Che ci siano in campo prospettive d'opposizione, macchinazioni di stampo terroristico o semplice divulgazione di controinformazione, è innegabile che la Rete si stia sempre più facendo notare come **un potente mezzo che le minoranze adoperano per combattere quella che è una battaglia ideologica asimmetrica**. Il cosiddetto "dark web" e i programmi di messaggistica criptati hanno fatto sì che il discutere pubblicamente di argomenti ritenuti scabrosi sia ormai alla portata di tutti, cosa che a sua volta ha portato a interazioni più rapide ed efficienti, nel bene e nel male.

Non tutto è oro ciò che luccica, però. Sebbene il tramandare le idee e i contenuti sia innegabilmente sempre più agile, risulta anche più facile che Governi, dittature e potenti riescano a risalire alla fonte dei proselitismi, mettendo profondamente a rischio tutti coloro che osano alzare la voce contro l'establishment. Un esempio chiaro di queste dinamiche apparentemente paradossali lo abbiamo in Alexei Navalny, politico russo d'opposizione che è stato capace di fare dei social un'arma, un'arma che si è dunque parzialmente ritorta contro il suo stesso entourage. Il dubbio è quindi chiaro: la Rete ci libera o ci rende schiavi?

Le origini del World Wide Web

Non è corretto sostenere che la Rete per come la conosciamo oggi, il World Wide Web, sia nato con intenti democratici: la primissima iterazione, l'**Arpanet**, era stata pensata in seno alla Difesa statunitense, quindi la tecnologia è immediatamente passata in mano alle alte sfere accademiche degli USA. Neppure le università si sono approcciate allo strumento con fare libertario, la loro priorità era infatti quella di consolidare un network che permettesse di consultare comodamente tutte le informazioni depositate nei singoli computer degli atenei, un sistema che ha preso progressivamente la forma degli hyperlink che ancora oggi sono alla base del protocollo HTTP.

Sebbene il World Wide Web non sia stato generato da una profonda ricerca di libertà, il più celebre dei suoi padri, **Tim Berners-Lee**, ha sempre mantenuto un atteggiamento dichiaratamente "open source" alla digitalizzazione, un approccio che al giorno d'oggi pare alquanto anacronistico, ma che viene portato avanti da molti hacker, soprattutto da quei "white hat" convinti che **una maggiore condivisione dei dettagli informatici possa ottimizzare le macchine in chiave umanistica**.

Da che si è diffusa la Rete – nei primi anni Novanta – si è però consolidato un cartello aziendale che è finito con il monopolizzare le prospettive, presenti e future, del digitale. Il sogno di un'infrastruttura orizzontale sviluppata dal basso è stato lacerato e alcuni, Berner-Lee compreso, si rifugiano nell'idea di un nuovo web decentralizzato in cui si possa

ricominciare da zero. Si tratta di una speranza utopica che però viene contrastata dai piani delle Big Tech e dei Governi, i quali vorrebbero puntare rispettivamente sul **trasformare la Rete in un gigantesco centro commerciale virtuale e sulla tracciabilità degli utenti**.

Eccoci dunque al punto nevralgico della questione: **le parti che stanno dettando l'evoluzione informatica sono quelle indissolubilmente legate all'economia della sorveglianza**. Ai tempi di George W. Bush Jr., gli Stati Uniti, area madre delle principali aziende digitali occidentali, sono stati ben felici di lasciare terreno libero ai traffici commerciali di imprenditori desiderosi di assorbire i dati degli utenti, dati che formalmente erano poi convogliabili all'interno del programma governativo **PRISM**. Si era formato un rapporto stabile in cui Stato e industrie hanno camminato fianco a fianco per anni, un rapporto che però si è andato progressivamente a deteriorare a causa di fughe di informazioni, gravi incidenti commerciali e una marcata alterazione degli equilibri di potere. Le Big Tech, sempre più influenti, stanno offrendo mezzi e assistenze che modificano esplicitamente le tendenze sociali e politiche, con il risultato che le Amministrazioni di tutto il mondo si sono scoperte **violentemente sensibili a ciò che succede nei dietro le quinte del settore tecnologico**, minacciando sanzioni, normative o ripercussioni disperatamente pensate per arginare com'è possibile la situazione.

Un approccio aziendale 4.0

La cultura della globalizzazione precedente agli anni Duemila era dominata da aziende di matrice statunitense la cui influenza veniva adoperata anche per **propagandare i valori ideologici del gigante d'oltreoceano**. Almeno per quanto riguarda lo sviluppo di un immaginario condiviso, della produzione del concetto di "progresso". Da allora le cose sono cambiate, le comunicazioni e i trasporti sono divenuti fulminei e nazioni che prima venivano solamente sfruttate si sono oramai elevate a giganti economici. In generale, si è strutturato **un mondo più interconnesso e interdipendente**, un mondo ibrido in cui diverse culture sentono la necessità di esprimere i propri valori e i propri interessi.

Contemporaneamente, diverse aziende tech americane si sono rese conto di aver ormai saturato il Mercato occidentale, consapevolezza che le ha portate a cercare uno spazio di crescita nelle cosiddette aree in via di sviluppo, prime tra tutte **India e Cina**. Le due nazioni, ambo estremamente popolose, rappresentano infatti un bacino d'utenza più che desiderabile e i mastodonti americani hanno volentieri limato i loro tratti più caratteristici per accomodare i loro gusti, le loro sensibilità e i loro interessi politici.

Le Big Tech, in particolare, si trovano quotidianamente a ridimensionare i contenuti legali e

valoriali delle proprie policy per assecondare le leggi delle Amministrazioni per loro più influenti, dando il via ad **atteggiamenti manageriali ambigui e disomogenei** dettati dal bieco calcolo del rapporto costi-benefici. Non che la posizione dei leader d'impresa sia semplice: da una parte bisogna tutelare l'identità dei brand, dall'altra è doveroso sottostare alle norme locali, norme che magari sono state introdotte strada facendo da cariche politiche dallo smaccato carattere autoritario. Come comportarsi dunque nel caso un Governo antidemocratico decida di imporre delle leggi contrarie alla sensibilità occidentale? La risposta ovvia sarebbe quella di operare solamente in nazioni di cui si rispetta e condivide l'etica, tuttavia è ben noto che questa prospettiva sia smaccatamente anti-economica.

Le imprese più ingombranti si dimostrano quindi ben pronte a esibire una certa elasticità: quando legge e policy aziendali non combaciano, si decide di confinare l'applicabilità della legge al solo territorio coinvolto. In altre parole, un dissidente indiano sarà oscurato in India, ma i suoi post potranno essere intercettati da coloro che vivono fuori confine. Si definisce quindi un atteggiamento per cui **la tutela degli utenti ha un valore subordinato ai capricci del Mercato**, con molti dei giganti del settore che accomodano anche le dittature, ammesso che dette dittature gestiscano corposi interessi finanziari.

Fossero rimaste confinate in aree remote del globo, l'Occidente sarebbe anche stato anche pronto a tollerare queste ambiguità, tuttavia l'assalto a Capitol Hill da parte di invasati internettiani ha convinto la Casa Bianca a ridiscutere il suo rapporto con le Big Tech. Allo stesso tempo, l'Unione Europea ha iniziato a questionare quanto siano tollerabili, economicamente e strategicamente, i soprusi subiti dal settore digitale nella sua inquadratura normativa di stampo americano, inquadratura che è tendenzialmente poco compatibile con il GDPR europeo.

La sicurezza è sconveniente (e insicura)

Nella lingua tedesca, "sicurezza" può essere tradotto con le parole **"sicherheit" e "geborgenheit"**. Sono due forme di sicurezza qualitativamente differenti: la prima è affine alla lettura comunemente accettata anche nel nostro idioma, mentre la seconda esplora un'altra forma più emotiva della sicurezza, una che sfocia nel contesto della "stabilità". Nel parlare della sicurezza in campo digitale è opportuno tenere in considerazione ambo le sfumature, se non altro perché questa deriva filologica nasconde al suo interno un'insidia che rischia altrimenti di rendere effimero il dibattito.

Nella lettura tradizionale, l'ideale della "sicherheit" combacia con la **sorveglianza**

ossessiva in cui molti Governi stanno defluendo. Secondo questo approccio, meglio affidarsi a un Governo che nuclearizza su di sé il controllo, che ad aziende pronte ad approfittare dei cittadini o ad abbandonare la Rete nelle mani dei terroristi che prolificano nel sottobosco digitale. Da qui, il passo verso l'ur-fascismo codificato da Umberto Eco è breve. Vale dunque la pena di sviluppare consapevolezza sulla **tutela autonoma della privacy**, sia perché il confine tra legge e oppressione non è sempre chiaro, sia perché le fughe di dati sono considerate ormai un problema endemico della digitalizzazione, un problema la cui soluzione non rientra certamente nelle priorità governative italiane o europee.

L'uso di app quali WhatsApp, Instagram, Facebook è praticamente fuori questione e anche adoperare Google è poco lungimirante. Quelle citate sono realtà che raccolgono in maniera compulsiva i dati dei loro utenti, che li tracciano in maniere sorprendenti e che in tutta probabilità non comprendiamo ancora pienamente, realtà che sarebbe raccomandabile evitare in assoluto, ma che sono anche talmente **intrecciate con la socialità 4.0** che la loro esclusione rasenta l'impossibile. Tralasciando la sfera privata, esistono contesti in cui la presenza sui social è essenziale alla dimensione professionale: vuoi che sia indispensabile per fare conoscere all'estero il proprio brand o che la creazione degli account sia "suggerita" da una dirigenza che vuole aumentare la visibilità dei propri contenuti, resta il fatto che **l'emarginarsi dai social possa avere ripercussioni sociali e lavorative**.

Molti cercano di compensare affidandosi a Telegram, servizio di chat il cui sistema di archiviazione in cloud è accusato di enormi fragilità. Meglio piuttosto divergere su **Signal**, programma che, essendo meno popolare, difficilmente vi permetterà di rimanere in contatto con amici, familiari e colleghi. Utile sarebbe anche cambiare le proprie abitudini a proposito dei motori di ricerca. Al posto di appoggiarsi al già citato Google, si potrebbe far riferimento a portali quali **Startpage, Searx e DuckDuckGo**, i quali non targettizzano l'utenza, ma si limitano a mostrare inserzioni affini alle tematiche delle ricerche eseguite. Manco a dirlo, questi siti incappano però in un'indicizzazione meno efficiente, soprattutto per quanto riguarda la ricerca di e per immagini, con il risultato che molte delle indagini che passano per i loro server potrebbero risultare infruttuose o frustranti.

Esistono dunque le reti virtuali private sicure (Secure **VPN**), reti che possono essere consolidate attraverso software o estensioni che cifrano i dati trasmessi e simulano gli IP, ovvero **alterano il codice di identificazione del dispositivo** usato per navigare, così da concedere agli internauti un maggiore anonimato. Si tratta di strumenti che potrebbero essere poco accessibili a coloro non avvezzi all'informatica, tuttavia si dimostrano sempre più essenziali per sopravvivere al mondo digitale odierno. La loro esistenza permette infatti di simulare IP di qualsiasi parte del mondo, uno stratagemma che è in grado di **valicare le censure imposte a livello nazionale**. I servizi di VPN mostrano tuttavia delle limitazioni

evidenti: i migliori richiedono il pagamento di un abbonamento e, a ben vedere, neppure loro garantiscono l'immunità completa dalla fuga di dati. Solo lo scorso marzo è emerso che i dati di almeno 21 milioni di user di VPN sono stati compromessi e non si è neppure trattato di un caso isolato: grandi aziende del settore hanno manifestato criticità già a partire dal 2019.

Un'ulteriore difesa la si può cercare nel software open-source The Onion Router, comunemente detto **TOR**. Si tratta di un programma pensato per massimizzare l'anonimato nella comunicazione dei dati, un presupposto che però dev'essere mantenuto preservando un rigoroso codice di condotta: è necessario alterare a monte il proprio IP, ricordarsi di non aprire il browser di navigazione a tutto schermo (rivelerebbe ad eventuali osservatori dei dettagli sull'hardware in uso), evitare i siti che non usano il protocollo HTTPS e assicurarsi di aprire i file scaricati solamente dopo essersi disconnessi dalla Rete. **Usare TOR in maniera efficiente è complesso**, inoltre la sua navigazione è estremamente lenta e poco pratica poiché i server non vantano portata e dimensione di quelli a disposizione delle Big Tech. Per evitare le censure dittatoriali, poi, il programma si appoggia a "nodi" indipendenti, sistemi di supporto sparpagliati in diverse nazioni e gestiti da volontari che non sempre vengono selezionati con la dovuta accortezza. A inizio 2021 è infatti emerso che un'entità dotata di immense risorse stesse foraggiando centinaia di nodi con l'intento di **compromettere il sistema annichilendo l'anonimato della piattaforma**.

L'ideale sarebbe approcciarsi alla Rete con un computer dedicato, con le opportune tutele e attraverso TOR, ricordandosi di non fare o scrivere nulla che possa rivelare dettagli importanti su di sé. Qui entra in campo il problema della "geborgenheit": una simile sicurezza di navigazione rischia di **ledere la stabilità socio-economica garantita da un'esperienza internettiana tradizionale**. L'uso intensivo di sistemi che tutelano la privacy va infatti a discapito di un universo globalizzato che fa della rapidità del consumo e della visibilità dei paradigmi essenziali. La dissonanza tra tutela e presenza digitale rischia di ledere i rapporti sociali e limitare le possibilità professionali, trainando l'utente in quello che si potrebbe definire un **ascetismo virtuale** che ha forti ripercussioni sulla vita privata.

In verità, i casi in cui sia opportuno non lasciare alcuna traccia del proprio passaggio sono comunque casi estremi, spesso non ha senso abbandonarsi ad atteggiamenti che sono di per loro propensi a tramutarsi in ossessioni, basta piuttosto affidarsi ad accorgimenti basilari quali l'evitare il più possibile i prodotti di aziende note per i loro abusi, evitare l'acquisto di accessori che si connettono immotivatamente alla Rete e, magari, pretendere che sia la politica a difendere gli interessi dei cittadini. Dopotutto la "sicherheit" non può limitarsi alla mera sorveglianza, deve fornire anche qualche forma di tutela, altrimenti il contratto sociale si va a lacerare.

Rete, chat e dark web: croce e delizia per le voci di opposizione sociale

[di Walter Ferri]