RUBRICA
STIP: SCIENCE, TECHNOLOGY, AND INNOVATION POLICY

OrizzonteCina
Vol. 11 (2020), n. 3: 70-75
doi: 10.13135/2280-8035/5604

Questa rubrica
è promossa da:
ESCP BUSINESS SCHOOL

La Cina e lo spazio digitale. Questioni di *governance* nello spazio digitale globale

Giulio Santoni
Università degli Studi di Roma "Tor Vergata" e China University of Political Science and Law
Contatto: giuliosantoni14@gmail.com

Introduzione

Nei Paesi occidentali, e più in particolare negli Stati Uniti, la regolazione di Internet si è caratterizzata per aver favorito l'autoregolazione da parte dei fornitori di servizi online a discapito della normazione statale.[1] Per ragioni di tutela della riservatezza e delle libertà individuali, le autorità pubbliche rimangono neutrali rispetto ai dati necessari a imporre le norme. Si tratta, in particolare, delle informazioni relative all'identità, la posizione e le attività degli utenti.

Queste medesime informazioni possono essere volontariamente cedute dagli utenti ai soggetti che forniscono servizi online, gli OSP.[2] D'altro canto, la migliore dottrina ha sostenuto nel modo più convincente che la struttura della comunicazione via Internet consente di implementare forme di regolazione alternative alla norma-precetto tradizionale.[3] Si tratta di modalità di regolazione incentrate sulla predisposizione di un'architettura tecnica all'interno del quale le attività online si svolgono. Questa medesima architettura è rappresentata in parte dai protocolli tecnici che determinano il funzionamento di Internet. Ma rientra in misura ancora maggiore nella disponibilità di soggetti privati, gli OSP, che forniscono servizi quali motori di ricerca, sistemi di pagamento online, *social media*, ecc.

La regolazione statale dell'attività di Internet può avvalersi (come avviene in Cina) della mediazione degli OSP per regolare l'attività degli utenti. In Occidente ciò si è verificato solo in misura minima. Da un lato, la regolazione dell'attività su Internet incide essenzialmente sul diritto alla libera espressione dei cittadini. L'imposizione di obblighi di cooperazione in capo agli OSP avrebbe sostanzialmente incentivato questi soggetti privati a censurare le espressioni dei propri utenti. D'altra parte, vista la rapida evoluzione delle tecniche di comunicazione Internet, si è ritenuto che l'autoregolamentazione da parte dell'industria sarebbe stata meglio in grado di adattarsi alla rapida evoluzione della materia.

Per via della natura transfrontaliera delle comunicazioni via Internet, le decisioni del legislatore statunitense hanno avuto ripercussioni in un sistema di regolazione globale. L'approccio

[1] Si veda nota 6.

[2] Si veda ad esempio l'art. 6 del GDPR.

[3] Su tutti, si veda L. Lessig, *Code: And Other Laws of the Cyberspace, Version 2.0* (New York: Basic Books, 2006).

c.d *multistakeholder* alla regolazione di Internet, minimizza il ruolo della regolazione statale nel cyberspazio, in favore di una diffusione uniforme a livello internazionale delle pratiche auto-regolatorie che si affermano sul mercato. Più nello specifico, l'importanza delle entità private nella regolazione di Internet come rete globale si traduce in due aspetti fondamentali. Il primo è che gli enti internazionali preposti all'uniformazione degli *standard* tecnici di Internet, quali l'ICANN e l'ITU, sono partecipati da un ampio numero di entità (*stakeholders*). Entità riconducibili agli Stati non sono assenti, ma operano sullo stesso piano di entità private quali OSP, associazioni ed individui. D'altro canto, nella misura in cui, come si è detto, l'architettura tecnica degli OSP implica scelte normative, il successo degli OSP americani nel mercato delle informazioni si traduce in un'influenza determinante in scelte fondamentali quali gestione dei dati degli utenti, tutela del diritto d'autore online, rimozione di contenuti politicamente scorretti, ecc.

La strategia cinese di contenimento del sistema globale di regolazione di Internet

Fin dalle prime fasi della diffusione di Internet negli anni Novanta, la dottrina cinese ha ritenuto che l'approccio *multistakeholder* desse luogo a notevoli rischi per la sicurezza nazionale. Alla base delle considerazioni diffusesi in Cina, sta una diversa comprensione della natura delle attività che hanno luogo in Internet. L'insieme dei rapporti giuridici che si cristallizzano in rete affonda le proprie radici e produce effetti rilevanti nello spazio fisico. Alla nozione di cyberspazio (*wǎngluò kōngjiān*, 网络空间) si sostituisce spesso la diversa idea di cyber-sfera, concetto con il quale si vuole definire la relazione tra fisico e digitale non più come un binomio che coinvolge due piani indipendenti tra loro, bensì come un fascio di rapporti che si compenetrano reciprocamente.

L'enfasi sulla stretta correlazione tra il piano fisico ed il piano digitale impone di ricavare un ambito di sovranità esclusiva dello Stato cinese nella regolamentazione di Internet o cyber-sovranità (*wǎngluò zhǔquán*, 网络主权). Fin dagli anni Novanta, l'obiettivo primario di questa strategia fu di impedire che entità estere regolassero rapporti giuridici in Internet rilevanti per l'ordinamento giuridico cinese, nonché più in generale evitare che infrastrutture fondamentali dello Stato cinese, quali i sistemi di pagamento e i sistemi di telecomunicazioni fossero detenute da uno Stato estero e quindi vulnerabili. Non sorprende pertanto che la diffusione di Internet in Cina sia stata accompagnata dall'introduzione di tecniche di filtraggio, via via più efficienti. I meccanismi di censura automatizzata sono ispirati a un principio di filtraggio selettivo, in virtù del quale l'ossatura delle pagine Internet è disponibile, mentre solo i contenuti espressamente contrari alla legge sono indisponibili.[4] In altre parole, il sito Internet tende ad essere mantenuto disponibile, sebbene privato dei contenuti contrari alla legge.

[4] Si noti al contempo che le leggi cinesi che vietano contenuti Internet, posseggono di norma un carattere estremamente vago. Ad esempio, le Misure ad interim sulla gestione delle reti di informazioni trasmesse per computer, emanate dal Consiglio degli affari di Stato nel '96, proibiscono varie categorie di contenuti informatici. Nel novero dei divieti rientravano in particolare le informazioni lesive della sicurezza nazionale o di segreti di Stato, informazioni contrarie all'ordine pubblico o che promuovessero materiale sessualmente esplicito. In mancanza di definizioni più precise, è evidente che l'ordine di rimuovere materiale illecito, rivolto a soggetti pubblici e privati, è estremamente ampio. F. Proutè, in "Censoring Pornography, the role of sexual media in the fight for freedom of expression in the People's Republic of China", *Mapping China Journal*, 2018, disponibile all'Url https://mappingchina.org/wp-content/uploads/2019/01/MCJ-No-2-2018-Proute.pdf, delinea ad esempio un legame tra censura politica e limitazione del materiale pornografico.

I siti Internet sono invece oscurati per intero qualora offrano sistematicamente materiale vietato dalla legge, come è il caso per le maggiori testate giornalistiche internazionali, ad esempio il sito BBC in cinese, blog come Reddit e altri siti che criticano abitualmente la situazione dei diritti umani in Cina, come Amnesty International e Human Rights Watch.[5] Queste limitazioni sono dovute all'esigenza strategica del Partito comunista cinese di mantenere un'egemonia sulle narrazioni politiche più rilevanti.[6]

La letteratura occidentale s'interroga sul legame tra le finalità difensive del sistema di filtri cinese e le ambizioni cinesi di ottenere una supremazia militare sul cyberspazio.[7] Gli aspetti strettamente militari, o comunque legati alla sicurezza nazionale, sono senz'altro centrali nello sviluppo della teoria della sovranità sul cyberspazio, come peraltro più volte apertamente dichiarato dal Presidente Xi Jinping, nella sua veste di Presidente della Commissione centrale per la cyber-sicurezza (*Zhōngyāng wǎngluò ānquán hé xìnxīhuà wěiyuánhuì*, 中央网络安全和信息化委员会), in ossequio al principio "non può esservi sicurezza nazionale senza sicurezza della rete".[8] L'importanza che la Cina attribuisce alla sua capacità di difendere la propria cyber-sfera, si evince anche dalla recente istituzione di un corpo d'armata nell'Esercito di liberazione popolare specificamente dedicato alle operazioni militari nel cyberspazio, la Forza di supporto strategica, che affianca esercito, marina, aviazione e forze missilistiche nella composizione dell'esercito cinese.

Un aspetto centrale della teoria della sovranità sul cyberspazio si risolve dunque in aspetti strategico-militari, quali l'utilizzo di tecnologie di filtraggio e la creazione di strumenti di deterrenza. La dottrina occidentale omette tuttavia di cogliere che la dottrina della sovranità del cyberspazio, oltre che sulla censura, si poggia anche sul diverso pilastro della regolazione economica e che in campo economico produce effetti altrettanto degni di nota.

La sovranità nazionale sul cyberspazio come tecnica legislativa

Si è detto come il sistema di *Internet governance* cinese abbia fatto largamente uso di forme di censura come filtraggio automatico dei contenuti online ed il blocco di alcuni siti. A queste misure, se ne affiancano altre, incentrate invece su sanzioni irrogate contro gli autori materiali di contenuti Internet vietati. Questi possono essere multati, vedere i propri account bloccati o essere soggetti ad ulteriori sanzioni amministrative. Il potere dello Stato d'imporre sanzioni in capo agli utenti si poggia necessariamente sulla collaborazione degli OSP. Questi debbono identificare gli utenti, nonché monitorarne il comportamento, ai sensi dell'art. 20 della Legge sulla sicurezza della rete (*wǎngluò ānquánfǎ*, 网络安全法).

---

[5] Zheng Haiping, "Regulating the Internet: China's law and practice", *Beijing Law Review* 4 (2013) 1.

[6] Su questo punto si rinvia al dibattito interno all'Esercito popolare di liberazione (*jiěfàngjūn*, 解放军), in particolare si veda Cheng D., *Cyber Dragon: inside China's information warfare and cyber operations* (Westport: Praeger, 2016). L'Epl sottolinea numerosi aspetti politicamente problematici che la libera diffusione di contenuti Internet in Cina potrebbe esasperare. La superiorità qualitativa di molti prodotti informatici occidentali, abbinata alla suggestività delle narrative diffuse in occidente e alla relativa diffusione della lingua inglese in Cina potrebbero infatti portare alla perdita del ruolo guida del Partito comunista cinese.

[7] Sul tema si veda M. Kolton, "Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence", *The Cyber Defense Review* 2 (2017) 1.

[8] Si veda ad esempio il discorso tenuto da Xi Jinping nel corso della cerimonia di apertura della World Internet Conference, tenutasi a Wuzhen il 16 dicembre 2015.

Oltre alle sanzioni amministrative che assicurano che gli OSP obbediscano a queste previsioni, l'art. 36 della Legge cinese sulla responsabilità per danno da fatto illecito (*qīnquánfǎ*, 侵权法) prevede che tali soggetti rispondano civilmente per i danni causati dal materiale illecito distribuito dai propri utenti. La responsabilità, con il conseguente obbligo di risarcire i danni non si verifica solo nel caso in cui la natura illecita del materiale non sia evidente e a condizione che l'OSP abbia comunque implementato un sistema che consenta a chi abbia interesse di segnalare il materiale.[9]

Qualora dunque un utente cinese commetta un illecito online, l'OSP è tenuto a risarcire le parti lese da questo illecito. Quali condotte siano illecite è stabilito da una molteplicità di fonti legislative, che non è questa la sede di esaminare nel dettaglio. Ciò che realmente rileva è che gli illeciti "politici" su cui si concentra l'attenzione degli studiosi occidentali, sono disciplinati nelle medesime norme che regolano la posizione degli OSP rispetto a illeciti "civili", quali diffamazione, lesioni online della proprietà intellettuale e distribuzione di materiale osceno.[10] Si manifesta così con chiarezza come il controllo dello Stato cinese sulle infrastrutture informatiche e sugli OSP non sia solo strumentale a reprimere il dissenso politico e a prevenire attacchi informatici da parte di potenze estere, ma anche a garantire l'applicazione della legge alle condotte online.

Del resto, l'introduzione di regole sulla responsabilità degli OSP è al centro di una dettagliata regolamentazione dell'attività economica di questi soggetti. Si deve in primo luogo premettere che tale disciplina ha di fatto escluso i maggiori OSP internazionali dal mercato cinese, o perché ritenuti inidonei ad assicurare il rispetto della normativa, come nel caso di Facebook, o perché non intenzionati ad offrire un servizio conforme alle prescrizioni del governo cinese, come nel caso di Google. Ciò ha creato spazio nel mercato interno cinese per lo sviluppo di numerosi OSP

[9] E' interessante notare come la struttura dell'art. 36 della Legge cinese sulla responsabilità per danno da fatto illecito ricalchi con esattezza la sezione 512 del U.S. Digital Millennium Copyright Act (DMCA) statunitense, che si applica alle sole lesioni del diritto d'autore. Quest'ultima norma si inserisce nel contesto della legislazione americana, dominata dalla sez. 230 del Communication Decency Act, che prevede come regola generale l'immunità assoluta per le condotte illecite degli utenti in favore degli OSP. La portata dell'immunità è stata via via ampliata da un indirizzo giurisprudenziale costante e continuo, che ha nel corso degli anni affermato da un lato che la conoscenza da parte dell'OSP di fatti illeciti commessi dai propri utenti non implicasse alcun obbligo di rimozione (si vedano i famosi casi *Zeran v. AOL* e *Barrett v. Rosenthal*), e d'altra parte esteso il principio dell'immunità a un ampio numero di fattispecie concrete, quali lesioni della riservatezza altrui, diffamazioni online, incitamento all'odio razziale, ecc. Nella casistica americana rientrano, dunque, tutti gli illeciti per i quali la giurisprudenza americana ha ritenuto che l'attribuzione di una responsabilità per il fatto illecito dell'utente (*secundary liability in common law*) avrebbe comportato un rischio di censura indiretta: gli OSP, al fine di evitare la perdita economica dovuta all'attribuzione di responsabilità, avrebbero preventivamente censurato le espressioni dei propri utenti, impedendo la realizzazione del principio di libertà di parola consacrato nel Primo emendamento della Costituzione statunitense. Effetto ulteriore dell'immunità è di impedire che le norme di common law sull'editoria, che prevedono che chi modifichi un testo scritto debba essere responsabile al pari dell'autore, impedissero l'autoregolamentazione da parte degli OSP. L'immunità in questione si applica dunque alla maggior parte dei contenuti online. L'eccezione principale è rappresentata appunto dalla sez. 512 del DMCA, secondo cui, quando l'OSP ospiti una condotta lesiva del diritto d'autore, mantiene la propria immunità solo nel caso in cui non abbia conoscenza specifica della condotta e abbia implementato un sistema c.d. di *takedown on notice*, vale a dire una sezione del sito Internet che consenta a chi vanta diritti d'autore su di un contenuto di portare a conoscenza l'OSP sull'asserita lesione del diritto attraverso un modulo online. La regola trova la propria giustificazione nell'interesse che gli OSP manifestano normalmente nel diffondere materiale tutelato dal diritto d'autore, interesse che li renderebbe inadatti all'autoregolamentazione. Ma se queste ragioni di carattere economico giustificano l'eccezionalità della disciplina del diritto d'autore, non può non rilevarsi come, nel suo complesso, il sistema statunitense finisca con l'offrire tutele più ampie a diritti patrimoniali di quanto non faccia con riferimento a diritti della persona, quali il diritto alla riservatezza ed all'onorabilità.

[10] Si ricordi in ogni caso che in una certa misura le due categorie si sovrappongono, nel senso che la regolazione di contenuti non strettamente politici, quali materiale pornografico o comunque osceno, finisce spesso con l'essere indirizzato a reprimere movimenti politici o civili.

nazionali, in particolare quelli controllati dai gruppi Baidu, Alibaba e Tencent. Le tre società, note anche con l'acronimo BAT, offrono servizi equivalenti a quelli forniti dai grandi OSP statunitensi in occidente, quali motori di ricerca e social media.

La posizione di mercato delle imprese cinesi, peraltro, è ulteriormente rafforzata dalle previsioni delle leggi in tema di investimenti esteri, che escludono soggetti partecipati da entità estere dai cosiddetti Value Added Telecommunication Services.[11] E' questa una categoria estremamente ampia, che include servizi Internet quali pagamenti online (estremamente diffusi nel paese), servizi di *e-commerce* ed altri servizi di carattere principalmente economico. Tutto il sistema dei servizi online operativo al di fuori della Cina, con il suo bagaglio di normative affermate nel corso di tre decenni di pratiche autoregolatorie,[12] è di fatto sradicato dall'ambiente online cinese.[13]

Proiezione internazionale della dottrina della sovranità sul cyberspazio

La dottrina cinese della sovranità nazionale sul cyberspazio risponde alla necessità di salvaguardare non soltanto la sicurezza nazionale, ma più in generale il potere dello Stato di affermare le proprie norme anche sulle attività dei propri cittadini che avvengano attraverso l'utilizzo di Internet. Si tratta a ben vedere di un'esigenza avvertita non solo da paesi autoritari, ma sempre di più anche da paesi dell'Europa e del Sudamerica che inizialmente avevano appoggiato la visione "*multistakeholder*" proposta dagli Stati Uniti.[14]

La proiezione internazionale della dottrina cinese sulla sovranità del cyberspazio contrappone al sistema *multistakeholder* un sistema di governo di Internet incentrato sulla regolazione statale. Regolazione statale che è dunque una prerogativa legittima di ogni Stato, a prescindere dal proprio sistema politico.[15] Ciò implica da un lato il diritto degli Stati sovrani di regolare le attività che si svolgono nelle "proprie" porzioni di cyberspazio e dall'altro la necessità di determinare *standard* e norme della rete globale fondati sul consenso tra Stati e non più su una compartecipazione tra entità private ed entità statali.

La prospettiva futura delle politiche di *Internet governance* cinesi presenta punti di forza e debolezze. Da un lato, la Cina ha anticipato di numerosi anni la questione centrale dell'*Internet governance*. All'aumentare di rilevanza delle comunicazioni via Internet, la natura globale della regolazione proposta nel sistema *multistakeholder* si sarebbe necessariamente scontrata con gli interessi particolari dei singoli Stati. La massa di utenti Internet che il mercato cinese da solo è in grado di assicurare e i mezzi di gestione di cui il governo dispone hanno garantito la possibilità di sviluppare sistemi di comunicazione Internet paralleli, ispirati a un principio di normazione statale sul cyberspazio.

---

[11] Si veda in particolare la Negative List.

[12] Si veda la nota 6.

[13] Ma W., *China's mobile economy: opportunities in the largest and fastest information consumption boom* (New Jersey: Wiley Online Library, 2017).

[14] Si veda ad esempio la posizione del Presidente francese Macron https://www.reuters.com/article/us-cyber-un-macron/macron-and-tech-giants-launch-paris-call-to-fix-internet-ills-idUSKCN1NHoFS.

[15] Zhang X. e Xu K., "A Study on Cyberspace Sovereignty", *China Legal Science* 33 (2016) 75.

A partire dal 2015, la politica cinese di *Internet governance* si è arricchita di un respiro internazionale, grazie all'inclusione della Digital Silk Road nel progetto nuova Via della Seta. Il progetto, in breve, consiste nella fornitura di infrastrutture tecniche quali il 5G, al fine di garantire l'accesso al mercato di servizi forniti da OSP cinesi. La DSR è partecipata da oltre 30 Stati, tra cui spiccano per importanza Turchia, Egitto, Kazakistan, Corea del Sud e Arabia Saudita, oltre a numerosi Paesi dell'Est Europa, quali Polonia, Ungheria e Repubblica Ceca. Accordi bilaterali a margine del Secondo forum della Via della Seta, tenutosi a Shanghai nel Dicembre 2019, sono stati conclusi con Stati quali Israele, il Brasile e Giappone.

Ciò dimostra una certa attrattività anche del modello di *governance* cinese. Del resto, come si è detto, la necessità di affermare la sovranità statale sul cyberspazio è ormai avvertita anche in numerosi sistemi democratici, come ad esempio l'Unione europea. D'altra parte, gli obiettivi prioritari del governo cinese sono limitati a incrementare la "sicurezza della rete", laddove la circolazione di informazioni a livello globale è considerata elemento desiderabile ma non prioritario. La concezione cinese del governo del cyberspazio come pratica volta primariamente ad escludere ingerenze esterne nella politica interna ha prodotto una reazione a catena anche nei paesi occidentali, esemplificata dall'esclusione di TikTok dal mercato statunitense e di Huawei da quello europeo. Eppure, come la dottrina cinese ha ben chiarito, la sovranità sul cyberspazio non consiste nella mera esclusione di soggetti riferibili a governi esteri. Alla capacità di garantire la cyber-sicurezza si deve aggiungere la facoltà di controllare i soggetti attivi, facoltà che presuppone una suddivisione di competenze ed una dimestichezza nell'utilizzo dei mezzi informatici di cui l'Ue e gli Stati membri sono al momento drammaticamente privi.[16]

[16] L. Floridi, "The fight for digital sovereignty: what it is, and why it matters, especially for the EU", *Philosophy & Technology* (2020) 33, disponibile all'Url https://link.springer.com/article/10.1007/s13347-020-00423-6.