Answers to "Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC)" by the European Commission
(Directorate-General for Internal Market and Services)

ScambioEtico è un movimento grassroots, con sede in Italia, che promuove il libero accesso alla conoscenza, difende il carattere aperto e non discriminatorio di Internet e si propone di informare i cittadini in merito ai diritti e alle libertà nell'era digitale.

Contatti:
portavoce@scambioetico.info (Paolo Brini)
coordinatore@scambioetico.info (Luigi Di Liberto)

http://scambioetico.org

1. I answer as

b) An association of citizens or consumers

56. What practical experience do you have regarding the procedures for notice and take-down? Have they worked correctly? If not, why not, in your view?

Le procedure di notice and take-down, in assenza di parametri specifici nel quadro legale dell'Unione, si estrinsecano essenzialmente in pratiche di autoregolamentazione dei gestori delle piattaforme che ospitano contenuti generati dagli utenti e più in generale dei fornitori di servizi nella società dell'informazione, con modalità conformi alle disposizioni del Digital Millennium Copyright Act in vigore negli Stati Uniti d'America.

Il fornitore di servizi tende ad aderire alle richieste di take-down senza controllare la loro attendibilità e di norma senza informare della rimozione l'utente che ha eseguito l'upload del contenuto. Questa pratica apre le porte ad abusi di ogni tipo e dobbiamo infatti rilevare che il notice and take-down è non infrequentemente usato da soggetti privati a scopo di censura.

In Italia è particolarmente noto il caso di rimozione del video di un giornalista, Marco Travaglio, insignito nel 2009 del Premio della JDV per la libertà di stampa per la sua opera in difesa della libertà di espressione in Italia. Nel 2010 il giornalista aveva pubblicato dei servizi sulla piattaforma UGC YouTube fortemente critici nei confronti del governo italiano: http://beppegrillo.it/2010/02/travaglio_oscurato_per_copyright/index.html La richiesta di take-down è partita sulla base di una presunta violazione del copyright di Mediaset, la società di proprietà del Presidente del Consiglio dei Ministri del governo italiano.

Sebbene tale violazione di copyright fosse del tutto inesistente, i video da YouTube sono stati rimossi senza alcuna verifica. Questo caso esemplare mostra come un regime di notice and take-down analogo a quello in vigore negli Stati Uniti si può trasformare in un sistema di censura politica e in uno strumento per ostacolare la libertà di espressione.

Varie ricerche compiute dalla Electronic Frontier Foundation mostrano come il notice and take-down in 12 anni di applicazione negli Stati Uniti sia diventato realmente uno strumento per limitare la libertà di espressione. http://www.eff.org/takedowns

Un'altra analisi che mostra come il sistema di take-down sia attualmente utilizzato negli Stati Uniti come strumento o mezzo di censura o comunque per limitare la libertà di espressione è contenuta nell'articolo

http://www.readwriteweb.com/archives/twitter_dmca_takedowns_the_prior_restraint_of_first_amendment_speech.php

Qualsiasi ulteriore espansione del notice and take-down può aprire le porte a rischi di distorsione del mercato interno, in uno scenario in cui le richieste di rimozione potrebbero essere utilizzate come strumento per ostacolare la diffusione di contenuti concorrenti.

In considerazione di quanto sopra, riteniamo che sia essenziale emendare la Direttiva 2000/31/CE al fine di proteggere la libertà di espressione e il mercato interno, e prevenire un sistema di abusi finalizzati alla censura. Occorre proibire un sistema di notice and take-down come quello attualmente implementato da soggetti privati e conforme al DMCA americano. In particolare, in caso di assenza dell'ordine di un magistrato, si dovrebbe fornire la possibilità a colui che ha eseguito l'upload del contenuto, di cui si richiede la rimozione, di un tempo ragionevole per poter replicare alle accuse. Appare inoltre urgente imporre delle misure sanzionatorie contro le richieste abusive di take-down ed imporre un obbligo di trasparenza per fare in modo che gli utenti del fornitore di un servizio siano chiaramente informati della politica di notice and take-down eventualmente adottata.

57. Do practices other than notice and take down appear to be more effective? ("notice and stay down"13, "notice and notice"14, etc)

Con riferimento alla risposta alla domanda 56, **un sistema di notice and notice è capace di risolvere i gravi problemi che affliggono il notice and take-down, preservando la libertà di espressione ed evitando distorsioni del mercato, e allo stesso tempo non compromette i diritti dei detentori del copyright. Il notice and notice offre il diritto di replica tramite la possibilità di un counter-notice alla persona il cui contenuto è contestato, unica modalità per rendere più difficoltosi gli abusi di richieste di rimozione.**

58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?

Mentre non ci risultano obblighi generali di sorveglianza a carico degli ISP, abbiamo effettuato un'estesa analisi della situazione di blocchi, filtraggi e oscuramenti imposti in Italia da varie autorità. Risulta una situazione in cui si ricorre essenzialmente al filtraggio del World Wide Web al fine ufficiale di impedire ai cittadini italiani l'accesso a giochi di scommesse

online di operatori non italiani, impedire l'accesso a contenuti concernenti abusi sessuali sui minori, impedire l'accesso a siti di informazione che sono sospettati di favorire la violazione del copyright o sono ritenuti stampa clandestina, impedire l'acquisto di sigarette all'estero. Nella realtà, come si può vedere dai casi riportati di seguito, il sistema di filtraggio italiano sta rischiando di provocare distorsioni al mercato, favorendo pratiche anti-concorrenziali. Inoltre, appare che la libertà di espressione sia stata di fatto limitata dall'esteso filtraggio o blocco dei siti web.

I diversi soggetti che sono per legge autorizzati ad imporre agli ISP il blocco dei siti web indicati (anche in assenza della sentenza di un magistrato) sono riportati di seguito.

Amministrazione Autonoma Monopoli di Stato (AAMS): l'Amministrazione Autonoma Monopoli di Stato italiana ha elaborato una lista nera di circa 1.750 siti web che forniscono diversi servizi di gioco d'azzardo. Questa lista è pubblica e gli ISP sono tenuti per legge a bloccare tutti questi siti.

Polizia italiana: basandosi sulla lista di blocco segreta internazionale CIRCAMP, la polizia italiana ha aggiunto altri siti senza intervento giudiziario. Questo ha portato ad un elenco complessivo compreso tra 600 e 900 siti che si sostiene contengano immagini di abusi sui minori. Gli ISP sono obbligati per legge a bloccare tutti questi siti.

Magistratura: anche le Ordinanze delle Corti di Giustizia sono utilizzate per aggiungere alla lista i siti che i Fornitori di Servizi Internet devono bloccare. I siti bloccati includono un sito anti-mafia (accadeinsicilia.net), per essere una "pubblicazione di stampa clandestina"; un'organizzazione di consumatori (aduc.it), per diffamazione; un sito di pubblicazione in rete gratuita (Bakeca.it), per aver facilitato la prostituzione; ed un sito di condivisione di file (thepiratebay.org). Attualmente il sito Bakeca.it è stato riabilitato solo dopo aver concordato con le forze dell'ordine l'oscuramento volontario di alcuni settori. Al contrario accadeinsicilia.net (un sito del professor Ruta, storico siciliano), che raccoglieva una estesa e precisa documentazione sulla storia della mafia, è rimasto oscurato per anni (dal 2004) per poi essere fisicamente rimosso. Thepiratebay.org resta a tutt'oggi oscurato (un provvedimento che non è stato preso in Svezia, paese in cui i gestori del sito sono stati condannati in primo grado ad 1 anno di carcere).

Altri tipi di contenuto bloccato: i siti che favoriscono l'acquisto di sigarette all'estero, un sito web contenente informazioni sull'uso degli steroidi, un sito web di un'università coreana e un sito web gay sono stati aggiunti alle liste di blocco.

In considerazione di quanto sopra riteniamo auspicabile che il processo di revisione della Direttiva 2000/31/CE tenga conto di come il filtraggio operato nel World Wide Web stia portando a potenziali violazioni della libera concorrenza nel mercato interno e ad effettive limitazioni della libertà di espressione.

59. From a technical and technological point of view, are you aware of effective specific

filtering methods? Do you think that it is possible to establish specific filtering?

La definizione "filtraggio specifico" appare riferirsi ad una situazione in cui gli intermediari tecnici di Internet introducono degli strumenti capaci di bloccare il flusso di specifici dati. Da un punto di vista tecnico, la specificità del filtraggio presuppone un monitoraggio attivo dei flussi di dati scambiati in Rete, una pratica che non solo appare sproporzionata ed inefficace, ma che può originare sia serie preoccupazioni per la privacy dei cittadini sia compromettere l'architettura di Internet.

Filtraggi basati su DNS poisoning e su IP blocking sono facilmente aggirabili e sono quindi inefficaci. Essi possono essere utili solo per prevenire che un utente inavvertitamente acceda al contenuto "censurato", ma non possono nulla contro coloro che volontariamente vogliono accedere a tale contenuto, che è pur sempre disponibile e accessibile in rete tramite semplicissimi accorgimenti tecnici. Allo stesso tempo il filtraggio è controproducente. Come mostrato dalla ricerca di Tyler Moore e Richard Clayton, "The Impact of Incentives on Notice and Take-down", Computer Laboratory, University of Cambridge (2008), l'implementazione nel Regno Unito del filtraggio al fine di combattere gli abusi sessuali sui minori ha disincentivato la cooperazione internazionale, le indagini e la volontà di perseguire i criminali responsabili di tali abusi, traducendosi quindi in un danno terribile per le giovani vittime. Infine, queste tecniche di filtraggio danno origine, come dimostrato dal caso Italia riportato in risposta alla domanda 58, a bloccaggio eccessivo, giungendo, per errore o per inadeguatezza tecnica, a bloccare siti e/o contenuti perfettamente legali. Si veda anche il caso di blocco a Wikipedia avvenuto nel Regno Unito:
http://en.wikinews.org/wiki/British_ISPs_restrict_access_to_Wikipedia_amid_child_pornography_allegations

Filtraggi basati su tecniche di Deep Packet Inspection presuppongono il monitoraggio indiscriminato di tutti i contenuti in transito sulla rete. Le tecnologie di Deep Packet Inspection andrebbero severamente regolamentate in quanto esse sono capaci di violare la segretezza della corrispondenza nonché violare le direttive concernenti la protezione dei dati (95/46/CE) e la privacy nelle comunicazioni elettroniche (2002/58/CE) ad un livello indiscriminato ed esteso a tutti i cittadini, in assenza dell'ordine di un magistrato. Un monitoraggio invasivo darebbe inoltre stimolo ad un uso esteso della crittografia, contro la quale la DPI è impotente, che renderebbe le indagini sui crimini o le indagini internazionali estremamente difficoltoso, come anche sottolineato dalle preoccupazioni dei servizi di intelligence del Regno Unito e degli Stati Uniti
http://www.techdirt.com/articles/20101006/04135311311/us-intelligence-agencies-angry-at-france-over-three-strikes-worried-it-will-drive-encryption-usage.shtml%29

Occorre infine considerare che gli apparati di Deep Packet Inspection hanno un costo elevato che potrebbe non essere sostenibile per i fornitori di accesso medi e piccoli, mentre per i fornitori di accesso più grandi e le società di telecomunicazioni essi possono rappresentare un pericoloso incentivo a favore di modelli di business basati sul razionamento della larghezza di banda e sull'inserimento di parametri discriminatori su contenuti, mittenti e destinatari, contro modelli di business basati sull'espansione dell'infrastruttura al fine di fornire migliori servizi e maggiore larghezza di banda ai cittadini e agli operatori commerciali dell'Unione.

Ci appare quindi evidente che la promozione di strumenti di filtraggio andrebbe

accuratamente evitata al fine di non soffocare lo sviluppo della società dell'informazione, non compromettere l'infrastruttura di Internet e non violare i diritti fondamentali dei cittadini. La Direttiva 2000/31/CE potrebbe essere utilmente emendata per stabilire che il filtraggio contro un sito presente sul World Wide Web andrebbe effettuato solo negli estremi casi in cui non è possibile rimuovere fisicamente i contenuti e solo in seguito alla sentenza di un magistrato.

60. Do you think that the introduction of technical standards for filtering would make a useful contribution to combating counterfeiting and piracy, or could it, on the contrary make matters worse?

Le tecniche di filtraggio, come esposto nella risposta alla domanda 59, sono di base inefficaci, e riteniamo che l'introduzione di standard tecnici non possa far nulla per correggere la loro inefficacia. Allo stesso tempo, occorre effettuare un'importante distinzione fra "contraffazione" e "pirateria", se con quest'ultimo termine si vuole intendere la violazione del copyright nell'ambiente digitale senza scopo di lucro tramite i cyberlocker, il file sharing, le piattaforme serverless o gli altri numerosissimi metodi (in questo caso riteniamo il termine leggermente fuorviante). Dal punto di vista della contraffazione, un fenomeno che danneggia i consumatori e il mercato, il filtraggio dei siti web che vendono prodotti contraffatti può essere efficace solo per prevenire l'accesso ad essi a coloro che accidentalmente dovessero accedervi, mentre coloro che volontariamente volessero acquistare prodotti contraffatti potrebbero comunque farlo tramite l'utilizzo di semplici accorgimenti tecnici (per es. CGI proxy, elite proxy, Virtual Private Network ecc.). Riteniamo quindi che la lotta alla contraffazione non possa prescindere da una collaborazione internazionale che miri non a nascondere ma a colpire direttamente il traffico illecito dei beni contraffatti.

Per quanto riguarda la "pirateria", con la precisazione sopra riportata, le tecniche di filtraggio sul World Wide Web sarebbero semplicemente irrilevanti, perché l'indicizzazione e la catalogazione delle informazioni utili al tracciamento delle opere si sposterebbe ancor più di quanto non sia ora su siti decentralizzati che sono semplicemente al di fuori del World Wide Web (per es. siti che risiedono in network distribuiti in Internet e che si duplicano integralmente nel computer di ogni utente che accede al network con semplicissimi software). Le tecniche di monitoraggio invece dell'infrastruttura di Internet andrebbero solo a colpire la privacy dei cittadini, in quanto coloro che, senza scopo di lucro, violano il copyright nell'ambiente digitale potrebbero continuare a farlo indisturbati spostando gli strumenti atti allo scopo in ambiti non tracciabili per mezzo di crittografia, multiplexing del flusso dei dati ed altre semplici tecniche di anonimizzazione alla portata di utenti con preparazione informatica di basso livello.

In sostanza, i tentativi di repressione di tale fenomeno andrebbero solo a minare l'infrastruttura di Internet e la privacy dei cittadini dell'Unione Europea, con il paradossale risultato di ottenere un risultato opposto a quello desiderato, cioè deprimere il mercato interno ed intaccare i diritti fondamentali. Pertanto riteniamo che nella Direttiva 2000/31/CE non si dovrebbe cedere all'illusoria tentazione di imporre il rispetto della legge tramite strumenti di filtraggio e/o di monitoraggio.

64. Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?

In alcuni casi giudiziari all'interno dei Paesi Membri (caso Bakeca.it in Italia, caso Rapidshare in Germania), il fornitore di una piattaforma che ospita contenuti generati dagli utenti non ha beneficiato dell'esenzione di responsabilità espressamente riservata dalla Direttiva 2000/31/EC agli intermediari tecnici. Tuttavia, i fornitori di servizi che creano spazi partecipativi, i gestori di piattaforme che ospitano contenuti generati dagli utenti, ed anche i blogger non professionisti, potrebbero grandemente beneficiare da una maggiore certezza legale concernente l'esenzione di responsabilità per i contenuti immessi dagli utenti. Tale esenzione permetterebbe ai gestori di investire maggiormente sugli spazi partecipativi, di potenziare i propri servizi e di concentrarsi sulla qualità piuttosto che su tecniche di sorveglianza, con il risultato di incoraggiare la partecipazione e la libertà di espressione dei cittadini online.

Riteniamo pertanto che la Direttiva 2000/31/EC andrebbe emendata per proteggere esplicitamente i gestori delle piattaforme che ospitano contenuti generati dagli utenti e in generale i gestori di qualsiasi spazio partecipativo in maniera identica a quella riservata agli intermediari quali ISP e hosting provider (articoli 12, 13 e 14).

67. Do you think that the prohibition to impose a general obligation to monitor is challenged by the obligations placed by administrative or legal authorities to service providers, with the aim of preventing law infringements? If yes, why?

Riteniamo che la proibizione ad imporre un obbligo generale di sorveglianza stabilita dall'articolo 15 sia effettivamente messa a rischio da una serie di pratiche emergenti nei Paesi Membri dell'Unione: inviti verso una ”autoregolamentazione” per prevenire abusi della libertà di espressione e pressioni legali dei copyright holder che in molti Paesi Membri (Irlanda, Italia, Spagna fra gli altri) trascinano gli ISP in tribunale al fine di addossare loro responsabilità per i contenuti veicolati dai clienti. Queste operazioni sembrano mirate a creare un clima di pressione legale che rappresenti una coercizione per gli ISP verso un obbligo generale di sorveglianza, in maniera analoga alla pressione esercitata dal governo cinese sugli ISP della Cina per costringerli ad effettuare monitoraggio e censura dei contenuti veicolati dai cittadini. Un obbligo “de facto” di sorveglianza sui contenuti degli ISP aprirebbe le porte nell'intera Unione Europea al rischio di filtraggio e censura attiva da parte degli ISP.

Riteniamo quindi che l'articolo 15 della Direttiva 2000/31/CE debba essere accuratamente protetto.