Uno zaino digitale contrasta i nuovi rischi di censura e totalitarismo

di Andrea Granelli

Ogni innovazione tecnologica apre uno spazio potenziale anche per ripensare le norme che ne regolano il comportamento, orientando e facilitando l'uso "corretto" e virtuoso e ostacolando se non addirittura reprimendo quelli perniciosi.

Il digitale – rispetto alle altre tecnologie – pone una sfida in più in quanto aumentando la complessità delle sue soluzioni e la loro integrabilità con le soluzioni già in uso rende possibile funzionalità e comportamenti imprevedibili anche per gli stessi progettisti. Ciò rende quasi **impossibile la normazione ex ante** – prima cioè che la tecnologia venga lanciata sul mercato – e richiede un processo molto sofisticato e attento di monitoraggio degli utilizzi per costruire una legislazione ex post ogni qualvolta diventi manifesta la nascita di comportamenti non desiderabili.C'è quindi, in un certo senso, uno **spazio creativo molto ampio nell'inventare modalità perniciose di uso del digitale** – i suoi lati oscuri. Un fenomeno recente, interessante ma anche preoccupante è stato riportato dalla rivista Technology Review del prestigioso Mit di Boston. La scrittrice cinese nota con lo pseudonimo di Mitu si è improvvisamente vista negare l'accesso alle bozze del romanzo a cui stava lavorando e che erano archiviate sul suo spazio personale in un cloud pubblico.

Cercando di accedere al documento, l'accesso risultava bloccato e compariva un avviso che segnalava che **i contenuti erano inaccessibili in quanto erano "contenuti sensibili"**. Il fatto, di rilevante gravità, ha aperto un dibattito sul tipo di controllo che le aziende tecnologiche possono operare per conto di un governo.

La scrittrice stava lavorando con Wps, una versione nazionale di un software di videoscrittura basato sul cloud, come Google Docs o Microsoft Office 365. Il 25 giugno, nel forum di letteratura cinese Lkong, la scrittrice ha accusato Wps di "spiare e bloccare le mie bozze", indicando la presunta presenza di contenuti illegali. La notizia è letteralmente esplosa sui social media l'11 luglio, dopo la ripresa da parte degli account di alcuni importanti influencer. Quel giorno la notizia è diventata il top trending topic su Weibo; **molti utenti hanno incominciato a chiedersi se Wps stesse violando la loro privacy**. A questo punto la rivista cinese The Economic Observer ha riferito che era già capitato diverse volte che altri scrittori avessero viste bloccate online le loro bozze senza una spiegazione chiara del perché. L'azienda ha rilasciato due dichiarazioni dopo il reclamo iniziale, chiarendo che il software non censura i file memorizzati localmente, ma rimanendo vaga su ciò che accade ai file condivisi online.Che lezioni possiamo trarre da questo evento? Sicuramente è l'inizio di un percorso dove i governi nazionali – con varie sfaccettature – saranno sempre più attenti (anche per contrastare la criminalità organizzata, il terrorismo e lo spionaggio di Paesi stranieri) a **monitorare la produzione e lo scambio di informazioni** da parte di figure o organizzazioni considerate "sensibili" (e già sul significato operativo di questa parola ci sarebbe moltissimo da dire). Oltretutto l'evidente deriva globale verso la riduzione dei princìpi democratici e l'aumento dei sovranismi nazionali non è certo di buon auspicio. Sarà quindi molto difficile aumentare le difese della privacy dei cittadini.

Ma abbiamo diverse leve a disposizione per **auto-tutelarci** che dipendono dalla nostra digilità – abilità e agilità nell'usare il digitale. Innanzitutto, la consapevolezza che queste cose possono accadere, e saranno sempre più frequenti in quei servizi in cu l'utente non paga nulla, mettendosi quindi nelle mani del fornitore di servizi. È noto, infatti, che quasi nessuno legge le clausole di questi contratti a titolo gratuito. Come ci ricorda il pay-off del docufilm The Social Dilemma: "If you're not paying for the product, then you're the product". Comprando un servizio – e ancora di più se lo usiamo a titolo gratuito – **ricordiamoci che non siamo i proprietari delle infrastrutture digitali che utilizziamo**: dobbiamo sempre domandarci cui prodest – quali sono i benefici di queste aziende – e soprattutto dobbiamo avere sempre a portata di mano valide alternative.

In secondo luogo, **le infrastrutture si possono "rompere"** – sia per super-uso che per obsolescenza tecnologica (rendendole incompatibili con le nuove versioni). È quindi necessario pianificare l'utilizzo di servizi di upgrade o di conversione ai nuovi standard free di interscambio. Infine, le infrastrutture digitali sono violabili dall'esterno con furti, danneggiamenti, manipolazione delle informazioni. Dobbiamo quindi sempre affiancare ai servizi standard di sicurezza e back-up le nostre procedure di sicurezza.

Io, ad esempio, ho caricato il mio zaino digitale in un cloud pubblico di cui ho preliminarmente studiato le **procedure di sicurezza e di back-up** adottate. Oltre a ciò, ho diverse copie continuamente aggiornate dei miei archivi: innanzitutto sul Pc da cui gestisco il cloud; poi – con cadenze mensili – su un hard disk rimovibile e anche su un pen drive che mi porto sempre dietro. Ogni semestre, infine, copio i contenuti anche su un Cd read-only, cioè non riscrivibile (e quindi non modificabile da virus esterni). Dulcis in fundo, per i documenti più importanti su cui sto lavorando – ho spesso **copie cartacee**. Fidarsi è bene, non fidarsi è meglio.