

Publicato il: ottobre 2022

©Tutti i diritti riservati. Tutti gli articoli possono essere riprodotti con l'unica condizione di mettere in evidenza che il testo riprodotto è tratto da www.qtimes.it
Registrazione Tribunale di Frosinone N. 564/09 VG

Pandemic, online education, privacy, democracy: the Google affair

Pandemia, didattica online, privacy, democrazia: il caso Google

di

Martina De Castro

martina.decastro@uniroma3.it

Umberto Zona

umberto.zona@uniroma3.it¹

Università degli Studi di Roma Tre

Abstract:

Google is the most widely used search engine in the world (Statcounter, 2022) and many users consider it an indispensable tool for accessing any content on the Web. Nevertheless, one cannot overlook the fact that the service offered by the Mountain View company is subordinate to the profits it makes from selling user data to third parties—for advertising purposes. During the pandemic, the latter aspect became even more evident and took on particular relevance in the case of minors who, in order to follow distance education, were forced by schools to open their own institutional email in order to use Google's platforms. The objective of this paper is to explore the worrying implications that this massive digital migration to the empire created by Page & Brin entails in terms of privacy and, more generally, of democracy.

Keywords: Google; online education; pandemic; privacy; democracy.

¹ Il presente testo è frutto delle riflessioni e del lavoro congiunto dei due autori. Tuttavia, ai fini dell'attribuzione delle singole parti, si specifica che la stesura del primo e del secondo paragrafo è a opera di Martina De Castro mentre quella del terzo è a opera di Umberto Zona.

Abstract:

Google è il motore di ricerca più utilizzato al mondo (Statcounter, 2022) e molti utenti lo ritengono uno strumento indispensabile per accedere a qualsiasi contenuto presente in Rete. Tuttavia, non si può sottacere il fatto che il servizio offerto dall'azienda di Mountain View sia subordinato ai profitti che essa ricava dalla vendita a terze parti – per fini pubblicitari – dei dati degli utenti. Durante la pandemia, quest'ultimo aspetto è divenuto ancora più evidente e ha assunto una particolare rilevanza nel caso dei minori che, per seguire la didattica a distanza, sono stati obbligati dalle scuole ad aprire una propria mail istituzionale per poter utilizzare le piattaforme di Google. Obiettivo del presente contributo è quello di approfondire i preoccupanti risvolti che questa imponente migrazione digitale verso l'impero creato da Page & Brin comporta sul piano della privacy e, più in generale, della democrazia.

Parole chiave: Google; educazione online; pandemia; privacy; democrazia

1. Introduzione. Un esercito di lavoratori-fantasma non retribuiti

Per lungo tempo, si è ritenuto il Web una sorta di organismo matematico/statistico “neutro” ma, negli ultimi anni, si sono moltiplicate le ricerche che contestano radicalmente questo assunto (Noble & Tynes, 2016; Noble, 2018; Benjamin, 2019; Zona & De Castro, 2020). In questa sede ci occupiamo dei preoccupanti risvolti in fatto di privacy connessi alle attività di aziende come Google, il cui motore di ricerca è il più utilizzato al mondo (Statcounter, 2022) e ai cui servizi sembra oramai impossibile rinunciare. Se è vero che gli utenti sono soddisfatti dall'aver accesso a Google e a tutti i servizi che offre gratuitamente (Gmail, Drive, Meet, Maps, YouTube), è anche vero che l'azienda creata da Brin e Page – in quanto piattaforma commerciale – guadagna dai dati che raccoglie su ciascun utente e che, come vedremo, spesso cede ad altre aziende. Poiché sono i dati che permettono di “personalizzare” le navigazioni attraverso suggerimenti pubblicitari “cuciti addosso” all'internauta, Google ha bisogno di continue interazioni per reperire tali dati e necessita, di conseguenza, del “lavoro” degli utenti per poter implementare i propri algoritmi: “Google beneficia direttamente e materialmente di quello che può essere chiamato il ‘labortainment’ degli utenti, quando gli utenti acconsentono a dare liberamente il loro lavoro e i loro dati personali per l'uso di Google e dei suoi prodotti, generando un incredibile profitto per l'azienda” (Noble, 2018, p, 36). È illusorio, dunque, credere che i risultati di ricerca che otteniamo quando facciamo una ricerca su Google siano oggettivi o neutri, in quanto la maggior parte dei link che ci vengono proposti, organizzati secondo una logica gerarchica, sono annunci pubblicitari.

Ma come si arriva al monopolio Google? Nel 1998, due giovani studenti della Stanford University, Lawrence Page e Sergey Brin, scrivevano un saggio dal titolo *The Anatomy of a Large-Scale Hypertextual Web Search Engine* in cui presentavano un primo progetto di PageRank, l'algoritmo di Google, capace di funzionare come una sorta di ipertesto che, attraverso un sistema di link, avrebbe facilitato le ricerche e permesso di calcolare la forza sociale d'attrazione e, dunque, l'autorevolezza di un determinato sito. L'obiettivo dichiarato di Page e Brin, infatti, era quello di ridurre l'uso aziendale-pubblicitario dei motori di ricerca, orientato al profitto, e incrementare il loro utilizzo accademico, il che oggi suona in modo abbastanza surreale. Attraverso la creazione di mappe fondate su collegamenti ipertestuali, PageRank sarebbe stato in grado di compiere rapidi calcoli per definire

la centralità di una pagina web e spostarla in alto nei risultati ottenuti effettuando una ricerca per parole chiave. PageRank, dunque, nasceva con l'ambizione di mappare la popolarità di un certo sito o di una certa pagina a vantaggio del consumatore che, in questo modo, sarebbe stato al sicuro da risultati manipolati per interessi economici o commerciali. Avendo come riferimento il sistema di citazioni accademiche, dunque, Page e Brin decisero di utilizzare come metodo di misurazione, classificazione e indicizzazione delle pagine web il numero di volte in cui queste erano ri-linkate o condivise. La differenza tra il web e il sistema accademico, tuttavia, consiste nel fatto che, mentre i prodotti delle ricerche accademiche devono essere vagliati mediante un processo di *peer-review* prima di essere pubblicati – e, pertanto, verificati e valutati da esperti *super partes* – ciò non avviene per i siti web, che possono essere condivisi e linkati senza dover necessariamente adempiere a principi di credibilità, in quanto le informazioni vengono vagliate e giudicate a posteriori – quando, cioè, sono già state messe in circolazione – direttamente dalla “saggezza” degli utenti. Man mano che Google ha acquisito centralità come motore di ricerca, fino a diventare il più utilizzato a livello globale, ha iniziato a utilizzare uno strumento pubblicitario e di ottimizzazione del prodotto chiamato AdWords, che permette agli inserzionisti di personalizzare il proprio modo di fare pubblicità. Essi, infatti, possono decidere quanto spendere quotidianamente per proporre i loro prodotti e, a quel punto, Google si occupa di inserirli all'interno delle pagine di ricerca di ciascun utente. Se l'utente, poi, clicca sull'inserzione, allora l'inserzionista paga Google; si tratta del sistema conosciuto come “costo per click” (CPC). Safiya Umoja Noble (2018) descrive nel dettaglio il funzionamento di questa strategia di marketing: “L'inserzionista seleziona una serie di 'parole chiave' che ritiene strettamente allineate con il prodotto o servizio che sta pubblicizzando, e un cliente [l'inserzionista] può utilizzare uno strumento di Keyword Estimator per vedere quanto potrebbero costare le parole chiave associate al proprio sito. Questo meccanismo pubblicitario è una parte essenziale di come PageRank dà priorità agli annunci su una pagina” (pp. 46-47). Pratiche come quella del *Google bombing* (linkare eccessivamente un sito web), perciò, si servono delle fragilità teoriche su cui è stato costruito PageRank – in particolare l'idea che più un sito o una pagina si trovano in alto nei risultati di una ricerca più essi possono essere considerati attendibili – per vendere spazi agli inserzionisti, i quali, in tal modo, possono incrementare visibilità e profitti. Gli unici che non guadagnano da questo sistema, in effetti, sono i semplici utenti, che, anzi, pagano i servizi ricevuti con i loro dati e ricevono in cambio informazioni spesso artefatte, sponsorizzate o non aderenti alle loro ricerche. Continua la Noble (2018): “Nonostante la convinzione diffusa che Internet sia uno spazio democratico in cui le persone hanno il potere di partecipare dinamicamente alla pari, esso, in realtà, è organizzato a vantaggio di potenti élite, comprese le società che possono permettersi di acquistare e reindirizzare le ricerche ai propri siti. Ciò che è più popolare in Internet non è il risultato diretto di ciò che gli utenti cliccano e di come i siti Web sono collegati: ci sono una varietà di processi in gioco” (pp. 47-48). Attraverso l'uso accorto di strumenti come Keyword Estimator o del *Google bombing*, dunque, è possibile associare a specifiche parole chiave link che apparentemente non hanno con esse alcuna diretta connessione. La Noble, ad esempio, ha iniziato a interessarsi al funzionamento degli algoritmi di Google nel 2010, quando, dopo che aver googlato la parola “Black girls”, aveva ricevuto in risposta suggerimenti di ricerca che facevano direttamente riferimento all'industria pornografica. Gli algoritmi più all'avanguardia dell'azienda di Mountain View, poi, si servono del *machine learning*, sono, cioè, in grado di apprendere dai dati e di registrare tutti i comportamenti agiti in Rete da ogni singolo utente. Le ricerche che facciamo, i beni che acquistiamo, i siti che visitiamo, le app

che installiamo sui nostri *device*, gli elettrodomestici *smart* che possediamo, dicono molto su quali sono le nostre opinioni, i nostri gusti, interessi, preferenze, su quali siano i nostri comportamenti più frequenti. Questa enorme mole di dati che quotidianamente e gratuitamente cediamo ai Giganti delle Piattaforme viene utilizzata da questi ultimi per farsi un'idea piuttosto precisa di chi siamo e per avviare delle strategie di profilazione e di personalizzazione delle nostre esperienze digitali. In questo modo, Google, oltre a tenere traccia di articoli, beni, servizi, siti verso i quali abbiamo mostrato interesse in passato, riesce a dedurre anche informazioni personali (età, stato civile, stato parentale, proprietà di un'abitazione) che potremmo non avergli mai fornito direttamente. Ciò avviene, come apertamente dichiarato (Fig. 1), in quanto le attività svolte sui servizi Google e su altri siti web e app dopo aver effettuato l'accesso sono simili a quelle di persone che hanno comunicato a Google di appartenere a quelle categorie demografiche nelle quali veniamo poi inseriti anche noi.

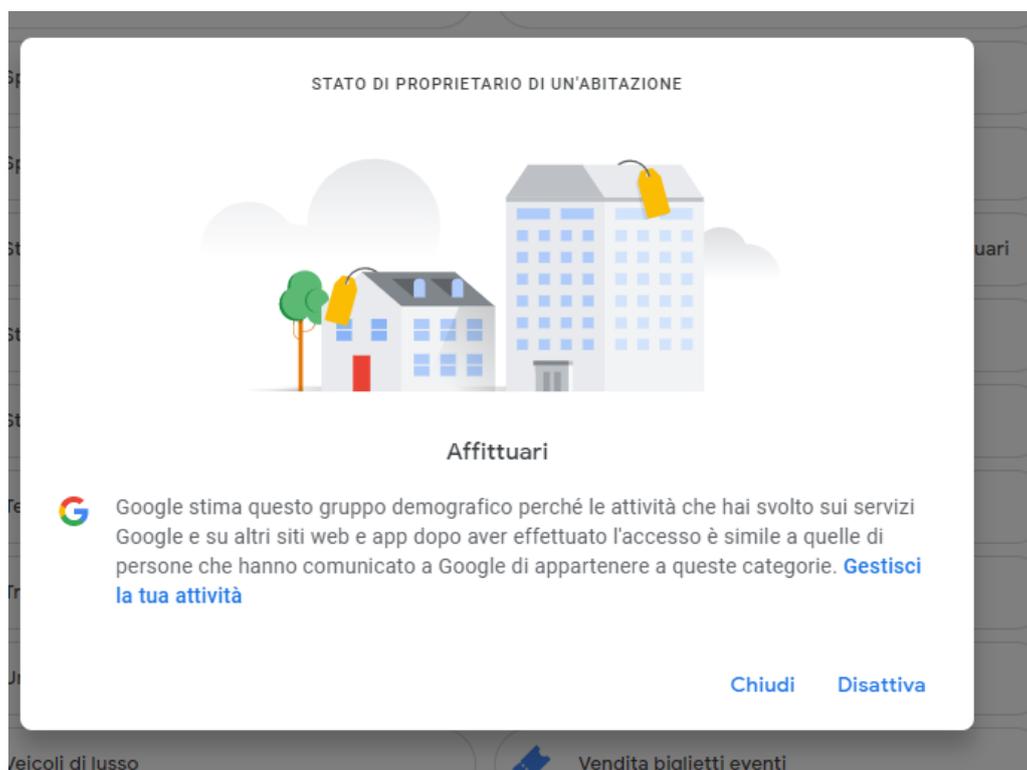


Fig. 1: Schermata di approfondimento di Google Ads Settings.

La nostra esistenza digitale, pertanto, non conosce angoli bui, spazi all'interno dei quali poterci nascondere dagli sguardi indiscreti di chi monitora ogni nostro movimento per venderci prodotti o per reperire dati sul nostro conto da rivendere al miglior acquirente. E così, mentre ci illudiamo di godere gratuitamente dei servizi offerti dalla Rete, in realtà stiamo lavorando, di fatto, per aziende come Google o Facebook. La strategia che aziende come Google sembrano aver adottato, dunque, è quella di trasformare ciascun soggetto in un individuo digitale "decorporizzato" ma reso materiale dai dati. Sono proprio questi dati che vengono incessantemente analizzati dagli algoritmi per farci rientrare in modelli individuali misurabili o in idealtipi quantificabili. In ambito digitale, quindi, gli algoritmi scandagliano continuamente i dati che ci riguardano per mappare i nostri modelli comportamentali e compararci con soggetti che condividono con noi gusti, preferenze e ricerche: "L'algoritmo *impara* confrontando un profilo con quello di altri internauti che hanno effettuato la

stessa azione. In modo probabilistico, esso ipotizza che una persona potrebbe fare tale o tal'altra cosa che non ha ancora fatto, visto che, invece, delle persone che le somigliano l'hanno già fatta” (Cardon, 2016, p 26). Questi algoritmi, perciò, non posseggono un potere predittivo ma si fondano sui nostri comportamenti passati e, sovrapponendo il nostro profilo a quello di utenti simili, sono in grado, ad esempio, di raccomandarci determinati prodotti su Amazon o di consigliarci una nuova serie tv su Netflix.

Tornando a Google, abbiamo visto come attraverso strumenti come Ads Settings, esso ci inserisca all'interno di *filter bubble* (bolle di filtro) costituite da soggetti a noi affini. Dunque, come dichiara lo stesso Google (Fig. 2), la personalizzazione degli annunci – ma, per estensione, anche l'organizzazione gerarchica dei link che ci vengono proposti quando eseguiamo una ricerca – avviene in base alle informazioni che volontariamente abbiamo aggiunto al nostro Account Google e ai dati accumulati da inserzionisti che collaborano con Google e che, pertanto, sono interessati a mappare i nostri gusti. I nostri desideri e gli argomenti di interesse potenziale sono invece dedotti direttamente da Google attraverso la comparazione con altri utenti a noi affini: “Potresti pensare che finché gli stessi link vengono mostrati agli utenti, il loro ordine è relativamente irrilevante, ma non è così. Un determinato collegamento riceve solo la metà dei clic rispetto al collegamento precedente e il doppio dei clic rispetto al collegamento successivo. In altre parole, l'ordinamento dei collegamenti è molto importante perché le persone fanno clic sul primo collegamento molto più del secondo e così via” (DuckDuckGo, 2018).

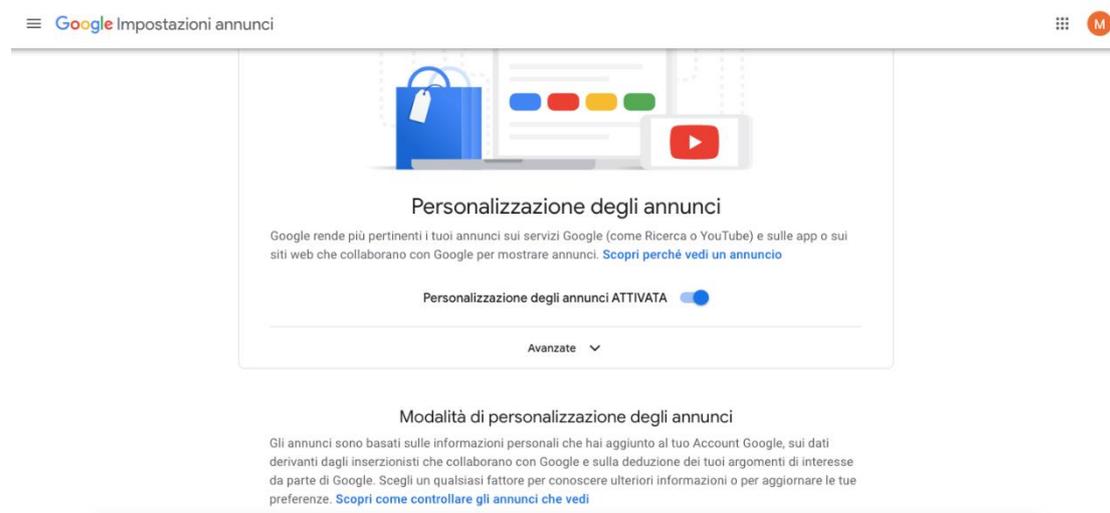


Fig. 2: Modalità di personalizzazione degli annunci di Google Ads Settings.

Ciò significa che soggetti tipizzati all'interno di bolle di filtro diverse potrebbero avere accesso a informazioni e contenuti diversi; Google, in altri termini, è in grado di determinare ciò che possiamo reperire online e ciò che deve rimanerci nascosto, polarizzando ulteriormente le posizioni del gruppo al quale si appartiene.

Il potere culturale esercitato dagli algoritmi è ormai in grado di minacciare anche le nostre stesse democrazie, come ha dimostrato lo scandalo Cambridge Analytica. Facebook, ad esempio, ha la capacità di farci pensare che tutto ciò che accade all'interno della nostra cerchia di amici sia contenuto nella sezione Notizie, quando in realtà ciò che vediamo è soltanto una piccolissima parte di quanto viene quotidianamente prodotto e dipende da parametri oscuri ma collegati al modo in cui siamo stati

profilati e alla bolla sociale nella quale siamo stati inseriti. Oltre all'azienda di Zuckerberg, però, "altre società ad azionariato diffuso fra cui Google, Apple, Microsoft, Amazon e gestori di servizi di telefonia mobile posseggono abbondanti informazioni su gran parte dell'umanità, e i mezzi per pilotarci come meglio credono. In genere [...] il loro principale obiettivo è quello del guadagno. I loro profitti, tuttavia, sono strettamente legati alle politiche di governo" (O'Neil, 2017, p. 263).

2. La violazione della privacy dei più piccoli può configurarsi come lavoro minorile?

Con l'aggravarsi della situazione epidemiologica a livello nazionale, il DPCM del 4 marzo 2020 prevedeva la sospensione delle attività didattiche in presenza nelle scuole di ogni ordine e grado ma concedeva la possibilità di avviare attività formative a distanza. La nota (prot. 388) del Ministero dell'Istruzione del 17 marzo definiva le attività di didattica a distanza come "una costruzione ragionata e guidata del sapere attraverso un'interazione tra docenti e alunni" (p. 3) e proseguiva dichiarando che essa si sarebbe dovuta realizzare nella forma di collegamenti diretti o indiretti (videoconferenze, videolezioni, chat di gruppo) tra insegnanti e studenti/; impiego di registri con funzione di comunicazione e di supporto alla didattica; interazione su sistemi e app educative interattive. Con l'avvio dell'emergenza pandemica e l'inizio del lockdown, pertanto, le scuole si sono dovute riorganizzare sul piano non solo didattico, ma anche logistico, migrando, di fatto, all'interno di piattaforme digitali che permettessero ai docenti di interagire direttamente con i discenti. Con il decreto 22 dell'8 aprile 2020, la didattica a distanza diveniva ordinaria e, di fatto, obbligatoria.

Una delle principali questioni sollevate dalla migrazione delle scuole nel Web riguarda la privacy degli studenti ed è per tale ragione che già i primissimi documenti emessi in materia si occupavano del problema. Nella nota del MI del 17 marzo 2020, infatti, si legge che le istituzioni scolastiche non devono chiedere il consenso per effettuare il trattamento dei dati personali – in quanto esso viene rilasciato dai genitori al momento dell'iscrizione –, ma sono tenute "a garantire che i dati personali siano trattati in modo lecito, corretto e trasparente, che siano raccolti per finalità determinate, esplicite e legittime, che siano trattati in modo non incompatibile con tali finalità, evitando qualsiasi forma di profilazione, nonché di diffusione e comunicazione dei dati personali raccolti a tal fine, che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati, e 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 accidenti" (p. 4). Il Ministero, però, si prodigava a consigliare sulle sue pagine solo tre piattaforme per la didattica a distanza: Google Suite for Education (che include Gmail, Drive, Calendar, Documenti, Fogli, Presentazioni, Moduli, Hangouts Meet, Classroom), Office 365 Education A1 di Microsoft e Weschool di TIM, dimenticando anche soltanto di menzionare il software libero (Garofalo, 12 ottobre 2020) o la rete GARR – ideata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca – sulla cui pagina si legge che essa rappresenta "la rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca" e il cui principale obiettivo è quello di "fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale".

Dal report preliminare dell'INDIRE (20 luglio 2020) dal titolo *Indagine tra i docenti italiani. Pratiche didattiche durante il lockdown*, che riporta i risultati ottenuti da un questionario semi-strutturato a cui hanno risposto in maniera volontaria 3.774 docenti di ogni ordine e grado, si apprende che tra le

applicazioni per videoconferenze più utilizzate per erogare la DaD svetta Google Meet (66,5%), seguito a grande distanza da Zoom, Microsoft Teams e Webex, mentre Google Classroom ha rappresentato lo strumento privilegiato per la creazione di classi virtuali (Fig. 3).

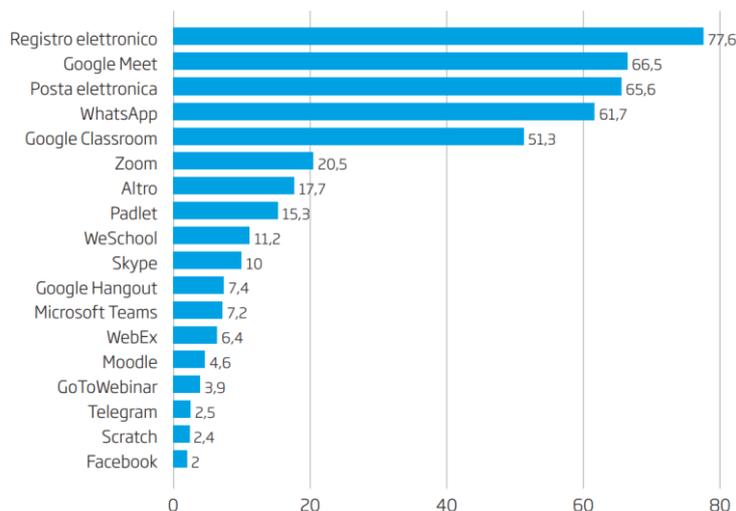


Fig. 3: Applicazioni tecnologiche utilizzate durante il lockdown. [Da: Indire (20 luglio 2020). Indagine tra i docenti italiani. Pratiche didattiche durante il lockdown. Report preliminare, p. 24].

Da quanto emerge dal grafico, dunque, le applicazioni maggiormente utilizzate dalle scuole per svolgere la DaD appartengono all'azienda di Mountain View. Meet, infatti, è un'applicazione gratuita di teleconferenza sviluppata da Google nel 2017, alla quale si accede attraverso un account Google, mentre Classroom è un servizio web gratuito attivato da Google nel 2014 e volto alla creazione e alla distribuzione di materiale didattico.

Sulla base di quanto dichiarato dai docenti, sembrerebbe che la scelta degli ambienti e degli strumenti a supporto della DaD sia avvenuta a livello d'istituto, sia stata il risultato di analisi tra opportunità diverse, sia ricaduta su piattaforme/strumenti già utilizzati in precedenza o sia stata consigliata dall'animatore digitale (Fig. 4).

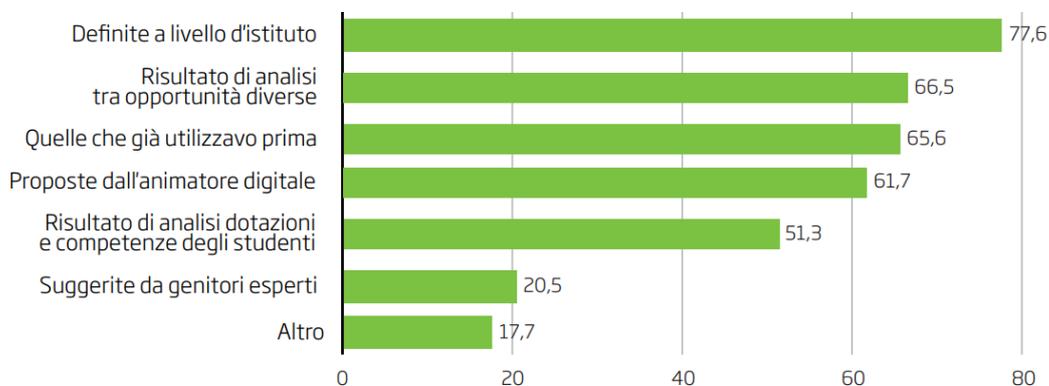


Fig. 4: Criteri di scelta delle tecnologie utilizzate durante il lockdown. [Da: Indire (20 luglio 2020). Indagine tra i docenti italiani. Pratiche didattiche durante il lockdown. Report preliminare, p. 25].

Gli Istituti scolastici che hanno scelto di affidarsi ai servizi offerti dall'azienda di Brin e Page, dunque, hanno creato un'email con il dominio edu.it – di proprietà di Google – per ciascun/a alunno/a e, proprio per tale ragione, la comunicazione dell'apertura dell'email istituzionale del/la bambino/a è arrivata ai genitori da The Google Workspace Team e non dalla segreteria della scuola; la stessa sorte è toccata, ovviamente, anche alle/agli insegnanti.

Google (30 settembre 2020), nelle intere pagine dedicate alla descrizione delle proprie norme sulla privacy, sostiene di proteggere le nostre informazioni lasciandocene il controllo, in quanto possiamo in qualsiasi momento regolarne e modificarne le impostazioni. Al fine di migliorare le proprie prestazioni e di fornirci servizi personalizzati – anche quando non eseguiamo l'accesso con il nostro account personale – Google raccoglie informazioni tramite identificatori univoci legati al browser, all'applicazione o al dispositivo che stiamo utilizzando, mentre, quando eseguiamo l'accesso, le informazioni che archivia con il nostro account riguardano:

- dati personali (nome, password, numero di telefono, dati di pagamento);
- contenuti che vengono creati, caricati o ricevuti da altri (comprese email scritte e ricevute, foto e video, documenti e fogli di lavoro creati, commenti lasciati su YouTube);
- le nostre attività (termini cercati, video guardati, visualizzazioni e interazioni con contenuti e annunci, informazioni vocali e audio quando si utilizzano le funzionalità audio, acquisti, persone con cui comunichiamo o condividiamo contenuti, attività su siti e app di terze parti, cronologia di navigazione di Chrome sincronizzate con l'account Google);
- la nostra posizione (GPS, indirizzo IP, dati dai sensori del dispositivo, informazioni su ciò che si trova nelle vicinanze del nostro dispositivo, ad esempio sui punti di accesso Wi-Fi e sui ripetitori di segnale dei cellulari, nonché sui dispositivi dotati di Bluetooth).

Per quanto concerne la condivisione delle nostre informazioni con terze parti, Google dichiara di avere sempre necessità del nostro consenso, ma questo non vale per fini pubblicitari oppure se siamo studenti o lavoriamo per un'organizzazione che utilizza i servizi Google: in questo caso, infatti, l'amministratore di dominio e i rivenditori che gestiscono il nostro account potrebbero avere accesso al nostro Account Google in qualunque momento e accedere alle nostre informazioni, visualizzare le statistiche relative al nostro account, ma anche “ricevere informazioni dell'account per rispettare una legge o una norma vigente, un procedimento giudiziario o una richiesta di governo applicabile” (Google, 30 settembre 2020). Se guardiamo più specificamente all'informativa sulla privacy di Google Suite for Education², possiamo leggere che Google colleziona i dati del cliente (oggetti forniti o creati dall'utente attraverso i servizi principali) e quelli del servizio (informazioni raccolte durante l'utilizzo dei servizi principali) ma non permette l'utilizzo di tali informazioni al fine di personalizzare gli annunci pubblicitari. Tuttavia, è la stessa azienda a dichiarare che gli utenti potrebbero ricevere “annunci basati su fattori generali come la query di ricerca, l'ora del giorno o il contenuto di una pagina che si sta leggendo” (Google Workspace). Nel momento in cui l'istituto crea un account Google Workspace for Education, Google riceve il nome, l'indirizzo mail e la password dell'insegnante e/o dello/a studente/essa, ma in fase di utilizzo dei servizi digitali raccoglie informazioni relative all'attività dell'utente (visualizzazione e interazione con i contenuti, persone con cui si comunica o si condividono contenuti, contenuti creati); app, browser e dispositivi utilizzati

² Google Workspace, https://workspace.google.com/terms/education_privacy.html#privacy-police-revamp-your-info.

per accedere ai servizi; posizione. Per quanto concerne la condivisione di informazioni, sapendo di avere a che fare con minori, è la stessa Google a mettere le mani avanti e ad ammonire gli utenti: “L’amministrazione della scuola può consentire agli studenti di accedere ai servizi di Google, come Google Docs e YouTube, che dispongono di funzioni che consentono agli utenti di condividere informazioni con altri o pubblicamente. Ad esempio, se lasciate una recensione su Google Play, il vostro nome e la vostra foto appaiono accanto alla vostra attività. E se si condivide una foto con un amico che poi ne fa una copia o la condivide di nuovo, la foto può continuare a comparire nell’account Google dell’amico anche dopo che l’utente l’ha rimossa dal proprio account Google. Ricordate che quando condividete informazioni pubblicamente, i vostri contenuti possono diventare accessibili attraverso i motori di ricerca, compresa la ricerca Google” (Google Workspace).

A seguito dell’adozione delle misure di gestione della pandemia da Covid-19, la scelta degli strumenti più idonei allo svolgimento della didattica a distanza è stata demandata alle singole scuole in quanto titolari del trattamento (GPDP, 26 marzo 2020). Il Garante della privacy, però, ha posto l’accento sin da subito sulla necessità di includere tra i criteri di selezione degli strumenti e degli ambienti virtuali da utilizzare a scopo didattico, “oltre all’adeguatezza rispetto alle competenze e capacità cognitive di alunni e studenti, anche le garanzie offerte sul piano della protezione dei dati personali” (GPDP, 26 marzo 2020). Per tale ragione, il Garante consigliava – prima di rivolgersi a piattaforme più generaliste che richiedono l’attivazione di un account – di verificare la possibilità di erogare la DaD attraverso il registro elettronico. Le scuole, tuttavia, sono state lasciate sole in questa scelta e soprattutto il Ministero dell’Istruzione non ha dato cenni di aver recepito gli studi condotti da diverse agenzie che dimostrano quanto sia opaco il trattamento dei dati da parte delle principali piattaforme tech mainstream. Il NOYB, centro europeo per i diritti digitali, in un report del 2 aprile 2020, ad esempio, ha valutato la conformità di alcune delle principali piattaforme per videoconferenze – Zoom, Webex Meetings (Cisco), Meeting (LogMeIn), Skype e Teams (entrambi Microsoft), Wire – denunciando come esse siano spesso non rispettose dei principi del Regolamento generale sulla protezione dei dati (GDPR), mentre, in uno studio pubblicato il 2 luglio 2020, il Garante europeo della protezione dei dati (GEPD o EDPS in inglese) riportava gli esiti di un’indagine sull’uso di servizi e prodotti Microsoft da parte di istituzioni, organi e organismi europei, giungendo alla conclusione che: l’UE ha una scarsa capacità di controllare l’ubicazione dei dati gestiti da Microsoft, i trasferimenti internazionali e il rischio di divulgazione illecita; Microsoft mantiene una certa discrezionalità nella gestione dei flussi di dati personali generati da prodotti e servizi Microsoft e nella possibilità di modificare unilateralmente gli accordi di licenza e le condizioni di protezione dei dati. C’è un altro fatto che va considerato in questa sede. Il 16 luglio 2020 la corte di giustizia dell’Unione europea ha emesso la sentenza Schrems II con la quale ha stabilito che gli Stati Uniti non garantiscono una protezione dei dati personali analoga a quella garantita dell’UE. La sentenza ha, di fatto, dato ragione al cittadino austriaco Maximilian Schrems, il quale aveva denunciato all’autorità irlandese di controllo che i propri dati personali fossero stati trasferiti da Facebook Ireland verso server appartenenti a Facebook Inc., situati negli Stati Uniti. Il signor Schrems chiedeva, perciò, che i propri dati non fossero soggetti a tali trasferimenti, sostenendo che il diritto e le prassi degli Stati Uniti non garantiscono una protezione sufficiente contro l’accesso, da parte delle autorità pubbliche, a tali dati (Corte di giustizia dell’Unione europea, 16 luglio 2020). Ciò significa che i giganti delle piattaforme statunitensi (Google, Amazon, Facebook, Apple, Microsoft) non possono rispettare il GDPR, anche se dichiarano di farlo. Di fatto, perciò, anche se Google Ireland Limited è la società

consociata di Google che si occupa del trattamento delle informazioni e del rispetto delle leggi sulla privacy vigenti per gli utenti residenti nello Spazio Economico Europeo o in Svizzera, “la legge americana [Cloud Act (Calderini, 11 giugno 2019)] concede al governo USA il diritto di richiedere i dati in possesso delle aziende USA e delle loro controllate, ovunque siano fisicamente collocati, nonché di vincolare le aziende al segreto circa queste richieste” (Garofalo, 7 agosto 2020). Viene dunque legittimo chiedersi se le scuole italiane siano state in grado di controllare le condizioni di privacy delle aziende tech statunitensi alle quali hanno affidato i dati di milioni di studenti/esse, spesso minorenni, obbligati/e ad aprire un proprio account personale per fruire della didattica a distanza, dal momento che neanche le istituzioni europee che hanno concluso contratti con i GAFAM ci sono riusciti. E, a tale proposito, Pievatolo (31 agosto 2020) si domanda se “la singola istituzione scolastica ha le conoscenze e il personale specializzato per poter concludere un contratto con Microsoft o Google [...] che la metta effettivamente in grado di assicurare e controllare che l’uso dei dati di studenti e docenti sia destinato rigorosamente ed esclusivamente alle esigenze didattiche e non sia invece esteso alla sorveglianza capitalistica o governativa”. Questi timori sembrano essere stati recepiti dal Garante della privacy che nel luglio 2020, nel corso di un’audizione davanti alla Commissione bicamerale per l’infanzia e l’adolescenza, si esprimeva in questi termini: “Con specifico riferimento ai minori, abbiamo posto all’attenzione del ministro dell’Istruzione l’esigenza di una svolta nel ricorso alle piattaforme in generale. Dicendo che intanto forse è più prudente utilizzare il registro elettronico, che pure non è privo di problemi: fra il registro elettronico e la piattaforma di una multinazionale di cui non si sa nulla è meglio nel presente dare indicazioni perché le scuole ricorrano tutte le volte che è possibile al primo” (Carlino, 8 luglio 2020).

3. Conclusioni. Monopoli dispotici e destini della democrazia in Rete

Attraverso strategie di marketing molto sapienti, i GAFAM ci hanno fatto credere che non sia possibile avere accesso ai principali servizi online senza la loro intercessione e soprattutto che essi sono in grado di metterci a disposizione le straordinarie risorse della Rete a titolo completamente gratuito. Come abbiamo tentato di far emergere nel corso di questa trattazione, invece, ogni volta che utilizziamo tali piattaforme cediamo loro una merce particolarmente preziosa: i nostri dati personali. Siamo noi, dunque, a lavorare più o meno inconsapevolmente e gratuitamente per queste aziende che, attraverso sofisticati algoritmi, sono in grado di tenere traccia di tutte le “briciole” digitali che ci lasciamo alle spalle nel corso delle nostre navigazioni e, in seguito, di elaborarle al fine di “pungolarci gentilmente”, per dirla con Thaler & Sunstein (2014), verso prodotti ai quali potremmo potenzialmente essere interessati. Il capitalismo delle piattaforme (Srnicsek 2016) è riuscito a far risultare i servizi che ci mette a disposizione così attraenti da rendere completamente invisibile il nostro lavoro e il sistema di sorveglianza continua alla quale siamo sottoposti. Secondo Cheney-Lippold (2017), questo processo assicura alle aziende che commerciano in dati, beni e servizi in Rete i maggiori profitti possibili: “L’economia digitale, come parte di un ecosistema che produce capitale, riconfigura il modo in cui concepiamo il lavoro, la retribuzione e persino la produzione. Se le nostre vite costituite di dati sono fatte dalle nostre stesse azioni, esse ordinano e rappresentano un nuovo tipo di lavoro. [...] Questa è ora una realtà non sorprendente della nostra esistenza quotidiana e in rete. Ma requisito di tale mercificazione è il rovesciamento della privacy” (pp. 256-257). Questione che non è possibile sottovalutare soprattutto se si parla di minori. Come mostrato nelle pagine precedenti, infatti, con l’avvento della pandemia e la conseguente necessità di dematerializzare i

luoghi della scuola, gli/le studenti/esse sono stati obbligati ad avere un proprio account personale per poter fruire della didattica a distanza, in quanto la maggior parte delle scuole ha scelto di avvalersi dei servizi messi a disposizione dall'azienda di Page e Brin. Google, perciò, in pochi mesi ha avuto accesso a una mole di dati senza precedenti sui bambini e sulle bambine che frequentano le nostre scuole, avendo la possibilità, peraltro, di distinguere in maniera quasi chirurgica i beni e i servizi di interesse dei genitori da quelli dei figli e, in tal modo, di determinare con straordinaria precisione i bersagli delle proprie strategie pubblicitarie. Inoltre, l'azienda di Mountain View, avendo soddisfatto l'urgenza delle/degli insegnanti e degli/delle alunni/e di trovare nuovi ambienti all'interno dei quali far proseguire la didattica durante il lockdown e avendo offerto loro spazi e servizi accattivanti e rispondenti ai loro bisogni, ha fidelizzato un numero consistente di nuovi clienti, molti dei quali appartenenti alle giovani generazioni, il che le assicurerà di sopravvivere e prosperare per molti anni a venire. Facendosi trovare pronta a rispondere alle esigenze insorte nel corso del periodo pandemico, Google ha dimostrato, ancora una volta – in questo caso anche alle bambine e ai bambini – che non esistono alternative apparenti o comparabili ai servizi che essa è in grado di fornire, estendendo ulteriormente il proprio controllo, che sembra andare ormai dalla culla alla tomba. Se prima della pandemia, infatti, la tendenza largamente prevalente era quella di creare un proprio account a partire dal periodo adolescenziale, con l'avvento del Covid-19 l'ingresso nell'ecosistema Google è stato anticipato addirittura ai primi anni della scuola dell'infanzia, rafforzando ulteriormente la posizione di predominio di Big G nel settore delle ricerche online e della pubblicità. Il dispotismo del monopolio Google, però, sembra cominciare a essere oggetto di indagini da parte della Commissione europea, tanto che soltanto pochi giorni fa l'Antitrust gli ha comminato una sanzione per “abuso di posizione dominante” che non ha precedenti nella storia. Ad essere messe sotto accusa sono state tre casistiche legate al sistema operativo Android che rafforzerebbero ulteriormente il potere di Google: “Primo: le restrizioni imposte ai produttori di smartphone, che devono pre-installare come applicazioni di default quelle della galassia di Google, come Search o Chrome, ‘per poter ottenere da Google una licenza operativa per il suo portale di vendita (Play Store)’. Secondo: il fatto che i produttori debbano accettare di non commercializzare dispositivi con versioni di Android non approvate da Google, pur di avere in concessione le app del colosso di Mountain View. Terzo: gli accordi di ripartizione del fatturato. Produttori di smartphone e compagnie telefoniche che vogliono ricevere una percentuale da Google, devono rinunciare a installare sui dispositivi app generiche concorrenti” (Zorloni, 14 settembre 2022).

Si tratta di un passo importante, che, anche se nel breve periodo non modificherà in maniera sostanziale le strategie commerciali di Google, costituisce un precedente prezioso a cui fare riferimento in futuro e, soprattutto, l'occasione per avviare una riflessione che, con il coinvolgimento di tutti gli attori della Rete – aziende, enti di controllo, consumatori –, possa sfociare in un riequilibrio del delicato rapporto fra democrazia e profitto nel cyberspazio.

Riferimenti bibliografici:

Benjamin, R. (2019). *Race After Technology. Abolitionist Tools for the New Jim Code*. Medford (MA): Polity Press.

Brin, S. & Page, L. (1998). The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Computer Networks*, vol. 30, 107-117.

- Calderini, B. (11 luglio 2019). Cloud act, la norma USA che fa a pugni con la privacy europea: i nodi. *AgendaDigitale.eu*, <https://www.agendadigitale.eu/sicurezza/privacy/cloud-act-la-norma-usa-che-fa-a-pugni-con-la-privacy-europea-i-nodi/> [ultimo accesso 16/09/2022].
- Cardon, D. (2016). *Che cosa sognano gli algoritmi? Le nostre vite al tempo dei big data*. Milano: Mondadori.
- Carlino, A. (8 luglio 2020). Garante Privacy: per la didattica a distanza meglio affidarsi al registro elettronico che ad una multinazionale. *Orizzontescuola.it*, <https://www.orizzontescuola.it/garante-privacy-per-la-didattica-a-distanza-meglio-affidarsi-al-registro-elettronico-che-ad-una-multinazionale/> [ultimo accesso 16/09/2022].
- Cheney-Lippold, J. (2017). *We Are Data. Algorithms and the Making of Our Digital selves*. New York: New York University Press.
- Corte di giustizia dell'Unione europea (16 luglio 2020). *Sentenza nella causa C-311/18. Data Protection Commissioner/Maximilian Schrems e Facebook Ireland*. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf> [ultimo accesso 21/09/2022].
- Decreto Legge 22 (8 aprile 2020). *Misure urgenti sulla regolare conclusione e l'ordinato avvio dell'anno scolastico e sullo svolgimento degli esami di Stato*. <https://www.gazzettaufficiale.it/eli/id/2020/04/08/20G00042/sg> [ultimo accesso 21/09/2020].
- DPCM (4 marzo 2020). *Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale*. <https://www.gazzettaufficiale.it/eli/id/2020/03/04/20A01475/sg> [ultimo accesso 21/09/2022].
- DuckDuckGo (2018). *Measuring the "Filter Bubble": How Google is influencing what you click*. <https://spreadprivacy.com/google-filter-bubble-study/> [ultimo accesso 17/09/2022].
- EDPS (2 July 2020). *Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services*. https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html [ultimo accesso 15/09/2022].
- Garofalo, L. (12 ottobre 2020). La privacy degli studenti e Google: le domande al ministro dell'istruzione. *privacyitalia.eu*, <https://www.privacyitalia.eu/la-privacy-degli-studenti-e-google-le-domande-al-ministro-dellistruzione/14099/> [ultimo accesso 21/09/2022].
- Garofalo, L. (7 agosto 2020). "Le Big Tech dopo la sentenza Schrems II non possono rispettare il GDPR, anche se dicono di farlo". Cosa fare? *Key4biz*, <https://www.key4biz.it/LE-BIG-TECH-DOPO-LA-SENTENZA-SCHREMS-II-NON-POSSONO-RISPETTARE-IL-GDPR-ANCHE-SE-DICONO-DI-FARLO-COSA-FARE/317971/> [ultimo accesso 16/09/2022].
- GARR. *Chi siamo*. <https://www.garr.it/it/chi-siamo> [ultimo accesso 21/09/2022].
- Google (30 settembre 2020). *Norme sulla privacy di Google*. https://www.gstatic.com/policies/privacy/pdf/20200930/r9u74aii/google_privacy_policy_it_eu.pdf [ultimo accesso 16/09/2022].
- Google Workspace. *Google Workspace for Education Privacy Notice*. https://workspace.google.com/terms/education_privacy.html#privacy-police-revamp-your-info [ultimo accesso 21/09/2022].

- GPDP (26 marzo 2020). *Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"*. <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784> [ultimo accesso 15/09/2022].
- INDIRE (20 luglio 2020). *Indagine tra i docenti italiani. Pratiche didattiche durante il lockdown. Report preliminare*. https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/004/598/MEMORIA_INDIRE_completa.pdf [ultimo accesso 15/09/2022].
- Ministero dell'Istruzione (17 marzo 2020). *Nota prot. 388*. https://www.miur.gov.it/ricerca-tag/-/asset_publisher/oHKi7zkjcLkW/document/id/2598016 [ultimo accesso 15/09/2022].
- Noble, S. U., Tynes, B. M. (ed.) (2016). *The Intersectional Internet. Race, Sex, Class and Culture Online*. New York: Peter Lang.
- Noble, S.U. (2018). *Algorithms of Oppression. How Search Engines Reinforce Racism*. New York: New York University Press.
- Noyb (2 april 2020). *Report on privacy policies of video conferencing services*. https://noyb.eu/sites/default/files/2020-04/noyb_-_report_on_privacy_policies_of_video_conferencing_tools_2020-04-02_0.pdf [ultimo accesso 15/09/2022].
- O'Neil, C. (2017). *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*. Milano: Bompiani.
- Pievatolo, M. C. (31 agosto 2020). *Didattica digitale, perché non si crea una piattaforma nazionale basata sul software libero?* *key4biz*, <https://www.key4biz.it/didattica-digitale-perche-non-si-crea-una-piattaforma-nazionale-basata-su-software-libero/319069/> [ultimo accesso 15/09/2022].
- Srnicek, N. (2016). *Capitalismo digitale. Google, Facebook, Amazon e la nuova economia del web*. Roma: Luiss University Press.
- Statcounter (August 2022). *Search Engine Market Share Worldwide (Aug 2021 – Aug 2022)*. <https://gs.statcounter.com/search-engine-market-share> [ultimo accesso 17/09/2022].
- Thaler, R. S. & Sunstein, C. S. (2014). *La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*. Milano: Feltrinelli.
- Zona, U., De Castro, M. (2020). *Edusfera. Processi di apprendimento e macchine culturali nell'era social*. Lecce: Pensa Multimedia.
- Zorloni, L. (14 settembre 2022). *Google condannata in Europa a pagare 4,1 miliardi per il sistema Android*. *Wired*, <https://www.wired.it/article/google-multa-4-miliardi-android-corte-giustizia-europa/> [ultimo accesso 18/09/2022].