Designed for democracy

pattern di interferenza tra codici giuridici e codici informatici nei recenti casi di censura online e offline

Alberto Cammozzo – 3 aprile 2011[1]

2010, *l'anno del contatto*: tra la fine del 2010 e l'inizio del 2011 una serie di eventi hanno messo in evidenza come le reti di comunicazione globale possano esprimere entità in grado di fare fronte ai poteri territoriali tradizionali. Le vicende Wikileaks e quelle delle rivoluzioni egiziana e tunisina, per quanto diverse, hanno dimostrato quali possono essere le interferenze tra due poteri: quelli organizzati territorialmente dei governi nazionali e quelli di cittadini più o meno organizzati ma dotati volontà comune e di infrastrutture di comunicazione. Il dipanarsi delle mosse di attacco e difesa [2] tra i due poteri hanno messo in evidenza punti di forza e di debolezza dell'architettura della Rete e quindi – stando a Lessig [3] – del suo codice. Da una parte i governi hanno dimostrato una grande facilità di esercitare censura e controllo (sia sugli individui che e sulle infrastrutture). Dall'altra la facilità di replicare e spostare dati rende inefficaci questi processi di controllo. I punti critici si sono rivelati quelli in cui gli spazi territoriali si incontrano con il cyberspace. Le scelte che verranno effettuate oggi decideranno se la Rete di domani sarà disegnata per il controllo o per la democrazia. Dall'esperienza Wikileaks abbiamo appreso che ridondanza e policentrismo, ove presenti, hanno efficacemente combattuto la censura nel cyberspace. Le vicende Wikileaks e quelle nordafricane hanno mostrato invece che le strutture accentrate e legate al territorio sono quelle più soggette al controllo.

Occorre, per elaborare una matrice concettuale nella quale analizzare i fatti avvenuti, una breve premessa teorica. Immaginiamo il complesso spazio comunicativo umano come composto da due piani paralleli. Uno è il territorio, fisico e tangibile. L'altro è lo spazio delle comunicazioni chiamato cyberspace. Nel cyberspace non c'è solo internet e il web, ma anche tutto lo spazio delle comunicazioni telefoniche, radio, delle intranet. L'insieme dei due spazi forma quella che Luciano Floridi ha chiamato **infosfera** [4], uno spazio nel quale ormai si estende la nostra percezione. I due piani entrano in contatto in più punti, e il cyberspace costituisce una matrice di interscambio dati che consente ai segnali di passare da ogni punto sul territorio a qualsiasi altro punto sul territorio. Possiamo immaginarlo come l'imbottitura dei divani Chesterfield, tenuta assieme da dei bottoni: le due superfici del cuscino, quella inferiore (cyberspace, intangibile, invisibile) e superiore (lo spazio territoriale, tangibile e visibile), sono collegate dai bottoni (i nodi della rete). Diciamo quindi che il cyberspace non "esiste" fisicamente in modo separato, ma concettualmente possiamo pensarlo (e siamo abituati a farlo) come una realtà spaziale autonoma. Diciamo che i file – ad esempio quelli di Wikileaks – "sono in Internet" anche se sappiamo che sono sempre in qualche server da qualche parte sul territorio. I dati hanno bisogno di un supporto fisico e pertanto sono territoriali: *stanno* da qualche parte in un dato istante. Tuttavia la replicabilità dei dati e la velocità delle transazioni producono un effetto che possiamo chiamare di de-

1 Queste pagine sono un adattamento di quanto già espresso nel mio blog nobrainnopain.org il 5 dicembre 2010
2 Markoff, "The Asymmetrical Online War."
3 *Code and other laws of cyberspace*.
4 Floridi, "A Look into the Future Impact of ICT on Our Lives."

territorializzazione: quando sono disponibili per la fruizione da qualsiasi punto del mondo connesso alla rete, sembra che *stiano* nella rete. Al processo di de-territorializzazione corrisponde un processo simmetrico di ri-territorializzazione: quando vengono effettivamente acceduti, i dati si ri-territorializzano, cioè vengono copiati materialmente da qualche altra parte. Il concetto di territorializzazione / deterritorializzazione, di origine filosofica [5] viene applicato alla Rete nel senso da Alexander Galloway [6] che li associa ai protocolli IP associati a indirizzi collocabili sul territorio, e quello DNS, che converte tra questi e nomi a dominio, non territoriali[7]. I due piani, paralleli, sono molto diversi tra loro. Mentre tutto il territorio è suddiviso in Stati, zone geopolitiche rigorosamente non sovrapposte (salvo in caso di conflitto), il cyberspace è strutturato come un fitto groviglio (rizomatico) di reti di comunicazione e nodi in cui risiedono, si spostano e si duplicano enormi moli di dati a grande velocità. Queste reti appartengono, nella loro manifestazione territoriale, tutte a operatori commerciali o statali, e i nodi a imprese oppure a privati. E' importante ricordare che le imprese hanno sempre sede in qualche territorio e sono sempre soggette alle leggi vigenti in quel territorio, così come lo sono anche i privati cittadini. In sostanza, nessuna singola istanza di dati "risiede" realmente nel cyberspace; tuttavia –come vedremo– la massiccia ridondanza di dati che possono spostarsi rapidamente possono concretamente apparire come stanziali nella rete e non nello spazio fisico.

Premesso ciò, in cosa consiste la **censura**? Come vi si può sfuggire? Se la censura, definita in senso lato, consiste nell'impedire o alterare il flusso dei dati, possiamo classificare le censure possibili in base all'origine e alla destinazione della comunicazione. I dati possono fluire da spazio territoriale a spazio territoriale (T-T), da spazio territoriale a cyberspace (T-C), da cyberspace a territorio (C-T) e da cyberspace a cyberspace (C-C). Il caso Wilileaks rappresenta un buon esempio delle possibili censure, in quanto nei suoi confronti sono stati applicate le tecniche di censura disponibili in ciascuno dei quattro casi, e sono anche state messe in atto efficacemente risposte congruenti.

T-T. Il *primo* caso è quello in cui la comunicazione avviene esclusivamente nel territorio. Ad esempio via voce, via stampa, libri, lettera, eccetera. La censura si applica impedendo di parlare (minaccia, detenzione), alterando la comunicazione (distruzione o mutilazione dei supporti materiali, sommersione del messaggio nel rumore, alterazione dei codici, ecc.). Attualmente il fondatore e leader di Wikileaks, Julian Assange, è libero di comunicare liberamente con la stampa. Per un certo periodo ciò non è stato possibile, essendo detenuto. In un precedente periodo la comunicazione con la stampa era possibile, ma non pubblicamente, essendo ricercato. Anche le minacce di morte costituiscono il caso estremo di questo tipo di censura. A tutela della propria incolumità, Assange ha predisposto – come deterrente – il rilascio di una password che svelerebbe segreti ancora più imbarazzanti, racchiusi in files già messi in circolazione settimane fa [8]. Il file è già distribuito nella rete con quelle proprietà di ridondanza e rapida copia di cui abbiamo parlato.

T-C. Il *secondo* caso è quello che abbiamo chiamato de-territorializzazione. I dati escono dallo spazio territoriale e si immettono nella rete di comunicazione. Nel caso di Internet, il protocollo in gioco è quello IP, in quanto a blocchi di numerazioni contigue corrispondono spazi territorialmente contigui o comunque strettamente connessi. I dati sulla localizzazione geografica (geolocalizzazione) dei singoli indirizzi IP nel territorio passa attraverso le imprese che li detengono, e che devono risponderne alle autorità nazionali. La censura consiste dunque nello scollegare un dato IP o nel costringere il provider alla rimozione dei dati dal server fisicamente collocato nel territorio. Il tratto originale della risposta degli Stati nazionali sta nell'esercitare il potere o l'influenza dei governi sul

5 Deleuze and Guattari, *Capitalisme et schizophrenie*.
6 *Protocol*, 55.
7 i TLD "nazionali" sono tali solo sul piano amministrativo. I dati possono risiedere ovunque.
8 Zetter, "WikiLeaks Posts Mysterious 'Insurance' File."

territorio non tanto per censurare la fruizione dei dati, ma di inibire la loro preventiva diffusione. Nel caso di Wikileaks è impedita la presenza o ostacolata la funzionalità dei server che ospitano nei territori nazionali i dati sui cablogrammi e li diffondono nella rete, o che sostengono l'organizzazione che li diffonde. Ciò fino ad ora si è concretizzato in una catena di eventi: 1) la decisione di Amazon, che ospitava Wikileaks come un qualsiasi cliente sui suoi server, di interrompere il servizio, ufficialmente per timore di attacchi informatici, ufficiosamente per pressioni governative: 2) il servizio Paypal, usato da Wikileaks per raccogliere finanziamenti, ha annunciato[9] di aver bloccato il conto di Wikileaks [10] 3) in Francia, con una lettera poi resa pubblica, il ministro dell'industria ha fatto pressioni esplicite sulla della società OVH che ospita i dati wikileaks in terra Francese.
Che io sappia è la prima volta che si verifica una così massiccia anche se non coordinata risposta censoria dei governi al processo di deterritorializzazione. Di solito la rimozione di un server o dei dati segue una indagine della magistratura, se non una condanna.
A questo attacco alla de-territorializzazione wikileaks ha risposto con una replicazione massiccia dei dati in siti territorialmente così dislocati da essere sostanzialmente privi di una sede nazionale. Cioè con quel processo di deterritorializzazione spinto che abbiamo detto rende i dati virtualmente residenti nel cyberspace. Più importante della struttura ridondante è il processo di riconfigurazione dinamica e fluida della struttura stessa, che rende quasi impensabile —allo stato attuale delle leggi e delle tecnologie— una rincorsa delle autorità a ogni singolo sito in ogni singolo paese.

C-T. Il *terzo* caso è quello della ri-territorializzazione, con cui i dati, su richiesta di un utente sul territorio, possono essere raggiunti ovunque si trovino, sempre nel territorio. Il protocollo in gioco è il DNS (Domain Name System) che gestisce la corrispondenza tra il nome che identifica un servizio ("wikileaks.org") e l'indirizzo di un server sul territorio. Chi vuole accedere al dato lo fa attraverso un nome a dominio che corrisponde a uno o più indirizzi IP. Occorre ricordare che anche i vertici dei nomi a dominio "appartengono" a Stati, come ".it" o ".com". Questo significa che il servizio di risoluzione dei nomi viene svolto da autorità che operano su base nazionale, il più delle volte su delega statale.
La censura nel processo di ri-territorializzazione consiste nel dirottamento di un dato nome a dominio verso un altro indirizzo, il blocco di determinato indirizzi corrispondenti ai nomi a dominio censurati o la rimozione del nome a dominio.
Anche in questo caso è uno dei processi "standard" in presenza di una sentenza della magistratura, ma anche quello più usato dai governi autoritari, che filtrano il traffico verso siti che offrono informazioni pericolose o ostili. Gli enti governativi USA hanno bloccato l'accesso al sito Wikileaks, inclusa la biblioteca del congresso[11]. Occorre aggiungere che EveryDNS, il servizio (gratuito) DNSstatunitense di cui Wikileaks era cliente ha interrotto il servizio per wikileaks a causa dell'elevato traffico dovuto ai tentativi di "abbattere" il sito. Wired riferisce che più che alla censura, l'interruzione del servizio sia dovuta a una serie di gravi errori di Wikileaks [12]. Qualsiasi sia la causa di questa "censura", la risposta è stata la sostituzione di un DNS automatico e centralizzato con uno manuale e distribuito. I nuovi siti di Wikileaks spesso non hanno nemmeno un nome a dominio nuovo (come wikileaks.fr, wikileaks.ch, …), ma direttamente un indirizzo IP che viene notificato agli interessati o reso disponibile su una miriade di canali diversi (twitter, skype, wikipedia, …). Il sistema DNS automatico e centralizzato è stato sostituito con un sistema di nomi distribuito e manuale, ma facilmente automatizzabile (e che —con un certo sforzo tecnologico— potrebbe essere altrettanto autorevole). La vicenda Wikileaks potrebbe segnare l'inizio della fine del DNS come lo conosciamo oggi.

C-C. Il quarto caso è quello delle transazioni "interne" al piano delle comunicazioni a distanza.

9 https://www.thepaypalblog.com/statement.html
10 Poulsen, "PayPal Freezes WikiLeaks Account."
11 http://blogs.loc.gov/loc/2010/12/why-the-library-of-congress-is-blocking-wikileaks/
12 Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities."

Sia chiaro che si tratta di una finzione, di una astrazione, per indicare quei processi che per la massiccia replicazione dei dati in una varietà di nodi o per l'impossibilità di localizzare, cioè rintracciare l'origine o destinazione territoriale di un dato traffico, sono sostanzialmente privi di una origine o destinazione localizzabile. In questo caso gli interventi di censura si sono manifestati con degli attacchi telematici, degli eventi rubricabili sotto il nome di *cyberwarfare*, guerra telematica. Wikileaks è stato attaccato apparentemente non dalla nuovissima sezione *cyberwar* [13] del dipartimento della difesa, ma da un tale "The Jester"[14] celebre per rivendicare su twitter i suoi attacchi a siti di reclutamento di terroristi integralisti islamici, con mezzi propri[15]. La risposta di Wikileaks ancora una volta è stata la ridondanza delle risorse e probabilmente una migliore gestione della sicurezza. Nel caso della censura in Egitto, su ordine del governo, gli operatori egiziani hanno isolato funzionalmente i loro apparati in modo da non consentire alcun traffico da e verso gli indirizzi esterni, con alcune eccezioni (la borsa valori egiziana, ma non le ambasciate).

La vicenda dei cablogrammi diffusi da Wikileaks rivela **aspetti nuovi** della interazione tra spazio territoriale e cyberspace ed evidenzia tutti i possibili processi di censura dell'infosfera. A questi sono stati opposti diversi tipi di risposte, adeguate al mezzo.
Tra le novità vi è l'ampiezza dell'attacco, su tutti i fronti possibili, e il ricorso alla *sovranità nazionale* per silenziare il sito. Nonostante l'anticipo (annuncio il 24/11) dato alla notizia della diffusione dei cablogrammi (avvenuto il 28/11) il governo USA ha subito la diffusione dei dati, dimostrando che la delocalizzazione dei dati in Internet è possibile, anche se con qualche sforzo. Nei prossimi tempi vedremo da una parte dei tentativi di rafforzare il controllo delle sovranità territoriali sul Cyberspace, (sperabilmente con l'intervento di magistratura e parlamenti, e non solo degli esecutivi). Dall'altro lato osserveremo lo sforzo degli architetti della Rete di renderla sempre più indipendente da autorità o risorse soggette alla localizzazione nazionale e alle pressioni degli esecutivi. Da una parte codice giuridico: accordi internazionali verso una maggiore celerità di intervento transfrontaliero e un controllo delle risorse sul territorio (ISP, società di hosting, cittadini); dall'altra codice informatico per l'automazione della ridondanza e del policentrismo dei servizi essenziali ai processi di delocalizzazione e rilocalizzazione: in particolare nuovi sistemi di risoluzione dei nomi e di replicazione delle risorse. In mezzo, forse, il singolare processo politico chiamato "Internet Governance", il cui ruolo forse non riguarderà solo Internet. L'infosfera del futuro emergerà dall'interazione di questi processi.

Possiamo vederne i semi nei **progetti** in cantiere oggi. Evgeny Morozov [16] elenca alcuni dei programmi che possono affrontare le attuali debolezze e rendere la rete più resiliente nei confronti di interventi "esterni".

> *Remarkably, the Cablegate saga has already spurred (or boosted) several nonprofit initiatives that aspire to provide the kind of online services that are essential to a controversial project like Wikileaks—and do so in a more decentralized and resilient fashion. A handful of projects bearing unashamedly geeky names like P2P DNS, ProjectIDONS, and 4LW seek to create an alternative system for managing domain names that would be less pliable to political interference. Another new project—called Unhosted —seeks to decouple applications that run in the cloud from the user data that they store or generate; the idea is that if the data is stored in a distributed and encrypted manner across*

13 http://en.wikipedia.org/wiki/Cyber_Command
14 http://twitter.com/th3j35t3r
15 Si veda ad esempio: http://vimeo.com/17268609
16 Morozov, "Wiki Rehab."

a number of unrelated servers, it may reduce the power of whoever owns the app.

P2P DNS[17] pare ancora un embrione, anche se l'idea di un DNS peer-to-peer non è nuova [18]. Project IDONS[19] è ancora una lista di discussione. 4LW (four little words)[20] è un progetto (per così dire) già finito: sostituisce lo spazio gerarchico dei nomi a dominio con dei nomi mnemonici. Un algoritmo mnemotecnico sostituisce parole ai numeri. Unhosted[21] non riguarda il DNS e sembra il progetto più maturo, già a livello di *proof-of-concept*. La filosofia è quella del "FLOSS as a service on top of a commodity infrastructure": disaccoppiare la piattaforma hardware dal servizio che il software svolge. Un vero salto qualitativo che consentirebbe alle applicazioni una elevata mobilità (e replicabilità).

Oltre alla replicazione massiccia dei dati e la loro mobilità, occorre rendere conto della loro autenticità ed integrità. In ciò giocano un ruolo fondamentale le tecnologie di crittografazione dei dati. E' prevedibile che queste, attualmente impiegate a livello soprattutto di rete e trasporto si sposteranno verso l'alto a livello applicazione. Un'altra possibile previsione è che vi saranno risposte anche da parte degli Stati sovrani, che cercheranno di difendere la loro capacità di esercitare il potere con nuovi strumenti. Rivoluzione in corso: occorre tenere gli occhi aperti sui nuovi codici che emergono: al codice informatico delle nuove architetture della rete si accompagneranno i codici giuridici di nuove architetture istituzionali. L'interferenza tra questi codici dirà de la rete di domani sarà uno strumento per il controllo o per la democrazia [22].

Riferimenti

Deleuze, Gilles, and Félix Guattari. *Capitalisme et schizophrenie*. Éditions de minuit, 1980.

Floridi, Luciano. "A Look into the Future Impact of ICT on Our Lives." *The Information Society* 23, no. 1 (2007): 59-64.

Galloway, Alexander R. *Protocol*. MIT Press, 2004.

Lessig, Lawrence. *Code and other laws of cyberspace*. Basic Books, 1999.

Markoff, John. "The Asymmetrical Online War." *New York Times*, April 3, 2011. http://bits.blogs.nytimes.com/2011/04/03/the-asymmetrical-online-war/.

Morozov, Evgeny, and John Palfrey,. "Economist debates: Internet democracy", February 23, 2011. http://www.economist.com/debate/days/view/662.

Morozov, Evgeny. "Wiki Rehab." *The New Republic*, January 7, 2011. http://www.tnr.com/article/politics/81017/wikileaks-internet-pirate-party-save.

Poulsen, Kevin. "PayPal Freezes WikiLeaks Account." *Wired*, December 4, 2010. http://www.wired.com/threatlevel/2010/12/paypal-wikileaks.

———. "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities." *Wired*, December 3, 2010. http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.

Zetter, Kim. "WikiLeaks Posts Mysterious 'Insurance' File." *Wired*, July 30, 2010.

Zhang, Qiang, Zheng Zhao, and Shu Yantai. "P2PDNS: A Free Domain Name System Based on P2P Philosophy." *Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on* (May 2006): 1817 - 1820.

17 http://p2pdns.baywords.com Il sito ora è vuoto. La discussione sembra essere ora su http://dns-p2p.openpad.me/1?

18 Zhang, Zhao, and Yantai, "P2PDNS: A Free Domain Name System Based on P2P Philosophy."

19 http://forums.gctip.org/forum-34.html

20 http://4lw.org/

21 http://www.unhosted.org/

22 Morozov and Palfrey,, "Economist debates: Internet democracy."