

L'ombra digitale della pandemia

La pandemia sta alimentando la repressione digitale in tutto il mondo

di Adrian Shahbaz e Allie Funk

Tratto dal rapporto *FREEDOM ON THE NET 2020* pubblicato da Freedom House

Traduzione di Matteo Negrini

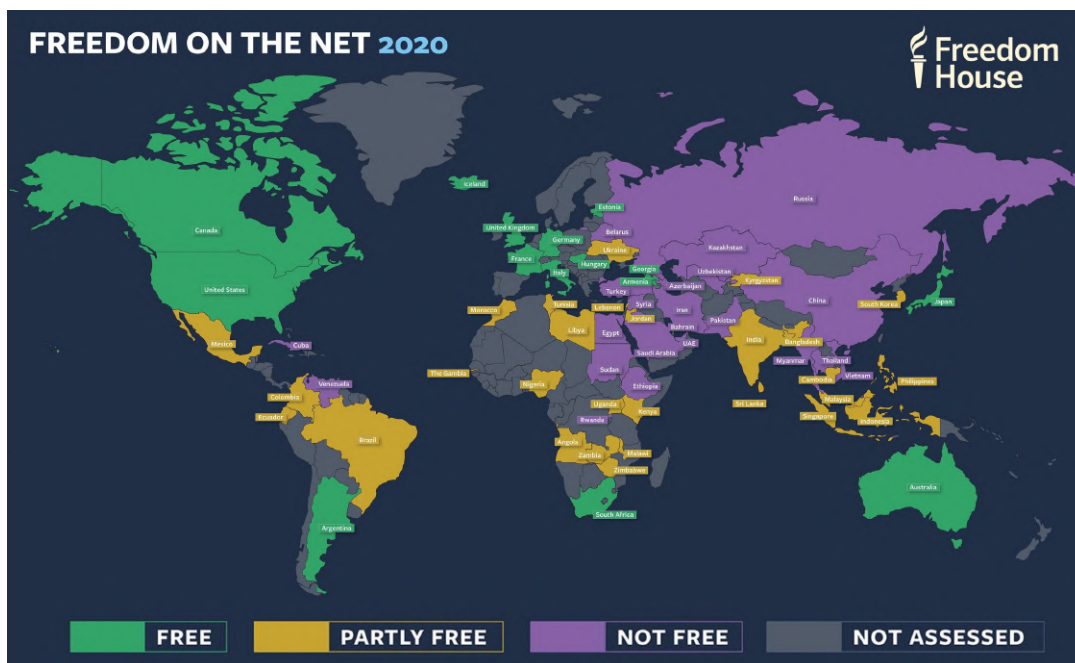
A livello globale, la pandemia da coronavirus sta drammaticamente accelerando il degrado della libertà di internet.

Per il decimo anno consecutivo, gli utenti hanno subito una generale contrazione dei loro diritti e il fenomeno è parte di una più ampia crisi della democrazia in tutto il mondo.

Nell'era Covid-19, la connettività non è un lusso, ma una necessità.

Praticamente tutte le attività umane - commercio, istruzione, sanità, politica, socializzazione - sembrano essersi spostate *online*. Eppure, il mondo digitale presenta chiare sfide, sia per i diritti umani, sia sulla *governance* democratica.

In molti Paesi, vi sono soggetti - statali e non - che stanno sfruttando le opportunità create dalla pandemia per creare narrazioni *online*, censurare le critiche e costruire nuovi sistemi tecnologici di controllo sociale.



Tre importanti tendenze hanno segnato un anno particolarmente triste per la libertà di internet.

In primo luogo, i leader politici hanno utilizzato la pandemia come pretesto per limitare l'accesso alle informazioni.

Spesso, le autorità hanno bloccato siti indipendenti di notizie e arrestato individui con pretestuose accuse di diffusione di *fake news*.



In realtà, in molte parti del mondo, sono stati proprio i funzionari statali e i loro zelanti fiancheggiatori a diffondere notizie false e fuorvianti per cercare di coprire quelle vere e documentate, con l'obiettivo di distrarre il pubblico da azioni politiche inefficaci e per indicare come capri espiatori determinate comunità etniche o religiose.

Taluni Stati tolgono la connettività a gruppi emarginati, rendendo, così, ancora più profonde le divisioni digitali già esistenti.

In breve, i governi di tutto il mondo hanno fallito nel promuovere una sfera pubblica *online* che fosse, al contempo, vivace e affidabile.

In seconda battuta, le autorità hanno usato il Covid-19 per giustificare l'ampliamento dei loro poteri di sorveglianza e l'utilizzo di tecnologie che prima venivano considerate troppo invadenti.

La crisi sanitaria ha creato una breccia per digitalizzare, raccogliere e analizzare i dati più intimi delle persone senza adeguate regole e/o protezioni contro gli abusi.

Governi ed enti privati stanno aumentando l'uso dell'intelligenza artificiale (AI), della sorveglianza biometrica e dei cosiddetti "*big data*"¹ per prendere decisioni che vanno ad impattare sui diritti economici, sociali e politici degli individui.

In linea di massima, i processi di cui parliamo sono spesso privi di trasparenza, senza controlli esterni né meccanismi correttivi.

Queste pratiche aumentano la prospettiva di un futuro distopico in cui aziende private, agenzie di sicurezza e criminali informatici accedono facilmente non solo alle informazioni sensibili sui luoghi che visitiamo o sugli articoli che acquistiamo, ma anche alle cartelle mediche, ai modelli facciali e vocali e, perfino, ai codici genetici.

La terza tendenza è la trasformazione di quella che - fino a poco tempo fa - era la "frammentazione al rallentatore" di internet in una corsa verso la "sovranità informatica", con i governi che impongono le proprie leggi per cercare di limitare il flusso dei dati attraverso i confini nazionali.

Tendenza, questa, in aperto contrasto con ciò che era accaduto fin dalla creazione di internet, quando le imprese, la società civile e i governi si erano fatte parti attive di un comune processo, basato sul consenso, teso ad armonizzare in tutto il mondo i protocolli tecnici, gli standard di sicurezza e le normative commerciali.

Era stato questo tipo di approccio a permettere di collegare miliardi di persone ad una rete globale di informazioni e servizi, con benefici incommensurabili per lo sviluppo umano, ivi compresa la possibilità di avere un forte strumento di pressione sui potentati globali.

Il fascino della sovranità informatica

Invece di proteggere gli utenti, l'applicazione della sovranità nazionale al cyberspazio ha consentito alle autorità di reprimere i diritti umani, ignorando le obiezioni delle società civili locali e della comunità internazionale.

Il regime cinese - un pioniere in questo campo e, per il sesto anno consecutivo, il primo violatore al mondo delle libertà di internet - ha bloccato a lungo popolari servizi stranieri e ha centralizzato l'infrastruttura tecnica per riuscire a monitorare pervasivamente e filtrare tutto il traffico in entrata nel Paese.

Seguendo questo stesso modello, le autorità russe hanno approvato una legislazione per isolare il Paese dall'internet globale durante le emergenze nazionali; parimenti, il governo iraniano ha interrotto le connessioni per nascondere la violenta repressione delle proteste di massa di fine 2019 da parte della polizia.

I recenti avvenimenti di Hong Kong illustrano, con spaventosa evidenza, cosa implichi un maggiore controllo dello Stato sullo spazio civico *online*.

La *leadership* di Pechino ha imposto direttamente alla regione autonoma una legge draconiana di Sicurezza Nazionale che prescrive dure punizioni per i reati di parola in senso lato, compresa qualsiasi espressione di solidarietà per coloro che manifestano a favore della democrazia.

Per sfuggire a tali sanzioni, sono stati chiusi o cancellati in via preventiva siti web di politica, *forum online*, *account* personali sui *social network* e intere *app*.

Le società tecnologiche statunitensi hanno annunciato che avrebbero sospeso gli ac-



cordi di condivisione dei dati con le forze dell'ordine locali per non essere complici nella violazione di diritti umani.

Di rimando, le autorità cinesi, hanno minacciato di inasprire le pene in caso di inadempienza, imponendo alle aziende il dilemma tra l'archiviare i dati degli utenti nell'ambito della giurisdizione cinese oppure subire il blocco delle attività e pesanti sanzioni, fino all'arresto dei rappresentanti dell'azienda.

Allarma il fatto che pratiche di questo tipo non siano limitate soltanto ai regimi più repressivi del mondo.

Paesi di tutto lo spettro democratico stanno, infatti, erigendo i propri confini digitali nel segno di una ormai logorata fiducia nell'internet aperta.

Gli Stati Uniti e l'India hanno vietato molte popolari *app* cinesi, adducendo preoccupazioni per la sicurezza nazionale.

In Brasile, Nigeria e Turchia sono state approvate o sono in discussione norme che impongono alle aziende di non far uscire dal Paese i dati degli utenti, facilitando, in questo modo, l'accesso ad informazioni sensibili da parte delle forze dell'ordine.

La più alta corte di giustizia dell'Unione Europea ha stabilito che i programmi di sicurezza nazionale degli Stati Uniti violano i diritti alla privacy degli europei, invalidando, così, uno dei più grandi accordi di condivisione di dati al mondo. ²

Anche quando mirano a frenare pratiche repressive, queste azioni legittimano la tendenza di ogni Stato a controllare la propria "internet nazionale", cosa che, in precedenza, era sostenuta solo dai governi autocratici di Paesi come la Cina, l'Iran o la Russia.



PIÙ DI 3,8 MILIARDI DI PERSONE NEL MONDO HANNO ACCESSO AD INTERNET

Di questi, secondo le stime di Freedom House, il

73% vive in Paesi in cui persone sono state fermate o incarcerate per aver pubblicato *online* contenuti politici, sociali o religiosi

64% vive in Paesi in cui, a partire da giugno 2019, persone sono state attaccate o uccise per le loro attività *online*

61% vive in Paesi in cui le autorità hanno utilizzato commentatori filogovernativi per manipolare le discussioni *online*

56% vive in Paesi in cui contenuti *online* di carattere politico, sociale o religioso sono stati bloccati

47% vive in Paesi in cui le autorità hanno disconnesso internet o le reti mobili, spesso per motivi politici

34% vive in Paesi in cui l'accesso ai social media è stato temporaneamente o permanentemente limitato

Un ruolo più forte per la società civile globale

Il modo migliore per evitare l'ascesa della cybersovranità nazionale è ripristinare la fiducia nella legittimità e nell'efficacia del modello *multistakeholder* ³ attualmente in essere. Ciò significa immaginare per internet e le sue piattaforme nuovi sistemi di *governance* che sostengano i principi democratici di rappresentanza e partecipazione popolare.



Gli attuali meccanismi di autoregolamentazione incontrano delle difficoltà quando l'interesse pubblico contrasta con gli interessi privati dell'industria tecnologica. Mentre la vastità della discussione internazionale - e delle stesse piattaforme *leader* - rende difficile considerare ed integrare il contributo dei singoli individui, le organizzazioni della società civile globale possono fornire l'esperienza e quella supervisione indipendente necessarie per contrastare alcuni problemi che riguardano l'impatto della tecnologia sui diritti umani.

Le future iniziative sulla *governance* delle piattaforme e sulla moderazione dei contenuti dovrebbero andare ben oltre la semplice trasparenza.

Dovranno garantire che i deficit di sistema sui diritti umani segnalati da varie fonti indipendenti siano affrontati e risolti con pratiche nuove e con l'applicazione, in tutta l'industria di internet e delle telecomunicazioni, di politiche rispettose di tali diritti.

Come ha dimostrato il Covid-19, affrontare le sfide di un mondo interconnesso richiede un coordinamento efficace tra i responsabili politici e la società civile di tutti i Paesi.

Per le questioni relative alla concorrenza, alla tassazione e ai flussi di dati che passano da uno Stato all'altro, ad esempio, è probabile che - a causa della natura globale di internet - il coordinamento intergovernativo si riveli più efficace della regolamentazione statale *ad hoc*.

Le nuove istituzioni costruite per l'era digitale sono in grado di gestire i problemi transnazionali che non ricadono perfettamente sotto la giurisdizione di un governo o dell'altro, garantendo, al contempo, che gli utenti dei Paesi più piccoli, o meno potenti, ricevano la stessa protezione e cura di coloro che vivono nelle grandi democrazie.

Questo approccio internazionale e multilaterale non fermerà gli sforzi del governo cinese e di quello russo per rendersi più forti e imporre la loro volontà rispetto alla rete globale, ma potrebbe limitare le miopi iniziative normative di democrazie consolidate (e/o aspiranti tali), prevenendo un'ulteriore frammentazione di internet.

Una risorsa insostituibile per la democrazia

Un'internet aperta, gratuita e globale ha un valore enorme.

Persino in contesti che, altrimenti, sarebbero altamente oppressivi, uno spazio *online* senza restrizioni offre incommensurabili possibilità per la libera espressione, il coinvolgimento della comunità e lo sviluppo economico.

Quando il coordinamento civico e il dissenso politico trascinano dall'ambito dei *social media* per riversarsi nelle strade di città come Minsk, Khartoum o Caracas, i dittatori chiudono le reti per soffocare qualsiasi richiesta di maggiore democrazia e di diritti umani.

Vi sono soggetti - statali e non - che contrastano il dissenso politico diffondendo paura e disinformazione sulle piattaforme *online*, ricorrendo talvolta anche ad arresti ed intimidazioni fisiche.

Da Hong Kong a Minneapolis, i manifestanti - dotati solo di telecamere e del coraggio delle loro convinzioni - rischiano di essere puniti dalle forze di sicurezza tecnologicamente più avanzate del mondo.

Se le piattaforme di comunicazione digitale vogliono propugnare la causa dei diritti umani nel XXI secolo, il movimento per la libertà di internet deve far crescere le sue ambizioni dalla semplice richiesta di politiche rispettose dei diritti fondamentali alla effettiva costruzione di solide strutture di *governance* che sanciscano e applichino tali protezioni.

Respingere l'autoritarismo digitale e la sovranità informatica repressiva, invertendo l'attuale trasformazione antidemocratica di internet, è un passo fondamentale per prevenire risultati ancora peggiori che potrebbero derivare dalle tecnologie digitali di domani.

Note del traduttore



raccogliere grandi quantità di dati (provenienti da diversi tipi di dispositivi) che consentono di identificare modelli comportamentali degli individui, nella loro veste - di volta in volta - di cittadini, utenti, consumatori, etc...

- 2 Il 16 luglio 2020, la Corte di Giustizia dell'Unione Europea ha invalidato la decisione n. 2016/1250 della Commissione Europea sull'adeguatezza della protezione offerta dal regime del cosiddetto "Scudo UE-USA" per la privacy.
- 3 *Multistakeholder* - Che mira al coinvolgimento di più soggetti interessati ad un'attività. (Dizionario Treccani)

Freedom House è un'organizzazione non governativa internazionale che svolge attività di ricerca e sensibilizzazione sulla democrazia, le libertà politiche e i diritti umani.

Costituita nel 1941, si caratterizzò fin da subito per la sua indipendenza ed imparzialità: basti pensare che tra i fondatori vi furono anche Eleanor Roosevelt (moglie dell'allora Presidente degli Stati Uniti) e Wendell Lewis Willkie (il candidato del Partito Repubblicano che, alle precedenti elezioni presidenziali, era stato sconfitto da Franklin Delano Roosevelt).

Freedom House pubblica ogni anno gli autorevoli rapporti:

- *Freedom in the world* sul grado di libertà civili e diritti politici garantiti in ciascun Paese del mondo;
- *Freedom of the Press* sulla libertà di stampa;
- *Freedom on the Net* sulla libertà di internet.