

La sovranità digitale

di

Stelio Mangiameli*

Sommario: 1. La sovranità digitale e la rete. – 2. La rete come infrastruttura appartenente allo Stato. – 3. La governance di Internet tra interessi generali e interessi privati. – 4. Forme e limiti della regolazione tecnica degli operatori privati della rete. – 5 La garanzia dei diritti fondamentali tra poteri privati e pubblici. – 6. La Cybersecurity come primo elemento costitutivo della sovranità digitale. – 7. Sulla necessità di una regolazione internazionale per internet attraverso un trattato sul Cyberspace.

1. La sovranità digitale e la rete. – «Governi del mondo industriale, stanchi giganti di carne e acciaio, vengo dal cyberspazio, la nuova casa della mente. A nome del futuro, chiedo a voi del passato di lasciarci soli. Non siete i benvenuti tra noi. Non avete la sovranità dove ci riuniamo». Così affermava John Perry Barlow, che vedeva nel *cyberspace* una dimensione pienamente in grado di resistere al potere dei governi, in nome della libertà di pensiero.

«Dobbiamo dichiarare il nostro sé virtuale immune alla vostra sovranità, anche se continuiamo ad acconsentire alla vostra regola sui nostri corpi. Ci allargheremo attraverso il pianeta in modo che nessuno possa arrestare i nostri pensieri», in modo da creare «una civiltà della mente nel cyberspazio». L'auspicio, più che la conclusione, era che questa civiltà «Possa essa essere più umana e giusta del mondo che i vostri governi hanno già fatto»¹.

* Professore ordinario di Diritto costituzionale – Università di Teramo.

¹ Barlow J. P., *A Declaration of the Independence of Cyberspace* (Davos, Switzerland, February 8, 1996).

Mai una visione del mondo è stata così errata e fuorviante, perché la “sovranità” è elemento costitutivo di ogni ordine, compreso quello virtuale. E senza sovranità non è possibile alcun ordine, almeno nel mondo dei viventi.

Il termine “sovranità digitale” viene utilizzato per indicare la prerogativa degli Stati nazionali di imporre regole sulle attività e sull’economia della rete, persino se transnazionali e globali, quando esse riguardano i propri cittadini².

Oggi la sovranità digitale è diventata attuale, perché il pubblico reclama una regolazione del *cyberspace*, per molteplici ragioni: innanzi tutto, nell’*onlife* si manifesta una condizione esistenziale caratterizzata da una non netta distinzione del virtuale rispetto al reale, per cui molte esigenze di tutela della persona, tipiche del reale, hanno assunto consistenza anche nel virtuale; in secondo luogo, le informazioni che circolano in rete sono reificate (i dati) e sono diventate beni in senso giuridico, cioè “cose che possono formare oggetto di diritti” (art. 810 del Codice civile) e, come tali, oggetto di attività economica, per via dell’accessibilità, della specificità e della loro limitatezza; infine, le grandi piattaforme non sono più attori, ma registi della rete³ e, anche quando regolano il loro comportamento, in realtà non guardano alla libertà del popolo della rete, ma esclusivamente al loro interesse e ogni loro auto-rappresentazione come alfieri della libertà e del *commonweal* è semplicemente strumentale⁴.

A prescindere dalla domanda dell’opinione pubblica che sempre più spinge per una regolazione politica della rete per la salvaguardia dei diritti fondamentali, risulta chiaro che atti di sovranità sulla rete sono stati possibili sin dalla sua creazione. Non a caso gli inizi di internet sono militari e non civili e non esiste un potere militare che non utilizzi strumenti di qualsivoglia genere sotto un comando

² Bertola V., *La sovranità digitale e il futuro di Internet*, in *Riv. it. inf. dir.*, n. 1/2022, 39-47; Pohle J., Thiel T., *Digital sovereignty*, in *Internet policy review*, December 17, 2020, in *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>; Simoncini A., *Sovranità e potere nell’era digitale*, in T.E. Frosini, O. Pollicino. E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, 2017.

³ Salvatori, R., *Piattaforma*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023, 369: “in the broadest sense of the term, the platform is a structure capable of managing different contents and making them available to authorized users”, 369.

⁴ V. Rosen J., *Google’s Gatekeepers*, in *New York Times Magazine*, November 28, 2008.

sovrano. Successivamente, la rete ha goduto di una grande libertà soprattutto in ambito accademico, dando luogo al sogno di una comunità scientifica mondiale, in grado di scambiarsi messaggi, studi e scoperte, senza limitazione alcuna e a vantaggio di tutti. Solo dopo è arrivato l'uso commerciale della rete e la creazione del mercato digitale nel quale si sono inserite le grandi piattaforme economiche. Anche queste hanno goduto e, in parte, godono di una grande libertà, quasi uno "stato di natura" della rete, senza autorità e regole⁵.

Tuttavia, sarebbe errato scambiare il fenomeno per la causa. La libertà totale di cui si parla, l'assenza di autorità e la carenza di regole che sembrano caratterizzare il *cyberspace*, sono solo apparenti e non strutturali del fenomeno virtuale. Infatti, sono gli Stati e, per essi, i più potenti che dominano i "grandi spazi"⁶ e rappresentano le "grandi potenze", ad avere permesso un simile sviluppo del *cyberspace*, astenendosi dal regolare la rete. È stata una scelta per favorire lo sviluppo tecnologico e l'economia tecnologica, ma internet è stata sempre sotto il controllo politico delle autorità di governo; e questo – come accade per ogni aspetto delle società – non è di per sé scevro di problemi.

A fondamento di questa pretesa "anomia" del *cyberspace*, si suole porre un parallelo tra questo e il "mare", ascrivendo la regolazione esclusivamente agli spazi fisici, alla "terra". Così, con questa ripresa della distinzione schmittiana⁷, si pensa alla rete come al luogo in cui "amanti della libertà e dell'autodeterminazione" respingono "le autorità di poteri distanti e disinformati", come al mondo nel qual "tutti i sentimenti e le espressioni dell'umanità, dai degradati agli angelici, sono parti di un insieme senza soluzione di continuità, la conversazione globale dei bit", come a una civiltà nuova quale la "civiltà della mente nel cyberspazio"⁸.

⁵ Sull'evoluzione della rete e le sue caratteristiche v. Amato Mangiameli A. C. – Campagnoli M. N., *Strategie digitali. #diritto_educazione_tecnologie*, Torino, Giappichelli, 2020.

⁶ Schmitt, C., *L'ordinamento dei grandi spazi*, 1941, ora in *Stato Grande Spazio Nomos*, Milano, 2015, 101-198.

⁷ Schmitt, C., *L'ordinamento dei grandi spazi*, cit.; Id., *Terra e mare. Una riflessione sulla storia del mondo*, trad. it., II ed. Milano, 2002.

⁸ Barlow J. P., *A Declaration of the Independence of Cyberspace*, cit.

Chi però pensa in questo modo commette due errori: il primo è che non sa o simula di non sapere che cosa è stato il principio della libertà dei mari; il secondo è che il mare non è più quello di un tempo.

La visione del mare come di una realtà senza legge derivava dalla circostanza che il mare veniva collocato fuori dalla Comunità degli Stati europei (*Comunitas christianorum*) e dal diritto di questa (*jus publicum europaeum*). In questo modo si è consentito a quegli Stati di compiere le peggiori nefandezze, dalla tratta degli schiavi, alla pirateria e alla guerra di corsa. In tal senso, è esatto affermare che i timori e i pericoli dell'alto mare sono gli stessi di quelli che si corrono in rete e che l'assenza di regole non significa affatto libertà assoluta, bensì una condizione di fatto e, per di più, precaria.

Se si approfondisce, poi, l'evoluzione delle tecnologie, ci si avvede immediatamente che il mare, lo spazio aereo e ora anche lo spazio fuori dell'atmosfera terrestre sono diventati tutti spazi regolamentati e controllati dai poteri sovrani. Lo stesso accade con il *cyberspace* che è esso stesso una invenzione tecnologica, quella di uno spazio nuovo senza un "dove" fisico.

Per i giuristi l'ingresso in nuovi spazi, come già prima in quello marino e aereo e ora in quello virtuale, costituiscono una sfida, essendo la scienza giuridica, ancorché nata per giuridificare rapporti e relazioni terrestri, perfettamente in grado di portare la legge ovunque, anche negli spazi virtuali, purché la legge stessa sia supportata da un potere sovrano⁹.

2. La rete come infrastruttura appartenente allo Stato. – L'espressione "sovranità" indica un potere in fatto assoluto e perpetuo su un gruppo umano e su un territorio, che si pone sul crinale del *Sein* e del *Sollen* e in via di principio unificante. Un potere effettivo, perciò, che pone un ordinamento e, più specificamente, le fonti del diritto di un determinato ordinamento, e cioè un potere che è capace di

⁹ V. le considerazioni di Kaiser J. H., *Das Recht im Cyberspace. Eine spontane Ordnung noch ohne Hierarchie*, in *Staat und Recht*, FS für Günther Winkler, Wien, Springer, 1997, 397-409.

autolegittimarsi da sé (perché *superiorem non recognoscens*), di legittimare ogni altro potere e di dare validità ad ogni norma. Un potere non subordinato esso stesso al rispetto dell'ordinamento che fonda e in grado di interpretare autenticamente il diritto. Un potere che rende l'ordinamento, verso l'esterno, indipendente e impenetrabile. Un potere, infine, che può solo autolimitarsi, ma che non ammette ingerenze o limitazioni esterne.

Quali effetti ha la sovranità con i suoi attributi su internet che è una realtà virtuale, aspaziale e i cui utenti non si qualificano per la loro cittadinanza?

Apparentemente – come già detto – questa realtà sembra sfuggire all'ipotesi che internet si possa ricondurre nell'alveo del dominio dei soggetti sovrani, ma in realtà è anch'essa il frutto della loro capacità politica, oltre che della tecnologia che questi sono in grado di sviluppare.

Del resto internet, per quanto singolare possa apparire il fenomeno, appartiene al novero delle "reti" che sono strutture tecnologiche create dagli Stati, secondo l'evoluzione dei bisogni umani e i risultati della ricerca scientifica.

Sin dal suo apparire lo Stato si è occupato e preoccupato di costruire reti, di regolarne l'uso e di sottoporle sotto il proprio controllo, perché queste reti sono una leva importante del suo dominio.

In origine furono le strade consolari, come hanno insegnato i Romani, che avevano una funzione militare precisa: tenere divisi i nemici di Roma e intercettare ogni tentativo di alleanza tra di loro. Successivamente, con la pacificazione le strade divennero uno strumento civile di comunicazione e su di esse viaggiavano persone e merci e si sviluppavano altri servizi a rete, tra cui il principale fu il servizio postale che consentiva la corrispondenza tra gli uomini in luoghi diversi. Certo, all'inizio alla velocità del cavallo, poi a quella del motore a scoppio e, quando la posta abbandonò la strada, alla velocità del treno, delle navi e a quella dell'aereo, oggi anche a quella di internet.

L'obiezione che internet è una rete transnazionale costruita in modo decentrato e da privati non è decisiva. In primo luogo, le tecnologie di internet non producono solo un sistema policentrico, ma danno vita anche a forme di centralizzazione

inedita, come emerge dalle esperienze degli Stati che adoperano la rete per mettere in campo forme di sorveglianza di massa e distorcere la verità. Non è senza significato, a tal riguardo, considerare la forte presenza sin dalla sua creazione del potere politico-militare degli Stati.

In secondo luogo, la circostanza che internet sia transnazionale non è una peculiarità che possa sottrarlo al dominio dei soggetti sovrani, atteso che vi presiede una specifica organizzazione internazionale (*International Telecommunication Union* [ITU]) costituita da Stati, nell'ambito delle Nazioni Unite. In tal senso, l'idea di internet come di un sistema senza un centro¹⁰, che farebbe pensare al medioevo¹¹, più che ad un mondo nuovo, deve fare i conti con tendenze unificatrici che operano anche a livello sopranazionale e che rendono possibile un ordine mondiale, frutto della collaborazione internazionale e caratterizzato da un equilibrio di poteri.

In tal senso, appunto, internet è solo uno dei frutti della collaborazione interstatale e diverse sono ormai le reti transnazionali, basti pensare al gas e all'elettricità, che ubbidiscono a logiche geopolitiche ed economiche. Reti, cioè, che interconnettendosi migliorano gli standard di vita e quelli economici degli uomini che ne usufruiscono, ma che creano una interdipendenza degli Stati, la quale può essere positiva, perché li induce a comportamenti pacifici e collaborativi, ma anche negativa, perché, a prescindere dalle ipotesi di conflitto, può creare una dipendenza di alcuni stati verso altri, incidendo sul loro stato di eguaglianza e di indipendenza.

Anche nel caso di internet, perciò, vi è un elemento strutturale del quale bisogna tenere conto, per chiarire i rapporti che si instaurano nella rete e che da questa si dipartono. Per quanto strano possa sembrare la "rete virtuale" è invero dotata di una "fisicità" autentica, fatta dai cavi che attraversano gli oceani, oltre che i continenti, e che portano il segnale dappertutto, sia pure ancora con grandi buchi.

¹⁰ Castells M., *Volgere di millennio*, trad. it., Milano 2003.

¹¹ Su questo fenomeno Rodotà S., *Una Costituzione per Internet?*, in *Politica del diritto*, 2010, 3, 337-351; D'Andrea D., *Oltre la sovranità. Lo spazio politico europeo tra post-modernità e nuovo medioevo*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 31, I, 2002.; Venanzoni A., *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *media Laws*, n. 3/2020.

Sono stati gli Stati a implementare questa fisicità della rete, che implica una proprietà della stessa e la proprietà comporta la disponibilità del bene. La rete, perciò, appartiene agli Stati, al pari di ogni rete di pubblico servizio, e questo anche quando alla sua costruzione partecipano i privati o quando sulla rete vengono concesse prerogative e privative.

La circostanza che esista una multipolarità di internet non impedisce allo Stato di compiere atti sovrani sulla rete; anzi, è proprio questo uno dei problemi principali cui è esposta la realtà virtuale. Infatti, ogni rete, anche quella più interconnessa, può essere segmentata, isolando i nodi che interessano per atto del principe e questa decisione non è sindacabile da alcuno. Sono noti i casi in cui i siti vengono oscurati dai governi e, addirittura, è accaduto che intere popolazioni sono state private dell'uso di internet. Per esecrabili che possono essere simili situazioni, per la violazione dei diritti fondamentali di quelle popolazioni, tutto ciò può accadere proprio per il dominio sovrano sulla rete.

Quanto, poi, alla circostanza che la rete è implementata e aggiornata (anche) dai privati, questa modalità di intersecazione tra pubblico e privato è tipica dell'azione degli Stati. Si pensi al treno e al mito della frontiera americana, alimentato da forti investimenti privati; un esempio che è presente anche nella storia di altri Stati, tra cui l'Italia, dove la nazionalizzazione delle ferrovie, doveva servire a spingere i privati a costruire la rete elettrica. Si pensi, ancora, allo sviluppo delle trasmissioni radio e televisive e ai grandi trust mondiali che vi operano accanto a migliaia di televisioni piccole (un tempo si diceva "libere"), che pure dipendono sempre dal potere degli Stati e rientrano nella sfera del loro dominio. Lo stesso vale per internet, come struttura fisica in sé, e per le piattaforme che sulla rete operano, basti pensare a tutte le vicende dei social, da facebook, a yahoo, a google, che hanno occupato tribunali e corti del mondo.

Certamente questa sovranità digitale, come ogni forma di potere, non è un fatto statico, ma una dimensione dinamica e in continuo divenire che implica lotte (di potere) e sfide permanenti.

3. La governance di Internet tra interessi generali e interessi privati. – Le direzioni della sovranità digitale non differiscono da quelle della sovranità *tout court*, in quanto implicano un potere di governo della rete, da un lato, sugli operatori (i provider e i gestori delle piattaforme) e, per l'altro, sugli utenti (il popolo della rete) e questo potere non è soggetto, in via di principio, a restrizioni esterne; anzi, sugli atti di sovranità interna gli altri soggetti che vantano la qualità della statualità dovrebbero astenersi da ogni forma di ingerenza, e ciò consentirebbe di configurare il potere sovrano come assoluto.

In realtà, nel caso della sovranità digitale, la ricostruzione storica della sovranità statale non appare sufficiente, non solo per le peculiarità della rete, quanto soprattutto perché la sovranità, in quanto tale, non corrisponde più allo stereotipo westfaliano; e la ragione principale di ciò deriva dalla emersione di Imperi che interagiscono con gli Stati, dominando lo scenario della globalizzazione e della rete e rendendo porosa la sovranità statale¹². In tal senso, questa avrebbe ormai un carattere relativo e interdipendente e, nel caso della rete, sarebbe costretta a ricercare un sostegno in chi è più avanzato tecnologicamente, sperando che nel frattempo possa sorgere una struttura, frutto della collaborazione multilaterale e sotto l'egida internazionale del controllo reciproco, in grado di organizzare il "cyberambiente globale".

Ciò peraltro non vuol dire che la sovranità digitale degli Stati sia priva di contenuti; anzi, essa ha specifiche forme di espressione e contenuti determinati.

Con riferimento alle forme, il modo in cui uno Stato esercita il suo potere sulla rete è eminentemente dato dalla legislazione, cui però devono conseguire competenze

¹² Per una accurata analisi del pluralismo dei grandi spazi e delle nuove forme dei sistemi politici, con particolare riferimento all'"impero", si rinvia a Mangiameli S., *Imperi e stati e le nuove relazioni internazionali*, in *Diritto e Società*, 2022; nonché, con riferimento alla costruzione di una "sovranità digitale europea", v. Celeste E., *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic. Perspectives on Extraterritoriality and Sovereignty*, Hart 2021, January 2020 in https://www.researchgate.net/publication/349495575_Digital_Sovereignty_in_the_EU_Challenges_and_Future_Perspectives; Credi O., Vianini C., *Spazio e sovranità digitale europea*, in IAI, 11 luglio 2021; Santaniello M., *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Riv. it. inf. dir.*, n. 1/2022.

amministrative specifiche, soprattutto la vigilanza e la capacità sanzionatoria, e la giustizia comprensiva del potere punitivo e risarcitorio.

Ora, è noto che gli operatori di internet tendono a dettare delle normative che impongono agli utenti, per l'accesso ai servizi; inoltre, hanno istituito degli organi propri preposti all'applicazione delle loro normative, che possono sanzionare la violazione delle rispettive regolamentazioni anche con la sospensione o l'esclusione dalla rete o dalla piattaforma dei singoli.

Che cosa differenzia la legislazione dello Stato e la sua attività di vigilanza e sanzione dalla regolazione, vigilanza e sanzione degli attori privati della rete?

Il tratto più evidente è dato dalla circostanza che solo la legislazione dello Stato è caratterizzata dal crisma della legittimità, mentre ogni altra regolazione è una disciplina di fatto, salvo che non operi in modo derivato dall'autorità dello Stato e, in tal caso, segue la forma del diritto privato.

Vi è, poi, una differenza di contenuto tra la legislazione dello Stato e quella degli attori privati della rete. Lo spazio virtuale si è immediatamente riempito della legislazione statale, di quella in atto esistente che è stata adattata interpretativamente alla rete, o riferita anche a questa, e di quella che gli Stati hanno varato specificamente per la rete (si pensi ai *computer crimes* o al *cyberbullismo*)¹³. La legislazione dello Stato soddisfa in ogni caso interessi generali legati alla vita della comunità. Differentemente, le regolazioni degli operatori privati che investono nella rete tende principalmente a preservare la loro posizione economica e i propri interessi che possono avere anche un carattere politico, oltre che economico.

Infine, solo le regole pubbliche possono garantire diritti agli utenti, mentre quelle private, culminando nella stipula di un contratto con un contraente forte, possono facilmente sacrificare i diritti degli individui in nome del codice contrattuale.

¹³ Sul fenomeno del cyberbullismo e la normativa su questo, v. Lodevole L., *Cyberbullismo*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023, 88 ss.

4. Forme e limiti della regolazione tecnica degli operatori privati della rete. –

Anche la c.d. “legislazione tecnica”¹⁴ che regola l’accesso alla rete e lo svolgimento di attività da parte degli operatori privati, in tanto si può considerare vera legislazione, in quanto a monte si situano una serie di accordi e di Agenzie internazionali che hanno raccordato i profili tecnici della rete globale e, in questo ambito, gli Stati vengono prima dei vari *stakeholder*. Nel tempo ci sono stati anche cambiamenti che possono fare pensare il contrario, come la privatizzazione di qualche Agenzia governativa (è il caso della successione tra l’IANA e l’ICANN), ma in realtà ciò non esclude mai la primazia del potere pubblico su quello privato. Inoltre, l’intera architettura tecnologica che sostanzia la “*Lex informatica*” non ha un carattere neutrale ed è per questo che necessita sempre della protezione di un potere politico che le garantisca ruolo e funzione. In questo, peraltro, sussiste una perfetta somiglianza con la “*Lex mercatoria*”, la quale – servendosi della rete essa stessa – si atteggia come un potere economico che regola da sé i rapporti giuridici con i consumatori. Invero, però, questa capacità della *Lex mercatoria* presuppone comunque la protezione di un potere politico che la protegga, senza il quale questa verrebbe fatta a pezzi non appena il primo consumatore si rivolga al proprio giudice domestico.

È pur vero che i rapporti tra potere pubblico e attori della rete¹⁵, soprattutto con i provider e le piattaforme, sono estremamente complicati dalla circostanza che questi vorrebbero simulare nel mondo virtuale forme e strutture che sono proprie della realtà statuale e non è da escludere peraltro che le loro azioni possano rivestire un carattere politico; basti in proposito richiamare il preteso carattere etico delle loro regolazioni e della loro vigilanza, o anche le dichiarazioni da parte di questi di salvaguardare i diritti umani e la democrazia.

¹⁴ Per un’ampia riflessione sulle capacità delle piattaforme di regolare l’architettura della rete v. Santaniello *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, n. 3/2021.

¹⁵ Per un’analisi di questa relazione v. recentemente Betzu M., *Poteri pubblici e poteri privati nel mondo digitale*, in *Il diritto costituzionale e le sfide dell’innovazione tecnologica*, Genova, 18-19 giugno 2021, in https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Marco_Betzu_-_Poteri_publici_e_poteri_privati_nel_mondo_digitale.pdf.

Ma in realtà, sono proprio questi che tengono comportamenti in violazione dei diritti con forme di censura nei confronti delle idee che non si conformano al c.d. “political correctness” e di sospensione o espulsione di individui dalla rete, di cui si è sempre proclamata la libertà assoluta.

È sintomatico, in proposito, il cambio di atteggiamento di *Elon Musk*, prima e dopo l’acquisto di Twitter. Quando ancora era in corso la trattativa, le sue esternazioni erano a favore della “assoluta libertà di parola” come “base del funzionamento di una democrazia”, asserendo che la piattaforma sarebbe “la piazza digitale in cui si discutono questioni vitali per il futuro dell’umanità”. Tuttavia, subito dopo l’acquisto, proprio per non preoccupare gli inserzionisti lo stesso *Musk* ha subito cambiato tono dichiarando che il social “non può diventare un paesaggio infernale dove si può dire qualsiasi cosa senza conseguenze”. Di qui, la probabile istituzione di un sistema di revisione dei “cinguettii”, in modo da evitare il discorso d’odio e la disinformazione.

Insomma, non si può essere dimentichi che siamo di fronte ad operatori economici di rilievo globale, in grado di disporre di risorse finanziarie superiori a quelli di molti Stati di media grandezza, che hanno accumulato una quantità inimmaginabile di informazioni e dati, attraverso profilazioni nascoste e forme di sorveglianza discreta, che consente loro di esercitare una influenza sui bisogni e sui desideri degli individui e sulle loro inclinazioni (anche politiche) ¹⁶.

Ora, che questi grandi “poteri privati” si atteggiino a difensori dei diritti umani e della democrazia, si riqualifichino come grandi filantropi, adesso garanti anche dell’ambiente, nonostante i loro server siano tra le più grandi fonti di inquinamento, appare essere un modo di atteggiarsi che è in linea con la “rappresentanza degli interessi organizzati” ¹⁷ ed è, in tal senso, qualcosa di già noto, anche se la scala adesso è globale.

L’azione dei “poteri privati” ha dato luogo a importanti servizi e continua a realizzare dei benefici a favore di gruppi umani o di singoli individui. Tuttavia,

¹⁶ Su questo argomento v. Michetti M., *Surveillance and technological (R)evolution. implications and repercussions on human rights*, in *Humanities and Rights global network journal*, 2023, 5(2).

¹⁷ Kaiser J. H., *La rappresentanza degli interessi organizzati*, trad. it., Milano, Giuffrè, 1993, *passim*.

nella realtà sono diventati il problema principale che richiede un intervento legislativo degli Stati, quanto meno per fare pagare loro imposte proporzionate ai profitti accumulati.

Invero, poi, può dirsi che le loro azioni non raggiungono mai la dimensione propria delle garanzie dei diritti e della democrazia del potere pubblico e non hanno le stesse capacità di intervento di questo. Le recenti crisi, quella economico-finanziaria e quella pandemica, ed ora anche quella energetica, mostrano chiaramente questa differenza; ed è anche per questo che, dopo anni di gloria, la stessa globalizzazione è entrata in crisi (si parla adesso di deglobalizzazione e di riglobalizzazione selettiva) e con essa sono entrati in crisi i suoi strumenti come la *Lex informatica* e la *Lex mercatoria*.

5 La garanzia dei diritti fondamentali tra poteri privati e pubblici. – La legislazione che gli utenti della rete invocano da parte del potere pubblico trova perciò fondamento in questa posizione dominante degli operatori privati e nelle insufficienze delle loro pretese regolative e di governo.

Nella rete non sono più in gioco lo sviluppo tecnologico, o l'economia tecnologica; la prima è appannaggio quasi esclusivo di alcune grandi potenze, come Cina e Stati Uniti, e la seconda ha consolidato in capo a piccoli gruppi, poste al vertice delle strutture economiche, un grande potere, assicurando loro una inedita concentrazione di capitali e un forte controllo del mercato elettronico. Nella rete, inoltre, vi sono in gioco i diritti fondamentali e la democrazia, per cui non si può accettare che le strutture politiche di vertice dei governi abbiano una condizione di potere che minacci i diritti fondamentali e consenta la manipolazione del consenso democratico, attraverso l'elaborazione e il monitoraggio dell'informazione, l'orientamento del dibattito e, in una certa misura, la definizione della verità.

Di qui la richiesta ineludibile da parte del popolo della rete, nei confronti degli operatori privati e dei governi, di una nuova regolamentazione del *cyberspace* secondo una proiezione tipicamente costituzionale, e cioè con riferimento alla

salvaguardia dei diritti fondamentali e della democrazia, così come degli altri valori europei (art. 2 TUE), che richiede il libero espletamento delle libertà, il divieto di manipolazione della verità, il superamento dello stato di sorveglianza e di accumulo dei dati da parte di operatori privati e governi e, soprattutto, l'interdizione dell'uso politico dei dati.

Può la sovranità digitale realizzare tutto ciò?

Il rispetto dei diritti e dei principi democratici certamente potrebbe attuarsi attraverso una legislazione multilivello e/o degli accordi multilaterali. Si potrebbe in questo modo formalizzare, se non una costituzione (globale) di internet, quanto meno un *Internet Bill of Rights*¹⁸, che contrariamente ad alcune affermazioni non travolgerebbe le ultime trincee della sovranità statale, perché semmai avrebbe bisogno di questa per inverarsi. Tuttavia, anche l'azione del singolo Stato può considerarsi decisiva per realizzare i diritti di internet.

In tal senso, una proiezione del costituzionalismo sulla rete pone, in primo luogo, una domanda di regolazione che si muove tutta nell'efficacia dei diritti verso i terzi (*Drittwirkung*)¹⁹; e una tale richiesta può trovare accoglienza, in assenza ancora di un "costituzionalismo globale", solo se la sovranità che guida l'ordinamento statale sia permeata effettivamente dai principi dello "Stato di diritto", nell'accezione più attuale e completa del termine, per cui gli stessi apparati pubblici sono sottoposti al rispetto dei diritti fondamentali e questi sono costituzionalmente conformati in modo da essere uno strumento di tutela nei confronti del potere pubblico (*Abwehrrechte*). Negli Stati che accolgono tali principi la legislazione ha dato luogo molto spesso ad una "cittadinanza digitale", anche se il complesso delle facoltà e delle pretese che questa espressione può racchiudere non è sempre del tutto chiaro, ma sicuramente vi rientrerebbe il diritto di accesso ad internet, il diritto alla formazione digitale, il diritto alla partecipazione democratica elettronica, ecc.

¹⁸ Rodotà S. *Una Costituzione per Internet?*, in *Politica del diritto*, cit., 343: "La scelta dell'antica formula della Carta dei Diritti ha una forza simbolica, evidenza che non vogliamo limitare la libertà online ma, al contrario, mantenere le condizioni affinché possa continuare a fiorire. Ecco perché occorrono garanzie «costituzionali»".

¹⁹ Sull'efficacia orizzontale dei diritti v. l'attento studio di Lombardi G., *Potere privato e diritti fondamentali*, Torino, Giappichelli, 1970, *passim*.

È ovvio che, dove lo Stato non segua la forma dello Stato di diritto e non riconosca i diritti fondamentali, questo sarà portato a sviluppare una forma di “cyberdominio”, con riferimento alla rete, sia nel rapporto tra utente e poteri privati, sia in quello tra cittadino e Stato. Infatti, nel primo caso l’intervento del potere politico nei confronti degli operatori privati della rete si può sempre dare, ma non per difendere i diritti degli utenti, quanto soprattutto per esercitare un controllo maggiore sulla rete e sugli stessi operatori privati attraverso una censura di Stato, imposta in nome della “sicurezza nazionale” (si può in proposito ricordare il conflitto tra Google e la Repubblica della Cina del 2010). Quanto, poi, al rapporto tra cittadino e Stato, qualora questo non sia improntato ai principi del costituzionalismo, assume un carattere autoritario nel quale la rete può essere assoggettata come un mezzo del dominio e del controllo sociale.

Peraltro, fenomeni di questo genere, cioè di “cyberdominio” si sono dati anche nelle democrazie occidentali. Si pensi alla denuncia di Edward Snowden sulla sorveglianza e compromissione di massa da parte della NSA nel 2013 in un contesto nel quale la lotta al terrorismo e la preservazione della sicurezza nazionale non potevano giustificare queste attività illecite, verso i cittadini americani e, parimenti, verso stati alleati. In questo caso, l’esistenza di una libera informazione (in rete e non) e di una società civile articolata con una forte presenza di associazioni che agiscono a difesa dei diritti hanno portato a conoscenza dell’opinione pubblica la violazione dei diritti fondamentali da parte del governo statunitense.

Ciò ci fa comprendere quanto potente sia la sovranità digitale e come persino nell’alterità tra governanti e governati delle democrazie si possa annidare il desiderio di privatizzare il potere pubblico.

6. La *Cybersecurity* come primo elemento costitutivo della sovranità digitale. – “Il cyberspace è diventato strategicamente indispensabile”²⁰ e gli Stati non vi possono

²⁰ Kissinger H., *Ordine mondiale* (2014), Milano, Mondadori, 2015.

rinunciare. Gli Stati hanno compreso che non possono non padroneggiare in un modo o nell'altro le tecnologie della rete, se vogliono ancora conservare la definizione di autorità statali.

Di conseguenza, il primo elemento della sovranità digitale è dato dalla capacità di organizzare cyberattacchi e di difendersi da questi, ben sapendo che le attività di aggressione attraverso la rete, in grado di minacciare e distruggere le infrastrutture di una comunità (si pensi al caso Stuxnet nei confronti dell'Iran), hanno dalla loro sia l'anonimato tecnico²¹ di simili azioni sia la mancanza di un sistema sanzionatorio internazionale.

La necessità di una funzione pubblica di *cybersecurity*²² nasce dall'esigenza di proteggere le attività digitali che ormai innervano ogni Stato, nelle politiche civili, come in quelle di carattere militare, per assicurare il suo funzionamento istituzionale e, al contempo, salvaguardare la protezione dei dati sensibili dei cittadini.

La sicurezza presuppone uno sviluppo tecnologico proprio dello Stato, in grado di liberarlo dai condizionamenti internazionali che possono derivare da forze esterne, sia politiche e sia private.

Ciò sostanzia un ulteriore compito di una vera sovranità digitale che richiede necessariamente nel bilancio dello Stato un cospicuo investimento di risorse pubbliche in infrastrutture digitali in modo da proteggere lo Stato inteso esso stesso come una "piattaforma indipendente" al servizio della propria comunità che raccolga le "identità digitali" dei propri cittadini. In tal senso, lo Stato dovrebbe spingersi sino alla costruzione di un "cloud nazionale e sovrano", in grado di

²¹ Su questo argomento v. Cipolloni C., *The right to anonymity. Overview of the institute and analysis of its evolution in the age of the web revolution*, in *Humanities and Rights global network journal*, 2023, 5(2).

²² Saraceni G., *Cybersecurity*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023, 98: "La cyber security può essere considerata come l'aspetto più evidente e allo stesso tempo problematico dell'era in cui viviamo; a causa della capillare diffusione del web, dei computer e degli smart mob, ci troviamo quotidianamente immersi in una fitta rete informatica; affidiamo agli strumenti informatici (...) i nostri dati sensibili, i nostri investimenti, i nostri risparmi, i nostri segreti".

esigere il versamento di tutte le informazioni riguardanti i propri cittadini anche se allocati su server stranieri e di imporre un controllo pubblico sulle piattaforme ²³.

7. Sulla necessità di una regolazione internazionale per internet attraverso un trattato sul Cyberspace. – Le sovranità, nella concezione storica della loro pluralità, vivevano tutte all'interno di una cornice generale data dalla Comunità e dal diritto internazionale, ma ognuna ben distinta dalle altre, grazie ai confini territoriali e al principio di non ingerenza negli "affari interni".

Già prima dell'avvento di internet non era più così. Non solo il commercio internazionale ha veicolato una forte interdipendenza tra gli Stati, e sempre più soprattutto gli affari interni hanno assunto un rilievo internazionale, così che diritto interno e diritto internazionale appaiono sempre più due aspetti di un unico problema normativo, superando la linea di ciò che è interno e ciò che è esterno.

Nel caso della rete e della sovranità digitale, questa condizione ha una proiezione ancora più evidente per via delle interdipendenze che la tecnologia ha imposto. Gli Stati adoperano internet per realizzare nuove forme di spionaggio, economico, politico e militare, e per realizzare attacchi veri e propri ai propri avversari. Non è priva di fondamento l'affermazione che "*The next war will begin in cyberspace*" ²⁴ e comunque sicuramente la tecnologia permette già ora una *cyberwarfare* che ha un ruolo importante accanto alle armi convenzionali, con il vantaggio che nei confronti dei cyberattacchi non è agevole mettere in campo forme di rappresaglia. La *cyberwarfare* mostra di essere una minaccia forse non superiore alla deterrenza delle armi nucleari, che è in grado però di dare luogo a una altrettanto pericolosa

²³ Costanzo P., *Lo "Stato digitale": considerazioni introduttive*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Genova, 18-19 giugno 2021, in https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale_Costanzo_-_Relazione_introduttiva.pdf che aggiunge: "È necessario insomma, per la sua stabilità, che anche lo Stato diventi protagonista nel cyberspazio, non solo dal punto di vista giuridico ma anche tecnico, se necessario, attraverso potenti investimenti nella creazione di infrastrutture di servizi digitali a al servizio delle sue funzioni, per il raggiungimento dei suoi scopi e per la sua conservazione (l'istituzione dell'Agenzia Nazionale per la Cybersecurity, avvenuta pochi giorni fa, sembra andare in quest'ultima direzione)" (11).

²⁴ Hughes R., *A Treaty for cyberspace*, in *International Affairs*, 2010, 2, 523-541.

escalation di tensioni geopolitiche, sino ad arrivare ad una situazione di continuo conflitto che minaccia la vita degli individui e formi nei loro governi una combinazione di insicurezza permanente e di intendimenti volti a farsi valere, per assicurarsi il primato nel *cyberspace*.

L'uso delle tecnologie nei rapporti tra gli Stati pone, perciò, il problema delle relazioni internazionali nell'era digitale.

L'ambivalenza della rete si proietta anche nei rapporti tra gli Stati: essa può fungere da veicolo per mettere in crisi e, persino, abbattere governi autoritari, rivendicare diritti e più democrazia, ma può dischiudere possibilità repressive inedite, il suo uso di per sé non assicura che a prevalere siano i valori di una convivenza libera, ordinata e fondata sulla verità.

Nella c.d. "diplomazia digitale" ciò che si avverte è la mancanza di "limiti" ai quali gli Stati, comprese le grandi potenze, si attengano in modo da creare un equilibrio condiviso e senza cedere alla tentazione di agire per provare i limiti medesimi.

Vari tentativi sono stati fatti per promuovere una regolazione internazionale di internet, alcune provenienti dagli Stati medesimi e guardano alle Nazioni Unite. Proprio su iniziativa del Segretario generale, sulla base del punto 72. dell'Agenda di Tunisi, nel 2006, è venuta la sollecitazione a istituire l'*Internet Governance Forum* come una piattaforma globale multistakeholder che facilita la discussione di questioni di politica pubblica relative a Internet, ma senza poteri di decisione. Nel 2019 è stato formulato il "*Contract for the Web*", con nove principi indirizzati ai governi, alle compagnie e agli individui, ad opera della Web Foundation e nel quale sono stati interessati alcuni governi (oltre a quello degli Stati Uniti, la Francia e la Germania), importanti trust come Pango (Anchor Free), Microsoft e Google e parecchie associazioni della società civile.

Tutto questo è ancora troppo poco. Per definire un regime internazionale della rete che abbia un carattere vincolante appare necessario un Trattato per il *Cyberspace*, che ricomponga le sovranità digitali degli Stati, limiti la conflittualità virtuale e consenta loro di gestire insieme internet, in modo trasparente e secondo una disciplina condivisa.

Bibliografia minima essenziale

- Amato Mangiameli A. C. – Campagnoli M. N., *Strategie digitali. #diritto_educazione_tecnologie*, Torino, Giappichelli, 2020.
- Barlow J. P., *A Declaration of the Independence of Cyberspace* (Davos, Switzerland, February 8, 1996).
- Bertola V., *La sovranità digitale e il futuro di Internet*, in *Riv. it. inf. dir.*, n. 1/2022, 39-47.
- Betzu M., *Poteri pubblici e poteri privati nel mondo digitale*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Genova, 18-19 giugno 2021, in [https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Marco Betzu - Poteri pubblici e poteri privati nel mondo digitale.pdf](https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Marco_Betzu_-_Poteri_publici_e_poteri_privati_nel_mondo_digitale.pdf).
- Castells M., *Volgere di millennio*, trad. it. di G. Pannofino, Milano, Università Bocconi Editore, 2003,
- Celeste E., *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic. Perspectives on Extraterritoriality and Sovereignty*, Hart 2021, https://www.researchgate.net/publication/349495575_Digital_Sovereignty_in_the_EU_Challenges_and_Future_Perspectives.
- Costanzo P., *Lo "Stato digitale": considerazioni introduttive*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Genova, 18-19 giugno 2021, in [https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale Costanzo - Relazione introduttiva.pdf](https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale_Costanzo_-_Relazione_introduttiva.pdf).
- Credi O., Vianini C., *Spazio e sovranità digitale europea*, in *IAI*, 11 luglio 2021.
- Hughes R., *A Treaty for cyberspace*, in *International Affairs*, 2010, 2, 523-541.
- Kaiser J. H., *Das Recht im Cyberspace. Eine spontane Ordnung noch ohne Hierarchie*, in *Staat und Recht*, FS für Günther Winkler, Wien, Springer, 1997, 397-409.

- Kaiser J.H., *La rappresentanza degli interessi organizzati*, trad. it., Milano, Giuffrè, 1993.
- Kissinger H., *Ordine mondiale 2014*, Milano, Mondadori, 2015.
- Lodevole, Luisa, *Cyberbullismo*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023.
- Lombardi G., *Potere privato e diritti fondamentali*, Torino, Giappichelli, 1970.
- Pohle J., Thiel T., *Digital sovereignty*, in *Internet policy review*, December 17, 2020, in <https://doi.org/10.14763/2020.4.1532>.
- Rodotà S., *Una Costituzione per Internet?*, in *Politica del diritto*, 2010, 3, 337-351.
- Rosen J., *Google's Gatekeepers*, in *New York Times Magazine*, November 28, 2008.
- Salvatori, R., *Piattaforma*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023.
- Saraceni, G., *Cybersecurity*, in Amato Mangiameli, Agata Cecilia, Saraceni, Guido, *Cento e una voce di informatica giuridica*, Torino, 2023.
- Santaniello M., *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Riv. it. inf. dir.*, n. 1/2022;
- Santaniello M., *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, n. 3/2021.
- Schmitt C., *L'ordinamento dei grandi spazi*, 1941, ora in *Stato Grande Spazio Nomos*, Milano, ADEPHI, 2015, 101-198.
- Schmitt C., *Il Nomos della Terra*, Milano, ADEPHI, 1991.
- Simoncini A., *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino. E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, 2017.