Ciberspazio e diritto, vol. 16, n. 54 (3-2015), pp. 387-401

Internet e le espressioni d'odio: influenza della tecnologia e strategie di contrasto

Giovanni Ziccardi[1]

Sommario: 1. Internet quale mezzo facilitatore dell'odio online? – 2. L'origine della rete quale causa di diffusione delle espressioni violente – 3. La rete quale strumento di contrasto nel panorama tecnologico attuale

1. Internet quale mezzo facilitatore dell'odio online?

Uno dei temi oggetto di dibattito quando si discute della circolazione delle espressioni d'odio online è quello dell'*eccessiva criminalizzazione della rete* o, comunque, di una visione distorta – soprattutto da parte del mondo politico e dei legislatori – dell'attuale architettura informatica.

L'idea errata è che Internet vada ulteriormente regolamentata in quanto mezzo *facilitatore* della diffusione e della potenzialità dell'odio che circola online e che è diretto nei confronti di gruppi, minoranze o singoli individui.

Si tratta di un punto molto importante: se non si mantiene salda la convinzione della rete come strumento *neutro*, cosa a nostro avviso necessaria, un simile approccio può portare a conseguenze sociali e legislative di grande conflitto.

Se il potere politico, ad esempio, continuerà a percepire la rete quale fonte di pericolo *ex se*, le riforme normative saranno portate in un'ottica di controllo, di soffocamento della libertà di manifestazione del pensiero, di raccolta indiscriminata dei dati degli utenti, di opzioni di blocco delle connessioni globali in un Paese grazie a un semplice *interruttore statale*, di una criminalizzazione sempre più stringente di reati delicati quali quelli d'opinione.

[1] Professore di Informatica Giuridica, Università degli Studi di Milano.

La diffusione dell'odio tramite Internet sarà vista come un'*aggravante*, l'anonimato sarà limitato o vietato e la crittografia proibita. In tal modo, tutta la forza positiva che la rete potrebbe portare, non solo per combattere l'odio online ma nella vita quotidiana dei cittadini e delle imprese, rischierebbe di essere vanificata.

Se gli utenti, a loro volta, percepiranno alcuni ambienti come più *pericolosi* e più frequentati da *haters* rispetto ad altri, migreranno verso servizi telematici più sicuri, proprio come avviene quando si abbandonano i quartieri a rischio per individuare zone più tranquille della città. La regolamentazione tecnologica dell'odio può avere, quindi, anche un grande impatto *economico*: la degenerazione dell'ambiente all'interno di alcuni social network per mancanza di controllo può portare a una perdita sensibile di utenti e clienti.

Se, infine, i grandi fornitori di servizi di telecomunicazioni dovessero percepire un ambiente sfavorevole sia dal punto di vista del quadro legislativo che devono rispettare – ad esempio con previsioni di ipotesi di responsabilità oggettiva, di obblighi di controllo non sostenibili economicamente o con indagini penali "esemplari" avviate nei confronti dei dirigenti delle aziende più importanti – sia dal punto di vista dell'immagine (ad esempio: apparendo ai loro utenti quali *censori* spietati e antidemocratici), potrebbero condizionare l'intero mondo delle comunicazioni variando le regole di accesso e contrattuali o, addirittura, abbandonando il mercato in alcuni Paesi.

I tre esempi riportati poco sopra dovrebbero far comprendere che l'intervenire sull'ecosistema digitale in maniera *liberticida*, pur con la nobile idea di osteggiare le espressioni più volente e lesive della dignità dell'uomo e, spesso, dei più deboli, porta a tre conseguenze immediate senza minimamente migliorare la situazione della circolazione delle espressioni d'odio: l'alterazione del sistema dei diritti e della protezione della libertà di manifestazione del pensiero, l'alterazione dei comportamenti e delle preferenze degli utenti e l'alterazione delle strategie commerciali dei grandi *player*, con una conseguenza diretta sull'economia del settore digitale.

Purtroppo, o per fortuna, l'architettura alla base di Internet e delle informazioni che vi circolano è molto particolare. È condizionata ancora dal modo in cui la rete è nata, ossia come mezzo di comunicazione poco sicuro ma, al contempo, molto *aperto* e *poco controllabile* (sono celebri le

Abstract

Internet e le espressioni d'odio: influenza della tecnologia e strategie di contrasto

Il tema delle espressioni d'odio in rete solleva, per il giurista, numerose problematiche nuove. In particolare, ci si domanda se Internet abbia agevolato la diffusione e le potenzialità delle espressioni violente sino a creare non pochi problemi politici e giuridici o se, al contrario, le nuove tecniche di comunicazione abbiano facilitato il contrasto e la lotta all'odio circolante. Nell'articolo l'autore analizza sia i lati negativi sia i lati positivi del quadro tecnologico attuale suggerendo spunti di riflessione e idee per il contrasto del fenomeno.

Internet and expressions of hatred: the influence of technologies and counter-strategies

The theme of the expressions of hatred on the net raises, for the jurist, many new problems. In particular, whether the Internet has facilitated the spread and potential of violent expressions up to create many political and legal issues or if, on the contrary, the new techniques of communication have facilitated the contrast and the fight of the hate speech circulating. In the article the Author analyzes both the negative and the positive aspects of the current technological framework, suggesting insights and ideas to combat the phenomenon.

Giovanni Ziccardi

Ciberspazio e diritto, vol. 16, n. 54 (3-2015), pp. 405-420

La disciplina dei nomi a dominio e i rimedi esperibili in caso di *cybersquatting*

Silvia Martinelli[1]

Sommario: 1. La nozione di nome a dominio – 2. Il ruolo dell'ICANN – 3. La tutela del nome a dominio ai sensi del Codice della Proprietà Industriale – 4. Il fenomeno del *cybersquatting* o "domain grabbing" – 5. La procedura di riassegnazione per i domini "gTLD" – 6. Le procedure di opposizione e di riassegnazione per i domini ".it" – 7. La procedura di riassegnazione per i domini ".eu" – 8. Il *cybersquatting* come pratica commerciale scorretta e l'ulteriore tutela presso l'AGCM

1. La nozione di nome a dominio

L'espressione "nome a dominio" o "dominio Internet" indica una serie di stringhe alfanumeriche separate da punti che identificano un sito web su Internet.

Le comunicazioni tra computer avvengono tramite l'Internet Protocol (IP), che assegna a ogni terminale sulla rete un indirizzo IP, composto di numeri separati da punti (ad esempio: 123.81.110.7).

Il 23 giugno del 1983 Paul Mockapetris, Jon Postel e Craig Partridge hanno ideato il Domain Name System (DNS), che converte gli indirizzi IP in parole, consentendo in tal modo l'utilizzo di indirizzi più facili da memorizzare (ad esempio: http://www.silvia.it).

Il DNS è realizzato tramite server su base gerarchica ad albero rovesciato ed esistono domini di primo, secondo e terzo livello.

Il nome a dominio di primo livello, cosiddetto Top Level Domain (TLD), costituisce il vertice della gerarchia ed è rappresentato, nel nome

[1] Dottoressa in Giurisprudenza, Perfezionata in "Informatica Giuridica" all'Università degli Studi di Milano.

a dominio, dall'ultima parte della stringa alfanumerica (ad esempio: ".it", ".net", ".com", ".eu").

Tramite il Top Level Domain s'identifica l'amministratore di tutti i nomi a dominio che riportano tale TLD.

La Internet Assigned Numbers Authority (IANA)[2], classifica i domini di primo livello in tre tipi differenti: domini di primo livello nazionali (country code top-level domain, o ccTLD); domini di primo livello generici (generic top-level domain, o gTLD); domini di primo livello infrastrutturali (infrastructure top-level domain).

I ccTLD sono solitamente riferiti a Stati o ad aree geografiche, mentre i gTLD sono stati liberalizzati nel 2012 e possono essere utilizzati da molteplici soggetti (ad esempio: organizzazioni internazionali, imprese, etc.).

I domini di secondo livello identificano uno specifico sito Internet (ad esempio: www.silvia.com), mentre i domini di terzo livello consentono al titolare di un dominio di secondo livello di creare delle sottosezioni all'interno del sito.

2. Il ruolo dell'ICANN

L'Internet Corporation for Assigned Names and Numbers (ICANN), istituito nel 1998 in California, è un ente no-profit incaricato della gestione del DNS tramite un contratto stipulato con il Dipartimento del Commercio degli Stati Uniti d'America.

Negli anni ha acquisito una fondamentale importanza nella gestione dei nomi a dominio di tutto il mondo ed è stato riconosciuto come autorità regolativa in materia dagli Stati nazionali, divenendo l'ente responsabile per la gestione e il coordinamento del Domain Name System sopra illustrato.

Le procedure di registrazione dei nomi a dominio sono gestite dai Registrar, soggetti accreditati dallo stesso ICANN (sulla base di requisiti tecnici, organizzativi e finanziari) al fine di fornire tale servizio.

[2] La Internet Assigned Numbers Authority (IANA), emanazione dell'ICANN (Internet Corporation for Assigned Names and Numbers) delega la gestione di blocchi di indirizzi IP ad enti locali denominati Regional Internet Registries.

Abstract

La disciplina dei nomi a dominio e i rimedi esperibili in caso di cybersquatting

Le procedure per ottenere giustizia in caso di questioni legali relative ai nomi di dominio sono varie e di differente complessità. In questo articolo l'autrice analizza il fenomeno del cybersquatting e le modalità migliori per ottenere la riassegnazione del nome di dominio rivolgendosi a enti per la risoluzione delle dispute nazionali e internazionali, descrivendo in sintesi i requisiti necessari e le procedure da seguire.

The discipline of dominion names and possible remedies in cases of cybersquatting

The procedures to obtain justice in the case of legal issues relating to domain names are different and of different complexity. In this article the Author analyzes the phenomenon of cybersquatting and wich are the best means to obtain the re-assignement of the domain name, addressing bodies for the resolution of national and international disputes and describing a summary of the requirements and procedures to be followed.

Silvia Martinelli

Ciberspazio e diritto, vol. 16, n. 54 (3-2015), pp. 423-438

Open source e profili di costituzionalità

Francesco Laprovitera[1]

Sommario: 1. Il Laboratorio di Information and Communication Technologies (ICTs) – 2. La legge regionale n. 9 del 26 marzo 2009 – 3. La sentenza n. 122/2010 della Corte Costituzionale – 4. L'esperienza del CSI-Piemonte – 5. Il progetto Open Innovation

1. Il Laboratorio di Information and Communication Technologies (ICTs)

La regione Piemonte, insieme all'Umbria, è ed è stata nell'ultimo decennio una delle regioni che hanno portato idee e innovazioni nell'ambito dell'*open source* nella Pubblica Amministrazione, manifestando attivamente il suo interesse nei confronti dei sistemi e delle applicazioni OS. Numerosi sono stati i progetti e i piani di lavoro elaborati dalla Regione, la quale si è posta fin da subito come apripista d'importanti attività a livello nazionale. Il 26 aprile 2004 con Deliberazione della Giunta Regionale nasce il Laboratorio di "Information and Communication Technologies (ICT)" il quale si propone di elaborare "modelli tecnologici ed organizzativi" da condividere con le altre Pubbliche Amministrazioni piemontesi e di rendere disponibile tutta la documentazione tecnica alle aziende del settore. Il laboratorio studia e sperimenta le nuove tecnologie dell'informazione e della comunicazione con il duplice obiettivo di: i) individuare le potenzialità e le possibili applicazioni di tali tecnologie all'interno del *Sistema Informativo Regionale* (*SIRe*), e ii) favorire l'elaborazione e la condivisione di nuovi modelli tecnologici e organizzativi tra le Pubbliche Amministrazioni piemontesi.

La rilevanza del modello proposto dal Laboratorio sta proprio nella possibilità di rappresentare un valido strumento per la gestione e la condivisione del patrimonio informativo – e conoscitivo – della Pubblica Ammi-

[1] Dottore in Giurisprudenza.

nistrazione. Il Laboratorio ha infatti adottato il concetto di "conoscenza aperta" per farne un vero e proprio "metodo di lavoro" e ha individuato nel codice sorgente uno dei principali temi di esplorazione, con l'obiettivo di promuovere "la diffusione di sistemi e di applicazioni *open source* all'interno della P.A. piemontese attraverso lo sviluppo e la realizzazione di progetti pilota". Il Laboratorio è un'iniziativa unica nel panorama delle PP.AA., uno strumento fondamentale e trasversale per le ICT piemontesi. Le attività del Laboratorio, nella fase attuale, riguardano alcuni filoni di attività ritenuti di particolare rilevanza. Si segnala l'impegno del laboratorio nei seguenti ambiti: *Business intelligence, Office automation*, Piattaforme tecnologiche, Sicurezza *ICT, Web* e Multimedia, *Wired* e *wireless.*

Nell'ambito dell'*office automation* si segnalano le più importanti innovazioni *open source*. La diffusione di sistemi e applicazioni *open source* di *office automation* alternativi a quelli proprietari all'interno della Pubblica Amministrazione piemontese è infatti uno degli obiettivi primari del Laboratorio ICT, che si concretizza con la realizzazione di alcuni progetti pilota, i quali utilizzano il famoso sistema operativo *open source* GNU/Linux. Poiché *Linux* è molto apprezzato e utilizzato come sistema operativo per macchine server si è deciso di orientare la sperimentazione verso un utilizzo di tipo *desktop*, più mirato alla postazione di lavoro. Il sistema operativo scelto è *Mandrake Linux*[2] (rinominato *Mandriva* dopo le fusioni con *Connectiva* e *Lycoris*). L'obiettivo principale del laboratorio di Innovazione *ICT* della Regione Piemonte è proprio il verificare concretamente quali soluzioni *ICT* possano essere impiegate nel contesto operativo dell'Ente per assicurarne una migliore qualità e un adeguato sviluppo tecnologico, e le sue attività si concentrano pertanto sul raggiungimento di questi obiettivi. Numerosi sono gli esempi[3] nei quali l'impiego di soluzioni OS è stato positivamente riconosciuto ed adottato: la creazione di una architettura di livello dipartimentale con *software OS* per il Parco della Collina Tori-

[2] *Mandriva Linux* (in precedenza conosciuta come *Mandrake Linux*), era una distribuzione GNU/Linux prodotta da *Mandriva SA*, orientata principalmente ai computer desktop, alla facilità di gestione ed installazione, particolarmente consigliata agli utenti meno esperti, il cui sviluppo è terminato nel 2012. www.linux.com/directory/Distributions/popular-distributions/mandriva-linux.

[3] M. Ancilli, G. Pastore, *L'Open Source della Regione Piemonte*, pubblicato in «*e-Gov*», 12 (2008), pp. 62-64. www.regione.piemonte.it/laboratorioict/studi_approf/21_04_09b.htm.

Abstract

Open source e profili di costituzionalità

La regione Piemonte, insieme all'Umbria, è stata nell'ultimo decennio una delle regioni che hanno portato idee e innovazioni nell'ambito dell'*open source* nella Pubblica Amministrazione, manifestando attivamente il suo interesse nei confronti dei sistemi e delle applicazioni OS. Numerosi sono stati i progetti e i piani di lavoro elaborati dalla Regione, la quale si è posta fin da subito come apripista d'importanti attività a livello nazionale. In questo articolo l'autore ripercorre le problematiche tecniche e giuridiche che sono state affrontate a livello locale e a livello nazionale.

Open source and outlines of constitutionality

The Piedmont region, along with the Umbria, has been in the last decade one of the regions that have brought ideas and innovations in the field of open source in the public administration, actively expressing his interest in systems and applications OS. There have been several projects and work plans developed by the Region, which has set itself right away as a forerunner of important activities at the national level. In this article the author traces the technical and legal issues that were addressed at a local and national level.

Francesco Laprovitera

Ciberspazio e diritto, vol. 16, n. 54 (3-2015), pp. 441-457

Il cyberstalking e il cyberbullismo: l'evoluzione del fenomeno a sei anni dall'entrata in vigore dell'art. 612-*bis* del codice penale

Marcello Bergonzi Perrone[1]

Sommario: 1. Introduzione. – 2. Lo stalking nella *letteratura* scientifica psichiatrico-forense – 3. Stalking e bullismo: differenze – 4. Il *cyberstalking* e il cyberbullismo – 5. Conclusioni: la diffusione del fenomeno del cyberbullismo e del cyberstalking

1. Introduzione

A distanza di ormai cinque anni da un mio primo intervento[2], vale la pena riprendere il tema non più sotto l'aspetto squisitamente tecnico-giuridico, di analisi della allora nuova normativa, ma meta-giuridico. Si affronterà qui, ora, un'indagine comparata da un punto di vista statistico e socio-criminologico, per individuare quali siano le differenze tra le figure "tradizionali" di stalking e bullismo e le loro manifestazioni "virtuali": il cyberstalking e il cyberbullismo.

Che si avverta l'esigenza di porre dei distinguo tra i due ambiti, e di affrontare l'indagine, è ormai intuitivo, visto l'ampio risalto dato ai mezzi di informazione a numerosi fatti di cronaca, che si sono purtroppo verificati negli ultimi anni. E anche l'esperienza comune rivela come i furti di identità, la pubblicazione online di immagini private, o di informazioni personali ed imbarazzanti a scopo malevolo, non rappresentino più un

[1] Avvocato in Pavia e Milano e cultore di "Informatica Giuridica" presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

[2] Cfr. «Ciberspazio e diritto», vol. 11 n. 3 del 2010, pp. 551-566, che venne pubblicato l'anno successivo l'entrata in vigore del decreto-legge 23 febbraio 2009, n. 11, che ha introdotto nel nostro ordinamento l'art. 612-*bis* (Atti persecutori).

unicum isolato appreso dai soli mass media, ma fatti che hanno riguardato anche persone a noi vicine, se non addirittura noi stessi.

Di qui l'opportunità di capire la diffusione reale dei fenomeni, come distinguerli dalle loro figure *offline* di riferimento, e determinare la loro incidenza rispetto alle fattispecie più classiche e studiate. Per fare ciò sarà necessario, da un lato, fare il punto sulle analisi condotte in letteratura sulle figure classiche, e poi entrare nello specifico, analizzando quali siano le peculiarità dei comportamenti lesivi perpetrati con mezzi informatici.

2. Lo stalking nella letteratura scientifica psichiatrico forense[3]

Nel loro noto trattato di psichiatria forense, criminologia ed etica psichiatrica[4], Mastronardi e Villanova collocano lo stalking (o sindrome delle molestie assillanti) tra i "comportamenti sessuali devianti" "nel cui ambito di gran lunga si manifesta", dopo la parte dedicata alla pedofilia e allo stupro.

Ciò a sottolineare non solo che tale modello di comportamento ha spesso come prodromo o corollario una connotazione di carattere sessualmente deviante,[5] ma anche che esso si manifesta maggiormente in un ambito che coinvolge le patologie dell'affettività, ed ha in comune una connotazione di "violenza" mirata principalmente alla sfera del privato.

Da un esame sinottico della letteratura scientifica sul tema, emerge una generica concordia nel ritenere una caratteristica comune del comportamento deviante la distorsione della percezione del senso di giustizia nello stalker, che si autoconvince della legittimità del suo comportamento. In breve, pur rendendosi spesso conto del "male" della sua azione, il reo arriva a scriminarla, sia perché reattiva a un male ingiusto patito, ovvero perché compiuta in nome di una inevitabile modalità di ricerca

[3] Si ringrazia il Dott. Luciano Magotti, psichiatra forense, per l'aiuto nella individuazione dei principali testi di riferimento sul tema.

[4] Cfr. *Trattato italiano di psichiatria - forense, criminologia ed etica psichiatrica*, terza ed., a cura di V. Volterra, Milano, Masson Ed. 2006, pp. 184 e ss.

[5] Anche il Prof. Fornari, nella parte dedicata allo stalking, propone una collocazione del fenomeno nell'ambito delle parafilie, con chiare connotazioni a sfondo sessuale: U. Fornari, *Trattato di psichiatria forense criminologia ed etica psichiatrica*, quinta ed., Assago, UTET ed. 2013, pp. 882. ss.

Abstract

*Il cyberstalking e il cyberbullismo: l'evoluzione del fenomeno a sei anni dall'entrata in vigore dell'art. 612-*bis *del codice penale*

I reati di stalking e di bullismo sono molto interessanti da analizzare anche nelle loro fattispecie "informatiche, ossia il cyberstalking e il cyberbullismo. In questo articolo l'Autore si propone di delineare le prime caratteristiche, e differenze, delle due fattispecie, con particolare attenzione sia al lato criminologico sia al lato giuridico. I due fenomeni si presentano, spesso, interconnessi tra loro, e pongono all'interprete delle questioni molto complesse da risolvere soprattutto con riguardo all'attenzione, sempre necessaria, alle vittime.

*Cyberstalking and cyberbullying: the evolution of the phenomenon six years after Para. 612-*bis *of the penal code first came into force*

The offenses of stalking and bullying are very interesting to analyze even in their digital issues, i.e. the cyberstalking and cyberbullying cases. In this article the author intends to outline the first elements, and differences, between the two cases, with particular attention to both the forensic side and the legal side. The two phenomena are often interconnected, and present to the interpreter very complex issues to be resolved especially with respect to the attention, always necessary, to the victims.

Marcello Bergonzi Perrone

Ciberspazio e diritto, vol. 16, n. 54 (3-2015), pp. 461-508

Effetti geopolitici del *Datagate*: appunti e spunti per la geopolitica della sorveglianza globale

Gabriele Suffia[1]

Sommario: 1. Differenti tipi di dati – 2. Le basi giuridiche del controllo dei dati: le due vie – 2.1. Accordo tra Stati e il paradigma Echelon – 2.2. Accordo tra Stati e privati – 3. Tutto genera conseguenze – 3.1. Sorveglianza e ruolo dei privati – 3.2. Reazioni dirette internazionali – 3.3. Europa e il TTIP – 3.4. Russia – 3.5. Cina – 3.6. Conclusioni? – 4. WikiLeaks, le torture e l'irrazionalità del sistema

1. Differenti tipi di dati

Quando Julian Assange[2] cerchiò alcune parole su un tovagliolino della hall dell'Hotel Leopold, nella centralissima Place Luxembourg a Bruxelles, il 21 giugno 2010, trasformandole in una password per trasmettere alla stampa il file forse più importante della storia delle "fughe di notizie"[3], nell'aria turbinavano tre grandi temi: i) il sistema di controllo dei dati digitali così come strutturato attualmente, dominato dai governi degli Stati nazionali e da poche grandi *corporation* private; ii) il tentativo di sottrarsi a questo controllo, trovando nuovi sistemi di protezione dei

[1] Dottore in Giurisprudenza.

[2] Julian Assange, com'è noto, è un *hacker* australiano fondatore nel 2006 di WikiLeaks (sito Internet www.wikileaks.org), organizzazione internazionale giornalistica senza scopo di lucro, che si occupa di ricevere anonimamente documenti riservati o coperti da segreto e di divulgarli sul proprio sito web o attraverso la stampa.

[3] Si veda per il racconto diretto dai giornalisti del Guardian che ricevettero la password D. Leigh, L. Harding, *Wikileaks, la battaglia di Julian Assange contro il segreto di Stato*, Roma, Nutrimenti 2011.

dati personali e nuove forme per il *leaking*[4] e il *whistleblowing*[5]; iii) il ruolo della stampa tradizionale nell'evoluzione del panorama globale, in cui le notizie raggiungono gli utenti (e sono spesso create dagli utenti stessi) con una rapidità senza precedenti nella storia.

Di tutti gli aspetti il meno dibattuto è forse il primo, probabilmente perché esso viene ritenuto un "dato di fatto" contro cui è impossibile scontrarsi e che, per il singolo e anche per comunità ben più numerose, è impossibile da modificare.

Tuttavia una breve analisi di questo "stato delle cose" può non essere del tutto inutile.

Quando David Foster Wallace si rivolgeva agli studenti del Kenyon College nel discorso per il conferimento delle lauree, e citava la celebre storiella dei due pesci che incontrano un pesce più anziano (due pesciolini stanno nuotando e finiscono per incontrare un pesce più anziano che va nella direzione opposta; il pesce più anziano passa loro accanto e dice: «Salve, ragazzi. Com'è l'acqua?». I due pesciolini allora nuotano un altro po', poi uno si ferma e se ne esce con: «Che cavolo è l'acqua?»[6]), ci richiamava proprio a focalizzare la nostra attenzione sullo "stato delle cose", perché conoscerlo, e non darlo per scontato, ci consente di operare delle scelte, maturare delle convinzioni, e indirizzare i desideri (*de sideribus*) verso cui vogliamo tendere e vogliamo che tendano le nostre società.

Quindi, in tema di sorveglianza, questa è l'acqua (in breve).

La password fornita da Assange ai giornalisti del Guardian, Nick Davies e Ian Traynor, consentiva l'accesso al file trafugato da Bradley Manning, all'epoca analista informatico per il 2nd Brigade Combat Team di stanza in Iraq, contenente le informazioni più segrete della guerra condotta dagli Stati Uniti d'America in Afghanistan.

[4] Dall'inglese "*leak*", traducibile con "perdita", è utilizzato per indicare principalmente la fuoriuscita accidentale di liquidi da un contenitore. Figurativamente, una "*news leak*" è una divulgazione non autorizzata di notizie e documenti riservati.

[5] Dall'inglese "*blow the whistle*", è letteralmente l'azione dell'arbitro che intende sanzionare un fallo di gioco o del poliziotto che intende interrompere un'azione illegale. Il *whistleblowing* è l'attività di chi, interno ad una organizzazione, ne denuncia all'esterno attività illecite o fraudolente.

[6] Così come riportata da D.T. Max, *Ogni storia d'amore è una storia di fantasmi*, Einaudi 2013

Abstract

Effetti geopolitici del Datagate*: appunti e spunti per la geopolitica della sorveglianza globale*

Il recente caso del Datagate, con la rivelazione da parte di Edward Snowden di informazioni riservate circa i sistemi di sorveglianza elettronica globale utilizzati oggi dagli Stati Uniti anche in Europa, ha mutato radicalmente sia il panorama della sicurezza sia gli equilibri geopolitici mondiali, aprendo nuove prospettive all'idea stessa di privacy del cittadino e di controllo statale. L'Autore ripercorre con dovizia di particolari, in questo articolo, le premesse al caso Datagate e le sue evoluzioni sino ad oggi, con particolare attenzione alle questioni giuridiche e politiche.

Geopolitical consequences of Datagate*: notes and reflections for geopolitics of global surveillance*

The recent case of Datagate, with the revelation by Edward Snowden of confidential information concerning global electronic surveillance systems used today by the US also in Europe, has radically changed the security landscape and the geopolitical balance of the world, opening up new perspectives about the very idea of privacy of citizens and of state control. The author recounts in great detail in this article the premises to Datagate case and its progress to date, with a focus on legal and policy issues.

Gabriele Suffia