Diritti digitali e liberta' negate.

(Marco A. Calamari – Progetto Winston Smith)

Abstract:
"*I diritti digitali negati e l'uso della Rete e delle nuove tecnologie telematiche a fini repressivi e di controllo sociale sono argomenti assolutamente sottovalutati anche da chi della difesa dei diritti civili ha fatto una missione. Le motivazioni economiche ed i mezzi tecnici che ne sono alla base sono in gran parte noti, e le previsioni su questa deriva tecnologico/autoritaria largamente condivise dagli addetti ai lavori. La sua pericolosita' sociale e politica e' purtroppo assai sottostimata quando non completamente trascurata anche nelle sedi storiche che di diritti civili si occupano*"

Devo iniziare questo intervento con una considerazione personale.

Parlare di diritti digitali e di liberta' negate nel cyberspazio in un contesto dove tortura, uccisioni, e schiavitu' sono discusse nella loro dimensione reale e spaventosa mi ha messo in difficolta'.
Da operatore di Internet, da attivista per i diritti civili della Rete con l'iniziale maiuscola, ho avuto difficolta' a trovare un modo per spiegare perche' io ritengo, perche' in tanti riteniamo che quello che succede oggi in Rete sia altrettanto grave, e forse per certi aspetti piu' grave delle violazioni dei diritti della persona perpetrate da tempo ed ancora oggi.

Provo a dirlo in una frase. Perche' non si tratta di lottare contro un male antico e noto, ma di permettere ad un male nuovo che, se non contrastato, portera' inevitabilmente a conseguenze tanto gravi quanto prevedibili, di crescere liberamente senza controllo. E' una situazione storica ben nota, come quella della crescita de potere di Hitler durante e dopo la Repubblica di Weimar.

Data la complessita' del fenomeno, consentitemi di descriverlo tramite un parallelo con la colonizzazione americana.

Internet fin dall'alba dei tempi (dei suoi tempi, il vicino 1970) e' stato un territorio di frontiera, per certi versi selvaggio, per altri quasi democratico alla maniera delle citta' greche o delle tribu' dei nativi americani.
E proprio come questo ultimo popolo gli abitanti della Rete prima dell'e-commerce e delle dot com erano (e cercano ancora di essere) un popolo di eguali in cui l'unica gerarchia valida e condivisa e' la reputazione.

Ma ora e' arrivata la "ferrovia", la civilta', gli interessi economici, politici, polizieschi e di potere, ed alle poche centinaia di migliaia di nativi si aggiungono miliardi di persone, tra poco una buona parte della popolazione del pianeta, e questo mondo viene inesorabilmente sommerso dal turismo e travolto dai fast food, e con esso una intera civilta' autonoma ed autoctona.

Ma questo fatto grave quanto triste di scomparsa di una minoranza non e' assolutamente il peggiore. Le risorse di questo mondo virtuale (che virtuale non e' affatto, meglio sarebbe parlare di "reale digitale"), il circolo virtuoso della creazione di conoscenza, il progresso non influenzato da interessi economici, e le sue ricadute positive sul mondo materiale, che tanto sviluppo e forza hanno dato agli individui, vengono inesorabilmente trasformate in strumenti di controllo oggi usati a fini di controllo sociale, intrinsecamente oppressivi e repressivi, che il Grande Fratello di Orwell non avrebbe nemmeno potuto sognare.

L'empowerment che gli individui ricevono da parte della Rete, quel superpotere che ha reso superflui servizi antichi come la posta o le biblioteche, e permette di aggirare propaganda e monopoli, si diffonde sempre piu', e proprio per la sua larghissima diffusione anche il suo lato oscuro diventa uno strumento oscuro persino piu' formidabile.

Mano a mano che la vita di relazione, telematica, commerciale, emozionale, si trasferisce in rete, una quantita' inimmaginabile di dati personali viene registrata dalle mille fonti tecnologiche che formano la Rete e memorizzata in archivi sia legali che paralegali od illegali. Questi archivi, consultati con tecniche sempre piu' sofisticate e spesso ben custoditi segreti di colossi industriali come Google, facebook od Acxiom, permette di conoscere attivita' passate e presenti di chiunque passi anche solo una piccola parte del suo tempo in Rete o collegato con altri mezzi telematici di massa, come i telefoni cellulari.

Tecniche ormai considerate elementari di elaborazione dati permettono anche di de-anonimizzare i dati personali che, come per esempio certi dati clinici, vengono resi disponibili per fini scientifici dopo che le informazioni identificative sono state cancellate per renderli anonimi. I dati personali raccolti possono essere utilizzati dopo anni, al momento del bisogno, in maniera e per fini oggi non prevedibili. I database si ingrandiscono e diventano sempre piu' pericolosi per la democrazia ed i diritti civili.

Cosa avrebbe potuto fare la STASI, la polizia politica della ex-DDR, se avesse potuto disporre di informazioni complete sulla localizzazione passata e presente di ogni cittadino tedesco, ed avesse potuto intercettare le comunicazioni di chiunque senza nemmeno sguinzagliare una spia, utilizzare un delatore od aprire un faldone? Con una semplice ricerca in un database avrebbero potuto individuare ogni riunione "sovversiva" presente o passata, ricostruire reti di relazioni tra persone. Avrebbero avuto insomma a disposizione strumenti incredibilmente piu' potenti e pericolosi del poveri microfoni e telecamere con cui il povero Grande Fratello era comunque riuscito a costruire la sua distopia autoritaria.

Il tecnocontrollo sociale e' molto piu' pericoloso, perche' puo' essere esercitato in maniera silenziosa, automatica e sopratutto economica, sulla totalita' della popolazione. Puo' quindi essere impercettibile e nascosto (come in effetti oggi e') e per questo e' piu' potente e piu' pericoloso di quello di una polizia segreta orwelliana.

E questo e' il problema di liberta' negata, di diritti cancellati.

Anche se in Europa ed in misura minore negli Stati Uniti alcune misure legali cercano di porre limiti all'abuso oltre ogni limite di dati personali, banali giochetti di scambi di dati transfrontalieri o tra societa' che sono scatole vuote permette a societa' ignote ai piu' (come Acxiom) o ad agenzie governative, che sono dotati di mezzi informatici del calibro di quelli di Google di creare ed utilizzare questi "archivi di tutti e di tutto". Persino agenzie governative americane hanno ormai appaltato ai privati molti dei servizi di intelligence una volta appannaggio di bureau come quelli de "I tre giorni del Condor". In questo modo possono evitare di rispettare quello poche norme garantiste (come il FOIA - Freedom of information act).

La rete e' penetrata anche nei paesi con regimi meno rispettosi dei diritti umani. In questi paesi, dove l'accesso alla Rete e' limitato in vari modi, talvolta soggetto ad autorizzazioni preventive e limitato ad una piccola frazione della popolazione, esiste la capacita' dei governi di intercettare il lavoro dei giornalisti e degli attivisti dei diritti civili, spiandolo, condizionandolo od impedendolo a piacimento, e percio' escludendolo da tutti i moderni mezzi di comunicazione e diffusione delle informazioni.

Ma cosa succede nei paesi delle cosiddette “democrazie compiute”?
Un ~~sottile filo rosso~~ percorre molte delle iniziative tecniche, commerciali e legislative che vengono discusse in questo periodo o che si affacciano all'orizzonte.

Una per tutte, l'accordo in discussione tra Google e Verizon, che rappresenta il primo esempio di violazione della neutralita' della Rete, cioe' del diritto di tutti i contenuti di circolare in rete alle stesse condizioni. Privilegiarne alcuni a scapito di altri ha un nome ben preciso, censura. ma il modo in cui queste notizie vengono riportate e commentate sui media impedisce anche a persone familiari con la Rete di cogliere le implicazioni sociali di una perdita della neutralita' della Rete. Aldila' dell'accordo tra i due big, gia' gli accessi wireless via cellulare, in cui il fornitore di accesso e' anche il fornitore di alcuni contenuti, non sono mai stati neutrali; solo la Rete cablata in effetti lo e'.

Che la Rete sia intercettata ed i dati di tutti i suoi cittadini frequentano siano sistematicamente raccolti e memorizzati e' cosa ormai nota; che questo succeda anche con i telefoni cellulari ed altri oggetti ed azioni comuni (telepass, carte di credito, transazioni bancarie) lo e' quasi altrettanto.

Il ~~filo rosso~~ che seguiamo unisce le iniziative che apparentemente riguardano la Rete, ma il cui impatto riguarda il mondo materiale. Le tecnologie di controllo sociale e di censura che la Rete ha permesso di realizzare sono ormai largamente usate. E se nel mondo occidentale gli esempi che se ne hanno viaggiano ancora sotto la soglia della percettibilita' dei cittadini, in altri paesi, Russia, Iran ma sopratutto Cina, il monitoraggio sistematico della Rete e l'applicazione di tecniche censorie automatizzate e' la regola. In questi ed altri Paesi la Rete non e' mai stata libera e neutrale, ma e' arrivata completamente permeata di censura e tecnocontrollo, attuati in maniera sistematica, paradossalmente maggiore persino dei paesi occidentali in cui la Rete esiste da molto piu' tempo.

La Rete possiede tuttavia anticorpi "naturali", che la rendono resistente ad iniziative di censura e controllo, prime tra tutti la crittografia ed il Software Libero ed aperto (quali Pgp, remailer anonimi, Tor, Freenet).
L'uso di queste tecnologie permette di recuperare in parte gli spazi di liberta' ed i diritti negati, aggirare la censura, sfuggire al tecnocontrollo e recuperare riservatezza e privacy.

Cosa succede in Italia, paese occidentale di democrazia compiuta? Lungo il tratto italiano del ~~filo rosso~~ si trovano legate insieme vecchie iniziative come la data retention del decreto Pisanu, la cui dipartita, come avrebbe detto Mark Twain, e' stata (purtroppo) largamente esagerata. Le previsioni del decreto Pisanu, ridotte ma sempre pericolose sono ancora li'.

Alle vecchie iniziative se ne sono aggiunte di nuove, come l'istituzione ed il pronto ed incredibilmente generoso finanziamento del CNCP (Centro nazionale di contrasto alla pedopornografia).

Questa istituzione, che ha uno scopo ineccepibile (ma anche "evergreen") usato in tante occasioni per giustificare iniziative repressive contro la Rete, e' un perfetto strumento di censura. Il CNCP viene infatti utilizzato per gestire il meccanismo di controllo della censura di siti internet. Insieme ad altre misure tecnologiche, rese obbligatorie per i provider, completa una struttura tecnico-legale che permette con un preavviso brevissimo di far scomparire dalla Rete come la vedono i cittadini italiani qualunque sito o risorsa internet.

Per gli attivisti italiani dei diritti civili in Rete era chiaro che si

trattava di prove generali di funzionamento di una struttura tecnico legale di censura di Stato. C'e' voluto il caso di The Pirate Bay per svegliare le coscienze dei non addetti ai lavori. Poche, ma alcune si sono svegliate. Esistono inoltre gia' precedenti di siti cancellati con procedura di urgenza per denunce di diffamazione senza nessuna tutela per il censurato e per la generalita' dei cittadini della Rete.

Riassumendo, in questi primi anni del nuovo millennio si sta configurando, anche nelle democrazie, l'apparato tecnico-legale di uno stato (o di un super-stato) di polizia, in cui il controllo sociale e' attuato in maniera infallibile e pervasiva.

Alla tecnologia usata per fini repressivi e' possibile e necessario opporre tecnologia per recuperare spazi di liberta', quindi oltre a:

- alzare il livello di percezione del problema dei diritti civili digitali, oggi vicino allo zero anche tra addetti ai lavori, e zero tra i politici a tempo pieno;

- portare avanti proposte legislative specifiche, come il DDL di Turco/Mecacci/PWS contro la Data Retention, finalizzate a "colpire" dettagli fondamentali del nuovo corpus legislativo che realizza e supporta il tecnocontrollo sociale;

e' anche necessario realizzare e diffondere soluzioni "tecnologiche" per mitigare od eliminare il problema della censura e del controllo sociale tecnologico

Tre proposte operative:

"Professione: inforeporter" - una iniziativa in/formativa che si propone di mettere a disposizione di giornalisti di paesi censurati e reporter in zone di guerra quelle tecnologie anticensura e di anonimato tecnologico che permettono di aggirare ogni forma di censura informatica e comunicare senza temere intercettazioni e ritorsioni, utilizzando strumenti quali Tor, Freenet e Pgp.
Il Progetto Winston Smith e Peacereporter hanno gia' realizzato una iniziativa di questo tipo,
"Libera l'informazione online" http://it.peacereporter.net/libera/
L'associazione radicale Agora' Digitale ed il Progetto Winston Smith sono pronti a realizzare documentazione e corsi destinati in prima battuta a giornalisti, per diffondere ed istituzionalizzare le tecnologie per la privacy e l'anonimato tecnologico.

RoseBox - un gruppo di lavoro nato in Agora' Digitale e supportato dal Progetto Winston Smith, ha realizzato un prototipo di RoseBox, una scatoletta senza comandi (e' preconfigurata) che permette di soddisfare le esigenze di privacy, di anonimato, di comunicazione libera e di non-tecnocontrollabilita' secondo necessita' e preferenze individuali. La RoseBox permette, se opportunamente configurata, anche di aiutare altri cittadini della Rete a non cadere vittime della censura e del tecnocontrollo sociale, fornendo servizi per la privacy come remailer anonimi, proxy anticensura e nodi Freenet

Parlamentari Anonimi - poiche' svariate legislazioni europee stanno "derivando" verso un quadro che vorrebbe limitare l'uso di queste tecnologie, e' stata elaborata un'azione di disobbedienza civile che prevede l'installazione di una RoseBox personale da parte di parlamentari e MEP, particolarmente in quei paesi in cui lo status della tecnologie crittografiche e' borderline, od in cui
Questo sara' accompagnato, ove possibile, dall'installazione di altre RoseBox configurate per il supporto pubblico delle comunicazioni libere e non intercettabili presso sedi pubbliche ed istituzionali.