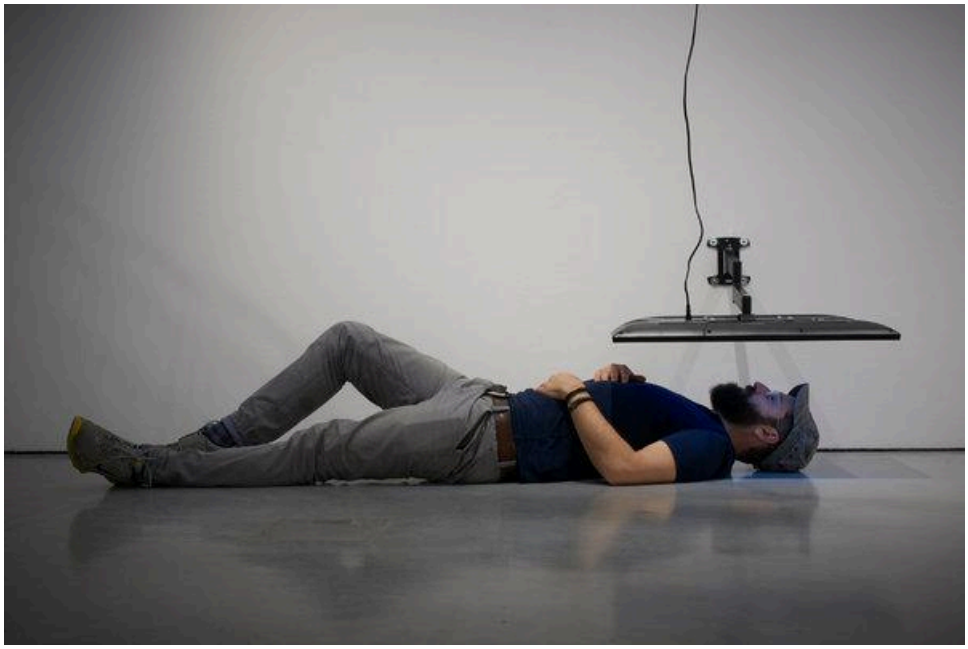
Privacy pubblica

«Il Parlamento europeo è il luogo dove Zuckerberg è venuto a scusarsi di fronte a tutti gli europei, e questo dimostra ancora una volta la centralità di questo parlamento.» Con queste parole il presidente del Parlamento europeo Antonio Tajani ha chiuso il suo discorso alla conferenza stampa di martedì 22 maggio successiva all'audizione del CEO di Facebook a Bruxelles. Un Tajani apparentemente soddisfatto, al quale sono poi state poste domande a pioggia su come sia stata stabilita la modalità di interrogatorio, conclusosi in 44 minuti di domande vaghe (con l'unica eccezione fatta da Guy Verhofstadt) e 26 minuti di non-risposte da parte del cittadino americano. Una discussione che ha mostrato ancora una volta (dopo le audizioni di Mark negli States, soprattutto al Senato) l'incapacità delle organizzazioni governative di occuparsi di temi digitali entrando nel merito delle questioni. O forse, pensandoci meglio, un loro disinteresse.

«Zuckerberg ci ha garantito che quanto successo con Cambridge Analytica *non succederà più*» rassicura Tajani. Cosa questo significhi, considerando che si sta parlando di una piattaforma che fa dell'analisi dati il suo *core business*, lo lasciamo alla libera interpretazione. Ma le parole del presidente rivelano di più, e diradano la nebbia di fuffa *catchy* per riportarci al centro della questione: il rapporto di forza tra poteri privati e poteri pubblici. Oltre a questo, le regolamentazioni dello spazio virtuale sollevano implicazioni complesse per quanto riguarda la territorialità. Nell'articolo 3 della GDPR, «territorial scope», si estende l'applicazione del regolamento a ogni organizzazione che tratta con dati di cittadini residenti nell'Unione Europea, indipendentemente che il processo di analisi dati abbia luogo o meno nell'Unione. Il regolamento è molto indicativo e per ora è più che altro un insieme di linee guida, ma sarà interessante vedere come si articolerà una politica sostanzialmente «extra-territoriale» e gli eventuali conflitti con imprese al di fuori del territorio europeo. Capiamo quindi che ad essere in gioco sono complessi rapporti di forza, dove da un lato il Capitale gioca sulla deterritorializzazione dell'informazione e dall'altro le istituzioni governative (nazionali e internazionali) tentano di riterritorializzare la loro giurisdizione in nuove forme. Il dibattito su privacy e gestione dei dati, esploso a partire dal non-scandalo di Cambridge Analytica, rilanciato dalla messa in atto del GDPR il 25 maggio (che comunque era programmata da mesi), deve essere inserito in un quadro molto più ampio per essere compreso appieno e che riguarda la dicotomia tra sfera pubblica e privata.



All’inizio del 2016 l’Fbi chiese ad Apple di potere entrare nell'iPhone di Syed Rizwan Farook, uno dei due attentatori della strage di San Bernardino dove morirono 14 persone, oltre i due attentatori. L'iPhone 5 di Farook fu requisito dall'Fbi, che non poteva però accedere a contenuti. Apple rifiutò la collaborazione, dando il via ad una battaglia comunicativa, legale e tecnologica memorabile, conclusasi con la dichiarazione dell’Fbi di essere riuscita a bucare il dispositivo grazie agli hacker di un'azienda di sicurezza israeliana, la Cellebrite. Apple, in risposta, chiese di poter conoscere i dettagli della vulnerabilità per poterla fixare. Sono state scritte pagine e pagine sulla vicenda, che sicuramente ha lasciato tante questioni in sospeso, dalla possibilità di un’azienda IT di disporre dei dati salvati sui «propri» dispositivi, ai doveri a cui questa è tenuta o meno nei confronti del Governo. In situazioni del genere è chiaro che le posizioni di movimenti tendenzialmente progressisti e vicini ad una qualsivoglia istanza di «libertà di informazione» e «gestione comunitaria della tecnologia» non sappiano bene da che parte stare.

Il diritto alla privacy, per come oggi viene difesa e sostenuta anche dai movimenti di sinistra, si rifà a una cultura hacker che si è rivelata avanguardia culturale, politica e tecnologica negli anni ‘90. La stessa cultura che, oltreoceano, nella Silicon Valley degli anni ’70, ha sfornato Bill Gates e Larry Page (e Richard Stallman). Le affinità tra spirito hacker e anarco-capitalismo non sono trascurabili: individualismo, elogio della meritocrazia, fiducia smodata nella tecnologia salvifica e, soprattutto, il culto della libertà. Libertà che, nell’ottica anarcocapitalista si traduce in primis in elaborazione di tecniche e strategie di difesa contro la sorveglianza statale, uno Stato interpretato principalmente come limite al libero mercato. La privacy è quindi diventata un’istanza centrale nelle posizioni dei big dell’IT come strumento di contrasto alle ingerenze governative. Gli stessi big che oggi vengono rappresentati dai governi come minacce alla privacy degli utenti. Se poi ripensiamo alle parole di Tajani, ci accorgiamo che quello dell’informazione è un terreno su cui si

gioca uno scontro non solo tra potere privato e pubblico, ma anche tra blocchi interni alle istituzioni, come nel caso di organismi internazionali che tentano costantemente di far valere la propria egemonia verso gli stati nazione. Una guerra che si consuma sia a colpi di regolamentazioni e policy che a livello di imposizione di un ordine del discorso, il tutto sul corpo virtuale dell'utente produttore di dati.

La confusione che ne deriva è la conseguenza naturale di una cristallizzazione del concetto di privacy durata anni, nei quali le dinamiche della produzione, cognitiva e non, sono mutate radicalmente, in cui il capitalismo dell'informazione è cambiato, sia nell'orientamento del business che nel linguaggio. Se pensiamo alla dicotomia *closeness/condivisione* le cose si fanno ancora più complesse. Da strumento di lotta al copyright, lo *sharing* è diventato un imperativo del capitalismo digitale, dove per *condivisione* si considera la messa a disposizione gratuita del proprio lavoro di produttore di informazione. Una complessità tale da rendere il campo della *privacy* un iperoggetto ormai difficile da valutare da un unico punto di vista.

È chiaro che, da soggetti sfruttati e subalterni, la della garanzia di uno spazio di azione (individuale o comune) è sia un'istanza fondamentale che un diritto da difendere. La privacy quindi va difesa dalla repressione dello Stato, ma anche dalla capitalizzazione delle esperienze intime. La privacy, quindi, è sinonimo di garanzia di una *zona sicura* dalla messa a valore e dagli autoritarismi.

Non sui nostri corpi

Nel suo articolo Violence Against Women and The Persistence of Privacy, pubblicato sull'Ohio State Law Journal nel 2000, Sally Goldfarb scriveva:

La legge americana ha a lungo abbracciato una distinzione fondamentale tra sfera pubblica e sfera privata. Di conseguenza, alcune questioni importanti per le donne, tra cui la violenza domestica e l'aggressione sessuale, sono state tradizionalmente considerate private e quindi esentate dal controllo legale. Gli studiosi femministi hanno criticato due versioni della dicotomia tra sfera pubblica e sfera privata, che sono state particolarmente potenti nel plasmare lo status sociale e giuridico delle donne: la divisione tra mercato e famiglia e la divisione tra stato e società civile.

La posizione di alcune teoriche femministe nei confronti della privacy, come argomentato anche da Anita Allen, è ambivalente, dato che questo diritto è tanto un indispensabile strumento di autodeterminazione quanto una barriera da superare, costituendo, in quanto forma di proprietà privata, un sinonimo della sfera domestica, quindi di dispositivo patriarcale. Partendo da queste considerazioni è più facile dipanare il filo della matassa, e riconoscere in ognuna delle due diramazioni (quella di dispositivo liberante e quella assoggettante), come il concetto di privacy si evolve e viene utilizzato. Pubblico e privato, anche in termini di proprietà dell'informazione, si rivelano entrambi soggetti predatori, il cui conflitto reciproco è un fattore cruciale del quale un ragionamento sulla privacy – tornando al caso dei dati per non allargare la discussione a un tema troppo vasto – deve tenere conto.

Julian Assange, il discusso fondatore di Wikileaks, non è esente da visioni anarcoliberiste. La pubblicazione di gigabyte di informazioni riservate, come nel caso di Vault7, costituisce un attacco frontale alla segretezza nazionale, e finisce per diventare indirettamente uno strumento di dominio delle tech companies sul terreno dell'informazione, godendo intanto di una retorica anti-repressiva e erigendosi a difesa della libertà di informazione.

In un trafiletto su *Le Monde Diplomatique* di maggio, in calce a un interessante articolo di Frank Pasquale, Pierre Rimbet sottolinea la narrazione totalmente differente dell'utilizzo dell'analisi dati fatta dalla stampa americana nel caso della vittoria di Obama e quella di Trump. È ovvio che nell'epoca del mondo digitale ogni partito o coalizione politica hanno fatto uso di metodi o strategie diverse di analisi dell'elettorato per potenziare la propria comunicazione. I democratici, dopo il caso di Cambridge Analytica, hanno risposto che loro, a differenza degli avversari, hanno usato dati aggregati e non profilati. Una risposta simile a quella di un post pubblicato da Zuckerberg nei giorni della tempesta, dove consolava gli utenti del fatto che Facebook non ha usato i nostri dati direttamente per elaborare strategie comunicative, ma ha «soltanto» ricavato analisi da aggregati delle nostre informazioni. Se nell'opinione pubblica è possibile rispondere con queste affermazioni senza scatenare nessun dubbio, è perché non abbiamo mai capito esattamente quale fosse il problema legato a Cambridge Analytica. Seguendo una certa interpretazione del diritto alla privacy, secondo i democratici o nella lettura di scusa di Mark, il problema di Cambridge Analytica consiste nell'aver bucato la nostra sfera privata individuale. Ma il punto non è questo, quanto semmai il ruolo che una multinazionale ha potuto esercitare nello sviluppo dei processi democratici, forte di una gigantesca proprietà di informazioni, e il fatto che un colosso dell'IT abbia potuto fare profitti incalcolabili usando dati prodotti da noi. Che poi ci fosse sopra o meno il nostro nome rimane una questione, in fondo, secondaria.

Tabula rasa. Immaginare nuove parole per una scienza dei common

La mappa non è il territorio, il linguaggio non è la realtà. La lotta per una tecnologia utile alla collettività è una battaglia che ora si gioca anche sul terreno lessicale. Gli ultimi anni sono stati un fiorire di neologismi (fake news, smart city, big data…) spesso spinti o addirittura coniati da giganti dell'industria dell'informazione con lo scopo di ri-plasmare i rapporti e l'immaginario della tecnologia, e riuscire così a svolgere un ruolo egemonico. La *privacy* non è che un esempio.

Tornando alla GDPR, tra le altre cose si garantisce un diritto all'oblio, ovvero la capacità di un utente di richiedere la cancellazione totale dei propri dati dalle piattaforme. Ma siamo sicuri che questa concezione di «propri dati» sia esente da contraddizioni? Pensiamo alle conversazioni fatte con altre persone, anche su bacheche pubbliche, o a dati che potrebbero effettivamente contribuire alla gestione delle risorse e dei beni comuni.

Negli ultimi anni si è sempre più diffusa, anche da parte di istituzioni pubbliche, la pratica di aprire portali *open data*, ovvero dati liberamente accessibili sotto licenze aperte. L'open data richiama alla più generale disciplina dell'*open government*, con la quale la pubblica amministrazione si rende trasparente di fronte ai cittadini. Ma anche sul terreno dell'*open* si continua a giocare la partita tra differenti poteri. Più informazione disponibile, questo l'abbiamo già capito, significa per il capitale maggiore profitto. Anzi, potremmo proprio dire che l'*open*, anch'esso strumento proveniente dai movimenti hacker anti-copyright, sia stato sussunto nelle logiche capitaliste. Paradossalmente, più che una piattaforma proprietaria, una di dati *aperti* può diventare miniera d'oro per l'estrazione di analisi e produzione di (plus-)valore. Non è un caso se sono anche gli stessi big dell'IT che mettono a disposizione le proprie informazioni (intese ad esempio anche come sorgenti di software), perché sanno così di poter contare su un esercito di analisti, programmatori e statistici non retribuiti.

Le possibilità sempre presenti di controllo sociale (Stato) ed estrazione di valore (Capitale) sembrano paralizzare le possibilità di azione su una gestione *common* dell'informazione.

È notizia di inizio maggio che il Comune di Torino ha stretto un accordo con la TIM per usare i dati della mobilità dei cittadini per poter progettare più efficacemente il tracciato della nuova linea 2 della metropolitana. Un risultato che, se ipoteticamente perseguito in una giusta direzione, potrebbe portare vantaggi ad una collettività. Di mezzo ovviamente c'è un privato/aggregatore di dati, con tutti i contratti e le clausole che senz'altro saranno state previste. Diventa così chiaro che se vogliamo immaginare una tecnologia comune non potremo che farlo ricalibrando l'intero apparato di cattura, analisi e fruizione dell'informazione. Affermare che l'algoritmo non è neutrale significa anche che nella progettazione di una piattaforma dell'informazione non dovremmo discutere solo se rendere i dati *open* o meno, ma affrontare la totalità del processo di gestione dell'informazione. Progetti in questa direzione iniziano a vedersene, come il progetto europeo Decode che coinvolge 13 città tra cui Barcellona e Amsterdam. «Il nostro scopo è creare "data commons" dai dati prodotti dalle persone, dai sensori, dai dispositivi. [...] I nostri dati hanno un

valore. Ecco come ce lo riprendiamo», spiega Francesca Bria sul *Guardian* illustrando il progetto che punta ad utilizzare tecnologie decentralizzate (come la blockchain per creare policy personalizzate dall'utente).

Infine, immaginare un'uscita dalla dicotomia privacy/privato implica la riformulazione delle relazioni sociali. Le stesse pratiche di autocoscienza femminista sono una de-/ri-costruzione della sfera privata, garantita però da una *safe zone* basata su orizzontalità, autodeterminazione, anti-autoritarismo. Le contraddizioni che si aprono sulla gestione dell'informazione possono essere grimaldelli per *exploitare* altre e più profonde contraddizioni. I progetti di contro-mappatura ne sono un esempio. Obiezione Respinta è una mappa delle farmacie e dei medici obiettori in Italia, realizzata grazie a continue segnalazioni. Compiendo una vera e proprio *contro*-sorveglianza, è un progetto che ricalibra fortemente il piano del discorso sulla privacy, e rimette al centro l'asimmetria dei rapporti di forza, quindi la distinzione tra un controllo repressivo e un monitoraggio *dal basso* nei confronti delle istituzioni.

Una recente elaborazione sul ruolo delle tecnologie nel plasmare relazioni e quindi rapporti di forza, nel quale viene citato anche l'esperimento di Obiezione Respinta, è l'antologia *Smagliature Digitali* (Cossutta, Greco, Mainardi, Voli – Agenzia X, 2018). In tutti i contributi del saggio è evidente l'ambivalenza della tecnologia come mezzo di liberazione sia di assoggettamento, così come l'esigenza del rompere con le dicotomie binarie per poter disinnescare dispositivi di potere. È nella parte conclusiva, *Sorveglianza, soggettività e spazio pubblico*, che le autrici tornano sulla questione del controllo, sempre più biopolitico e spostato sul campo del desiderio, sul quale la società disciplinare agisce con continue aperture e chiusure, tra le quali si può immaginare un'azione che ne amplifichi le contraddizioni schizofreniche, apra strade alternative sia al dominio pubblico che a quello privato: la rottura della distinzione tra pubblico e privato anticipa molti dei discorsi sulla precarietà e non solo in cui ogni soggetto deve farsi imprenditore di sé, essere capace di mettere a valore ogni aspetto della propria vita, dalle proprie competenze alle proprie relazioni. Se il controllo attraverso una telecamera, pur essendo pervasivo, permetteva forme di resistenza che passavano attraverso il semplice svelamento della sorveglianza, il complesso intreccio tra desiderio di inclusione nello spazio pubblico, pratiche confessionali digitali e esiti di sorveglianza e normalizzazione ci hanno spinto a interrogarci su come inceppare questo meccanismo. [...] Si tratta, perciò, di cercare tracce di resistenza, seppur minime, nelle condotte individuali (e collettive) di chi agisce nelle e attraverso le tecnologie, senza immaginare un soggetto resistente, ma tenendo gli sguardi aperti per individuare l'emersione, anche in forme inedite e collettive.