MERCATI EQUI E CONTENDIBILI NEL SETTORE DIGITALE* della Commissione Europea del 15/12/2020, URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0842&from=en>

*Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE* della Commissione Europea del 15/12/2020, URL: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0825&from=IT>

PwC, (2017), *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017*, According to PwC Survey, URL: <https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-pressrelease.html>

*Regolamento Generale Sulla Protezione Dei Dati, GDPR*, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. URL: <https://www.garanteprivacy.it/il-testo-del-regolamento>

S. Calzolaio, (2017), *Protezione dei dati personali*, Utet, Torino

Rodotà S. (2009), *Data Protection as a Fundamental Right*. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) *Reinventing Data Protection?*, Springer, Dordrecht

S. Zuboff, novembre 2019, *Molte sfaccettature di un solo diamante*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, URL: <https://www.garanteprivacy.it/documents/10160/0/Privacy+2030+-+Un+manifesto+per+il+nostro+futuro+-+Volume.pdf/8a243e2f-53e9-8dfa-a3be-0e80347499d3?version=2.1>

*The Digital Services Act: ensuring a safe and accountable online environment*, URL: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en)

*Tutti i numeri di Google, l'alfabeto del web*. (2016), URL: [https://www.repubblica.it/economia/2016/02/02/news/infografica\\_google\\_scheda-132560083/](https://www.repubblica.it/economia/2016/02/02/news/infografica_google_scheda-132560083/)

*Understanding Canvas Fingerprinting*, (2021), URL: <https://gologin.com/what-is-canvas-fingerprinting>

URL: <https://about.google/>

URL: <http://www2.sims.berkeley.edu/research/projects/how-much-info>

URL: <https://www.fitbit.com/global/us/about-us>

*Usa e Ue contro le Big Tech, ma così rischiamo un “feudalesimo digitale”*, (2020), URL: <https://www.agendadigitale.eu/cultura-digitale/usa-e-ue-contro-le-big-tech-ma-cosi-rischiamo-un-feudalesimo-digitale/>

*Wear Os By Google, Tutto Sul Sistema Operativo Per Dispositivi Indossabili*, Tuttoandroid, URL: <https://www.tuttoandroid.net/tag/wear-os-by-google/#funzioni>

Yassine Lefouili e Ying Lei Toh, (2019), *Privacy Regulation and Quality Investment*