Freedom House

LIBERTA' SU LA RETE 2022

Contrastare una revisione autoritaria di Internet

LIBERTA' SU LA RETE 2022

SOMMARIO

TABELLE, GRAFICI E GRAFICI

Questo rapporto è stato reso possibile grazie al generoso sostegno di Amazon, del Ministero degli Affari Esteri olandese, di Google, della Hurford Foundation, di Internet Society, di Lilly Endowment Inc., del New York Community Trust e del Bureau of Democracy, Human Rights del Dipartimento di Stato degli Stati Uniti. e Lavoro (DRL). Freedom House si impegna per l'indipendenza editoriale. I nostri donatori non influenzano le priorità di ricerca dell'organizzazione, i risultati dei rapporti o le raccomandazioni politiche.

Le seguenti persone hanno contribuito alla ricerca e alla stesura di questo rapporto: Grant Baker, Philip Friedrich, Cathryn Grothe, Maddie Masinsin, Manisha Vepa e Tessa Weal. Elisha Aaron, David Meijer, Shannon O'Toole, Tyler Roylance e Lora Uhlig hanno modificato il rapporto.

Questo opuscolo è un riepilogo dei risultati dell'edizione 2022 di *Freedom on the Net.* Rapporti narrativi sui 70 paesi valutati in questo studio sono disponibili sul nostro sito web all'indirizzo freedomonthenet.org.

SULLA COPERTINA

Illustrazione di Mitch Blunt

Risultati principali

1

La libertà globale di Internet è diminuita per il 12 anno consecutivo. I declassamenti più marcati sono stati documentati in Russia, Myanmar, Sudan e Libia. In seguito all'invasione illegale e non provocata dell'Ucraina da parte dell'esercito russo, il Cremlino ha intensificato drasticamente i suoi sforzi in corso per sopprimere il dissenso interno e ha accelerato la chiusura o l'esilio dei restanti media indipendenti del paese. In almeno 53 paesi, gli utenti hanno subito ripercussioni legali per essersi espressi online, spesso portando a pene detentive draconiane.

2

I governi stanno distruggendo l'Internet globale per creare spazi online più controllabili. Un numero record di governi nazionali ha bloccato siti web con contenuti politici, sociali o religiosi non violenti, minando i diritti alla libertà di espressione e all'accesso alle informazioni. La maggior parte di questi blocchi ha preso di mira fonti situate al di fuori del paese. Le nuove leggi nazionali hanno posto un'ulteriore minaccia al libero flusso di informazioni centralizzando l'infrastruttura tecnica e applicando regolamenti imperfetti alle piattaforme dei social media e ai dati degli utenti.

3

La Cina era il peggior ambiente al mondo per Internet libertà per l'ottavo anno consecutivo. La censura si è intensificata durante le Olimpiadi di Pechino del 2022 e dopo che la star del tennis Peng Shuai ha accusato di violenza sessuale un alto funzionario del Partito Comunista Cinese (PCC). Il governo ha continuato a rafforzare il proprio controllo sul fiorente settore tecnologico del paese, anche attraverso nuove regole che richiedono alle piattaforme di utilizzare i propri sistemi algoritmici per promuovere l'ideologia del PCC.

4

Un record di 26 paesi ha sperimentato miglioramenti della libertà di Internet. Nonostante il generale declino globale, le organizzazioni della società civile in molti paesi hanno guidato gli sforzi di collaborazione per migliorare la legislazione, sviluppare la resilienza dei media e garantire la responsabilità tra le aziende tecnologiche. Le azioni collettive riuscite contro le interruzioni di Internet hanno offerto un modello per ulteriori progressi su altri problemi come lo spyware commerciale.

5

La libertà di Internet negli Stati Uniti è migliorata marginalmente per la prima volta in sei anni. Ci sono stati meno casi segnalati di sorveglianza mirata e molestie online durante le proteste rispetto all'anno precedente, e il paese è ora al nono posto a livello globale, insieme ad Australia e Francia. Gli Stati Uniti mancano ancora a completa legge federale sulla privacy e i responsabili politici hanno fatto pochi progressi nell'approvazione di altre leggi relative alla libertà di Internet. In vista del midterm di novembre 2022 elezioni, l'ambiente online era pieno di disinformazione politica, teorie del complotto e molestie online rivolte a funzionari e funzionari elettorali.

6

I diritti umani sono in bilico in una competizione per il controllo del web. Gli stati autoritari stanno gareggiando per diffondere il loro modello di controllo digitale in tutto il mondo. In risposta, una coalizione di governi democratici ha aumentato la promozione dei diritti umani online nei forum multilaterali, delineando una visione positiva per Internet. Tuttavia, i loro progressi rimangono ostacolati dalle problematiche pratiche di libertà di Internet nei loro paesi.

introduzione

Di Adrian Shahbaz, Allie Funk e Kian Vesteinsson

In patria e sulla scena internazionale, autoritari sono impegnati in una campagna per dividere l'internet aperto in un mosaico di enclavi repressive. Più governi che mai stanno esercitando il controllo su ciò a cui le persone possono accedere e condividere online bloccando i siti Web stranieri, accumulando dati personali e centralizzando l'infrastruttura tecnica dei loro paesi. Come risultato di queste tendenze, la libertà globale di Internet è diminuita per il 12° anno consecutivo.

L'aumento della repressione digitale in molti paesi ha rispecchiato le più ampie repressioni sui diritti umani nell'ultimo anno. Da nessuna parte questo è stato più chiaro che in Russia, Myanmar, Libia e Sudan, che hanno sperimentato il calo più drastico al mondo della libertà di Internet. La censura online ha raggiunto il massimo storico, con un numero record di governi che hanno bloccato contenuti politici, sociali o religiosi, spesso prendendo di mira fonti di informazioni situate al di fuori dei propri confini. Più di due terzi del mondo gli utenti di Internet ora vivono in paesi in cui le autorità puniscono le persone per aver esercitato il loro diritto alla libertà di espressione online.

In modo allarmante, questi abusi antidemocratici non sono l'unico fattore alla base della frammentazione di Internet in segmenti nazionali. Alcuni governi stanno chiaramente coltivando uno spazio digitale domestico in cui le narrazioni approvate dallo stato dominano e i media indipendenti, la società civile e le voci già emarginate vengono soppresse più facilmente. Ma altri stanno inavvertitamente contribuendo a creare barriere nazionali attraverso i loro sforzi per contrastare la disinformazione, proteggere i dati degli utenti e scoraggiare i veri crimini informatici. Qualunque sia l'intenzione, tuttavia, la crescente frammentazione di Internet comporta gravi conseguenze per i diritti fondamentali inclusi libertà di espressione, accesso alle informazioni e privacy, in particolare per le persone che vivono sotto regimi autoritari o in democrazie in declino.

> Leader autoritari radicati e aspiranti hanno cercato di contenere il dissenso online impedendo ai residenti di raggiungere fonti di informazioni globali.

Internet più frammentato

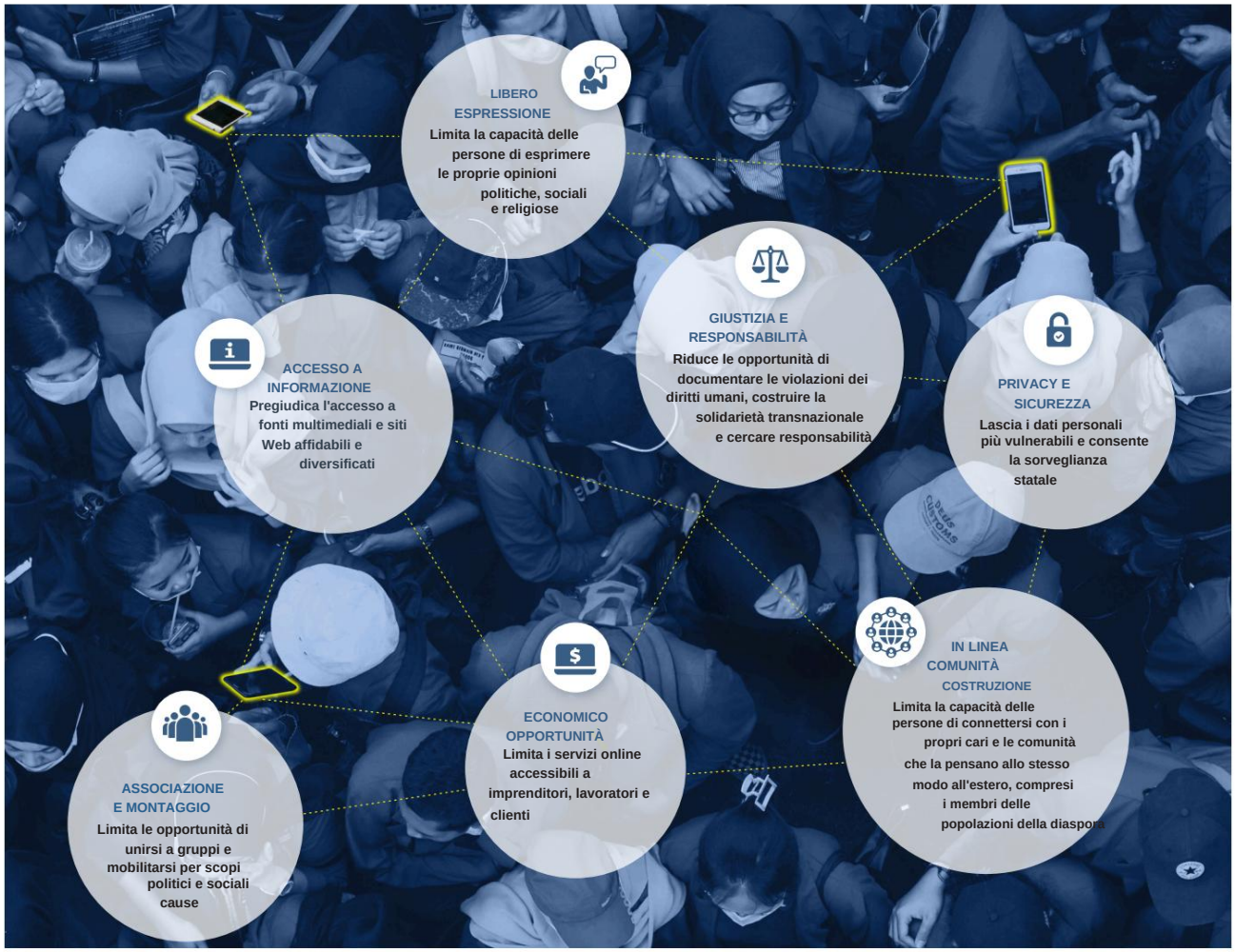
Internet è sempre stato soggetto a un certo grado di frattura lungo i confini nazionali, ma l'aumento dell'intervento statale nell'ultimo anno ha notevolmente accelerato il processo. Questo rapporto identifica tre principali cause di frammentazione, che hanno tutte contribuito al declino del rispetto dei diritti umani online: restrizioni al flusso di notizie e informazioni, controllo statale centralizzato sull'infrastruttura Internet e barriere ai trasferimenti transfrontalieri dei dati dell'utente.

Mentre la rete fisica di Internet globale rimane intatta, un numero crescente di utenti ha accesso solo a uno spazio online che rispecchia le opinioni del proprio governo e i suoi interessi. Le autorità di 47 dei 70 paesi coperti da *Freedom on the Net* hanno limitato l'accesso degli utenti alle informazioni fonti situate al di fuori dei loro confini. Praticamente tutte queste restrizioni costituiscono chiare violazioni della Dichiarazione universale dei diritti dell'uomo, che codifica il diritto "di cercare, ricevere e diffondere informazioni e idee attraverso qualsiasi mezzo e indipendentemente dalle frontiere". Nella maggior parte dei casi, leader autoritari radicati e aspiranti hanno cercato di contenere il dissenso online impedendo ai residenti di raggiungere fonti di informazioni con sede in paesi con un maggiore livello di libertà dei media.

Questa crescente frammentazione fa parte di una competizione globale e sfaccettata per il controllo della sfera digitale. Per la maggior parte del periodo dall'inizio di Internet, i rappresentanti del settore privato, della società civile e della comunità tecnica hanno partecipato a un processo guidato dal consenso per armonizzare gli standard di sicurezza ei protocolli tecnici. Ciò ha portato a un'infrastruttura decentralizzata che parla una lingua comune, consentendo agli utenti di comunicare tra loro e accedere alle informazioni indipendentemente dalla loro posizione. Poteri autoritari

FENCED IN: COME LA FRAMMENTAZIONE DI INTERNET DANNEGGIA I DIRITTI UMANI

Internet è più isolato che mai, impedendo a miliardi di persone di esercitare i propri diritti umani online.



hanno cercato a lungo di sostituire questo modello multistakeholder di governance di Internet con uno che promuova la sovranità informatica o un maggiore controllo da parte degli stati. Diplomatici provenienti da Cina e Russia hanno fatto breccia in istituzioni come l'Internazionale Telecommunication Union (ITU), cercando di trasformare l'agenzia delle Nazioni Unite in un regolatore globale di Internet che promuove interessi autoritari. Ciò altererebbe radicalmente l'Internet aperto, impedendo a miliardi di persone di comunicare tra loro e di accedere a risorse che cambiano la vita senza l'autorizzazione esplicita dei loro governi.

Una coorte di democrazie sta respingendo. Dopo essersi concentrati in precedenza su una serie più ristretta di interessi economici e di sicurezza legati al contrasto a Pechino, gli Stati Uniti hanno mostrato più recentemente segnali promettenti di un nuovo impegno nel cyber

rapporto

diplomazia con l'obiettivo di promuovere una visione positiva della democrazia nell'era digitale. Anche l'Unione europea (UE) ha adottato approcci normativi innovativi e rispettosi dei diritti per affrontare i danni aggravati da Internet. Ma molte democrazie devono ancora migliorare in modo significativo il rispetto dei diritti online all'interno dei propri confini. Dei 35 paesi coperti da questo rapporto che hanno partecipato al Summit per la democrazia ospitato dagli Stati Uniti, 13 hanno sperimentato un declino della libertà di Internet nell'ultimo anno, così come 10 dei 18 paesi *Freedom on the Net* che hanno firmato la Dichiarazione guidata dagli Stati Uniti per il Futuro di Internet. Adottando politiche imperfette in patria, le democrazie rischiano di minare gli stessi valori che cercano di difendere all'estero, escludendo potenzialmente i residenti di paesi autoritari da un Internet più libero e aperto.

Proteggere i diritti umani online attraverso la resilienza democratica

Le tecnologie associate a Internet globale hanno favorito connessioni e interessi comuni tra persone e comunità diverse, facilitato una governance più trasparente e partecipativa e portato enormi benefici economici diretti e indiretti. Tuttavia, la rapida digitalizzazione dei media e della comunicazione ha anche generato nuove opportunità di manipolazione, estremismo e repressione. I responsabili politici sono stati troppo lenti nell'affrontare i pericoli che accompagnano il cambiamento tecnologico e la loro enfasi sulle minacce digitali a livello statale - raggruppate in termini come guerra dell'informazione, guerra informatica e guerra commerciale - ha spesso elevato la sicurezza nazionale e le considerazioni economiche rispetto ai diritti fondamentali degli individui. La realtà è che gli interessi economici e di sicurezza sono direttamente legati al rispetto dei diritti individuali.

È improbabile che attraverso la frammentazione di Internet si ottengano soluzioni durature alla disinformazione, alle molestie online e ad altri danni presentati dagli strumenti digitali. La semplice imposizione di rigide leggi nazionali su un sistema di informazione globale è destinata a essere inefficace. Gli sforzi di Pechino per costruire e mantenere un Great Firewall, ad esempio, hanno fatto ben poco per affrontare le preoccupazioni della società in materia di privacy, sicurezza informatica, illeciti aziendali, contenuti falsi e comportamento online offensivo. Potrebbe essere difficile impedire a Pechino, Mosca e Teheran di farlo persistendo nei loro sforzi per isolare le loro popolazioni, ma rimane un'opportunità per convincere molti stati meno repressivi che un Internet aperto è nel loro migliore interesse.

Occorre prestare maggiore attenzione allo sviluppo della resilienza politica e sociale di fronte a questi danni. Giornalisti, difensori dei diritti umani e organizzazioni di difesa sono già stati in prima linea in molti recenti successi che hanno rafforzato la resilienza democratica nella sfera digitale. Ampie coalizioni hanno rafforzato le norme internazionali contro le chiusure di Internet, che si sono verificate in un minor numero di paesi nell'ultimo anno. Indagini collaborative sui fornitori di software di sorveglianza hanno portato a una crescente consapevolezza di un'industria sottoregolamentata che continua a prendere di mira funzionari statali, giornalisti, attivisti e membri delle comunità della diaspora. Gli informatori hanno reso al pubblico un grande servizio esponendo le inadeguatezze e i fallimenti di influenti aziende tecnologiche.

I leader democratici dovrebbero impegnarsi nuovamente a preservare i vantaggi di un Internet libero e aperto. La vera resilienza richiede nuove normative che sanciscano la protezione dei diritti umani nell'era digitale, un coordinamento multilaterale più forte sulla criminalità informatica e la responsabilità aziendale e investimenti più profondi nella società civile, che così spesso guidano l'azione collettiva per difendere la libertà di Internet e resistere all'autoritarismo digitale.

Monitoraggio del declino globale

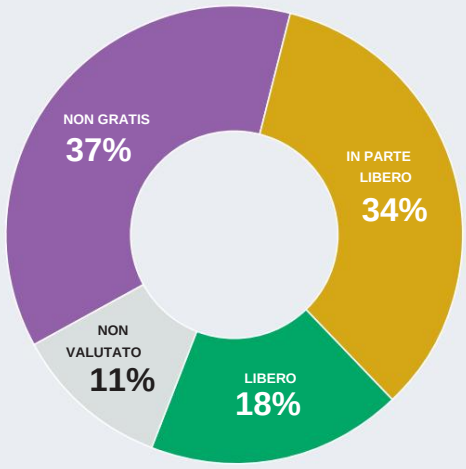
Una carrellata di modifiche importanti ai punteggi della libertà di Internet dei paesi

La libertà globale di Internet è diminuita per il 12 anno consecutivo. L'ambiente per i diritti umani online è peggiorato in 28 paesi, sebbene 26 paesi abbiano registrato guadagni netti, il maggior numero di miglioramenti dall'inizio del progetto. Il calo più marcato si è verificato in Russia, seguita da Myanmar, Sudan e Libia, mentre Gambia e Zimbabwe hanno registrato miglioramenti importanti. Gli Stati Uniti si sono classificati al nono posto assoluto e l'Islanda è stata ancora una volta la migliore. Per l'ottavo anno consecutivo, la Cina è risultata avere le peggiori condizioni per la libertà di Internet.

Freedom on the Net è uno studio annuale sui diritti umani nella sfera digitale. Il progetto valuta la libertà di Internet in 70 paesi, che rappresentano l'89% degli utenti Internet del mondo. Questo rapporto, il 12° della sua serie, ha coperto gli sviluppi tra giugno 2021 e maggio 2022.

POPOLAZIONE INTERNET GLOBALE ENTRO IL 2022 STATO FOTN

Freedom on the Net valuta l'89% della popolazione mondiale di utenti di Internet.



Oltre 80 analisti e consulenti hanno contribuito all'edizione di quest'anno, utilizzando una metodologia standard per determinare il punteggio di libertà di Internet di ciascun paese su una scala di 100 punti, con 21 indicatori separati relativi a ostacoli all'accesso, limiti sui contenuti e violazioni dei diritti degli utenti. Il sito web di *Freedom on the Net* presenta rapporti approfonditi e dati sulle condizioni di ogni paese.

L'invasione dell'Ucraina da parte del Cremlino mette a rischio la libertà di Internet

La libertà di Internet in Russia è diminuita di sette punti nel periodo che circonda la brutale invasione dell'Ucraina da parte del governo nel febbraio 2022, raggiungendo il minimo storico e rappresentando il più grande declino nazionale di quest'anno nella *libertà in rete* . A poche settimane dall'invasione, il Cremlino ha bloccato Facebook, Instagram e Twitter, privando i russi dell'accesso a informazioni affidabili sulla guerra e limitando la loro capacità di connettersi con utenti di altri paesi.

Il governo ha anche bloccato più di 5.000 siti web, ha costretto i media a riferirsi all'invasione come a una "operazione militare speciale" e ha introdotto una legge che prescrive fino a 15 anni di carcere per coloro che diffondono "false informazioni" sul conflitto. Le crescenti restrizioni del regime, sia prima che dopo il lancio dell'invasione, hanno notevolmente aumentato i rischi associati all'attivismo online e accelerato la chiusura o l'esilio del paese che rimane indipendente stazioni mediatiche.

Le azioni dell'esercito russo in Ucraina hanno anche minato la libertà di Internet di quel paese. Nella città meridionale di Kherson, le truppe russe hanno costretto i fornitori di servizi a reindirizzare il traffico Internet attraverso le reti russe durante la primavera e l'estate del 2022, lasciando gli utenti ucraini senza accesso alle principali piattaforme di social media e a una pletora di siti di notizie ucraini e internazionali. Sebbene i media online abbiano coraggiosamente continuato a coprire l'invasione, i loro giornalisti hanno affrontato un grande pericolo mentre svolgevano il loro lavoro. Diversi giornalisti affiliati a tali siti web sono stati uccisi dalle forze russe.

La libertà di Internet in Russia ha raggiunto il minimo storico in seguito alla brutale invasione dell'Ucraina da parte del governo.

Il governo e il popolo ucraini hanno mostrato una sorprendente capacità di recupero durante l'invasione. Funzionari governativi e società di telecomunicazioni hanno lavorato insieme per riparare l'infrastruttura Internet e garantire l'accesso a risorse e informazioni online, che possono salvare vite nel bel mezzo di un conflitto armato. Circa 11.000 stazioni Starlink sono state implementate per fornire servizi Internet via satellite nell'ambito di una collaborazione che ha coinvolto il governo, la società tecnologica statunitense SpaceX e altri partner. Gli operatori di telecomunicazioni ucraini hanno inoltre consentito agli utenti di passare da un operatore all'altro quando il segnale del loro operatore principale non era disponibile e hanno intrapreso grandi sforzi per fornire l'accesso Wi-Fi ai rifugi antiaerei. Subito dopo che le forze russe hanno invaso il paese, la società ucraina Ajax Systems ha collaborato con il governo per lanciare un'applicazione mobile - scaricata più di quattro milioni di volte a marzo - che avvisa gli utenti dei raid aerei in arrivo.

I colpi di stato e le elezioni guidano importanti cali e miglioramenti La libertà di Internet è diminuita di cinque punti in Myanmar, contribuendo a un precipitoso calo di 19 punti negli ultimi due anni. Il paese ora ospita il secondo peggior ambiente per i diritti umani online, superando solo la Cina. Da quando la giunta militare ha preso il potere da un governo civile eletto nel febbraio 2021, ha cementato il suo regime di censura, bloccando tutti i siti Web tranne 1.200, limitando l'accesso alle principali piattaforme di social media e imponendo la chiusura di Internet a livello locale. Le poche risorse online rimaste accessibili durante l'anno sono stati dominati da voci promilitari e attivisti, giornalisti e utenti ordinari hanno continuato a essere fatti sparire con la forza, detenuti e torturati. La giunta ha costretto il fornitore di servizi norvegese Telenor a vendere le sue operazioni nel paese a una società allineata ai militari, consolidando completamente il suo controllo sul settore delle telecomunicazioni.

Gli agenti di polizia russi corrono verso un uomo con in mano un poster con la scritta "No War" durante una protesta non autorizzata in piazza Manezhnaya a Mosca, di fronte al Cremlino, il 13 marzo 2022. Centinaia di persone sono state arrestate durante la manifestazione. *(Foto di collaboratore/Getty Images)*

Un uomo tiene in mano un poster con il primo ministro ungherese Viktor Orban con un messaggio anti-sorveglianza durante una protesta a Budapest, Ungheria, il 26 luglio 2021. *(Foto di Marton Monus/ Reuters)*

Il punteggio del Sudan è sceso di quattro punti dopo che i leader militari hanno organizzato un colpo di stato e sciolto il governo di transizione del paese nell'ottobre 2021, segnando una battuta d'arresto devastante per la democrazia sudanese. I militari hanno annullato gli articoli della costituzione provvisoria che proteggeva i diritti fondamentali e hanno dichiarato uno stato di emergenza che è durato fino a maggio 2022. Mentre i civili sudanesi hanno mobilitato proteste di massa in risposta, le autorità hanno limitato la connettività Internet, bloccato piattaforme di social media e giornalisti aggrediti e arrestati.

La libertà di Internet in Nicaragua è diminuita di tre punti durante le elezioni del novembre 2021 che hanno visto a dura repressione dei leader dell'opposizione, dei dissidenti e dei giornalisti indipendenti. La legislazione repressiva come la legge sulla criminalità informatica ha spianato la strada a una maggiore autocensura e lunghe pene detentive nei confronti degli utenti critici.

In Ungheria, lo status della libertà di Internet è passato da libero a parzialmente libero, rispecchiando il più ampio declino democratico del paese sotto la guida del primo ministro Viktor Orbán. Durante le elezioni primarie dell'opposizione a settembre e ottobre 2021, in cui gli elettori hanno scelto candidati a sfidare Orbán e il suo partito al governo, gli attacchi informatici da fonti sconosciute hanno afflitto i sistemi di voto elettronico e le testate giornalistiche indipendenti nel paese.

Gli organizzatori delle elezioni sono stati costretti a sospendere il voto dopo che il loro sistema informatico ha subito un attacco e indipendente i siti di notizie sono stati messi offline prima dell'annuncio dei risultati elettorali. Mesi prima, a luglio, un'indagine ha rivelato che almeno tre giornalisti erano stati presi di mira con Pegasus, un famigerato strumento spyware sviluppato dalla società israeliana NSO Group.

In Gambia, la libertà di Internet è migliorata di tre punti, contribuendo a un miglioramento di 23 punti dalla fine del regime repressivo dell'ex presidente Yahya Jammeh nel 2017.
I gambiani si sono mobilitati online senza restrizioni durante le elezioni presidenziali del dicembre 2021, in cui erano in carica Adama Barrow si è assicurato un secondo mandato. Il Carretto L'amministrazione ha anche approvato una legge storica che garantisce il diritto all'informazione pubblica, un passo importante per la trasparenza e la responsabilità.

Nuove e persistenti minacce alla libertà di espressione in tutto il mondo *Freedom on the Net* ha rilevato che i funzionari di almeno 53 paesi hanno accusato, arrestato o imprigionato utenti di Internet come rappresaglia per post su cause politiche o sociali. In Libia, che quest'anno ha subito il terzo maggior calo del punteggio insieme al Sudan, gli utenti che hanno condiviso commenti o segnalazioni criminali online sono stati fatti sparire con la forza prima di riemergere in detenzione. Le autorità ruandesi hanno condannato un YouTube

commentatore i cui video hanno criticato il governo a 15 anni di carcere nel settembre 2021.

Le autorità di almeno 40 paesi hanno bloccato i contenuti sociali, politici o religiosi online, un record assoluto per *Freedom on the Net.* Gli utenti di Internet in Giordania hanno riferito che il sito web dell'International Consortium of Investigative Journalists è stato brevemente bloccato nell'ottobre 2021, dopo che l'organizzazione ha pubblicato documenti finanziari trapelati che hanno rivelato la ricchezza segreta del re del paese e di altri leader mondiali. In Bielorussia, le autorità hanno bloccato i siti web delle organizzazioni della società civile per tutto il periodo di copertura, parte di un attacco su vasta scala ai gruppi che includeva raid, arresti e chiusure forzate.

In almeno 22 paesi, i funzionari governativi hanno bloccato l'accesso ai social media o alle piattaforme di comunicazione. Alcuni blocchi sono stati imposti per costringere le società a conformarsi ai requisiti di aprire uffici nel paese, archiviare dati all'interno del paese o modificare in altro modo le proprie operazioni in modo da facilitare l'applicazione della censura governativa o delle richieste di dati. In Uzbekistan, le autorità hanno bloccato una serie di social media e app di messaggistica internazionali a luglio e novembre 2021 perché non rispettavano i requisiti di localizzazione previsti da una legge sulla protezione dei dati; l'accesso alla maggior parte delle piattaforme è stato ripristinato entro agosto 2022. Nel marzo 2022, un giudice della Corte suprema brasiliana ha annullato un'ordinanza che avrebbe vietato Telegram, dopo che l'app ha accettato di rimuovere i contenuti contrassegnati come disinformazione e ha annunciato che avrebbe nominato un rappresentante locale. I funzionari nigeriani hanno revocato un blocco di sette mesi su Twitter nel gennaio 2022, sostenendo che la società aveva accettato di stabilire una presenza fisica nel paese.

Il futuro della libertà di Internet negli "stati oscillanti"

Paesi come il Brasile e la Nigeria sono spesso indicati come stati oscillanti a causa della loro potenziale influenza regionale o globale sul futuro della governance di Internet. Hanno oscillato tra la protezione e l'indebolimento dei diritti umani online, con molti classificati parzialmente liberi da *Freedom on the Net.* I progressi in questi paesi potrebbero garantire la sopravvivenza di un Internet libero e aperto, oppure potrebbero unirsi a poteri autoritari nella promozione del modello più chiuso di sovranità informatica.

Le istituzioni democratiche in alcuni stati in bilico sono intervenute per proteggere i diritti umani online durante il periodo di copertura. La Corte Suprema indiana ha ordinato al governo di rivalutare la legge sulla sedizione dell'era coloniale del paese, che è stata sempre più utilizzata per accusare i dissidenti online, nel maggio 2022, anche se i leader politici cercavano di estendere il controllo sui contenuti online attraverso una nuova legislazione problematica. I legislatori brasiliani hanno sancito la protezione dei dati personali nella costituzione nel febbraio 2022, un'azione storica che ha elevato i diritti alla privacy al di sopra dei capricci di qualsiasi governo o semplice maggioranza legislativa. Ma la decisione è arrivata nel mezzo di un controverso anno elettorale, in cui il presidente Jair Bolsonaro e i suoi alleati hanno bombardato lo spazio online con false affermazioni sui brogli elettorali. Nell'ottobre 2021, la più alta corte del Kenya ha sospeso l'implementazione di un ampio sistema di carte d'identità biometriche fino a quando non potesse soddisfare standard adeguati per la protezione dei dati. Il presidente Guillermo Lasso dell'Ecuador ha posto il veto alle disposizioni di una legge che criminalizzava la divulgazione di segreti online nel giugno 2021, proteggendo i media digitali da una grave minaccia legale.

Altri paesi di questo gruppo hanno perseguito pratiche che hanno aumentato la repressione digitale e minato la diversità dello spazio dell'informazione. In Tunisia, il presidente Kaïs Saïed ha sospeso parti della costituzione, ha imposto regole eccessivamente ampie che vietano quelle che lo stato considera informazioni "false" e ha supervisionato l'arresto dei suoi critici online: una svolta allarmante per il paese con la più alta libertà di Internet del mondo arabo punto. Le autorità indonesiane hanno bloccato brevemente diversi siti Web dopo il periodo di copertura, inclusi Yahoo e PayPal, per forzare il rispetto di una legge repressiva che

I progressi negli "Stati oscillanti" come il Brasile e l'India potrebbero garantire la sopravvivenza di un Internet libero e aperto, oppure potrebbero unirsi a poteri autoritari nella promozione della sovranità informatica.

INTERNET GLOBALE

STATISTICHE UTENTE

Oltre **4,5 miliardi di** persone avere accesso a Internet.

Secondo le stime di Freedom House:

Il 76% vive in paesi dove le persone sono state arrestate o imprigionato per la pubblicazione di contenuti su questioni politiche, sociali o religiose.

Il 69% vive in paesi dove le autorità hanno schierato commentatori filogovernativi per manipolare le discussioni online.

Il 64% vive in paesi dove politico, sociale o i contenuti religiosi sono stati bloccati online.

Il 64% vive in paesi dove i diritti sono stati attaccati o uccisi per le loro attività online dal giugno 2021.

Il 51% vive in paesi dove accesso ai social media piattaforme è stata temporaneamente o permanentemente limitata.

Il 44% vive in paesi dove autorità hanno imposto Internet o reti mobili, spesso per motivi politici.

Per l'ottavo anno consecutivo, la Cina è rimasta il peggior ambiente al mondo per la libertà di Internet.

richiede alle aziende di registrarsi presso il governo, nominare un collegamento locale e rimuovere i contenuti in tempi più stretti.

L'ambiente online più repressivo del mondo

Per l'ottavo anno consecutivo, la Cina è rimasta il peggior ambiente al mondo per la libertà di Internet. Contenuto correlato

alle Olimpiadi di Pechino del 2022 e la pandemia di COVID-19 è rimasta pesantemente censurata durante il periodo di copertura, in particolare perché i residenti di Shanghai hanno condiviso le loro esperienze durante un disastroso blocco di due mesi iniziato nell'aprile 2022. Il governo ha anche intensificato la censura dei contenuti online relativi alle donne diritti umani e represse le campagne sui social media contro le aggressioni e le molestie sessuali, anche attraverso l'arresto della star del tennis Peng Shuai dopo che aveva affermato sulla piattaforma dei social media Weibo di essere stata aggredita sessualmente da un alto funzionario del PCC Zhang Gaoli.

Separatamente, giornalisti, attivisti per i diritti umani, membri di gruppi di minoranze religiose ed etniche e utenti ordinari sono stati arrestati per aver condiviso contenuti online, con alcuni che hanno subito dure pene detentive.

Funzionari governativi hanno istituito nuove politiche per rafforzare il loro controllo sulle società tecnologiche cinesi. Il principale regolatore di Internet ha emesso una guida che richiede alle piattaforme di allineare i propri sistemi di moderazione e raccomandazione dei contenuti con il "pensiero di Xi Jinping", l'ideologia ufficiale dell'attuale leader del PCC. Un'altra bozza di regole imporrebbe pesanti sanzioni alle aziende che consentono agli utenti Internet cinesi di aggirare il Great Firewall. Nel frattempo, il quadro sulla protezione dei dati del Paese, entrato in vigore nel novembre 2021, ha stabilito garanzie di base per i dati personali detenuti dalle società cinesi, sebbene non abbia applicato gli stessi standard ai dati detenuti o richiesti dal governo.

Per gli Stati Uniti, progressi all'estero e stallo in patria

L'amministrazione del presidente degli Stati Uniti Joseph Biden ha fatto della promozione della libertà di Internet una delle massime priorità del suo estero

La mancanza di una legge sulla privacy completa e le riforme incomplete delle regole di sorveglianza hanno consentito alle agenzie governative di acquistare semplicemente i dati degli americani da broker oscuri.

politica. Nell'aprile 2022, la Casa Bianca ha contribuito a riunire più di 60 governi per firmare la Dichiarazione per il futuro di Internet, un accordo non vincolante per promuovere una visione positiva di Internet. Il Dipartimento di Stato degli Stati Uniti ha istituito il suo Bureau of Cyberspace and Digital Policy, ha contribuito a lanciare la Export Controls and Human Rights Initiative e ha rivelato che avrebbe presieduto la Freedom Online Coalition in

2023. Allo stesso modo, l'Agenzia statunitense per lo sviluppo internazionale ha annunciato un investimento fino a 20 milioni di dollari all'anno per espandere notevolmente il suo lavoro sulla democrazia digitale.

Questa raffica di attività sulla scena globale era in netto contrasto con la mancanza di movimento a casa. Mentre internet

la libertà è migliorata per la prima volta in sei anni, il cambiamento è stato marginale e le leggi proposte che rafforzerebbero i diritti umani online e aumenterebbero la trasparenza relativa alla tecnologia hanno fatto pochi progressi. La continua mancanza di una legge federale completa sulla privacy e riforme incomplete della sorveglianza

le regole hanno consentito alle agenzie governative di acquistare semplicemente i dati degli americani da broker oscuri con poca supervisione o garanzie. La decisione della Corte Suprema che ha ribaltato *Roe v. Wade* e ha negato il diritto costituzionale all'aborto ha anche suscitato nuove preoccupazioni sull'accesso delle forze dell'ordine alle informazioni sulla posizione, alle cronologie di navigazione e ad altre forme di dati che potrebbero essere utilizzate per indagini penali e civili nelle giurisdizioni statunitensi dove l'accesso legale all'assistenza sanitaria riproduttiva è limitato.

Durante il periodo di copertura, la negazione di massa dell'esito delle elezioni presidenziali del 2020 da parte dell'ex presidente Donald Trump e dei suoi sostenitori, spinta in parte dalle teorie del complotto online e dalla disinformazione, ha inquinato l'ambiente informativo e si è infiltrato nel più ampio sistema politico americano. I negazionisti elettorali hanno sfruttato il supporto online per montare valide candidature a cariche pubbliche in vista del ballottaggio di metà mandato del novembre 2022.

La disinformazione sulle elezioni rubate e la presunta vulnerabilità alle frodi ha alimentato gli appelli ai cittadini per "proteggere" il voto con la forza, se necessario. Gli operatori e gli amministratori elettorali hanno riferito di aver ricevuto una raffica di minacce e molestie online, portando un gran numero di loro a dimettersi per paura per la propria incolumità. In effetti, tale disinformazione e intimidazione hanno minato

la sicurezza di base dei meccanismi elettorali statunitensi, ha fornito ai leader del Partito Repubblicano in molti stati una falsa giustificazione per nuove misure antifrode che potrebbero limitare l'accesso al voto o distorcere i processi di conteggio e certificazione, e ha posto le basi per futuri disordini erodendo la fiducia del pubblico in qualsiasi risultati sfavorevoli.

La frantumazione di Internet globale

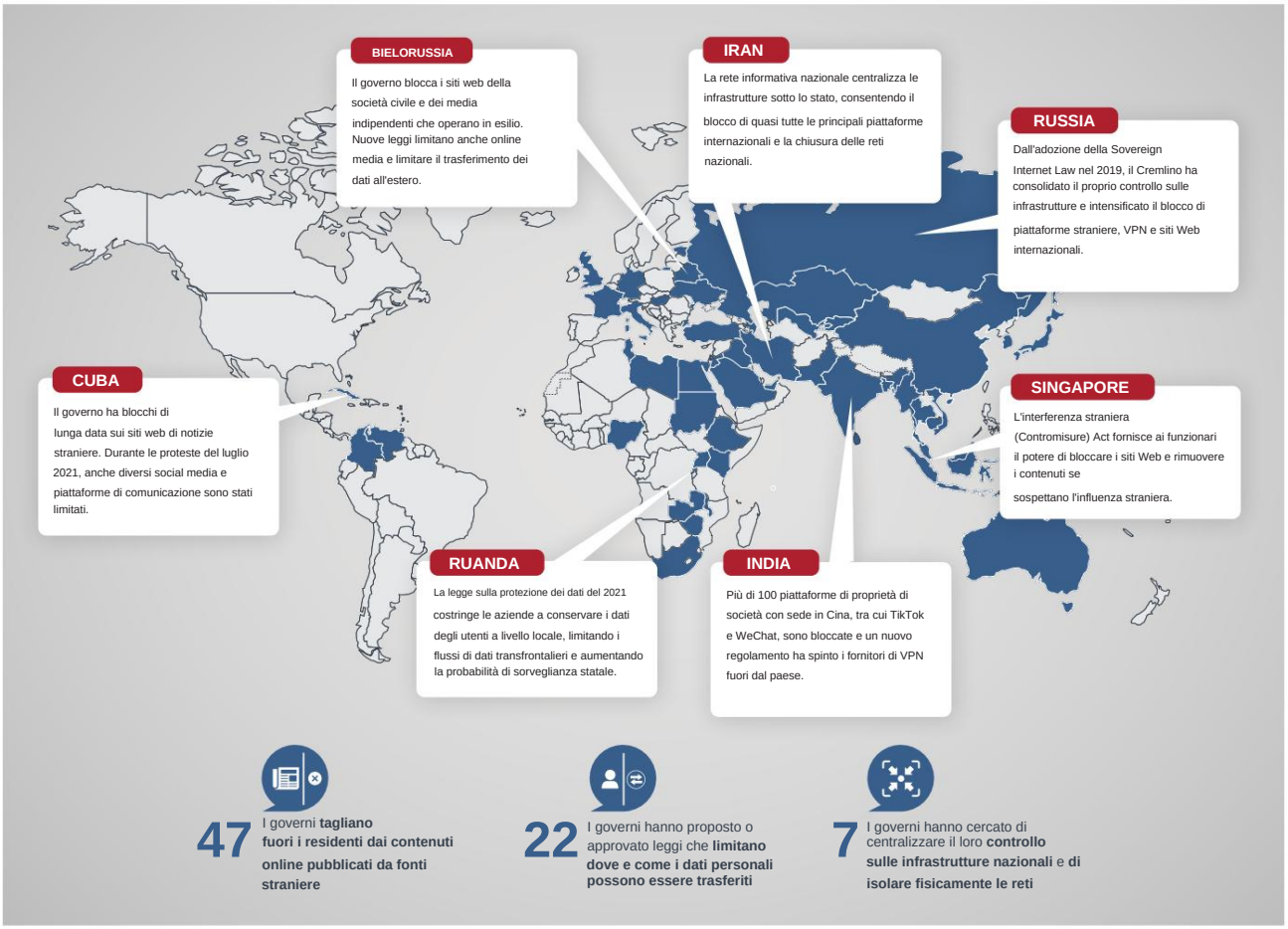
Internet è più frammentato che mai, impedendo miliardi di persone dall'esercizio dei loro diritti umani in linea. Autorità in oltre due terzi dei paesi intervistati in questo rapporto hanno utilizzato i loro poteri legali e normativi per limitare l'accesso a fonti di informazioni estere, lasciando i residenti in uno spazio informativo nazionale che è effettivamente modellato dallo stato. Sempre più governi stanno inoltre approvando leggi che pongono limiti al flusso di dati degli utenti attraverso i confini, con conseguenze contrastanti per l'Internet globale e i diritti umani. Le leggi più pericolose pretendono proteggere la privacy anche se delegano la supervisione alle autorità di regolamentazione legate alla leadership politica o costringono l'archiviazione dei dati in ambienti meno sicuri.

Pochi o nessun paese ha compiuto il passo estremo di disconnettersi completamente da Internet globale a livello tecnico. Ma un piccolo numero di leader autoritari lo è seguendo il PCC nella riprogettazione delle proprie reti domestiche per consentire un maggiore controllo sull'infrastruttura tecnica. Il loro successo rimane limitato dalla scoraggiante situazione economica e

UN INTERNET GLOBALE FATTO IN PEZZI

Un Internet globale in frantumi Sempre più governi stanno creando barriere al flusso di informazioni attraverso i confini nazionali.

Sempre più governi stanno creando barriere al flusso di informazioni attraverso i confini nazionali.



Questa infografica è tratta dal rapporto *Freedom on the Net 2022* , come si vede su www.freedomhouse.org.

i costi sociali di tali misure, nonché la persistenza delle norme internazionali a sostegno di un Internet globale aperto.

La miriade di normative e pratiche nazionali che contribuiscono alla frammentazione, intenzionalmente o meno, vengono imposte dai governi in tutto lo spettro democratico, ma ci sono distinzioni cruciali. Regimi autoritari in paesi come Cina, Iran e Russia stanno cercando di isolare la loro gente dal resto del mondo. Misure più democratiche in genere cercano di far rispettare la legislazione a tutela dei diritti che affronta il comportamento abusivo delle aziende o i veri danni online. Sebbene realizzate attraverso l'intervento statale, queste politiche sono spesso abbinate a salvaguardie che consentono il flusso continuo di informazioni e servizi

transfrontalieri, a condizione che i partner assicurino un livello simile di protezione dei diritti degli utenti.

Isolare gli utenti da informazioni esterne

In risposta a minacce sia reali che presunte online, le autorità di almeno 47 paesi hanno interrotto l'accesso ai residenti il flusso di notizie e informazioni attraverso le frontiere. Alcuni i governi hanno denunciato l'ingerenza straniera per giustificare nuove norme censorie, mentre altri hanno imposto interruzioni localizzate del servizio Internet, immergendo gli utenti nell'oscurità digitale nel tentativo di sopprimere le informazioni sulle violazioni dei diritti umani. In tandem con questa censura, molti leader politici hanno rafforzato il sostegno a piattaforme di social media allineate allo stato che sono più ricettive alle loro richieste.

Le restrizioni sono state in gran parte imposte nei paesi designati come non liberi o parzialmente liberi da *Freedom in the World*, dimostrando fino a che punto sia i leader autoritari radicati che quelli aspiranti si affidano ai controlli delle informazioni per mantenere il potere. È durante i pericolosi momenti di transizione politica e di possibile trasformazione - come proteste, elezioni e conflitti - che la censura delle informazioni straniere tende a intensificarsi.

Blocco dell'accesso a siti Web internazionali, piattaforme di social media o Internet nel suo complesso

Le autorità escludono sempre più gli utenti domestici dai siti Web e dalle piattaforme di social media che servono un pubblico internazionale. Queste restrizioni nazionali hanno un impatto globale, limitando le connessioni con i membri della famiglia in altri paesi e le comunità della diaspora che utilizzano le tecnologie digitali per rimanere in contatto con i loro paesi di origine.

Dal colpo di stato del febbraio 2021, la giunta militare del Myanmar ha coltivato una intranet interna per mettere a tacere l'opposizione alla sua presa di potere e consolidare il proprio potere. I residenti possono accedere solo a circa 1.200 siti Web e piattaforme tramite connessioni mobili. Facebook e Twitter, entrambi popolari tra i manifestanti anti-golp e strumenti chiave per comunicare con gli alleati all'estero, rimangono inaccessibili. La giunta ha anche imposto interruzioni del servizio Internet nelle città di tutto il paese, spesso in coincidenza con offensive militari contro milizie etniche, gruppi armati a favore della democrazia o comunità sospettate di sostenerle. In pratica, queste restrizioni hanno limitato la condivisione di prove di violazioni dei diritti umani con il pubblico esterno, hanno costretto i residenti a fare affidamento su fonti di informazioni dominate dai militari e hanno contribuito a contenere la mobilitazione civica e il dissenso.

In Etiopia, l'accesso a Internet è stato limitato nella regione del Tigray dal novembre 2020, quando è scoppiato il conflitto armato tra il governo federale e le forze associate al Fronte popolare di liberazione del Tigray. La chiusura ha impedito alle persone nel Tigray di condividere le loro storie e riferire sulle azioni dei combattenti che i gruppi per i diritti umani hanno descritto come crimini di atrocità di massa, limitando le opportunità di responsabilità e solidarietà globale.

Allo stesso modo nel luglio 2021, quando i cubani hanno mobilitato le più grandi manifestazioni antigovernative nel paese dalla rivoluzione del 1959, le autorità hanno limitato brevemente l'accesso a Internet e bloccato WhatsApp, Telegram e Signal. Questi passaggi hanno impedito ai manifestanti di utilizzare efficacemente gli strumenti digitali per coordinare le proteste e hanno separato il movimento dalle testate giornalistiche indipendenti e dai cubani con sede all'estero, che avevano raccolto sostegno per le manifestazioni sulle piattaforme dei social media internazionali.

Mentre la stragrande maggioranza dei governi che ha limitato l'accesso ai contenuti stranieri lo ha fatto per mantenere il proprio potere o ostacolare la responsabilità, un'eccezione degna di nota è arrivata dall'UE. Bruxelles ha ordinato le telecomunicazioni di ogni stato membro fornitori di bloccare i siti web dei servizi di media statali russi RT e Sputnik. Questi siti certamente promuovono contenuti incendiari e falsi e gli standard internazionali sui diritti umani consentono limiti alla libertà di espressione in circostanze specifiche, inclusi i conflitti armati. Tuttavia, l'ampio divieto dell'UE ha limitato tutti i contenuti di questi siti piuttosto che informazioni più ristrette relative alla guerra. Mancava anche chiare disposizioni di decadenza ed è stato imposto senza un'adeguata supervisione, trasparenza e consultazione con la società civile e le società di telecomunicazioni. L'insufficiente chiarezza e specificità dell'UE ha lasciato le aziende in difficoltà per determinare come conformarsi, portando a blocchi disomogenei tra i membri

stati. Inoltre, il divieto ha stabilito un precedente imperfetto su come le democrazie potrebbero rispondere alle informazioni problematiche diffuse da altri organi di informazione statali stranieri, come quelli con sede a Pechino.

Tecnologia di elusione mirata

Giornalisti, attivisti e utenti ordinari in molti paesi si sono riversati su strumenti di elusione come le reti private virtuali (VPN), che consentono loro di utilizzare Internet in modo sicuro e anonimo aggirando alcune forme di censura statale. In risposta, i governi bloccano, criminalizzano o impongono sempre più requisiti normativi

sugli stessi strumenti di elusione.

I blocchi alla tecnologia di elusione sono aumentati nei momenti di tensione politica durante il periodo di copertura, quando l'accesso a Internet internazionale senza censura sarebbe aumentato

coloro che cercano di cambiare gli equilibri di potere. Durante le elezioni regionali del novembre 2021 in Venezuela, in cui i partiti di opposizione hanno cercato di sfidare il governo autoritario di Nicolás Maduro, i fornitori di servizi hanno bloccato le VPN e il browser Web anonimo Tor, presumibilmente su ordine del governo, oltre al blocco diffuso di siti di media venezuelani internazionali e indipendenti. Gli utenti venezuelani di Internet sono stati tagliati fuori dalle informazioni critiche, in particolare dai rapporti dei media stranieri e dei gruppi di monitoraggio elettorale.

In India, sono stati introdotti nuovi requisiti normativi per i fornitori di VPN tra le richieste di censura del governo rivolte alle società tecnologiche con sede negli Stati Uniti e un blocco di due anni sulle piattaforme di comunicazione di proprietà delle società con sede in Cina, tra cui TikTok e WeChat. I servizi VPN dovranno conservare i record degli abbonati, come nomi e indirizzi IP (protocollo Internet), per cinque anni e fornirli al governo su richiesta, con multe salate per non conformità. I fornitori internazionali TunnelBear e Norton da allora hanno reso i loro servizi non disponibili per gli utenti

in India. Nel vicino Myanmar, secondo quanto riferito, i funzionari della sicurezza hanno impiegato tattiche più rozze per dissuadere le persone dall'utilizzare la tecnologia: hanno perquisito arbitrariamente i telefoni dei civili alla ricerca di VPN, arrestando le persone che si sono trovate ad averle scaricate.

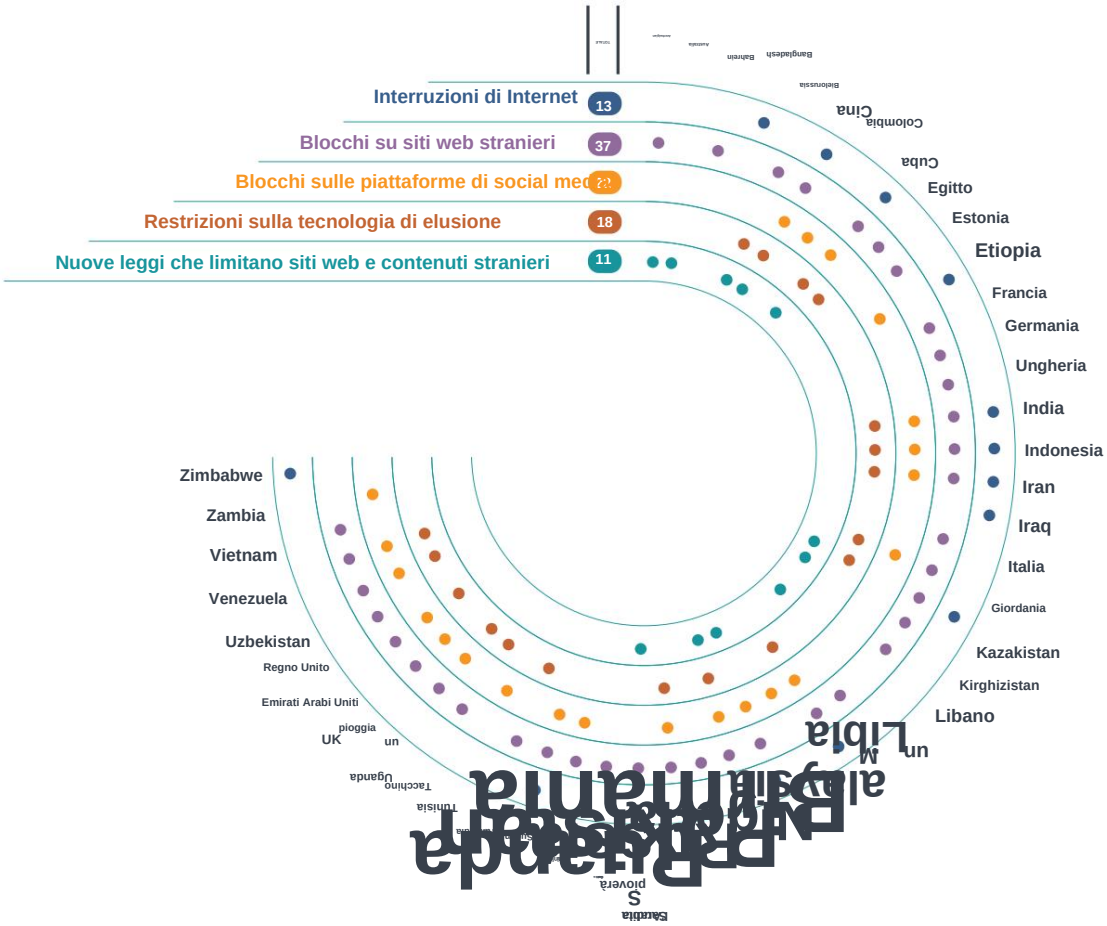
Il cittadino cubano Rolando Remedios mostra una foto del suo arresto, avvenuto durante le proteste diffuse sull'isola nel luglio 2021. *(Foto di Yamil Lage/ AFP)*

CONTARE I MODI IN CUI I GOVERNI Immergono GLI UTENTI NELL'OSCURITÀ

Conteggio dei modi in cui i governi fanno precipitare gli

Informazioni sulla libertà di Internet in ogni paese oggetto di

una forma di censura. utilizzando almeno una forma di censura.



Questa infografica è tratta dal rapporto *Freedom on the Net 2022* , come si vede su www.freedom

Sfruttare i timori di interferenze straniere per inibire i media indipendenti

Le autorità hanno anche invocato lo spettro dell'interferenza straniera per espandere la censura dei siti con sede all'estero o di quelli che ricevono finanziamenti dall'estero. I proprietari di siti web o i giornalisti che vivono al di fuori di un determinato paese spesso hanno più margine di manovra per resistere alle pressioni del governo e produrre reportage senza restrizioni. Richiedendo che i siti Web e le società correlate abbiano sede a livello nazionale o accettino solo finanziamenti nazionali, uno stato può migliorare la propria capacità di controllare lo spazio informativo locale.

Nell'ottobre 2021, il governo di Singapore ha aggiunto il Foreign Interference (Countermeasures) Act (FICA) al suo formidabile arsenale di poteri di censura. In nome della prevenzione dell'ingerenza straniera nella politica interna, FICA autorizza i funzionari a bloccare i siti Web e ordinare i social società di media e altri siti per rimuovere il discorso se sospettano che il contenuto in questione sia stato influenzato da un attore straniero. Un organismo di regolamentazione ha sospeso la licenza del sito di notizie per cittadini *The Online Citizen* entro un giorno dall'introduzione del disegno di legge in Parlamento, adducendo preoccupazioni sui finanziamenti esteri.

Una restrittiva legge azera sui media adottata nel febbraio 2022 limita i finanziamenti esteri che i media, definiti in senso lato per includere sia le testate giornalistiche che gli individui, possono accettare e richiede che gli operatori dei media abbiano sede nel paese. La legge ha ulteriormente represso quello che era già un ambiente mediatico online strettamente controllato, con molti giornalisti azeri costretti a operare dall'estero per evitare la persecuzione statale.

Sostenere alternative statali e di proprietà statale alle piattaforme internazionali

Anche se nell'ultimo anno hanno aumentato la pressione sulle piattaforme estere, molti governi repressivi hanno promosso flessibili alternative interne come parte di una strategia per creare un ambiente di informazione isolato e politicamente addomesticato. Se gli utenti migrano verso piattaforme allineate allo stato, i costi politici interni del blocco dei servizi internazionali sarebbero ridotti, facilitando un'ulteriore frammentazione.

In Cina, il governo ha avuto un discreto successo nell'accoppiare la censura sistematica dei servizi stranieri con solidi investimenti in piattaforme nazionali che sono legate al partito al potere. Un mercato dei social media più diversificato, compreso lo sviluppo di piattaforme più piccole e più locali che soddisfino le esigenze di una particolare comunità, è assolutamente necessario in tutto il mondo. Ma le aziende di proprietà o con stretti legami con governi autoritari hanno maggiori probabilità di censurare i contenuti sfavorevoli e diventare veicoli per

disinformazione statale rispetto alle loro controparti basate in contesti più democratici. Queste cosiddette piattaforme parallele sono spesso meno trasparenti nelle loro operazioni e politiche e possono essere meglio protette dalla difesa della società civile, dalle indagini dei media e da altre forme di controllo pubblico.

La strategia di Mosca per ridurre la dipendenza dalle società di social media straniere prevede l'obbligo per i telefoni cellulari di avere app domestiche precaricate. Dopo l'invasione dell'Ucraina nel febbraio 2022, i blocchi su Facebook, Twitter e Instagram hanno portato gli utenti a VK e Odnoklassniki, entrambi gestiti da una società madre che è in parte di proprietà degli alleati del Cremlino. Secondo quanto riferito, Yandex, un popolare motore di ricerca russo e rivale di Google, ha dato la priorità alle narrazioni di disinformazione e ha declassato i risultati di ricerca per i siti che criticavano l'invasione. Nel 2022, nel tentativo di conquistare basi di utenti più ampie per le piattaforme russe, le autorità avrebbero offerto pagamenti mensili agli influencer se fossero passati a RuTube e Yappy, al posto di YouTube e TikTok, e avessero aderito alla linea editoriale del governo.

La spinta verso le piattaforme domestiche ha spesso seguito attacchi espliciti o impliciti alla credibilità delle piattaforme internazionali, minando ulteriormente la fiducia nello spazio informativo globale. In Turchia, molte agenzie statali si sono riversate sul BiP alternativo di WhatsApp nel 2021, dopo che l'app di proprietà di Meta ha introdotto un problematico aggiornamento della politica sulla privacy. BiP è di proprietà dell'operatore di telefonia mobile Turkcell, controllato dal fondo sovrano statale. La piattaforma ha una base di utenti in crescita in Bangladesh, Indonesia, Pakistan e Bahrain.

Aumentare le barriere al flusso transfrontaliero dei dati degli utenti

In almeno 22 paesi coperti da *Freedom the Net,* durante il periodo di copertura sono state proposte o approvate leggi che limitano dove e come i dati personali possono fluire. I paesi interessati abbracciano lo spettro democratico, inclusi esempi classificati come Liberi, Parzialmente liberi e Non liberi da *Freedom in the World.* Il trasferimento di dati tra giurisdizioni è fondamentale per il funzionamento di Internet globale e avvantaggia gli utenti ordinari, anche migliorando la velocità di Internet, consentendo alle aziende di fornire servizi critici in tutto il mondo e consentendo l'archiviazione dei record nei data center più sicuri disponibili.

Poiché i responsabili politici impongono le necessarie leggi sulla privacy che salvaguardano le informazioni sensibili dagli abusi commerciali, possono involontariamente favorire la frammentazione creando una barriera tra i propri paesi e quelli senza

standard simili. Il conseguente mosaico di normative potrebbe incentivare le aziende, in particolare i servizi più nuovi o più piccoli, a concentrare la loro crescita in determinati paesi, con il risultato di ecosistemi online meno diversificati per gli utenti altrove.

Il regolamento generale sulla protezione dei dati (GDPR) dell'UE del 2018 consente il trasferimento di dati personali solo a giurisdizioni con un livello di protezione sufficiente. Mentre sempre più governi perseguono leggi che sembrano allinearsi con gli standard GDPR, alcuni hanno sepolto obblighi problematici che impongono l'archiviazione domestica dei dati, prevedono eccezioni generalizzate per la sicurezza nazionale o attori statali senza garanzie o delegano un maggiore potere decisionale a regolatori politicizzati: tutti che rende gli utenti vulnerabili agli abusi del governo nonostante i miglioramenti relativi all'uso dei dati personali per scopi commerciali. Tali misure contraddittorie di "lavaggio dei dati" alla fine non riescono a rafforzare la privacy e frammentano ulteriormente Internet.

Nell'agosto 2021, il governo cinese ha approvato una legge sulla protezione dei dati che regola l'uso commerciale dei dati personali, creando un importante insieme di garanzie per il miliardo di utenti Internet del Paese. Ma la legge non limita l'uso improprio dei dati da parte del governo e impone l'archiviazione interna dei dati per alcune aziende, aprendo la porta a ulteriori intrusioni e sfruttamento da parte dello stato e imponendo ulteriori onerose barriere al flusso di dati personali.

In Ruanda, una legge sulla protezione dei dati approvata nell'ottobre 2021 impone alle aziende di archiviare i dati nel paese a meno che

altrimenti autorizzato dall'autorità di regolamentazione della sicurezza informatica del paese, piuttosto che un'agenzia indipendente per la protezione dei dati che è più isolata dalle forze dell'ordine. Questo la clausola di localizzazione rende i dati personali vulnerabili agli abusi, in particolare dato che le autorità hanno incorporato agenti nelle società di telecomunicazioni a fini di sorveglianza e hanno perseguito i dissidenti sulla base dei loro messaggi privati.

Sebbene modellata sul GDPR, la nuova legge sulla protezione dei dati degli Emirati Arabi Uniti, in vigore dal gennaio 2022, esenta le entità governative incaricate del trattamento dei dati personali dal rispetto delle garanzie di base. Sebbene i suoi vincoli sull'accesso ai dati commerciali siano i benvenuti, la legge lascia a rischio la privacy dei residenti: le autorità del paese hanno ancora ampi poteri per monitorare le comunicazioni e sequestrare i dati dai fornitori di servizi.

Allontanarsi dall'infrastruttura globale

Governi di almeno sette paesi, tutti classificati Non liberi in *Libertà nel mondo,* ha cercato di centralizzare il controllo statale sulle infrastrutture nazionali e isolare fisicamente le proprie reti da Internet globale durante il periodo di copertura. Questa forma di frammentazione può essere la meno diffusa a causa delle capacità tecniche e amministrative eccezionalmente avanzate che richiede.

Implica anche una notevole volontà politica: l'isolamento infrastrutturale presenta costi economici per le imprese che operano a livello nazionale, può rallentare notevolmente la velocità di connessione e aggrava il rischio per i diritti umani. Queste sfide aiutano a spiegare perché i leader politici nei paesi con solidi spazi civici, fiorenti settori tecnologici e sistemi di governance più pluralistici hanno meno probabilità di imporre tali barriere.

Il PCC e le società collegate allo stato hanno coltivato il modello più sofisticato di isolamento informatico. Il traffico Internet dall'esterno del paese passa attraverso punti di strozzatura centralizzati e controllati dallo stato, facilitando il blocco di massa, il filtraggio e la sorveglianza. Seguendo il percorso di Pechino, il governo iraniano ha imposto barriere statali tra i locali infrastrutture e traffico globale. Nel luglio 2021, le autorità hanno introdotto il disegno di legge sulla protezione degli utenti per rafforzare la rete nazionale di informazioni del paese, che ha facilitato la restrizione dell'accesso a piattaforme e connessioni internazionali indirizzando gli utenti verso alternative nazionali.

La legge porrebbe i gateway Internet del paese sotto l'autorità di un gruppo di lavoro che comprende agenzie militari e di intelligence.

Il governo russo ha accelerato i propri progressi verso l'isolamento infrastrutturale nell'ultimo anno. Durante una serie di test a giugno e luglio 2021, le autorità hanno affermato di aver separato con successo il cosiddetto RuNet dalle connessioni globali, sebbene gli esperti tecnici rimangano scettici.

Nell'aprile 2022, in seguito alla sua invasione dell'Ucraina, il presidente Vladimir Putin ha nominato una commissione interagenzia per perseguire il suo obiettivo di isolamento tecnico.

Il governo cambogiano ha pianificato di instradare tutto il traffico Internet internazionale e nazionale attraverso un unico portale, soprannominato National Internet Gateway (NIG). Questo punto di strozzatura centralizzato consentirebbe alle autorità di censurare i contenuti di tutto il mondo e sorvegliare maggiormente i residenti facilmente. I funzionari cambogiani hanno inaspettatamente ritardato l'attuazione del NIG nel febbraio 2022, citando la pandemia di COVID-19 e problemi relativi alle licenze e all'installazione delle apparecchiature. La decisione è arrivata dopo un'ampia opposizione al NIG da parte del settore privato, della società civile e degli esperti delle Nazioni Unite.

La competizione per il controllo del web La frammentazione a livello nazionale fa parte di una battaglia globale per il controllo di Internet. Guidati da Pechino e Mosca, i diplomatici dei paesi autoritari hanno promosso il loro modello di sovranità informatica presso le istituzioni multilaterali. In qualità di segretario generale dell'ITU, il cinese Houlin Zhao ha incoraggiato uno spostamento del controllo sulla definizione degli standard tecnici lontano dagli organismi multistakeholder, dove la società civile e altri esperti non governativi hanno più influenza, e verso l'ITU stessa, dove solo i governi hanno il contributo.

Durante il mandato di Zhao, nel 2019 e nel 2020, il gigante cinese delle telecomunicazioni Huawei ha presentato la proposta New IP, un piano per alterare radicalmente l'interoperabilità dell'infrastruttura di Internet globale ridisegnando protocolli comuni per facilitare un maggiore controllo statale sulle reti domestiche. Sebbene inizialmente respinti dai membri dell'ITU, da allora sono riemersi elementi della proposta rinominati

> La frammentazione a livello nazionale fa parte di una battaglia globale per il controllo di Internet.

Zhao Houlin, segretario generale dell'Unione internazionale delle telecomunicazioni, parla durante la cerimonia di apertura della Convenzione mondiale 5G del 2021 a Pechino nell'agosto 2021. *(Foto di VCG via Getty Images)*

negli organismi di normazione. I funzionari cinesi hanno anche lanciato nel luglio 2022 la World Internet Conference International Organization a Pechino, destinata a fungere da comunità globale "condivisa" che determinerebbe standard tecnici e governance. L'organizzazione, nata dall'omonima riunione annuale che si è tenuta per la prima volta nel 2014, potrebbe creare un nuovo forum in cui il governo cinese possa promuovere e incentivare altri governi ad adottare il suo modello autoritario di controllo digitale.

Allo stesso modo, il governo russo ha sfruttato le istituzioni internazionali per influenzare la governance di Internet. Alle Nazioni Unite nel febbraio 2022 sono iniziati i negoziati per un nuovo trattato sulla criminalità informatica, inizialmente proposto da diplomatici russi e co-sponsorizzato da rappresentanti di Bielorussia, Cambogia, Cina, Corea del Nord, Myanmar, Nicaragua e Venezuela, tutti classificati Non liberi dalla *libertà nel mondo.*

La società civile ha clamorosamente condannato il trattato proposto come un nuovo vettore per la repressione digitale. Anche Mosca si è unita a Pechino nel giugno 2021 per chiedere un ITU più potente e sostenere il diritto di ogni stato a controllare il proprio "segmento nazionale di Internet". Un funzionario russo ha spiegato la necessità di una versione più energica dell'agenzia affermando che il modello di governance multistakeholder era "inefficace".

Gli ***stati democratici si intensificano a livello globale***

Alcuni leader democratici hanno ripreso gli sforzi per plasmare standard digitali globali che sostengano le libertà fondamentali, creando un contrappeso tanto necessario agli sforzi autoritari. Dopo aver consentito al segretario generale dell'ITU Zhao di candidarsi senza opposizione nel 2014 e nel 2018, Washington ha nominato Doreen Bogdan-Martin per cercare il posto, e ha sconfitto un candidato sostenuto da Mosca in una votazione del settembre 2022 da parte degli Stati membri. Due iniziative guidate dagli Stati Uniti, il Summit per la democrazia e la Dichiarazione per il futuro di Internet, hanno cercato di consolidare norme comuni come base per ulteriori azioni. Inoltre, gli Stati Uniti si sono impegnati a rafforzare ed espandere la Freedom Online Coalition nel suo prossimo ruolo di presidente nel 2023.

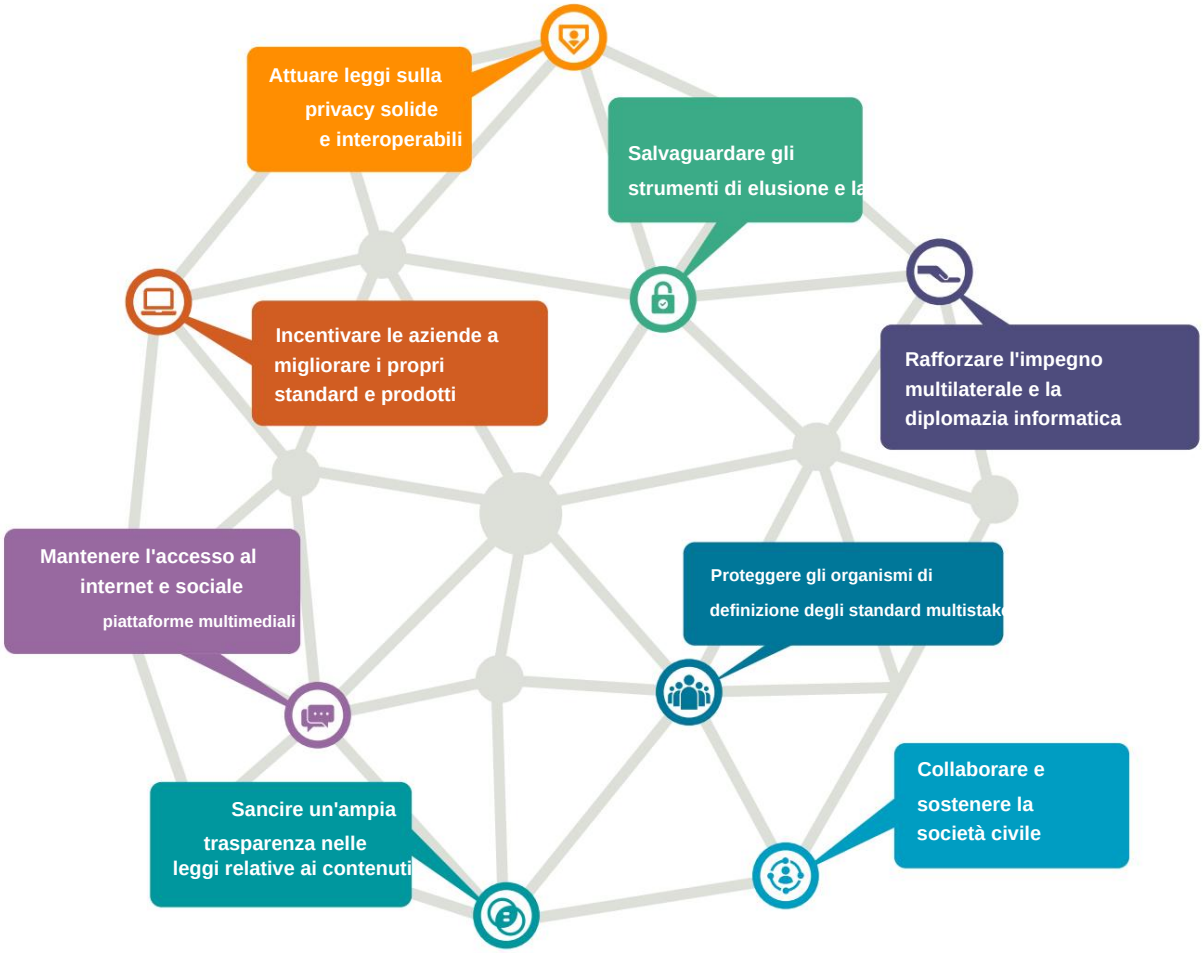
RIMONTARE L'INTERNET GLOBALE

Rimettere insieme l'Internet globale I

responsabili politici, gli organismi di regolamentazione e altre agenzie statali dovrebbero agire

dovrebbero intraprendere misure per proteggere

I responsabili politici, gli



Questa infografica è tratta dal rapporto *Freedom on the Net 2022* , come si vede su www.freedomh

Dall'altra parte dell'Atlantico, l'UE ei suoi Stati membri hanno intrapreso azioni simili. Il Copenhagen Pledge on Tech and Democracy, guidato dal governo danese, utilizza un formato multistakeholder invitando i governi, gli organismi multilaterali, la società civile e il settore privato a proteggere insieme i diritti umani nell'era digitale. Separatamente, il Digital Services Act (DSA) dell'UE è un'alternativa promettente ad approcci normativi più censoriali e potrebbe servire da modello globale. Rafforza la trasparenza, limita i sistemi pubblicitari e richiede che grandi piattaforme forniscano dati a ricercatori e organizzazioni indipendenti, che possono quindi portare a risposte più innovative ed efficaci ai danni online. Il DSA istituisce anche una forma di coregolamentazione più inclusiva di supervisione e applicazione, anche utilizzando revisori di terze parti indipendenti per verificare la conformità, il che può limitare il rischio di abusi.

Tuttavia, il framework DSA prevede una disposizione problematica di "avviso e azione" per le aziende per rimuovere i discorsi ritenuti illegali dalle autorità dell'UE o dagli Stati membri, che potrebbero essere abusati per mettere a tacere i discorsi politici, sociali e religiosi. Per limitare questo rischio, Bruxelles e gli Stati membri dovrebbero definire chiaramente e armonizzare le loro definizioni di ciò che costituisce un discorso "illegale" in linea con il diritto internazionale e garantire che autorità giudiziarie indipendenti sovrintendano a qualsiasi rimozione di contenuti.

Armonizzare la protezione dei dati per creare una corsa verso l'alto

Un maggiore coordinamento politico tra le democrazie è vitale per la protezione di un Internet libero e aperto. In un segno promettente dall'aprile 2022, i governi di Canada, Giappone, Filippine, Singapore, Corea del Sud, Taiwan e Stati Uniti hanno istituito il Global Cross-Border Privacy Rules Forum per colmare le discrepanze normative e promuovere il libero flusso di dati ai sensi ciò che determina come "migliore".

pratiche" per la protezione dei dati. L'UE e gli Stati Uniti hanno inoltre compiuto progressi durante il periodo di copertura successivo all'invalidazione da parte della Corte di giustizia europea del quadro dello scudo UE-USA per la privacy nel 2020, una sentenza che limitava i flussi di dati transatlantici a causa delle preoccupazioni relative agli Stati Uniti programmi di sorveglianza della sicurezza nazionale. Nel marzo 2022, i partner transatlantici hanno annunciato un accordo sul Privacy Shield 2.0, che dovrebbe essere formalizzato alla fine del 2022, che include un meccanismo di ricorso per i residenti dell'UE interessati sulle violazioni della privacy e sui nuovi impegni in materia di privacy da parte delle agenzie di intelligence statunitensi.

I governi hanno anche proposto, approvato o avviato l'applicazione di leggi sulla protezione dei dati compatibili con i diritti che rispettano le disposizioni dei quadri internazionali esistenti, una pratica che può ridurre al minimo gli effetti della frammentazione.
La legge sulla protezione dei dati del Sudafrica, entrata in pieno vigore nel luglio 2021, è stata redatta per armonizzarsi con parti del GDPR, così come quella dello Sri Lanka, approvata nel marzo 2022.
Entrambe le leggi pongono limiti al trasferimento di dati personali attraverso

> Un maggiore coordinamento politico tra le democrazie è vitale per la protezione di un Internet libero e aperto.

frontiere tranne in alcuni casi, compresi i trasferimenti verso un paese con adeguate garanzie. La protezione della privacy non richiede necessariamente di limitare la posizione fisica dell'archiviazione dei dati. Ad esempio, l'American Data Privacy and Protection Act proposto negli Stati Uniti evita di concentrarsi su dove i dati possono essere trasferiti e adotta invece un approccio di minimizzazione dei dati che limita ciò che può essere raccolto, come può essere archiviato e con chi può essere condiviso .

Resistere alla frammentazione di Internet proteggendo i diritti umani I valori dei diritti umani e delle società aperte si rafforzano a vicenda. Nell'attuare le leggi a tutela dei diritti, i governi dovrebbero cercare di ridurre gli attriti coordinando i loro sforzi oltre i confini e allineandoli ai quadri internazionali quando possibile. In definitiva, i funzionari democratici, le società tecnologiche e i gruppi della società civile globale dovrebbero mirare a consentire alle persone di svolgere un ruolo maggiore nel rendere gli spazi online più liberi, sicuri e inclusivi. Questo è il modo migliore per garantire che i diritti umani siano rispettati nell'era digitale.

Un Internet resiliente per a Futuro più democratico

Ventisei paesi hanno registrato netti miglioramenti nella libertà di Internet nell'ultimo anno, la cifra più alta dall'inizio di *Freedom on the Net.*
Sebbene la repressione digitale stia indubbiamente diventando più sofisticata e radicata nella vita di tutti i giorni, le risposte dei governi, della società civile e del settore privato stanno iniziando a dare risultati.

Freedom on the Net ha identificato strategie collaudate che mettono in campo le strutture, gli strumenti e le competenze necessarie per prevenire o affrontare gli usi illiberali della tecnologia da parte di attori nazionali e stranieri, nonché i danni sociali più ampi che Internet spesso aggrava. Alcune strategie forniscono risposte a breve termine a casi di repressione, mentre altre costruiscono meccanismi a lungo termine per la responsabilità, la governance e la supervisione che possono nel tempo impedire l'avanzata dell'autoritarismo. Questi approcci variano in efficacia a seconda del contesto politico di un paese: costruire la resilienza digitale in una democrazia in declino e farlo sotto un regime autoritario radicato comporta diverse serie di sfide. Collettivamente, tuttavia, tali sforzi hanno il potenziale per invertire il declino globale della libertà di Internet.

Sebbene il successo richieda la partecipazione di una serie di attori, la società civile è sempre stata in prima linea. Organizzazioni senza scopo di lucro, gruppi di media e difensori dei diritti umani con radici in un determinato paese o regione hanno svolto un ruolo di primo piano nell'identificare e aumentare la consapevolezza di un problema, spesso instancabilmente nel corso degli anni, e quindi creare una strategia per affrontarlo, con l'assistenza di altri che possono organizzarsi le necessarie risorse finanziarie e politiche. Governi, fondazioni filantropiche, aziende private e altri interessati a coltivare un Internet libero e aperto che funzioni per tutti i suoi utenti dovrebbero fare del loro meglio per impegnarsi in modo significativo con i gruppi della società civile coinvolti nella lotta contro la repressione digitale e la frammentazione di Internet , fornendo finanziamenti, competenze tecniche, rafforzamento delle capacità e altro sostegno per far progredire il loro lavoro.

La società civile ha svolto un ruolo di primo piano nell'identificare e aumentare la consapevolezza di un problema e quindi nella creazione di una strategia per affrontarlo.

Collaborare con la magistratura

In almeno 28 paesi coperti da questo rapporto, i tribunali hanno protetto la libertà di Internet. In molti casi, le leggi problematiche sono state abolite, creando precedenti per guidare le future azioni statali. L'intervento del tribunale sembra essere il più efficace per combattere la censura e la sorveglianza nei paesi classificati liberi o parzialmente liberi da *Freedom in the World,* dove le autorità giudiziarie rimangono indipendenti o in qualche modo resistenti al controllo politico. Gli sforzi per proteggere la libertà di Internet dovrebbero dare la priorità al rafforzamento dell'indipendenza dei tribunali e allo sviluppo della loro capacità di analizzare i concetti legali e tecnici che emergono nei casi che coinvolgono i diritti umani online.

In un esempio positivo, l'organizzazione per i diritti umani dello Zambia Chapter One Foundation ha citato in giudizio l'autorità di regolamentazione delle comunicazioni del paese dopo aver bloccato le piattaforme dei social media durante le elezioni presidenziali dell'agosto 2021. A seguito dell'azione legale, il regolatore ha firmato un accordo di consenso, impegnandosi a non agire al di fuori della propria autorità legale e impegnandosi a rafforzare la trasparenza in merito a eventuali future restrizioni sulle piattaforme di telecomunicazioni.

In India, diversi gruppi della società civile e dei media si sono impegnati in contenziosi strategici in risposta alle norme censorie sulla tecnologia dell'informazione del governo e nell'agosto 2021 un tribunale ha interrotto l'applicazione di disposizioni problematiche nei regolamenti nell'ambito di una causa intentata da un'organizzazione che rappresenta le emittenti. In un caso più recente, nell'aprile 2022 la Corte Suprema del Messico ha invalidato un registro biometrico di telefoni cellulari, rafforzando la capacità di comunicazione delle persone

online in forma anonima. La decisione è arrivata dopo che gli attivisti della società civile hanno sostenuto che il registro ha facilitato una sorveglianza diffusa, ha reso i dati personali meno sicuri e ha contribuito alle disuguaglianze sociali.

Spingere il settore privato all'azione

In almeno 30 paesi nell'ultimo anno, il settore privato si è mosso per proteggere la libertà di Internet. In molti casi, le aziende tecnologiche hanno agito in risposta alle pressioni della società civile, alle testimonianze degli informatori e al controllo dei media. Tali lusinghe possono essere necessarie, come sforzi del settore privato per proteggere la libertà di Internet sono state incoerenti e influenzate da richieste contrastanti, inclusa la raccolta di massa di dati degli utenti che costituisce il modello di business principale della rete internazionale piattaforme di social media.

In seguito all'invasione dell'Ucraina da parte del Cremlino, le aziende tecnologiche si sono affrettate a proteggere gli utenti vulnerabili ed evitare il sostegno involontario a una guerra di aggressione. Google, Twitter e Meta hanno tutti limitato la capacità dei media statali russi di monetizzare i contenuti attraverso le loro piattaforme. Hanno anche implementato nuove funzionalità di sicurezza per ridurre i rischi online, come l'espansione di Meta della crittografia end-to-end per gli utenti di Instagram in Russia e Ucraina e

UN APPROCCIO MULTIFUNZIONE ALLA SALVAGUARDIA DEI DIRITTI UMANI ONLINE

Un approccio su più fronti per la salvaguardia dei diritti umani online

il Collettivamente, queste strategie possono aiutare a invertire il declino globale della libertà di

Questa infografica è tratta dal rapporto *Freedom on the Net 2022* , come si vede su www.freedomhouse.org.

la sua introduzione di messaggi effimeri sull'applicazione Messenger per quelli in Ucraina. Twitter ha lanciato un servizio Tor Onion, consentendo agli utenti in Russia di accedere alla piattaforma in modo sicuro e anonimo dopo che è stata bloccata dal governo.

Sotto la pressione dell'opinione pubblica, le società di social media hanno respinto gli sforzi del governo indiano per aumentare il controllo sulla parola online. Dopo l'ampia condanna della società civile per la sua conformità alla censura statale, Twitter ha resistito agli ordini del governo di limitare i contenuti, inclusi i post di Freedom House, prima di acconsentire finalmente nel giugno 2022 dopo che un dipendente dell'azienda è stato minacciato di accuse penali. Twitter ha quindi portato il caso alla magistratura, intentando una causa nel luglio 2022 che potrebbe frenare l'ampia affermazione del governo dei poteri di censura.

Il settore privato ha talvolta collaborato con la società civile, gli attori governativi e il mondo accademico per progettare risposte innovative ai danni online. A Taiwan, che deve far fronte a una raffica di disinformazione riconducibile alla Cina, la popolare applicazione di messaggistica giapponese Line ha collaborato con gruppi della società civile per sviluppare uno strumento che consenta agli utenti di segnalare informazioni false quando si presentano sulla piattaforma. Il governo taiwanese ha lanciato uno sforzo di coordinamento simile dopo l'invasione russa dell'Ucraina, con l'obiettivo di rintracciare la disinformazione legata alla guerra proveniente dalla Cina.

Promuovere modifiche alle politiche del governo per ripristinare la libertà di Internet

I responsabili politici, gli organismi di regolamentazione e altre agenzie governative in almeno 26 paesi hanno adottato misure per proteggere i diritti umani online durante il periodo di copertura. Queste misure hanno rafforzato le salvaguardie istituzionali per la libertà di espressione, l'accesso alle informazioni e la privacy e hanno difeso gli utenti di Internet da pratiche aziendali manipolative. Nel

> Uno sforzo su più fronti, tra cui contenzioso strategico, ricerca basata su prove, impegno multilaterale e bilaterale e advocacy mirata, ha cambiato il comportamento dei governi che impongono chiusure.

in alcuni casi, i funzionari governativi stavano reagendo a campagne di advocacy mirate da parte di organizzazioni della società civile; in altri, le loro azioni sono state un risultato indiretto degli sforzi a lungo termine della società civile per plasmare il discorso pubblico sulle risposte politiche e normative a disinformazione, molestie, illeciti aziendali e altri danni online.

Il governo del Gambia ha promulgato una legislazione nel luglio 2021 che ha affermato il diritto di accedere alle informazioni pubbliche, autorizzando i giornalisti, le organizzazioni della società civile e i cittadini comuni a ritenere il governo responsabile delle sue prestazioni. La legge è stata redatta utilizzando un modello multilaterale, con il contributo della società civile gambiana e internazionale e del settore privato.

In Armenia, gruppi della società civile nazionale e internazionale hanno unito la condanna pubblica alla difesa privata per convincere il governo ad abrogare una clausola penale sulla diffamazione originariamente approvata nel luglio 2021. l'anno per perseguire gli utenti che hanno condiviso commenti critici, in particolare sul primo ministro Nikol Pashinyan. Attivisti della società civile hanno espresso le loro preoccupazioni in incontri privati con diplomatici e nei notiziari armeni, e le loro obiezioni sono state poi citate in un ricorso formale alla Corte costituzionale. Funzionari governativi hanno concordato di escludere la disposizione da un nuovo codice penale entrato in vigore nel luglio 2022 e si sono impegnati in un'ampia consultazione con gruppi non governativi durante lo sviluppo

leggi sui media in futuro.

La società civile ha invitato i responsabili politici democratici a garantire che le sanzioni imposte in risposta all'invasione russa dell'Ucraina non impediscano l'accesso critico a Internet. In una lettera del marzo 2022, più di 35 gruppi ed esperti per la libertà di Internet, tra cui Freedom House, hanno avvertito il presidente Biden dei pericoli e delle conseguenze indesiderate della limitazione dei servizi Internet per gli utenti in Russia e Bielorussia. Alcune settimane dopo, il Dipartimento del Tesoro ha esentato i servizi di telecomunicazioni dalle sanzioni statunitensi relative a l'invasione.

I regolatori indipendenti hanno chiesto consiglio alla società civile e ad altri esperti sul modo migliore per impedire alle aziende di minare i diritti degli utenti di Internet. Nell'agosto 2022, dopo il periodo di copertura, la Federal Trade Commission degli Stati Uniti ha annunciato che stava accettando il parere del pubblico sulla necessità di nuove regole per proteggere i residenti negli Stati Uniti

dalla raccolta dei dati aziendali. Tali regole potrebbero consentire all'autorità di regolamentazione di mitigare i danni in assenza di tutele complete della privacy ai sensi della legge federale.

Progressi sulle chiusure di Internet Le chiusure di Internet sono state a lungo una tattica fondamentale della repressione digitale. Ma questo potrebbe cambiare: il sottopunteggio *Freedom on the Net* relativo alle restrizioni governative sulla connettività Internet è migliorato in 13 paesi, il maggior numero di guadagni per un singolo indicatore attraverso la metodologia di 21 domande quest'anno. Durante il periodo di copertura, i governi di 14 dei 70 paesi hanno valutato l'interruzione o la limitazione dei servizi Internet fissi o mobili, rispetto ai 20 paesi dell'edizione 2021 del rapporto e ai 22 dell'edizione 2020. Nei paesi in cui continuano a verificarsi chiusure, sembrano essere più localizzate e temporanee, interessando meno persone per meno tempo rispetto alle restrizioni passate.

La tendenza suggerisce che uno sforzo su più fronti, tra cui contenzioso strategico, ricerca basata su prove, impegno multilaterale e bilaterale e advocacy mirata, ha contribuito a cambiare il comportamento dei governi che impongono chiusure. Ad esempio, i ricercatori hanno dimostrato che le chiusure hanno un impatto sulle economie locali e hanno dimostrato di essere correlate a livelli più elevati di violenza, minando l'argomentazione secondo cui sono necessarie per mantenere la pace e la sicurezza. Le azioni legali intentate da gruppi della società civile, giornalisti e altri hanno portato a interventi giudiziari contro le restrizioni alla connettività, più recentemente in India nel 2022 e in Sudan nel 2021.

La difesa proattiva rivolta sia ai governi che ai fornitori di servizi Internet è riuscita a prevenire possibili arresti in vista di eventi importanti. Ad esempio, i membri della coalizione #KeepItOn, che comprende più di 280 gruppi della società civile, tra cui Freedom House, e guidati dal gruppo per i diritti digitali Access Now, si sono mobilitati in vista delle elezioni generali in Kenya nell'agosto 2022 e delle elezioni parlamentari in Iraq nell'ottobre 2021 per sollecitare funzionari per mantenere la connettività. I funzionari kenioti hanno adempiuto ai loro impegni pubblici di astenersi dal limitare l'accesso a Internet e in Iraq non sono state segnalate interruzioni dell'accesso a Internet, a differenza delle elezioni del 2018.

I kenioti tengono traccia dei risultati delle elezioni presidenziali dell'agosto 2022. Il presidente della Commissione elettorale e dei confini indipendenti (IEBC) ha dichiarato vincitore il vicepresidente William Ruto dopo una corsa serrata. *(Foto di Boniface Muthoni, SOPA Images/LightRocket via Getty Images)*

La sorveglianza sproporzionata rimane uno dei problemi più evidenti che incidono sulla libertà di Internet delle democrazie.

Questa sostenuta difesa ha contribuito a un consenso a livello multilaterale sul fatto che le chiusure sono ingiustificabili e sproporzionate. Un rapporto delle Nazioni Unite, commissionato dal Consiglio per i diritti umani e rilasciato nel 2022 all'Assemblea generale, ha incorporato il contributo della società civile e del settore privato per delineare raccomandazioni su come limitare tale censura. Il Freedom Online Coalition ha chiesto la fine immediata di chiusure nel luglio 2021, lanciando una task force sulla chiusura di Internet per progettare le migliori pratiche per la difesa. I governi del Gruppo dei Sette hanno anche concordato pubblicamente nel 2021 di cooperare contro le chiusure quando sono "politicamente motivati", anche se secondo quanto riferito hanno ammorbidito il loro linguaggio dopo le obiezioni del governo indiano, leader globale nelle restrizioni alla connettività.

Il percorso verso una protezione dei diritti più forte e un Internet più resiliente

Il successo dello sforzo collettivo contro le interruzioni dei servizi offre un modello per affrontare altri problemi critici che stanno guidando la repressione digitale e la frammentazione dell'internet aperto. Le strategie che si basano sul lavoro della società civile per mobilitare il cambiamento nei tribunali, tra i governi e presso le aziende tecnologiche possono offrire migliori protezioni per i diritti umani online su scala nazionale e globale, in particolare quando arruolano istituzioni multilaterali e multistakeholder. Senza tali campagne, tuttavia, è probabile che Internet diventi più frammentato, ostacolando lo scambio di punti di vista diversi e idee innovative, limitando la capacità delle persone di organizzarsi per cause politiche e sociali e interrompendo le connessioni transfrontaliere tra le comunità.

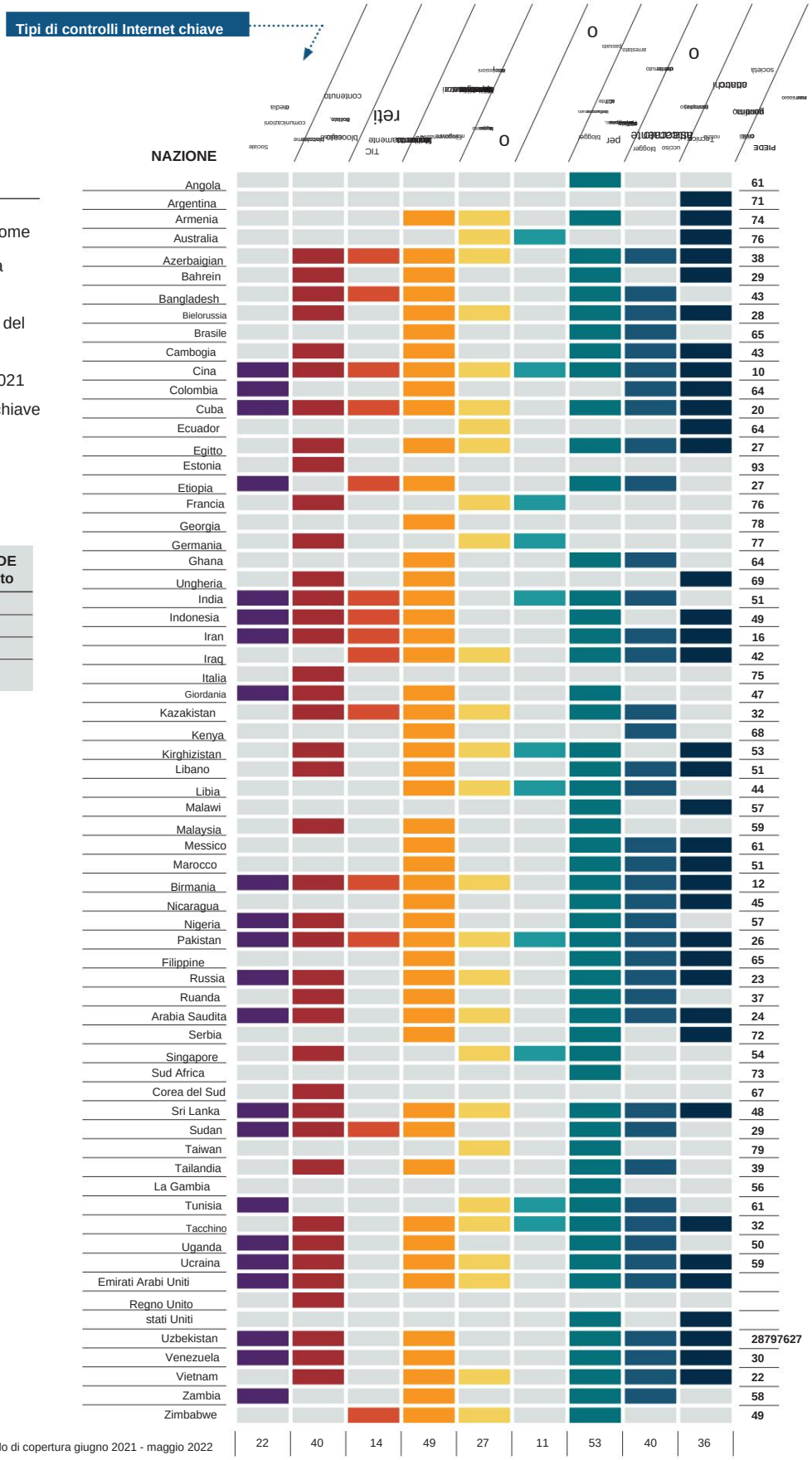
Uno sforzo di advocacy ha già individuato il suo obiettivo: l'acquisto e l'implementazione da parte dei governi di strumenti di sorveglianza commerciale intrusivi che violano i diritti degli utenti di Internet in tutto il mondo. Ricercatori tecnici, esperti di diritti umani e indagini sui media hanno recentemente documentato la portata e gli abusi dell'oscura industria dello spyware e i governi hanno iniziato a esplorare le restrizioni legali e normative sulla vendita di tali prodotti. Questi sono i primi passi benvenuti, ma è necessario di più.

La sorveglianza sproporzionata rimane uno dei problemi più evidenti che incidono sulla libertà di Internet delle democrazie. Troppo spesso, le considerazioni sui diritti vengono ignorate a favore dell'errata convinzione che strumenti più intrusivi e un maggiore accesso statale ai dati contribuiranno necessariamente a una società più sicura. Oltre ad affrontare la proliferazione di spyware, le democrazie dovrebbero imporre solidi controlli su altre forme di sorveglianza e proteggere la crittografia end-to-end, che limita l'impatto di tale monitoraggio eccessivo. Il modello di coalizione per raggiungere la resilienza digitale potrebbe essere impiegato per concentrare il tanto necessario controllo pubblico sulla questione di quali strumenti e pratiche di sorveglianza siano compatibili con i diritti umani. Tale azione getterebbe le basi affinché le democrazie adottino regolamenti nazionali basati sui diritti, spianerà la strada a restrizioni più coordinate ed efficaci sul mercato della sorveglianza privata e rimuoverà strumenti di monitoraggio potenti e in continua evoluzione dalle mani di attori governativi abusivi, in ultima analisi promuovere un futuro più democratico.

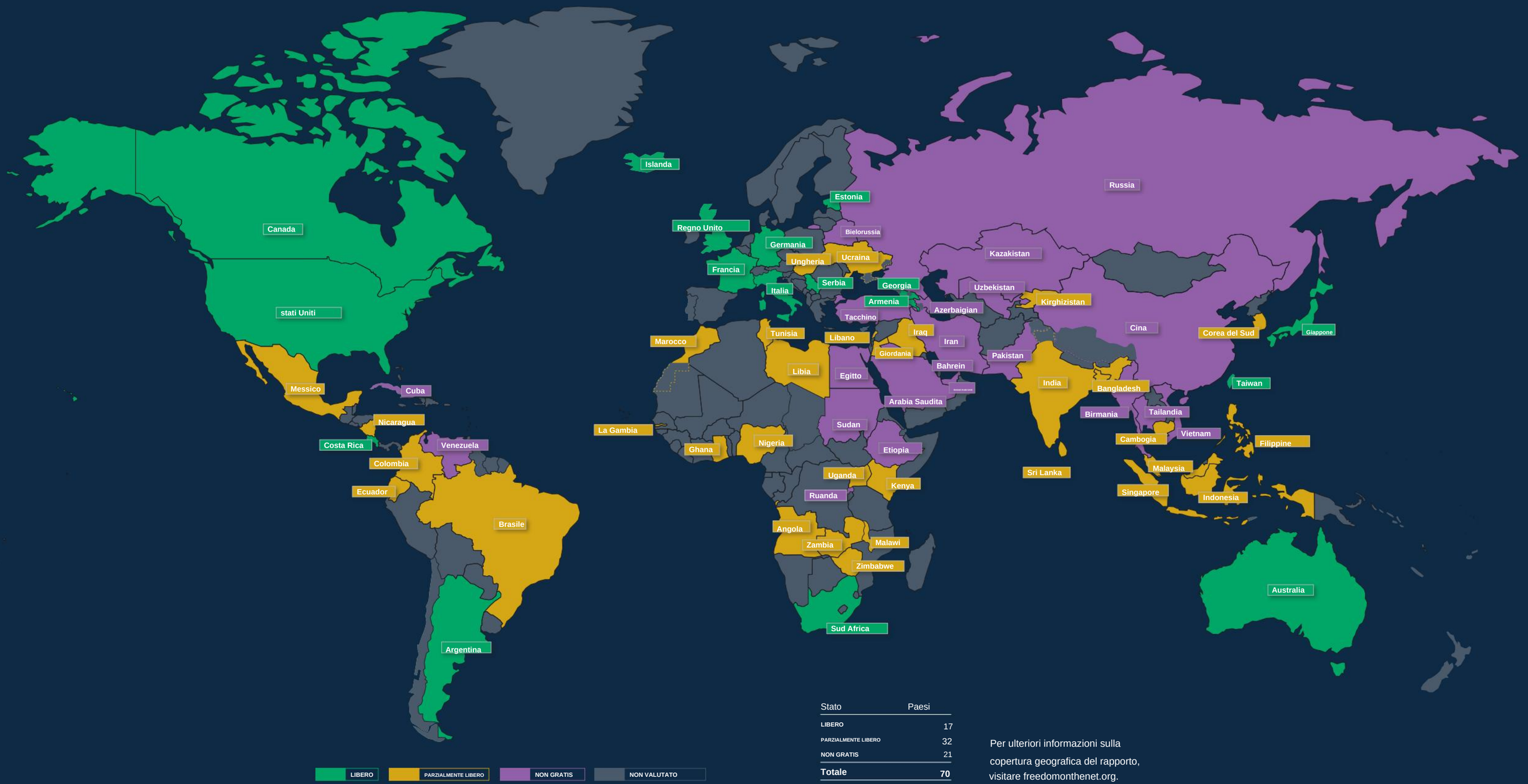
CHIAVE INTERNET CONTROLLI PER PAESE

Freedom House ha documentato come i governi censurano e controllano la sfera digitale. Ogni cella colorata rappresenta almeno un'occorrenza del controllo citato durante il periodo di copertura del rapporto da giugno 2021 a maggio 2022. I controlli Internet chiave riflettono le restrizioni su contenuti di natura politica, sociale o religiosa.

NESSUN INTERNET CHIAVE CONTROLLI RISPETTATI	PIEDE Punto
Canada	87
Costa Rica	88
Islanda	95
Giappone	77



LIBERTÀ IN RETE 2022

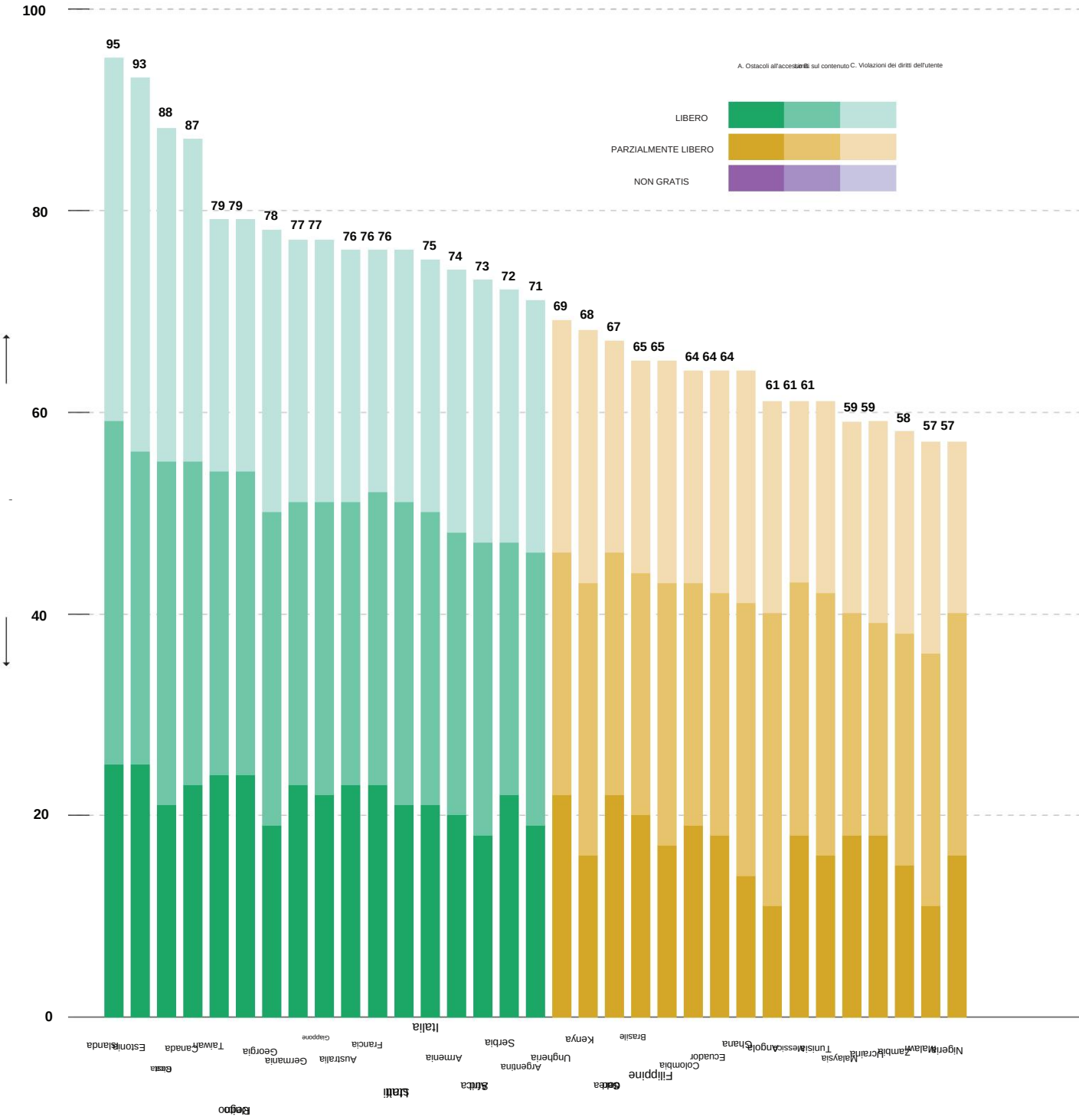


Stato	Paesi
LIBERO	17
PARZIALMENTE LIBERO	32
NON GRATIS	21
Totale	**70**

Per ulteriori informazioni sulla copertura geografica del rapporto, visitare freedomonthenet.org.

CLASSIFICHE GLOBALI

100 = Più libero 0 = Meno libero



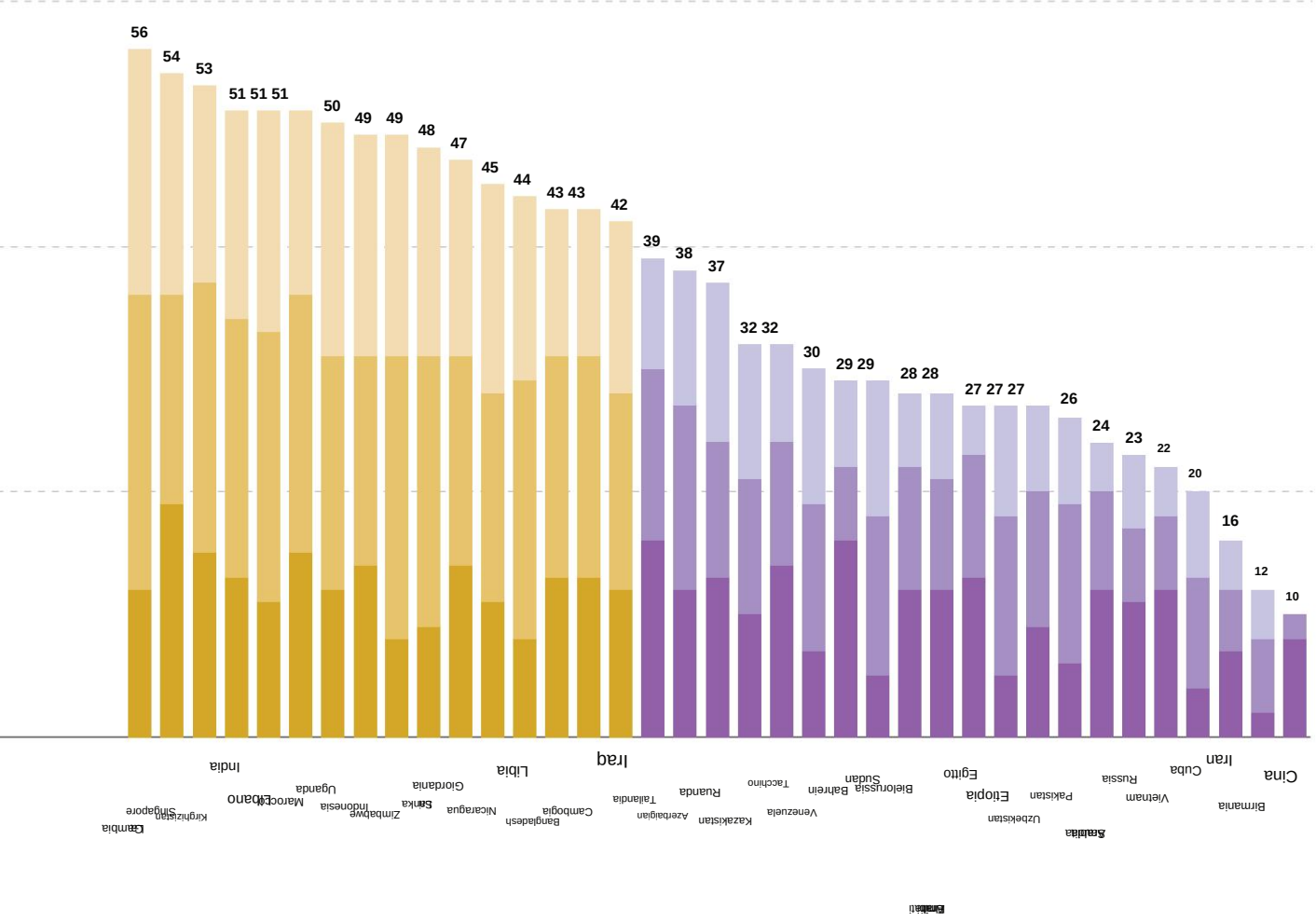
Freedom on the Net 2022 copre 70 paesi in 6 regioni del mondo. I paesi sono stati scelti per illustrare i miglioramenti e i cali della libertà di Internet in una varietà di sistemi politici. Ogni paese riceve un punteggio numerico da **100 (il più gratuito)** a **0 (il meno gratuito),** che funge da base per una designazione dello stato di libertà di Internet di **LIBERO (100-70 punti), PARZIALMENTE LIBERO (69-40 punti),** o **NON GRATIS (39-0 punti).**

Le valutazioni sono determinate attraverso un esame di tre grandi categorie:

A. OSTACOLI ALL'ACCESSO: Valuta le barriere infrastrutturali, economiche e politiche all'accesso; decisioni del governo di interrompere la connettività o bloccare applicazioni o tecnologie specifiche; controllo legale, normativo e di proprietà sui fornitori di servizi Internet; e indipendenza degli organismi di regolamentazione.

B. LIMITAZIONI SUI CONTENUTI: Esamina le normative legali sui contenuti; filtraggio tecnico e blocco dei siti web; altre forme di censura e autocensura; la vivacità e la diversità dell'ambiente online; e l'uso di strumenti digitali per la mobilitazione civica.

C. VIOLAZIONI DEI DIRITTI DEGLI UTENTI: specifica le protezioni legali e le restrizioni alla libertà di espressione; sorveglianza e privacy; e ripercussioni legali ed extralegali per le attività online, come procedimenti giudiziari, molestie extralegali e attacchi fisici o attacchi informatici.



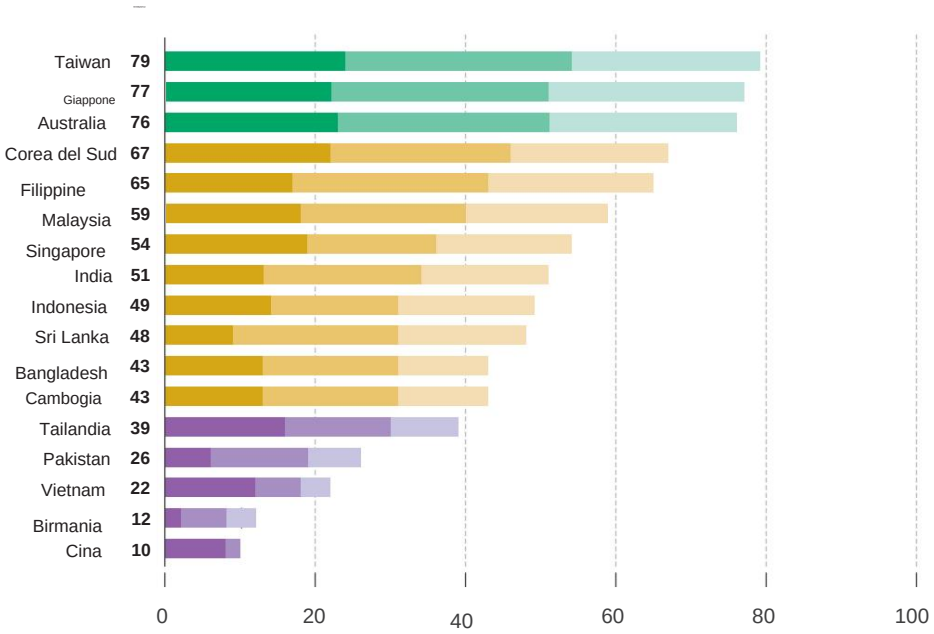
CLASSIFICHE REGIONALI

Libertà in rete 2022 copre 70 paesi in 6 regioni del mondo. I paesi sono stati scelti per illustrare internet miglioramenti e cali della libertà in una varietà di sistemi politici.

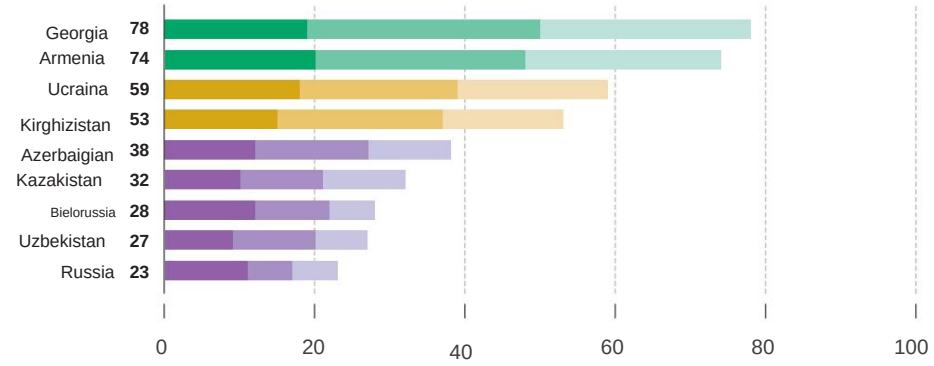
A. Ostacoli all'accesso
B. Limiti sul contenuto
C. Violazioni dei diritti dell'utente

0 = Meno libero
100 = Più gratuito

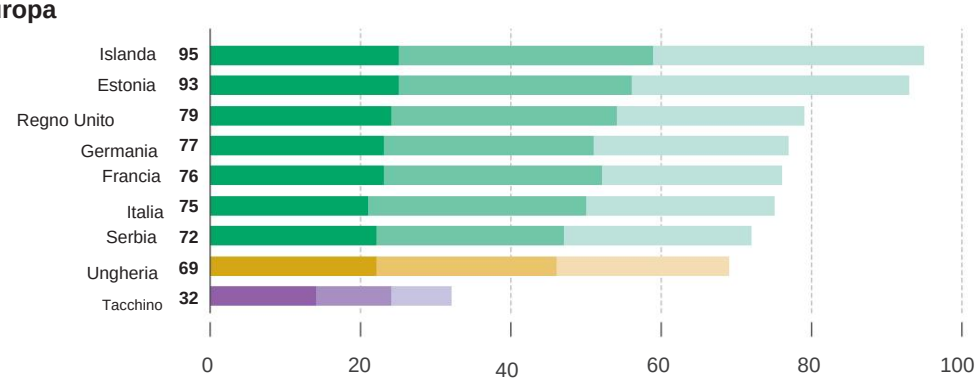
Asia-Pacifico



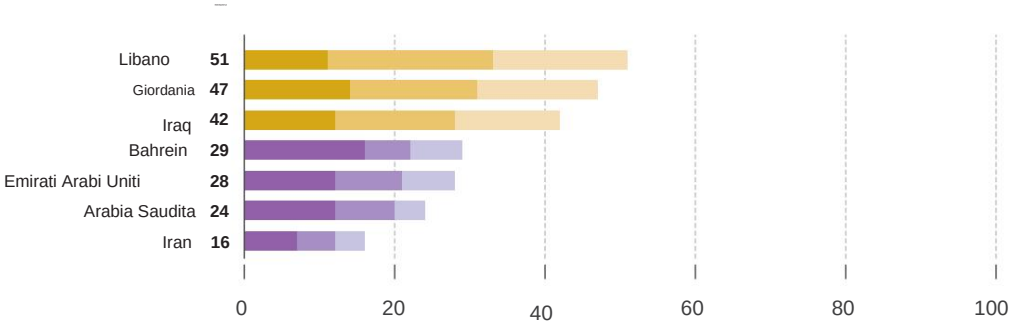
Eurasia



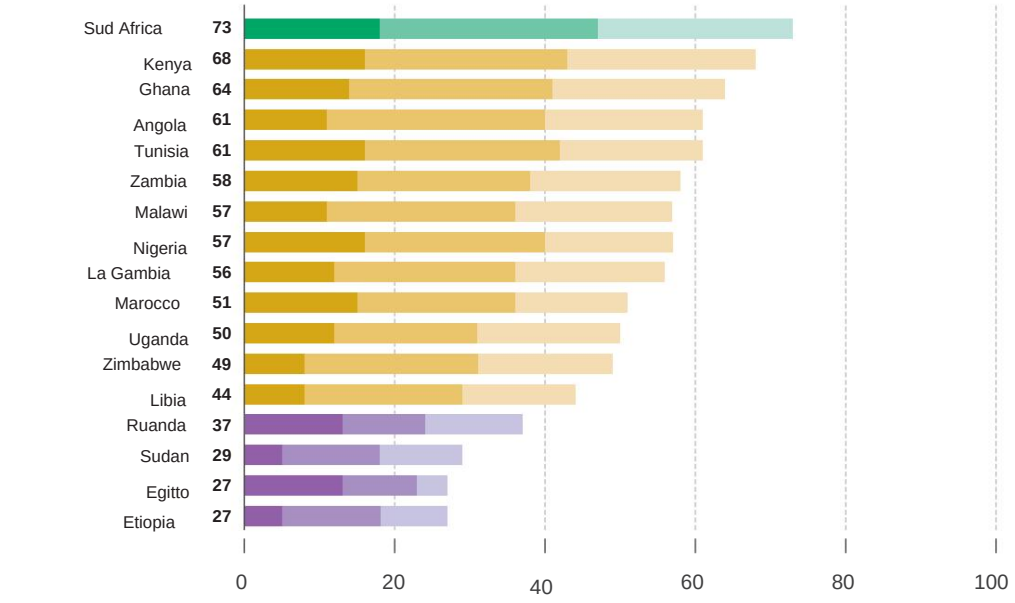
Europa



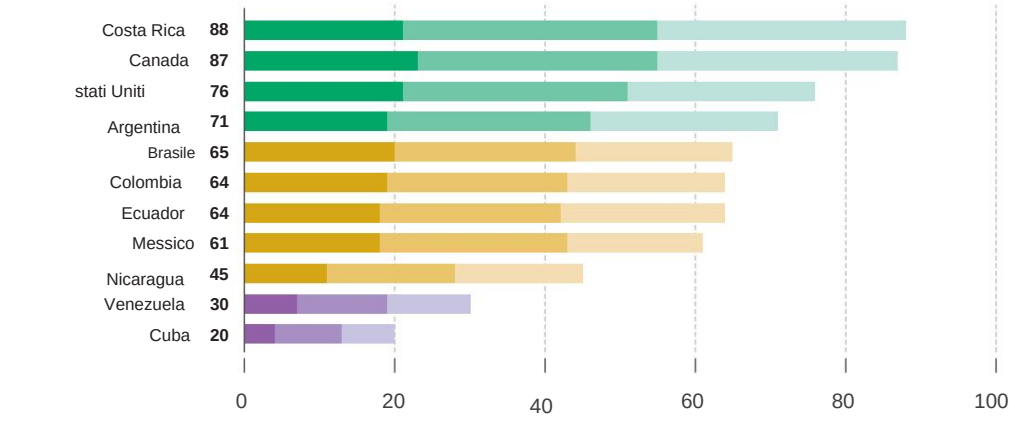
Medio Oriente



Africa



Americhe



Raccomandazioni

PER I POLITICI

Proteggi la privacy e la sicurezza **Regolamentare**

rigorosamente l'uso degli strumenti di sorveglianza e la raccolta di dati personali da parte del governo e delle forze dell'ordine. I programmi di sorveglianza del governo dovrebbero aderire ai principi internazionali sull'applicazione dei diritti umani alla sorveglianza delle comunicazioni, un quadro concordato da un ampio consorzio di gruppi della società civile, leader del settore e studiosi per proteggere i diritti degli utenti. I principi, che affermano che tutta la sorveglianza delle comunicazioni deve essere legale, necessaria e proporzionata, dovrebbero essere applicati anche alle tecnologie di sorveglianza biometrica e ai metodi di intelligence open source come il monitoraggio dei social media. Negli Stati Uniti, i legislatori dovrebbero riformare o abrogare le leggi e le pratiche di sorveglianza esistenti per allinearsi meglio a questi standard, compresi quelli ai sensi della Sezione 702 del Foreign Intelligence Surveillance Act (FISA) e dell'Executive Order 12333, e approvare il quarto emendamento bipartisan non è per Sale Act, che richiederebbe alle agenzie governative di ottenere un ordine del tribunale prima di acquistare dati dai data broker. I responsabili politici negli Stati Uniti dovrebbero anche indagare sulla misura in cui gli strumenti di sorveglianza commerciale, come lo spyware e la tecnologia di estrazione, sono stati utilizzati contro gli americani e garantire che siano messe in atto adeguate salvaguardie.

Proteggi la crittografia. Una crittografia solida è fondamentale per la sicurezza informatica, il commercio e la protezione dei diritti umani. L'indebolimento della crittografia mette in pericolo la vita di attivisti, giornalisti, membri di comunità emarginate e utenti ordinari in tutto il mondo. I governi dovrebbero astenersi dall'imporre l'introduzione di "backdoor", che richiedono la tracciabilità dei messaggi o riducono le protezioni di responsabilità degli intermediari per i fornitori di servizi di crittografia end-to-end. Negli Stati Uniti, qualsiasi riforma della Sezione 230 del Communications Decency Act non dovrebbe compromettere la capacità degli intermediari e dei fornitori di servizi di offrire una solida crittografia.

Rafforzare le protezioni della privacy dei dati promulgando regolamenti più severi e promulgando una legislazione completa. Le democrazie dovrebbero collaborare per creare regimi di privacy interoperabili che salvaguardino in modo completo le informazioni degli utenti, consentendo al contempo ai dati di fluire attraverso i confini verso giurisdizioni con livelli di protezione simili. Gli individui dovrebbero avere il controllo sulle proprie informazioni, incluso il diritto di accedervi, cancellarle e trasferirle facilmente ai fornitori di loro scelta. Le aziende dovrebbero essere tenute a limitare la raccolta di dati dei consumatori, in particolare informazioni intime come dati sanitari, biometrici e sulla posizione, divulgare in un linguaggio semplice come utilizzano i dati che raccolgono e limitare il modo in cui terze parti possono accedere e utilizzare questi dati. Le protezioni aggiornate sulla privacy dei dati dovrebbero includere disposizioni che forniscano a regolatori indipendenti e meccanismi di supervisione la capacità, le risorse e le competenze necessarie per far rispettare e garantire che le società straniere e nazionali rispettino le leggi sulla privacy, la non discriminazione e la protezione dei consumatori. Negli Stati Uniti, la Federal Trade Commission (FTC) ha avviato un'azione importante per rafforzare l'applicazione della privacy sotto le autorità esistenti emettendo un preavviso di regolamentazione proposta per valutare se sono necessarie protezioni più forti per quanto riguarda la sorveglianza commerciale e la sicurezza dei dati.
Nell'attuale assenza di una legge federale sulla privacy dei dati, la FTC dovrebbe emettere una norma finale che fornisca solide protezioni e faciliti l'applicazione. Anche negli Stati Uniti è necessaria una legislazione completa sulla privacy dei dati. La proposta dell'American Data Privacy and Protection Act (ADPPA), che istituirebbe un quadro completo che limiti i dati che possono essere raccolti dalle aziende, sarebbe un passo positivo. L'ADPPA sarebbe rafforzato chiarendo che gli stati sono liberi di approvare le proprie leggi più solide sulla protezione della privacy.

Limitare l'esportazione di tecnologia di censura e sorveglianza. Un fiorente mercato commerciale per le tecnologie di sorveglianza e censura ha dato ai governi una capacità ancora maggiore di violare lo stato di diritto, monitorare le comunicazioni private e limitare l'accesso alle risorse essenziali. Le democrazie dovrebbero porre limiti rigorosi alla vendita di tecnologie che consentono il monitoraggio, la sorveglianza, l'intercettazione o la raccolta di informazioni e comunicazioni, comprese le tecnologie che raccolgono e analizzano le informazioni biometriche (tra cui andatura, misurazioni facciali, voce e DNA, tra gli altri), spyware ,

tecnologia di estrazione dei dati e prodotti generici che forniscono la potenza di calcolo avanzata, l'apprendimento automatico, l'elaborazione del linguaggio naturale e le capacità di intelligenza artificiale che possono essere utilizzate per migliorare queste tecnologie. In un primo momento, il governo costaricano ha chiesto una moratoria globale sull'uso della tecnologia spyware nel 2022. Stati Uniti, Australia, Danimarca e Norvegia, sostenuti da Canada, Francia, Paesi Bassi e Regno Unito, hanno recentemente annunciato l'iniziativa per il controllo delle esportazioni e i diritti umani, intesa a "aiutare ad arginare l'ondata di uso improprio della tecnologia da parte del governo autoritario e promuovere una visione positiva per le tecnologie ancorate ai valori democratici". Gli Stati Uniti hanno inoltre aggiornato la loro politica di licenza per limitare l'esportazione di articoli se esiste "il rischio che gli articoli vengano utilizzati per violare o violare i diritti umani" e l'Unione Europea (UE) ha rafforzato i controlli sulle esportazioni per i prodotti a duplice uso e tecnologie di sorveglianza informatica. Nell'attuare tali nuove politiche, i funzionari governativi dovrebbero prestare maggiore attenzione all'idoneità delle esportazioni destinate ai paesi classificati come non liberi o parzialmente liberi da Freedom House, dove si verificano gli abusi di censura e sorveglianza più frequenti. Gli orientamenti governativi sulle esportazioni dovrebbero sollecitare le imprese ad aderire ai principi guida delle Nazioni Unite su imprese e diritti umani. Le imprese che esportano tecnologie di sorveglianza e censura che potrebbero essere utilizzate per commettere violazioni dei diritti umani dovrebbero essere tenute a riferire annualmente al pubblico sull'impatto delle loro esportazioni. I rapporti dovrebbero includere un elenco di paesi in cui hanno esportato tali tecnologie, potenziali preoccupazioni in materia di diritti umani in ciascuno di tali paesi, un riepilogo della dovuta diligenza pre-esportazione intrapresa per garantire che i loro prodotti non vengano utilizzati in modo improprio, violazioni dei diritti umani che si sono verificate di conseguenza dell'uso o del potenziale uso delle loro tecnologie e degli sforzi per mitigare il danno arrecato e prevenire futuri abusi. Negli Stati Uniti, il Congresso dovrebbe approvare il Foreign Advanced Technology Surveillance Accountability Act, che richiede al Dipartimento di Stato di includere informazioni sullo stato della sorveglianza e sull'uso della tecnologia avanzata nel suo rapporto annuale sulle pratiche globali in materia di diritti umani.

Salvaguardare la libertà di espressione, l'accesso alle informazioni e un ambiente online diversificato

Mantenere l'accesso ai servizi Internet, alle piattaforme digitali e alla tecnologia di elusione, in particolare durante le elezioni, le proteste e i periodi di conflitto. Le interruzioni intenzionali dell'accesso a Internet e dei servizi online hanno un impatto sui diritti economici, sociali, politici e civili degli individui. I governi dovrebbero evitare di bloccare o imporre onerosi requisiti normativi sugli strumenti di elusione e imporre divieti diretti o arbitrari sui social media e sulle piattaforme di messaggistica. Sebbene alcuni servizi possano presentare reali problemi di sicurezza sociale e nazionale, i divieti limitano indebitamente l'espressione dell'utente. I governi dovrebbero invece affrontare eventuali rischi legittimi posti dai social media e dalle piattaforme di messaggistica attraverso i meccanismi democratici esistenti, tra cui azioni normative, audit di sicurezza, controllo parlamentare e legislazione approvata in consultazione con la società civile e le parti interessate. Qualsiasi restrizione ai contenuti online dovrebbe aderire agli standard internazionali sui diritti umani di legalità, necessità e proporzionalità e includere una solida supervisione, trasparenza e consultazione con la società civile e il settore privato. Quando vengono imposte sanzioni, dovrebbe essere chiaro che i servizi di comunicazione Internet sono esentati per non limitare gli strumenti online essenziali per gli utenti nei paesi autoritari.

Racchiudere i principi dei diritti umani, la trasparenza e il controllo democratico nelle leggi che regolano i contenuti online. I quadri giuridici che trattano i contenuti online dovrebbero stabilire speciali obblighi orientati al tipo e alle dimensioni delle aziende, incentivare le piattaforme a migliorare i propri standard e richiedere la due diligence e la rendicontazione in materia di diritti umani. Tali requisiti dovrebbero dare priorità alla trasparenza tra i prodotti e le pratiche principali, tra cui la moderazione dei contenuti, i sistemi di raccomandazione e algoritmici, la raccolta e l'uso dei dati e le pratiche pubblicitarie politiche e mirate. Le leggi dovrebbero anche fornire opportunità ai ricercatori controllati di accedere ai dati della piattaforma, informazioni che possono fornire approfondimenti per lo sviluppo delle politiche e la ricerca e la difesa della società civile. Gli intermediari dovrebbero continuare a beneficiare di protezioni di sicurezza per la maggior parte dei contenuti generati dagli utenti e di terze parti che appaiono sulle loro piattaforme, in modo da non incoraggiare restrizioni che potrebbero inibire la libertà di espressione. Le leggi dovrebbero anche proteggere le regole del "buon samaritano" e riservare le decisioni sulla legalità dei contenuti alla magistratura piuttosto che alle società o alle agenzie esecutive. Gli utenti di Internet il cui account o contenuto è limitato o rimosso dovrebbero avere accesso ai sistemi di notifica, spiegazione, riparazione e ricorso. Organismi indipendenti e multilaterali e autorità di regolamentazione indipendenti con risorse e competenze sufficienti dovrebbero avere il potere di supervisionare l'attuazione delle leggi, condurre audit e garantire la conformità. Le disposizioni all'interno della legge sui servizi digitali dell'UE, in particolare le sue disposizioni sulla trasparenza, l'accessibilità dei dati per i ricercatori e una forma coregolatoria di applicazione, offrono un modello promettente per le leggi relative ai contenuti.

Supporta i media online e promuovi uno spazio informativo resiliente. La lotta alla disinformazione e alla propaganda inizia con l'accesso pubblico a informazioni affidabili e segnalazioni locali sul campo. Le democrazie dovrebbero intensificare gli sforzi per sostenere i media online indipendenti nei propri paesi e all'estero attraverso assistenza finanziaria e modelli di finanziamento innovativi, supporto tecnico e supporto allo sviluppo professionale. Dovrebbero associare questi sforzi a più ampie iniziative di educazione civica e formazione di alfabetizzazione digitale che aiutino le persone a navigare in ambienti multimediali complessi. Dovrebbero inoltre ampliare le protezioni per i giornalisti che affrontano attacchi fisici, rappresaglie legali e molestie per il loro lavoro online, anche sostenendo la creazione di visti di emergenza per le persone a rischio. Le leggi dovrebbero proteggere il libero flusso di informazioni, garantire ai giornalisti l'accesso a coloro che detengono il potere, consentire al pubblico di effettuare richieste di libertà di informazione e proteggersi dalla monopolizzazione statale dei media.

Integrare pienamente i principi dei diritti umani nell'applicazione della politica di concorrenza. Diversificare il mercato dei servizi online, in particolare attraverso la creazione di piattaforme più piccole che possono essere adattate alle esigenze di una particolare comunità o pubblico, è un passo fondamentale verso un ambiente informativo più resiliente. La concorrenza nel mercato digitale può anche incoraggiare le imprese a creare prodotti innovativi che tutelino i diritti fondamentali e affrontino danni online come le molestie. Quando applicano la politica della concorrenza, le autorità di regolamentazione dovrebbero considerare le implicazioni del dominio del mercato sulla libertà di espressione, sulla privacy, sulla non discriminazione e su altri diritti. I governi dovrebbero inoltre garantire che i quadri antitrust possano essere effettivamente applicati nell'era digitale e creare regimi giuridici che incentivino tale diversità, ad esempio introducendo disposizioni sull'interoperabilità e sulla portabilità dei dati come quelle contenute nella legge sui mercati digitali dell'UE.

Affrontare il divario digitale. L'accesso ineguale a Internet contribuisce alla disuguaglianza economica e sociale e compromette i vantaggi di un'Internet libera e aperta. A breve termine, i governi dovrebbero collaborare con i fornitori di servizi per sollevare i limiti di dati e rinunciare alle penali per ritardato pagamento; dovrebbero anche sostenere iniziative basate sulla comunità per fornire punti di accesso pubblico sicuri e prestare dispositivi elettronici a persone che ne hanno bisogno. Gli sforzi a lungo termine dovrebbero includere l'espansione dell'accesso e la costruzione di un'infrastruttura Internet per le aree e le popolazioni scarsamente servite, garantire che la connettività sia accessibile e adottare solide protezioni legali per la privacy degli utenti e la neutralità della rete.

Rafforzare la libertà globale di Internet

Garantire che la diplomazia informatica sia coordinata tra le democrazie e fondata sui diritti umani. Le democrazie dovrebbero facilitare il dialogo tra i responsabili politici e le autorità di regolamentazione nazionali per coordinarsi sulle migliori pratiche per la politica tecnologica e rafforzare l'impegno presso gli organismi internazionali di definizione degli standard. I diplomatici dovrebbero sviluppare approcci comuni per contrastare l'influenza autoritaria all'interno dell'Assemblea generale delle Nazioni Unite, dell'Unione internazionale delle telecomunicazioni (ITU) e di altri organismi multilaterali. Il processo decisionale multilaterale dovrebbe supportare e integrare, non sostituire, specifiche attività di governance di Internet e definizione degli standard da parte di organismi multilaterali come Internet Corporation for Assigned Names and Numbers (ICANN). Negli Stati Uniti c'è l'opportunità di istituzionalizzare e sostenere nuove iniziative e flussi di finanziamento incentrati sulla politica tecnologica globale e sulla libertà di Internet, in particolare quelli annunciati al vertice inaugurale per la democrazia. Il nuovo Bureau of Cyberspace and Digital Policy del Dipartimento di Stato dovrebbe fare dei diritti umani una componente centrale del suo mandato, anche garantendo che il personale abbia competenze pertinenti e coordinandosi strettamente con altri dipartimenti incentrati su Internet all'interno e tra le agenzie. Questi sforzi dovrebbero anche formalizzare un impegno regolare e continuo con la società civile e il settore privato.

Rafforzare la capacità della Freedom Online Coalition di proteggere la libertà di Internet. In qualità di prossimo presidente del 2023, gli Stati Uniti dovrebbero concentrarsi sul rafforzamento del riconoscimento del nome del FOC e sulla sua capacità di guidare il coordinamento diplomatico e l'azione globale. Ciò include articolare in modo più proattivo i vantaggi di un Internet libero e aperto ai governi, essere più pubblicamente e privatamente espliciti sulle minacce e le opportunità per i diritti umani online, integrare l'attività FOC in altre iniziative multilaterali come l'ITU e il Gruppo dei 7 (G7), e creare più strade per impegnarsi con la società civile e il settore privato, anche attraverso la diversificazione e l'espansione della rete di consulenza della coalizione. Il FOC dovrebbe prendere in considerazione l'aumento del personale interno per raggiungere questi obiettivi e la creazione di un meccanismo interno mediante il quale le attività degli Stati membri possano essere valutate per garantire che siano in linea con i principi del FOC. Un nuovo meccanismo di finanziamento, sostenuto dagli Stati membri, per programmi e attività

guidato da parti interessate non statali potrebbe anche far avanzare le priorità FOC. Qualsiasi espansione dei membri della coalizione dovrebbe essere effettuata in consultazione con la rete consultiva e i nuovi membri dovrebbero essere selezionati in base alla loro capacità di rafforzare il lavoro del FOC e contribuire a una maggiore diversità geografica all'interno del corpo.

Difendere ed espandere la programmazione della libertà di Internet come componente vitale dell'assistenza alla democrazia. L'assistenza alla democrazia mirata alle attività per la libertà di Internet dovrebbe dare la priorità alla sicurezza digitale e ai corsi di formazione sull'attivismo digitale, nonché alla fornitura di software in grado di proteggere o assistere gli utenti. I responsabili politici dovrebbero sostenere programmi che cercano di rafforzare l'indipendenza giudiziaria, migliorare l'alfabetizzazione tecnica tra i giudici e altri all'interno del sistema legale e fornire altre risorse finanziarie e amministrative per il contenzioso strategico. I governi dovrebbero aumentare il supporto per le tecnologie che aiutano le persone in ambienti chiusi a eludere la censura del governo, proteggersi dalla sorveglianza e superare le restrizioni sulla connettività. Tali strumenti dovrebbero essere open source, di facile utilizzo e reattivi a livello locale al fine di garantire elevati livelli di sicurezza e utilizzo. Infine, la programmazione dovrebbe sostenere gli sforzi volti a rafforzare l'indipendenza e la competenza delle autorità di regolamentazione, che possono fungere da organismi politicamente neutrali che proteggono la libertà di Internet durante i cambiamenti nella leadership politica.

Sostenere il rilascio immediato e incondizionato di coloro che sono stati imprigionati per l'espressione online protetta dagli standard internazionali. I governi dovrebbero incorporare questi casi, oltre alle più ampie preoccupazioni sulla libertà di Internet, nell'impegno bilaterale e multilaterale con i paesi autori. Dovrebbe diventare una pratica standard elevare i nomi delle persone detenute per i loro contenuti online, richiedere informazioni o azioni specifiche relative al loro trattamento e chiedere il loro rilascio e l'abrogazione delle leggi che criminalizzano l'espressione online.

PER LE AZIENDE

Garantire una moderazione dei contenuti equa e trasparente. Per garantire politiche di moderazione dei contenuti rispettose degli utenti, le aziende private dovrebbero:

- Dare priorità alla libera espressione degli utenti e all'accesso alle informazioni, in particolare per il giornalismo; discussione sui diritti umani; educativo materiali; ed espressione politica, sociale, culturale, religiosa e artistica.
- Spiegare in modo chiaro e completo nelle linee guida e nei termini di servizio quali discorsi non sono consentiti, quali sono le restrizioni mirate servire e in che modo il contenuto viene valutato per le violazioni. Un passo essenziale è garantire che i termini di servizio, così come i meccanismi per segnalare contenuti dannosi e decisioni sui contenuti accattivanti, siano tradotti in tutte le lingue in cui vengono utilizzati i prodotti dell'azienda.
- Se del caso, prendere in considerazione alternative meno invasive alla rimozione dei contenuti, come la retrocessione dei contenuti, l'etichettatura, il fact-checking, promuovere fonti più autorevoli e implementare modifiche al design che migliorino le discussioni civiche.
- Pubblicare rapporti di trasparenza dettagliati sulle rimozioni di contenuti, sia per quelle avviate dai governi che per quelle intraprese dalle aziende. I rapporti sulla trasparenza dovrebbero anche affrontare il modo in cui l'apprendimento automatico viene utilizzato per addestrare sistemi automatizzati che classificano, consigliano e danno priorità ai contenuti per la revisione umana.
- Fornire una via di ricorso efficiente e tempestiva per gli utenti che ritengono che i loro diritti siano stati indebitamente limitati, anche attraverso censura, divieto, assegnazione di etichette o demonetizzazione dei post.
- Astenersi dall'affidarsi a sistemi automatizzati per la rimozione di contenuti senza possibilità di revisione umana significativa.
- Espandere la capacità, la diversità geografica e linguistica dei team di moderazione dei contenuti e assicurarsi che siano sensibili a sfumature in una lingua parlata in più paesi o regioni. Condurre valutazioni di due diligence sui diritti umani per garantire che l'attuazione della moderazione non porti a conseguenze indesiderate, come un impatto sproporzionato sulle comunità emarginate.

Resistere agli ordini del governo di interrompere la connettività Internet, vietare i servizi digitali e consegnare indebitamente i dati o limitare gli account e i contenuti degli utenti. I fornitori di servizi dovrebbero utilizzare tutti i canali legali disponibili per contestare tali richieste da parte delle agenzie statali, siano esse ufficiali o informali, in particolare quelle relative a difensori dei diritti umani, attivisti, società civile, giornalisti o altri account a rischio. Se le aziende non possono resistere completamente alle richieste, dovrebbero garantire che eventuali restrizioni o interruzioni siano il più limitate possibile in termini di durata, ambito geografico e tipo di contenuto interessato. Le aziende dovrebbero documentare accuratamente le richieste del governo internamente e informare gli utenti sul motivo per cui la connettività o il loro contenuto potrebbero essere limitati, specialmente nei paesi in cui le azioni del governo mancano di trasparenza. Di fronte a una scelta tra il divieto dei loro servizi e il rispetto di richieste indebite di dati e ordini di censura, le aziende dovrebbero portare avanti casi legali strategici che sfidano l'eccessiva portata del governo, in consultazione o in collaborazione con la società civile.

Aderire ai principi guida delle Nazioni Unite su imprese e diritti umani, adottare i principi della Global Network Initiative sulla libertà di espressione e sulla privacy e condurre valutazioni dell'impatto sui diritti umani. Le aziende dovrebbero impegnarsi a rispettare i diritti dei loro utenti e ad affrontare qualsiasi impatto negativo che i loro prodotti potrebbero avere sui diritti umani.
I principi della Global Network Initiative fornire indicazioni concrete su come farlo. Le aziende dovrebbero investire ed espandere programmi e strumenti che consentano agli utenti, in particolare ai difensori dei diritti umani, ai giornalisti e a coloro che appartengono a popolazioni a rischio, di proteggersi facilmente dai danni online e offline, in particolare durante gli eventi di crisi. Le aziende dovrebbero inoltre ridurre al minimo la quantità di dati che raccolgono, vendono e utilizzano e comunicano chiaramente agli utenti quali dati vengono raccolti e per quale scopo. Laddove le aziende operano, dovrebbero condurre e pubblicare valutazioni periodiche per comprendere appieno in che modo i loro prodotti e le loro azioni potrebbero influire sui diritti, tra cui la libertà di espressione, la non discriminazione e la privacy.

Rafforzare i principi dei diritti umani nella progettazione e nello sviluppo del prodotto. La protezione dei diritti online inizia con la progettazione e lo sviluppo responsabile del prodotto. I tecnologi e gli ingegneri dovrebbero essere formati sulle implicazioni per i diritti umani dei prodotti che costruiscono e sulle migliori pratiche internazionali per prevenirne gli abusi. Le aziende dovrebbero condurre ricerche e consultarsi con le comunità colpite per comprendere i modi in cui i loro prodotti possono essere utilizzati per perpetrare danni online e offline e rispondere con forti barriere che diano priorità alla sicurezza. Quando si scopre che un prodotto è stato utilizzato per violazioni dei diritti umani, le aziende dovrebbero sospendere le vendite alla parte responsabile e sviluppare un piano d'azione immediato per mitigare i danni e prevenire ulteriori abusi. Le aziende dovrebbero inoltre supportare l'accessibilità della tecnologia di elusione, integrare la crittografia end-to-end nei loro prodotti e garantire altri solidi protocolli di sicurezza, anche resistendo alle richieste del governo di fornire un accesso speciale alla decrittazione.

Impegnarsi in un dialogo continuo con la società civile per comprendere gli effetti delle politiche e dei prodotti aziendali.
Le aziende dovrebbero cercare competenze locali sul contesto politico e culturale nei mercati in cui sono presenti o in cui i loro prodotti sono ampiamente utilizzati, specialmente in contesti repressivi a causa di serie uniche di sfide sui diritti umani che richiedono soluzioni specifiche per il contesto. Le consultazioni con i gruppi della società civile dovrebbero informare se le aziende scelgono di operare in un determinato paese, l'approccio delle aziende alla moderazione dei contenuti, lo sviluppo di prodotti e politiche, in particolare durante le elezioni o gli eventi di crisi, quando si gestiscono le richieste del governo e quando si lavora per contrastare l'online danneggia.

Metodologia

COSA MISURIAMO

L' indice *Freedom on the Net* misura il livello di libertà di Internet di ciascun paese sulla base di una serie di domande metodologiche. La metodologia è sviluppata in consultazione con esperti internazionali per catturare la vasta gamma di questioni rilevanti per i diritti umani online (vedi "Lista di controllo delle domande").

I valori fondamentali *di Freedom on the Net* si basano sugli standard internazionali sui diritti umani, in particolare sull'articolo 19 della Dichiarazione universale dei diritti umani. Il progetto si concentra in particolare sul libero flusso di informazioni, la protezione della libertà di espressione, l'accesso alle informazioni, i diritti alla privacy e la libertà dalle ripercussioni sia legali che extralegali derivanti dalle attività online.
Il progetto valuta anche fino a che punto un ambiente online che abilita i diritti viene promosso in un determinato paese.

L'indice riconosce che alcuni diritti possono essere legittimamente limitati. Lo standard di tali restrizioni all'interno della metodologia e del punteggio è in linea con i principi internazionali di necessità e proporzionalità dei diritti umani, lo stato di diritto e altre salvaguardie democratiche. Le politiche e le procedure di censura e sorveglianza dovrebbero essere trasparenti, minime e includere vie di ricorso disponibili per le persone colpite, tra le altre garanzie.

Il progetto valuta i diritti e le libertà reali di cui godono gli individui all'interno di ciascun paese. Sebbene la libertà di Internet possa essere principalmente influenzata dal comportamento dello stato, vengono prese in considerazione anche le azioni di attori non statali, comprese le società tecnologiche. Pertanto, le valutazioni dell'indice generalmente riflettono l'interazione di una varietà di attori, sia governativi che non governativi. Nel corso degli anni, *Freedom on the Net* è stato continuamente adattato per catturare i progressi tecnologici, le mutevoli tattiche di repressione e le minacce emergenti alla libertà di Internet.

IL PROCESSO DI RICERCA E PUNTEGGIO

La metodologia comprende 21 domande e quasi 100 sottodomande, suddivise in tre categorie:

1. **Ostacoli all'accesso** specifica le barriere infrastrutturali, economiche e politiche all'accesso; decisioni del governo di interrompere la connettività o bloccare applicazioni o tecnologie specifiche; controllo legale, normativo e di proprietà sui fornitori di servizi Internet; e l'indipendenza degli organismi di regolamentazione;

2. **Limitazioni sui contenuti** analizza le normative legali sui contenuti; filtraggio tecnico e blocco dei siti web; altre forme di censura e autocensura; la vivacità e la diversità dello spazio informativo online; e l'uso di strumenti digitali per la mobilitazione civica;

3. **Violazioni dei diritti degli utenti** affronta le tutele legali e le restrizioni alla libertà di espressione; sorveglianza e riservatezza; e ripercussioni legali ed extralegali per discorsi e attività online, come reclusione, attacchi informatici o molestie extralegali e violenza fisica.

Ogni domanda è segnata su una gamma variabile di punti. Le sottodomande guidano i ricercatori riguardo ai fattori che dovrebbero considerare durante la valutazione e l'assegnazione dei punti, sebbene non tutte si applichino a tutti i paesi. Per ogni domanda, viene assegnato un numero maggiore di punti per una situazione più libera, mentre un numero inferiore di punti viene assegnato per un ambiente meno libero. I punti si sommano per produrre un punteggio per ciascuna delle sottocategorie e i punti totali di un paese per tutte e tre rappresentano il suo punteggio finale (0-100). In base al punteggio, Freedom House assegna le seguenti valutazioni sulla libertà di Internet:

• Punteggi 100-70 = Libero •
Punteggi 69-40 = Parzialmente libero
• Punteggi 39-0 = Non libero

Lo staff di Freedom House invita almeno un ricercatore o un'organizzazione a fungere da autore del rapporto per ciascun paese, addestrandoli a valutare gli sviluppi della libertà di Internet secondo la metodologia di ricerca completa del progetto. I ricercatori inviano bozze di rapporti nazionali e partecipano a una riunione di revisione delle valutazioni incentrata sulla loro regione. Durante gli incontri, i partecipanti rivedono, criticano e aggiustano le bozze dei punteggi, sulla base di linee guida di codifica stabilite, attraverso un'attenta considerazione di eventi, leggi e pratiche rilevanti per ciascun elemento. Dopo aver completato le consultazioni regionali e nazionali, lo staff di Freedom House modifica e controlla tutti i rapporti nazionali ed esegue una revisione finale di tutti i punteggi per garantirne l'affidabilità e l'integrità comparativa.
Lo staff di Freedom House conduce anche solide analisi qualitative su ogni paese per determinare i principali risultati globali di ogni anno e le tendenze emergenti.

Lista di controllo delle domande

• Ogni paese è valutato su una scala da 100 a 0, dove 100 rappresenta le condizioni più libere e 0 le meno libere. • Un punteggio combinato di 100-70 = gratuito, 69-40 = parzialmente gratuito e 39-0 = non gratuito.

A. OSTACOLI *ALL'ACCESSO (0-25 PUNTI)*

1. Le limitazioni infrastrutturali limitano l'accesso a Internet o la velocità e la qualità delle connessioni Internet?
(0–6 punti) •
Le persone hanno accesso a servizi Internet ad alta velocità a casa, sul posto di lavoro, negli internet café, nelle biblioteche, scuole e altri luoghi, oltre che sui dispositivi mobili?
• Infrastrutture scadenti (inclusa elettricità inaffidabile) o danni catastrofici alle infrastrutture (causati da eventi come disastri naturali o conflitti armati) limitano la capacità dei residenti di accedere a Internet?

2. L'accesso a Internet è proibitivo o è fuori dalla portata di determinati segmenti della popolazione per motivi geografici, sociali o di altro tipo? *(0–3 punti)* • I vincoli finanziari, come i prezzi elevati per i servizi Internet, le tasse eccessive imposte su tali servizi o la manipolazione statale dei mercati rilevanti, rendono l'accesso a Internet proibitivo per ampi segmenti della popolazione?

• Esistono differenze significative nella penetrazione e nell'accesso a Internet in base all'area geografica, o per determinate etnie, religiosi, di genere, LGBT+, migranti e altri gruppi rilevanti?
• Le pratiche tariffarie, come i piani a tariffazione zero, da parte dei fornitori di servizi e delle piattaforme digitali contribuiscono a creare un divario digitale in termini di quali tipi di contenuti possono accedere le persone con mezzi finanziari diversi?

3. Il governo esercita un controllo tecnico o legale sull'infrastruttura Internet ai fini di limitare la connettività? *(0–6 punti)* • Il governo limita o obbliga i fornitori di servizi a limitare la connettività Internet rallentando o interrompendo le connessioni Internet durante eventi specifici (come proteste o elezioni), a livello locale o nazionale? • Il governo centralizza l'infrastruttura Internet in modo da facilitare le restrizioni sulla connettività? • Il governo blocca o obbliga i fornitori di servizi a bloccare le piattaforme dei social media e le app di comunicazione che fungono in pratica da importanti canali per l'informazione online?

- Il governo blocca o obbliga i fornitori di servizi a bloccare determinati protocolli, porte e funzionalità all'interno di tali piattaforme e app (ad es. protocollo Voice-over-Internet o VoIP, streaming video, messaggistica multimediale, Secure Sockets Layer o SSL) , in modo permanente o durante eventi specifici?
- Le restrizioni alla connettività colpiscono in modo sproporzionato le comunità emarginate, come gli abitanti di determinate regioni o coloro che appartengono a diversi gruppi etnici, religiosi, di genere, LGBT+, migranti e altri gruppi rilevanti?

4. Esistono ostacoli legali, normativi o economici che limitano la diversità dei fornitori di servizi? *(0–6 punti)* • Esiste un monopolio legale o di fatto sulla fornitura di accesso a Internet fisso, mobile e pubblico? • Lo stato pone ampi requisiti legali, normativi o economici per l'istituzione o il funzionamento di fornitori di servizi?

- I requisiti di licenza, come la conservazione dei dati dei clienti o l'impedimento dell'accesso a determinati contenuti, rappresentano un onere onere finanziario per i fornitori di servizi?

5. Gli organismi di regolamentazione nazionali che sovrintendono ai fornitori di servizi e alla tecnologia digitale non operano in modo libero, modo giusto e indipendente? *(0–4 punti)* • Esistono garanzie legali esplicite che proteggono l'indipendenza e l'autonomia di qualsiasi organismo di regolamentazione che sovrintende a Internet (esclusivamente o come parte di un mandato più ampio) da interferenze politiche o commerciali? • Il processo di nomina dei membri degli organismi di regolamentazione è trasparente e rappresentativo delle diverse parti interessate? interessi legittimi?

- Le decisioni prese dagli organismi di regolamentazione sono considerate eque e tengono conto in modo significativo dei commenti delle parti interessate nella società? • Le decisioni prese dagli organismi di regolamentazione sono considerate apolitiche e indipendenti dai cambiamenti di governo? • Si ritiene che le decisioni prese dagli organismi di regolamentazione proteggano la libertà di Internet, anche garantendo il servizio fornitori, piattaforme digitali e altri host di contenuti si comportano in modo corretto?

B. LIMITI AI CONTENUTI *(0-35 PUNTI)*

1. Lo stato blocca o filtra, o obbliga i fornitori di servizi a bloccare o filtrare, in particolare i contenuti Internet materiale protetto dalle norme internazionali sui diritti umani? *(0–6 punti)* • Lo Stato utilizza o obbliga i fornitori di servizi a utilizzare mezzi tecnici per limitare la libertà di opinione e espressione, ad esempio bloccando o filtrando siti Web e contenuti online che trattano giornalismo, discussioni sui diritti umani, materiali educativi o espressioni politiche, sociali, culturali, religiose e artistiche?

- Lo stato utilizza, o obbliga i fornitori di servizi a utilizzare, mezzi tecnici per bloccare o filtrare l'accesso a siti web che possono essere socialmente o legalmente problematici (ad es. quelli relativi al gioco d'azzardo, alla pornografia, alle violazioni del copyright, alle droghe illegali) invece di metodi più rimedi o in un modo che infligga danni collaterali a contenuti e attività protetti dagli standard internazionali sui diritti umani?
- Lo Stato blocca o ordina il blocco di intere piattaforme di social media, app di comunicazione, blog piattaforme di hosting, forum di discussione e altri domini Web allo scopo di censurare il contenuto che appare su di essi? • C'è il blocco degli strumenti che consentono agli utenti di aggirare la censura? • Lo stato procura, o obbliga i fornitori di servizi a procurarsi, tecnologia avanzata per automatizzare la censura o ampliarne la portata?

2. Gli attori statali o non statali impiegano mezzi legali, amministrativi o di altro tipo per costringere gli editori, gli host di contenuti o le piattaforme digitali a eliminare i contenuti, in particolare il materiale protetto dagli standard internazionali sui diritti umani? *(0-4 punti)* • Vengono utilizzate misure amministrative, giudiziarie o extralegali per ordinare la cancellazione di contenuti da Internet, in particolare giornalismo, discussione sui diritti umani, materiale educativo o espressione politica, sociale, culturale, religiosa e artistica, prima o dopo la sua pubblicazione?

- Le piattaforme digitali e gli host di contenuti rimuovono arbitrariamente tali contenuti a causa di pressioni formali o informali da parte di funzionari governativi o altri potenti attori politici?
- I fornitori di accesso, gli host di contenuti e le terze parti sono esenti da responsabilità legale eccessiva o impropria per le opinioni espresse da terze parti trasmesse tramite la tecnologia che forniscono?

3. Le restrizioni su Internet e sui contenuti digitali mancano di trasparenza, proporzionalità rispetto agli obiettivi dichiarati o un processo di ricorso indipendente? *(0–4 punti)* • Esistono leggi nazionali, organi di controllo indipendenti e altre procedure democraticamente responsabili per garantire che le decisioni di limitare l'accesso a determinati contenuti siano proporzionate al loro obiettivo dichiarato? • Sono quelli che limitano i contenuti, tra cui autorità statali, ISP, host di contenuti, piattaforme digitali e altro intermediari: trasparenti su quali contenuti vengono bloccati o eliminati, anche al pubblico e direttamente all'utente interessato?

- Esistono vie di ricorso efficienti e tempestive per coloro che scoprono che i contenuti da loro prodotti sono stati sottoposti alla censura?
- I meccanismi di autoregolamentazione e gli organi di controllo sono efficaci nel garantire la protezione dei contenuti a livello internazionale le norme sui diritti umani non vengono rimosse?

4. I giornalisti online, i commentatori e gli utenti ordinari praticano l'autocensura? *(0–4 punti)*

- Gli utenti di Internet nel paese praticano l'autocensura su importanti questioni politiche, sociali o religiose, tra cui nei forum pubblici e nelle comunicazioni private? • Il timore di ritorsioni, censura, sorveglianza statale o pratiche di raccolta dati ha un effetto dissuasivo sul discorso online o induce gli utenti a evitare determinate attività online di natura civica?
- Laddove esiste un'autocensura diffusa, alcuni giornalisti, commentatori o utenti ordinari continuano a testare il confini, nonostante le potenziali ripercussioni?

5. Le fonti di informazioni online sono controllate o manipolate dal governo o da altri attori potenti per promuovere un particolare interesse politico? *(0–4 punti)* • I leader politici, le agenzie governative, i partiti politici o altri attori potenti manipolano direttamente le informazioni tramite testate giornalistiche statali, account/gruppi di social media ufficiali o altri canali formali?

- Funzionari governativi o altri attori impiegano o incoraggiano surrettiziamente individui o sistemi automatizzati per amplificare artificialmente narrazioni politiche o campagne diffamatorie sui social media? • Funzionari governativi o altri potenti attori esercitano pressioni o costringono i notiziari online, i giornalisti oi blogger a seguire una particolare direzione editoriale nei loro reportage e commenti? • Le autorità emanano linee guida o direttive ufficiali sulla copertura dei media online, comprese le istruzioni per minimizzare o amplificare alcuni commenti o argomenti di discussione?
- I funzionari governativi o altri attori corrompono o utilizzano stretti legami economici con giornalisti online, blogger o siti web proprietari al fine di influenzare i contenuti che producono o ospitano?
- La disinformazione, coordinata da attori stranieri o nazionali per scopi politici, ha un impatto significativo su dibattito pubblico?

6. Esistono vincoli economici, normativi o di altro tipo che influiscono negativamente sulla capacità degli utenti di pubblicare contenuti in linea? *(0–3 punti)* •

Sono necessarie connessioni informali favorevoli con funzionari governativi affinché i media online, gli host di contenuti o le piattaforme digitali (ad es. motori di ricerca, applicazioni di posta elettronica, piattaforme di hosting di blog) siano economicamente sostenibili? • Lo stato limita la capacità dei media online di accettare pubblicità o investimenti, in particolare da fonti estere, o scoraggia gli inserzionisti dal condurre affari con media online o fornitori di servizi sfavorevoli?

• Tasse, normative o diritti di licenza onerosi rappresentano un ostacolo alla partecipazione, costituzione o gestione di piattaforme digitali, testate giornalistiche, blog o gruppi/canali di social media? • Gli ISP gestiscono il traffico di rete e la disponibilità della larghezza di banda in modo trasparente, applicato uniformemente e non discriminano gli utenti o i produttori di contenuti in base alla natura o alla fonte dei contenuti stessi (ovvero, rispettano la "neutralità della rete" per quanto riguarda il contenuto)?

7. Il panorama dell'informazione online manca di diversità e affidabilità? *(0–4 punti)*

• Le persone sono in grado di accedere a una gamma di fonti di notizie locali, regionali e internazionali che trasmettono informazioni indipendenti, pareri equilibrati nelle principali lingue parlate nel paese?

• I media online, le pagine dei social media, i blog e i siti web rappresentano interessi, esperienze e lingue all'interno della società, ad esempio fornendo contenuti prodotti da diversi gruppi etnici, religiosi, di genere, LGBT+, migranti e altri gruppi pertinenti? • La mancanza di concorrenza tra host di contenuti e piattaforme digitali limita la capacità degli utenti di pubblicare contenuti online? • La presenza di disinformazione compromette la capacità degli utenti di accedere a fonti indipendenti, credibili e diversificate di informazione?

• I contenuti online falsi o fuorvianti contribuiscono in modo significativo a danni offline, come molestie o proprietà distruzione, violenza fisica o morte?

• In caso di censura estesa, gli utenti utilizzano reti private virtuali (VPN) e altri strumenti di elusione per accedere a una gamma più ampia di fonti di informazioni?

8. Le condizioni impediscono agli utenti di formare comunità, mobilitarsi e fare campagne, in particolare su questioni politiche e sociali? *(0-6 punti)* • Le persone possono unirsi liberamente a comunità online basate sulla loro identità politica, sociale o culturale, anche senza paura di ritorsioni?

• Le organizzazioni della società civile, gli attivisti e le comunità online si organizzano online su questioni politiche, sociali, culturali e questioni economiche, anche durante le campagne elettorali e le proteste nonviolente, anche senza timore di ritorsioni?

• Lo stato o altri attori limitano l'accesso a strumenti e siti web online (ad es. piattaforme di social media, gruppi di messaggistica, siti web di petizioni) allo scopo di limitare la libertà di riunione e associazione online? • Lo stato impone restrizioni legali o di altro tipo (ad es. disposizioni penali, detenzioni, sorveglianza) allo scopo di limitare la libertà di riunione e associazione online?

C. VIOLAZIONI DEI DIRITTI DELL'UTENTE *(0-40 PUNTI)*

1. La costituzione o altre leggi non tutelano diritti come la libertà di espressione, l'accesso alle informazioni e la libertà di stampa, anche su Internet, e sono applicate da un sistema giudiziario privo di indipendenza? *(0–6 punti)* • La costituzione contiene un linguaggio che prevede la libertà di espressione, l'accesso alle informazioni e la stampa libertà in generale? •

Esistono leggi o decisioni legali vincolanti che proteggono in modo specifico le modalità di espressione online? • Le autorità esecutive, legislative e altre autorità governative rispettano queste decisioni legali e queste decisioni vengono effettivamente applicate? • Ai giornalisti e ai blogger online sono concessi forti diritti e tutele per svolgere il proprio lavoro? • La magistratura è indipendente e gli alti organi giudiziari e funzionari sostengono la libertà di espressione, l'accesso alle informazioni e la libertà di stampa online?

2. Esistono leggi che assegnano sanzioni penali o responsabilità civile per le attività online, in particolare quelle che lo sono protetto dagli standard internazionali sui diritti umani? *(0-4 punti)* • Fare leggi specifiche, compresi i codici penali e quelli relativi ai media, alla diffamazione, alla criminalità informatica, alla sicurezza informatica e terrorismo: criminalizza l'espressione e le attività online protette dagli standard internazionali sui diritti umani (ad es. giornalismo, discussioni sui diritti umani, materiali educativi o espressioni politiche, sociali, culturali, religiose e artistiche)?

• Le restrizioni alla libertà di Internet sono definite dalla legge, strettamente circoscritte e necessarie e proporzionate per perseguire uno scopo legittimo?

3. Le persone sono penalizzate per le attività online, in particolare quelle che sono protette dalla protezione umana internazionale norme sui diritti? *(0-6 punti)* • Scrittori, commentatori, blogger o utenti di social media sono soggetti a responsabilità civile, reclusione, detenzione arbitraria, irruzioni della polizia o altre sanzioni legali per la pubblicazione, la condivisione o l'accesso a materiale su Internet in violazione delle norme internazionali norme sui diritti umani?

• Sono sanzioni per diffamazione; diffondere informazioni false o “fake news”; sicurezza informatica, sicurezza nazionale, terrorismo ed estremismo; bestemmia; insultare istituzioni e funzionari statali; o danneggiare le relazioni estere applicate inutilmente e in modo sproporzionato?

4. Il governo impone restrizioni alla comunicazione anonima o alla crittografia? *(0–4 punti)* • I proprietari di siti web, i blogger o gli utenti in generale sono tenuti a registrarsi presso il governo? • Il governo richiede che le persone utilizzino i loro veri nomi o si registrino presso le autorità quando pubblicano messaggi commenti o l'acquisto di dispositivi elettronici, come i telefoni cellulari?

• Agli utenti è vietato utilizzare i servizi di crittografia per proteggere le proprie comunicazioni? • Esistono leggi che impongono agli utenti o ai fornitori di servizi di crittografia di consegnare le chiavi di decrittazione al governo?

5. La sorveglianza statale delle attività su Internet viola il diritto alla privacy degli utenti? *(0-6 punti)*

• La costituzione, leggi specifiche o decisioni legali vincolanti proteggono dall'intrusione del governo nella vita privata? • Le autorità statali si impegnano nella raccolta generalizzata dei metadati delle comunicazioni e/o dei contenuti trasmessi all'interno Paese?

• Esistono linee guida legali e supervisione indipendente sulla raccolta, la conservazione e l'ispezione dei dati di sorveglianza da parte delle agenzie di sicurezza dello stato e, in tal caso, tali linee guida aderiscono agli standard internazionali sui diritti umani in materia di trasparenza, necessità e proporzionalità?

• Le autorità statali monitorano le informazioni pubblicamente disponibili pubblicate online (inclusi su siti Web, blog, social media e altre piattaforme digitali), in particolare allo scopo di scoraggiare il giornalismo indipendente o l'espressione politica, sociale, culturale, religiosa e artistica?

• Le autorità hanno la capacità tecnica di monitorare o intercettare regolarmente il contenuto delle comunicazioni private, come e-mail e altri messaggi privati, anche tramite spyware e tecnologia di estrazione?

• Le autorità locali come i dipartimenti di polizia sorvegliano i residenti (anche attraverso International Mobile Subscriber Identity-Catchers o la tecnologia IMSI catcher) e, in tal caso, tali pratiche sono soggette a rigorose linee guida e supervisione giudiziaria?

• Gli attori statali utilizzano l'intelligenza artificiale e altre tecnologie avanzate ai fini della sorveglianza online senza un'adeguata supervisione?

• Le misure di sorveglianza del governo prendono di mira o colpiscono in modo sproporzionato dissidenti, difensori dei diritti umani, giornalisti o determinati gruppi etnici, religiosi, di genere, LGBT+, migranti e altri gruppi pertinenti?

6. Il monitoraggio e la raccolta dei dati degli utenti da parte di fornitori di servizi e altre società tecnologiche violano il diritto alla privacy degli utenti? *(0-6 punti)* • Leggi specifiche o decisioni legali vincolanti sanciscono i diritti degli utenti sui dati personali, compresi quelli biometrici
informazioni, generate, raccolte o elaborate da soggetti pubblici o privati?
• Gli organismi di regolamentazione, come un'agenzia per la protezione dei dati, proteggono efficacemente la privacy degli utenti, anche indagando sulla cattiva gestione dei dati da parte delle aziende e applicando leggi o decisioni legali pertinenti?
• Il governo può ottenere informazioni sugli utenti dalle aziende (ad es. fornitori di servizi, fornitori di accesso pubblico, internet cafè, piattaforme di social media, fornitori di posta elettronica, produttori di dispositivi) senza un procedimento legale?
• Queste società sono tenute a raccogliere e conservare i dati sui propri utenti? • Queste società sono tenute a conservare i dati degli utenti su server situati nel paese, in particolare i dati relativi a
attività ed espressioni online protette dagli standard internazionali sui diritti umani (ad esempio, esistono requisiti di "localizzazione dei dati")?
• Queste aziende monitorano gli utenti e forniscono informazioni sulle loro attività digitali al governo o ad altri attori potenti (tramite intercettazioni tecniche, condivisione di dati o altri mezzi)?
• Lo stato tenta di imporre requisiti simili a queste società attraverso metodi meno formali, come ad esempio codici di condotta, minacce di censura o altre conseguenze economiche o politiche? • Le richieste del governo per i dati degli utenti di queste aziende sono trasparenti e le aziende hanno una strada realistica
per appello, ad esempio tramite tribunali indipendenti?

7. Le persone sono soggette a intimidazioni extralegali o violenza fisica da parte delle autorità statali o di qualsiasi altro attore in relazione alle loro attività online? *(0–5 punti)* • Le persone sono soggette a violenza fisica, come omicidio, aggressione, tortura, violenza sessuale o sparizione forzata, in
relazione alle loro attività online, inclusa l'appartenenza a determinate comunità online?
• Le persone sono soggette ad altre intimidazioni e molestie, come minacce verbali, restrizioni di viaggio, condivisione non consensuale di immagini intime, doxing o distruzione o confisca di proprietà, in relazione alle loro attività online?

• Le persone sono soggette a intimidazioni e molestie online proprio perché appartengono a una determinata etnia, religioso, di genere, LGBT+, migrante o altro gruppo rilevante?
• Giornalisti online, blogger o altri sono fuggiti dal paese o si sono nascosti per evitare tali conseguenze? • Gestire le attività online di dissidenti, giornalisti, blogger, difensori dei diritti umani o altri utenti all'esterno
il paese ha comportato ripercussioni per i loro familiari o collaboratori con sede nel paese?

8. I siti Web, le entità governative e private, i fornitori di servizi o i singoli utenti sono soggetti a hacking diffuso e ad altre forme di attacco informatico? *(0–3 punti)* • I siti web appartenenti all'opposizione, alle testate giornalistiche o ai gruppi della società civile nel paese sono stati temporaneamente o permanentemente disabilitati a causa di attacchi informatici, in particolare in periodi politicamente delicati?
• I siti Web oi blog sono soggetti ad attacchi tecnici mirati come punizione per la pubblicazione di determinati contenuti, ad esempio su argomenti politici e sociali? • Gli enti finanziari, commerciali e governativi sono soggetti a attacchi informatici significativi e mirati finalizzati al furto
dati o disabilitare le normali operazioni, compresi gli attacchi che hanno origine al di fuori del paese?
• Sono in atto leggi e politiche per prevenire e proteggere dagli attacchi informatici (compresi gli attacchi sistematici da parte di attori non statali) e vengono applicati?

Ringraziamenti

Freedom on the Net è uno sforzo collaborativo tra
Lo staff di Freedom House e una rete di oltre 80 persone
ricercatori, provenienti da organizzazioni della società civile, università, giornalismo e altri background, che coprono 70 paesi. In ambienti repressivi, Freedom House si preoccupa di garantire l'anonimato dei ricercatori e/o lavora con esperti residenti all'estero.

Questo rapporto è stato reso possibile grazie al generoso sostegno di Amazon, del Ministero degli Affari Esteri olandese, di Google, della Hurford Foundation, di Internet Society, di Lilly Endowment Inc., del New York Community Trust e del Bureau of Democracy, Human Rights del Dipartimento di Stato degli Stati Uniti. e Lavoro (DRL). Freedom House si impegna per l'indipendenza editoriale. I nostri donatori non influenzano le priorità di ricerca dell'organizzazione, i risultati dei rapporti o le raccomandazioni politiche.

Il team *di Freedom on the Net* esprime la propria gratitudine alla comunità globale per la libertà di Internet, compresi i numerosi individui e organizzazioni il cui instancabile e coraggioso lavoro informa questo rapporto.

Elisha Aaron, David Meijer, Shannon O'Toole, Tyler Roylance e Lora Uhlig hanno curato *Freedom on the Net.* Michael Abramowitz, Gerardo Berthin, Nicole Bibbins Sedaca, Annie Boyajian, Nate Schenkkan e Lara Shane hanno fornito un prezioso feedback sulla sintesi dei risultati. Sarah Cook e Angeli Datt sono state consulenti per la Cina. Mike Smeltzer e Noah Buyon hanno fornito consulenza sulle regioni Europa ed Eurasia.
Danielle Dougall, Dasha M e Eilidh Stalker hanno fornito assistenza alla ricerca.

CONTRIBUTORI

Personale della Casa della Libertà

• **Adrian Shahbaz,** Vicepresidente della ricerca e dell'analisi • **Allie Funk,** Direttore della ricerca per la tecnologia e la democrazia • **Philip Friedrich,** Senior Research Analyst per Tecnologia ed elezioni
• **Kian Vesteinsson,** Senior Research Analyst per Tecnologia e democrazia • **Grant Baker,** Analista di ricerca per la tecnologia e la democrazia

• **Cathryn Grothe,** Analista di ricerca per il Medio Oriente e Nord Africa

• **Maddie Masinsin,** specialista del coinvolgimento della comunità per la tecnologia e la democrazia • **Manisha Vepa,** ex ricercatrice associata • **Tessa Weal,** ricercatrice associata per la tecnologia e la democrazia

Autori del rapporto •

Argentina: Eduardo Ferreyra, ricercatore indipendente • **Armenia:** Samvel Martirosyan, co-fondatore di CyberHUB-AM • **Australia:** Elizabeth O'Shea e Lucie Krahulcova, Digital Rights Watch •
Azerbaigian: Arzu Geybulla, giornalista •
Brasile: Bruna Martins dos Santos, Cancelliere tedesco Fellow presso la Fondazione Alexander von Humboldt e Visiting Researcher al Berlin Social Science Center •
Cambogia: Sopheap Chak, direttore esecutivo di Centro cambogiano per i diritti umani •
Canada: Allen Mendelsohn, McGill University • **Colombia:** Emmanuel Vargas e Susana Echaverría, El Veinte •
Costa Rica: Oscar Mario Jiménez Alvarado, Fernando Martínez de Lemos, Johanna Rodríguez López, Programma per la libertà di espressione, il diritto all'informazione e l'opinione pubblica (PROLEDI), Università di Costa Rica (UCR) •
Cuba: Ted Henken, Baruch College, città Università di New York
• **Estonia:** Hille Hinsberg e Florian Marcus, Ingegneri orgogliosi
• **Etiopia:** Atnafu Brhane, Centro per il progresso di Diritti e Democrazia •
Francia: Dr. Suzanne Vergnolle, Professore Associato all'Istituto Cnam
• **Georgia:** Teona Turashvili, Istituto per lo Sviluppo della libertà di informazione
• **Germania:** Paul Ritzka e Lisa Schmechel, iRights.Lab • **Ungheria:** Dalma Dojcsák, Unione ungherese per le libertà civili

• **Islanda:** Arnaldur Sigurðarson, ricercatore indipendente

• **Indonesia:** Libertà del sud-est asiatico
di Expression Network (SAFEnet) • **Iraq:**
Hayder Hamzoz e Assia Abdulkareem,
Rete irachena per i social media •
Italia: Philip Di Salvo, Visiting Fellow al London
School of Economics; Antonella Napolitano, Privacy
Internazionale
• **Giappone:** Hamada Tadahisa, Japan Computer Access for
Empowerment • **Libano:** Marianne Rahme, SMEX • **Libia:** Jabir
Zain, Centro libico per la libertà di stampa

• **Malawi:** Jimmy Kainja, University of Malawi • **Malesia:**
Kelly Koh, Sinar Project • **Messico:** Mariel Garcia-Montes,
Massachusetts Institute of Technology • **Myanmar:** Free Expression
Myanmar • **Nicaragua:** Obadiah Zambrano, IPANDETEC • **Nigeria:**
Adeboro Odunlami, ricercatore indipendente • **Serbia:** Mila Bajic, Asja
Lazareviÿ, Bojan Perkov,

CONDIVIDI Fondazione
• **Singapore:** Kirsten Han, ricercatrice indipendente • **Sud Africa:**
Tshepiso Hadebe, PPM Attorneys • **Corea del Sud:** Yenn Lee,
SOAS University of London • **Sri Lanka:** Raisa Wickrematunge,
ricercatrice indipendente • **Taiwan:** Ming-Syuan Ho, ricercatrice
indipendente • **Thailandia:** Emilie Pradichit e Letitia Visan,

Fondazione Manushya •
Gambia: Nasiru Deen, Gambia Press Union • **Tunisia:** Yosr
Jouini, ricercatore indipendente • **Turchia:** Gürkan Özturan, Media
Freedom Rapid
Coordinatore della risposta presso il Centro europeo per la libertà della
stampa e dei media • **Regno Unito:** Edina Harbinja, Aston University •
Stati Uniti: Claire Park, ricercatrice indipendente • **Uzbekistan:** Ernest
Zhanaev, ricercatrice indipendente • **Venezuela:** Raisa Urribarri, Universidad
de Los

Ande (in pensione)
• **Vietnam:** Trinh Huu Long, Legal Initiatives for Vietnam • **Zambia:** Bulanda
T. Nkhowani, Paradigm Initiative • **Zimbabwe:** Nompilo Simanje, Legal and
ICT Policy Officer, Media Institute of Southern Africa

Ricercatori per Angola, Bahrein, Bangladesh, Bielorussia, Cina, Ecuador, Egitto, Ghana, India, Iran, Giordania, Kazakistan, Kenya, Kirghizistan, Marocco, Pakistan, Filippine, Russia, Ruanda, Arabia Saudita, Sudan, Uganda, Emirati Arabi Uniti Emirates e Ucraina hanno voluto rimanere anonimi.

Consiglieri

• Abrar Mohamed Ali, ricercatore, African Digital
Rights Network •
Eto Buziashvili, Digital Forensic dell'Atlantic Council
Laboratorio di ricerca
• Jonathan Corpus Ong, Professore Associato presso il
Università del Massachusetts Amherst e ricerca
Fellow allo Shorenstein Center dell'Università di Harvard • Angel Diaz,
Visiting Assistant Professor of Law alla USC
Scuola di Giurisprudenza Gould
• Alena Epifanova, Research Fellow International
Programma Ordine e Democrazia, Consiglio tedesco on
Relazioni estere
• Alyssa Kann, ricercatrice associata presso l'Atlantic Council
Laboratorio di ricerca forense digitale
• Jeff Kosseff, professore associato, Cyber Science
Dipartimento, Accademia Navale degli Stati Uniti •
Artur Pericles Lima Monteiro, Wikimedia Fellow,
Information Society Project, Yale Law School, e membro del
gruppo di ricerca Constitution, Politics, and Institutions, University of
São Paulo
• Iria Puyosa, Senior Research Fellow presso l'Atlantic Council
Digital Forensic Research Lab •
Hakeem Dawd Qaradaghi, ricercatore indipendente • Xiao Qiang,
fondatore e redattore capo della Cina
Digital Times e ricercatore presso la School of
Informazioni, Università della California Berkeley

COME CITARE QUESTO RAPPORTO

Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Libertà in rete 2022,* Freedom House, 2022, freedomonthenet.org.

Shahbaz, Funk e Vesteinsson, "Contrastare la revisione autoritaria di Internet", in Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Libertà in rete 2022,* Freedom House, 2022, freedomonthenet.org.

"Angola", in Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Libertà in rete 2022,* Freedom House, 2022, freedomonthenet.org.

Siamo orgogliosi di collaborare con singoli filantropi, fondazioni, aziende, ONG e governi che condividono i nostri valori e l'instancabile ricerca della democrazia e della libertà. Unisciti a noi in questo lavoro critico.

Per ulteriori informazioni sul sostegno a Freedom House, **visitare www.FreedomHouse.org/donate.**

Freedom House

Freedom House è un'organizzazione pro-democrazia che identifica le minacce alla libertà e mobilita il sostegno per gli attivisti e le organizzazioni che difendono la democrazia. Ci sforziamo di creare un mondo in cui tutte le persone siano libere. Ciò include garantire che gli Stati Uniti difendano la democrazia in patria e all'estero.

1850 M Street NW, 11° piano
Washington, DC 20036

Freedomhouse.org
facebook.com/FreedomHouseDC
@freedomhouse @freedomonthenet
202.296.5101

info@freedomhouse.org