Sachdokumentation:

Signatur: DS 1273

Permalink: www.sachdokumentation.ch/bestand/ds/1273

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

economiesuisse
DOSSIER POLITIK

7 / 2018

Nein zu Netzsperren und digitaler Abschottung

02.05.2018

Das Wichtigste in Kürze

Am 10. Juni 2018 stimmt die Schweizer Bevölkerung über das neue Geldspielgesetz ab. Zum Schutz der hiesigen Casinos enthält das Gesetz – dies ein Novum in der Schweiz – Netzsperren, mit denen der Zugriff auf ausländische Geldspielangebote im Internet künftig unterbunden werden soll. Bereits heute ist das Angebot solcher Spiele in der Schweiz zwar verboten, doch das Spielen ist erlaubt.

Bei diesen Netzsperren handelt es sich um staatlich verfügte Sperren, welche den Zugriff auf bestimmte Seiten im Internet für alle blockieren. Dabei werden in der Regel die Internetanbieter in die Pflicht genommen, spezifische Seiten im Internet zu sperren.

Was mit der Sperrung von Online-Glücksspielen beginnt, kann schnell zu weiterer Zensur in anderen Bereichen führen. Denn sind die entsprechenden Instrumente einmal vorhanden, finden weitere Interessengruppen schnell Gründe für zusätzliche Netzsperren.

Netzsperren sind ein Sündenfall für eine offene, moderne Volkswirtschaft wie die Schweiz. Sie sind ein Instrument der Abschottung, lassen sich mit wenigen Klicks selbst von Laien umgehen und richten gleichzeitig grossen Schaden an der Netzinfrastruktur an: zum Schaden von Wirtschaft und Gesellschaft.

Position economiesuisse

Die Schweiz verdankt ihren Wohlstand ihrer wirtschaftlichen Offenheit und den Freiheiten. Beide Werte sind gerade auch im digitalen Zeitalter von herausragender Bedeutung für unsere Gesellschaft und Wirtschaft.

Die uneingeschränkte Verfügbarkeit von Informationen und der freie Datenverkehr spielen eine Schlüsselrolle in der jüngeren Entwicklung. Heute ist das Internet das Rückgrat der digitalen Wirtschaft und Gesellschaft. Es darf darum nicht zum Spielball von Interessensvertretern jeglicher Art werden.

Netzsperren sind ein untauglicher und gefährlicher Versuch, die Grenzen der staatlichen Eingriffsmöglichkeiten auszudehnen. Netzsperren schaden unserer

Kontakt und Fragen

Erich Herzog
Stv. Leiter Wettbewerb & Regulatorisches
Christa Hofmann
Head Legal & Public Affairs, Swico

www.dossierpolitik.ch

freien Gesellschaft, dem Rechtsstaat und der (Internet-)Wirtschaft in der Schweiz. Ausnahmen sind ausschliesslich zum Schutz der öffentlichen Sicherheit zuzulassen (Schutz vor Terrorismus, Schutz vor Kinderpornografie usw.).

Die Einführung von Netzsperren könnte zu einem Dammbruch im Bereich Internetzensur führen. Die Signalwirkung auf andere Bereiche und auf unsere internationale Wahrnehmung als Standort für zukunftsgerichtete Technologieunternehmen wäre verheerend.

Netzsperren beschädigen die Netzinfrastruktur und sind dennoch leicht zu umgehen. Besonders gefährlich ist, wenn ineffiziente Sperren dann im Rahmen künftiger Gesetzesanpassungen noch weiter ausgebaut werden.

Das Internet als Treiber des Fortschritts

Das Internet ist das Rückgrat unserer modernen Gesellschaft und ist aus dem Alltag nicht wegzudenken.

Kein Alltag ohne Internet

Heute stehen wir an der Schwelle zur «digitalen Wirtschaft» beziehungsweise zur «digitalen Gesellschaft». Daten und Informationen sind die neuen Rohstoffe. Das Internet ist eine der Schlüsseltechnologien, die die digitale Transformation antreiben. Es ist das Rückgrat unserer modernen Gesellschaft und aus dem Alltag nicht mehr wegzudenken.

Technologien wie Smartphones, E-Mails, Cloud-Computing und vieles mehr sind ohne das Internet unmöglich. Alle, vom KMU über die Privatperson bis hin zur Hochschule, sind – je länger je mehr – auf einen freien und funktionierenden Austausch von Informationen angewiesen. Angesichts der Entwicklungen und der damit verbundenen neuen Möglichkeiten wird ein uneingeschränkter Datenverkehr aus wirtschaftlicher wie gesellschaftlicher Perspektive stets wichtiger.

Als Nervensystem der Vernetzung schafft das Internet grossen Mehrwert für Zivilgesellschaft wie auch Unternehmen.

Wirtschaftlicher und kultureller Mehrwert

Der durch das Internet ausgelöste Modernisierungsschub trägt nicht nur zur Entstehung neuer Wirtschaftszweige bei, sondern bewirkt auch einen grundlegenden Wandel des Kommunikationsverhaltens und der Mediennutzung im beruflichen und privaten Bereich. Die kulturelle Bedeutung dieser digitalen Vernetzung wird manchmal mit der Erfindung des Buchdrucks gleichgesetzt. Mit Fug und Recht kann heute festgestellt werden, dass das Internet als Nervensystem für Zivilgesellschaft wie Unternehmen von unschätzbarem Wert ist.

Staatliche Eingriffe in die Netzinfrastruktur gefährden die Funktionsfähigkeit von Wirtschaft und Gesellschaft.

Abhängigkeit steigert Verletzlichkeit

Die fortschreitende Digitalisierung führt zu einer zunehmenden Abhängigkeit von der Kommunikationsinfrastruktur und damit vom Internet. In der Folge steigt automatisch die Verletzlichkeit vieler Prozesse. Diese ist umso weitreichender, da diese Abhängigkeit weit über blosse Kommunikationsvorgänge hinausreicht. Es ist die zunehmende Vernetzung der Menschen und Geräte an sich, welche den substanziellen Mehrwert schafft.

Ein freier Internetzugang ist Ausdruck unserer generellen wirtschaftlichen Offenheit und ein bedeutender Standortfaktor.

Offenheit als Standortfaktor im Informationszeitalter

Die Schweiz verfügt dank ihrer traditionellen Offenheit über eine ausgezeichnete Ausgangslage, um von diesem digitalen Umbruch zu profitieren. Beleg dafür sind Unternehmen wie Google, IBM, Microsoft oder Oracle, die sich für die Schweiz als bedeutenden Entwicklungsstandort entschieden haben. Zudem ist die Schweiz attraktiv als Datentresor und steht hoch im Kurs für Unternehmen, die auf die Blockchain-Technologie setzen.

Alles in allem ist die Schweiz wegen ihrer wirtschaftlichen Offenheit, der guten (Netz-)Infrastruktur und dem freien Zugang zum Internet heute Anziehungspunkt für innovative Unternehmer und Investoren.

Offenheit prägt Denken und Handel
Die wirtschaftliche Offenheit ist Kernstück des Schweizer Erfolgsmodells. Unser hoher und breit gefächerter Wohlstand ist ohne offene Märkte und unternehmerische Freiheit undenkbar. Dank dieser Offenheit konnte unser kleiner Binnenstaat von der Globalisierung und dem technologischen Fortschritt der letzten Jahrzehnte stark profitieren. Dank dieser wettbewerbsfördernden Offenheit zeichnet sich unsere Wirtschaft durch eine hohe Anpassungs- und Innovationsfähigkeit aus, durch die wir Krisen und Strukturwandel oft erfolgreicher meistern wie im Ausland. Auch darum braucht sich die Schweiz vor der Digitalisierung nicht zu fürchten.

→ **Auch der Bundesrat hat die Bedeutung des ungestörten Datenverkehrs in der «Strategie Digitale Schweiz» festgehalten.**

Auch der Bundesrat hat dies erkannt und bereits in der «Strategie Digitale Schweiz» 2016 festgehalten, dass die Schweiz

- als sicherer internationaler Standort für Datenspeicher und Informatikdienstleistungen etabliert sein muss und über eine Datenpolitik verfügt, welche die Interessen der Schweiz auch im digitalen Bereich berücksichtigt;
- die Diskussion über die Zukunft des Internets mitprägt;
- ihre Chancen im Hinblick auf den virtuellen internationalen Wirtschaftsraum nutzt, um damit auch das Risiko einer Ausgrenzung abzuwenden.

Daraus ergibt sich, dass die Bedeutung des ungestörten Datenverkehrs für die weitere wirtschaftliche und gesellschaftliche Entwicklung unseres Landes nicht unterschätzt werden kann. Es handelt sich dabei um den Kern unseres künftigen wirtschaftlichen Erfolgs.

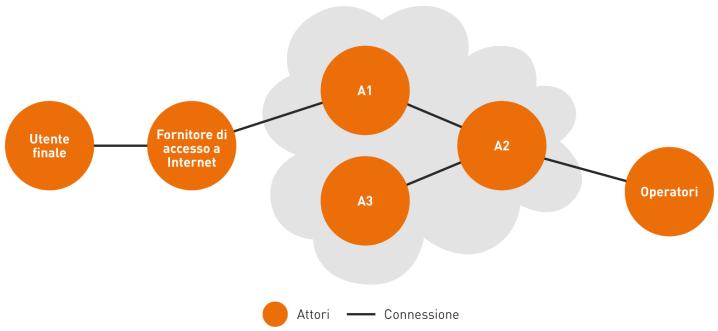
Struttura e funzionamento dei blocchi di rete

Funzionamento di internet

Internet è un vasto insieme di reti di computer o di terminali con possibilità di collegamento. Esso garantisce l'interconnessione di queste reti e permette dunque di sfruttare servizi e applicazioni come World Wide Web, e-mail, app e molto altro. Di principio, ogni terminale può collegarsi con qualsiasi altro apparecchio. Lo scambio di dati tra i terminali collegati a internet avviene attraverso protocolli internet standard.

Internet è un vasto insieme di reti indipendenti. Di principio, ogni terminale con connessione internet può collegarsi con qualsiasi altro apparecchio.

Rappresentazione semplificata di Internet con tre attori principali



Fonte: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic!, 2017, p. 704
www.economiesuisse.ch

In base alla sua struttura a rete, di principio internet è concepito in modo affidabile.

Costruzione affidabile

Di principio internet è concepito in modo affidabile. Per questo motivo nella rete vi sono sempre più vie che portano all'obiettivo: se non è possibile optare per una di queste vie, basta adottarne un'altra. I blocchi di rete rendono però internet più rischioso e meno sicuro dal punto di vista dell'utilizzo.

Internet quale rete decentralizzata

Internet è composto da reti di diversa gestione amministrativa reciprocamente interconnesse. Si tratta principalmente di reti dei fornitori di servizi internet (reti di provider) a cui sono collegati i terminali degli utenti finali di un internet service provider (ISP).

Nei punti di interscambio vengono collegati tra di loro molti dorsali di rete tramite connessioni e apparecchi (router e switch) ad alta prestazione. Qui viene organizzato lo scambio di informazioni di accessibilità tra due reti dal punto di vista contrattuale e tecnico come peering, dunque sulla base di reciprocità, e viene dunque reso possibile lo scambio di dati.

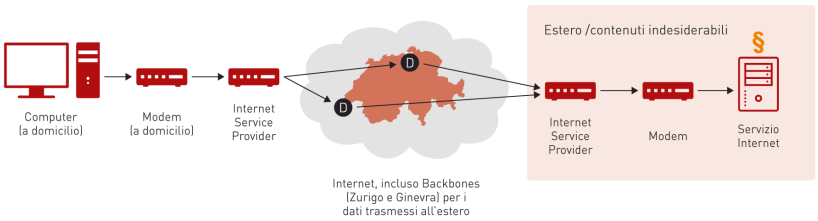
La rete principale di internet, Arpanet, era stata concepita come rete decentralizzata in un'ottica di massima affidabilità. Di conseguenza, nella pianificazione non era stato previsto alcun dispositivo centrale in cui far confluire

tutte le connessioni. La struttura a rete di internet contribuisce così fino a oggi ad avere un'elevata affidabilità. Per la comunicazione tra due utenti esistono perciò sempre più vie possibili tramite router con diversi sistemi operativi. In questo modo, il guasto di una connessione fisica nel settore chiave di internet non ha di regola gravi ripercussioni.

Il protocollo in cui viene determinato e usato l'indirizzo che identifica univocamente a livello mondiale i dispositivi connessi si chiama protocollo internet (IP). Per potersi collegare a un determinato terminale, il protocollo internet lo identifica con un indirizzo IP univoco. Questi indirizzi funzionano alla stregua di numeri di telefono e contengono anche un identificatore specifico dei paesi che permette il geotargeting. In termini più semplici, l'indirizzo IP può essere considerato l'identità di un utente finale in internet.

Il Domain Name System (DNS) funge da «elenco telefonico» automatico e rappresenta una parte importante dell'infrastruttura di internet. Questa banca dati internazionale mette a disposizione un meccanismo di traduzione che trasforma un indirizzo IP (ad esempio 86.125.22.1) in un nome di dominio più semplice da ricordare (ad esempio «economiesuisse.ch»). Questo avviene senza che l'utente se ne accorga ogni volta che in un browser web clicca su un nuovo hyperlink oppure digita direttamente un indirizzo web. Attraverso un pacchetto IP il browser chiede dapprima a un server DNS a lui noto l'indirizzo IP del nome sconosciuto e si scambia in seguito pacchetti IP con questo indirizzo per richiamare i contenuti dei servizi offerti, ad esempio siti web.

Circolazione dei dati su Internet



Fonte: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

I blocchi di rete mirano a evitare l'accesso a determinati siti web. Sono disponibili tre possibilità con conseguenze diverse.

Tipi e funzionamento di blocchi di rete

Con i blocchi di rete si mira a bloccare l'accesso di utenti finali a determinati siti web e ai relativi contenuti. Al centro vi sono contenuti indesiderati che minacciano la quiete pubblica. I blocchi di rete possono ad esempio essere impiegati per proteggere gli utenti finali da offerte dal chiaro contenuto illegale come ad esempio pornografia hard core, contenuti terroristici o estremistici.

Ogni dispositivo collegato a internet dispone di (almeno) un indirizzo IP univoco (ad

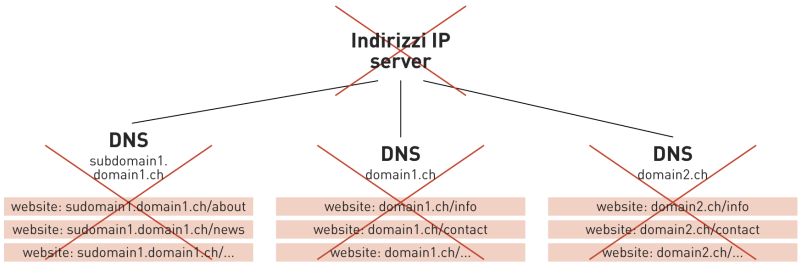
es. 86.125.22.1). Poiché questi indirizzi non sono di semplice lettura per le persone e sono anche difficili da ricordare, agli indirizzi IP meramente numerici viene assegnato un nome di dominio (ad es. www.swico.ch) in base al cosiddetto Domain Name System (DNS). Questo nome di dominio viene tradotto in modo standard in indirizzi IP dai server DNS dei fornitori di servizi internet (cosiddetta risoluzione dei nomi). Con un indirizzo IP è possibile accedere a siti web di diversi fornitori di servizi che offrono contenuti differenti con il rispettivo nome di dominio.
Oggi per i blocchi di rete sono in primo luogo tre le opzioni a disposizione.

1a variante: «blocchi di IP»

Con il blocco degli indirizzi IP i fornitori di servizi internet filtrano le ricerche dei propri clienti verso indirizzi IP specifici e salvati su una lista di blocco. Essi li bloccano oppure li reindirizzano su un sito web in cui il cliente viene informato che l'IP cercato è bloccato. Il blocco concerne tutti i contenuti – legali e illegali – consultabili all'indirizzo IP bloccato (vedi in seguito «overblocking»).

→ **Il blocco di IP impedisce di accedere a indirizzi di computer in internet. Tali richieste vengono di regola reindirizzate su una pagina di avviso.**

Blocco di indirizzi IP: bloccare indirizzi di computer



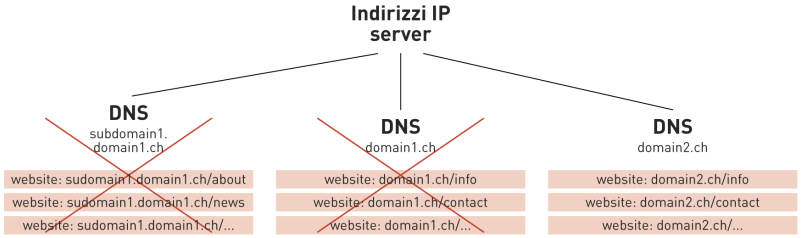
Fonte: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic!, 2017, p. 704
www.economiesuisse.ch

2a variante: «blocchi DNS»

Con blocchi DNS viene evitata la risoluzione del nome da parte del server DNS oppure le ricerche vengono reindirizzate dal fornitore di servizi internet su un sito di avviso che informa il cliente di aver tentato di accedere a un sito web bloccato. Il blocco DNS interessa tutti i contenuti del dominio bloccato. Non vengono per contro rilevati altri contenuti consultabili con lo stesso indirizzo IP (ma con un altro dominio).

→ **Nel caso di blocchi DNS l'«elenco telefonico» viene bloccato per determinati indirizzi IP. In questo modo è possibile accedere ai siti solo se si conosce l'indirizzo IP esatto.**

Il blocco del DNS impedisce la risoluzione di indirizzi del computer



Fonte: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic! 2017, p. 704
www.economiesuisse.ch

→ **I filtri applicazione analizzano i pacchetti di dati per quanto riguarda il loro scopo evitando ad esempio determinati servizi (telefonia IP, messaggistica).**

3a variante: «filtro applicazione»

Con i filtri applicazione i fornitori di servizi internet e gli operatori applicano dei filtri sul traffico internet scambiato. Simili strumenti tecnici noti comunemente come filtri d'applicazione (application filter in inglese) permettono tra l'altro anche di riconoscere contenuti dannosi dal punto di vista tecnico (come ad es. worm, virus o malware) in datagrammi IP trasportati. Una forma di questo filtro può essere realizzata anche attraverso Deep Packet Inspection (DPI). DPI mette a disposizione in particolare la possibilità di filtri di pacchetti dettagliati che dopo un'analisi dei dati di utilizzo di un datagramma IP e ad esempio la verifica del contenuto per quanto riguarda la presenza di determinate parole chiave può procedere a un'azione rilevante per questa interazione. DPI può essere applicata solo su dati di protocollo trasmessi in modo non criptato, comprende però anche interrogazioni di motori di ricerca.

Problemi dal punto di vista tecnico

I blocchi di rete creano rischi inutili per la sicurezza.

Rischi supplementari per la sicurezza

I blocchi di rete minacciano la sicurezza di internet poiché i fornitori di servizi internet vengono obbligati a falsificare i pacchetti di dati. Questi interventi indeboliscono le tecnologie per il riconoscimento di falsificazioni e manipolazioni (criminali) in internet. Con i blocchi di rete non è più nemmeno possibile determinare se dietro a un'offerta vi sia effettivamente l'offerente dichiarato. Se a seguito dei blocchi di rete sempre più utenti sono obbligati a navigare in rete in modo anonimo, ciò minaccia anche la sicurezza e rende più difficile la lotta contro la criminalità in rete. Sono sviluppi nella direzione sbagliata in un periodo in cui la cibercriminalità è in aumento a livello internazionale.

Effetti overblocking

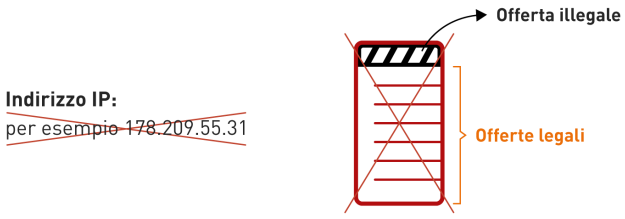
In base al loro funzionamento, in caso di blocchi di rete vi è anche il pericolo che venga bloccato l'accesso a contenuti legali. In questi casi si parla del cosiddetto overblocking. Questo pericolo è particolarmente elevato in caso di blocchi di indirizzi IP, poiché con un indirizzo IP possono essere consultati diversi offerenti con differenti contenuti. Con i blocchi DNS questo pericolo è più limitato; tuttavia, rispetto ai blocchi di indirizzi IP è ancora più semplice aggirare questo tipo di blocco.

La caratteristica perfida dell'overblocking è che i contenuti web legali spariscono letteralmente dalla nostra percezione. Di regola gli utenti finali non si accorgono che un'offerta sparisce da internet o che non è più disponibile.

Blocchi involontari in seguito a overblocking possono avere anche gravi ripercussioni economiche per singole imprese: spostano contenuti web assolutamente legali nel contesto di offerte criminali provocando un danno d'immagine o una perdita di fiducia che non giova certo agli affari. Nel caso estremo l'overblocking può minacciare l'esistenza dell'impresa semplicemente perché i clienti (svizzeri) non trovano ad esempio più lo shop online.

I blocchi di rete possono impedire l'accesso anche a contenuti web che non rappresentano assolutamente alcun problema dal punto di vista giuridico.

I blocchi sono spesso eccessivi e bloccano più pagine del previsto



Fonte: economiesuisse
www.economiesuisse.ch

Conseguenze della crittografia

Sempre più siti web scelgono di rendere più sicuro il loro sito internet con il protocollo HTTPS. La crittografia ha ripercussioni anche sui blocchi di rete. Essa evita ad esempio i blocchi di rete che puntano su filtri applicazione e server proxy. Spesso la crittografia evita anche il reindirizzamento dell'utente finale a un sito d'informazione che spiega perché la pagina cercata non è più disponibile.

→ I blocchi di rete provocano un enorme onere ai fornitori di servizi internet e rappresentano uno svantaggio per le PMI sul mercato.

Svantaggi per le PMI

I blocchi di rete statali sono gravi ingerenze nell'infrastruttura di rete. I fornitori di servizi internet vengono infatti obbligati ad agire contro la logica e la struttura di internet. Sono chiamati a bloccare singoli siti web in una rete decentralizzata programmata per ignorare simili interferenze o per aggirarle attraverso la rete. Per questo motivo i blocchi di rete rappresentano un onere enorme per i fornitori di servizi internet. L'onere legato ai blocchi significa uno svantaggio concorrenziale per i fornitori più piccoli. Con i blocchi di rete aumenta il rischio di una concentrazione poiché le PMI vengono estromesse dal mercato.

Possibilità di aggiramento

Ogni blocco di rete può essere aggirato

Blocchi di indirizzi IP e blocchi DNS possono essere aggirati grazie a semplici misure tecniche od organizzative. Vi sono addirittura possibilità che non permettono a terzi (ad es. autorità di perseguimento penale) di riconoscere, dimostrare o addirittura evitare l'aggiramento.

Aggiramento di blocchi di indirizzi IP

I blocchi di indirizzi IP e i blocchi DNS possono essere aggirati collegandosi a reti virtuali private (VPN). Questo permette agli utenti finali di accedere agli indirizzi IP bloccati attraverso un server VPN all'estero. La risoluzione del nome avviene attraverso un server DNS non interessato dal blocco. Entrambi i tipi di blocco possono essere aggirati anche con strumenti e sistemi per anonimizzare dal punto di vista tecnico il traffico internet, ad es. Tor (vedi in seguito).

Aggiramento di blocchi DNS

I blocchi DNS possono essere aggirati dal punto di vista tecnico ad esempio accedendo a server DNS esteri non interessati dal blocco o gestendo un proprio DNS locale. In molti casi non è nemmeno necessario un server DNS: basta usare l'indirizzo IP del server web che si può individuare ad esempio su appositi forum in internet o con comunicazione personale. Da poco è anche disponibile un nuovo standard DoH (DNS over HTTPS). La tecnologia sviluppata per la tutela della sfera privata è ora parte integrante dei browser (ad es. Firefox) e aggira automaticamente tutti i blocchi DNS.

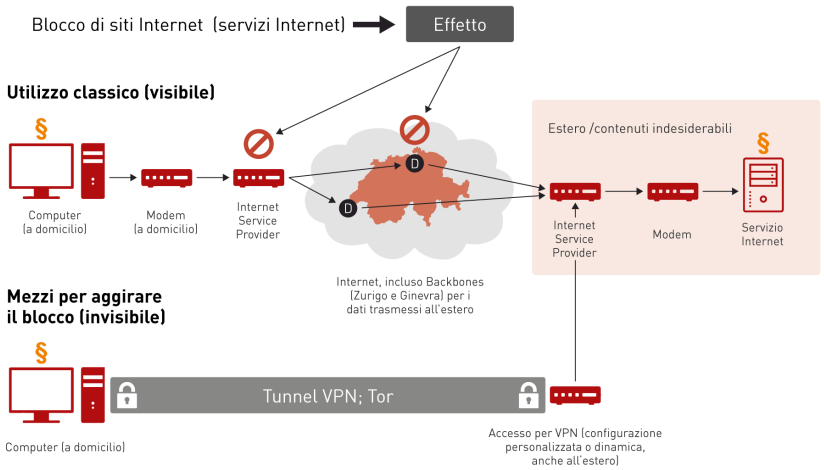
Aggiramento di filtri applicazione o server proxy

È possibile aggirare dal punto di vista tecnico anche i complessi filtri applicazione e server proxy. L'utente finale può usare una trasmissione cifrata, ad esempio sotto forma di VPN. Altre possibilità sono l'impiego di SSL/TLS (Secure Socket Layer/Transport Layer Security) o HTTPS (HTTP Secure). L'utente finale può creare anche dei propri server proxy o usare quelli che gli vengono offerti da internet.

Infine vi è un gran numero di strumenti e sistemi per anonimizzare il traffico d'origine dal punto di vista di chi naviga, ad esempio Tor.

Ogni tipo di blocco di rete può essere aggirato grazie a semplici misure tecniche od organizzative.

Effetti del blocco di siti Internet e possibilità di aggirarlo



Fonte: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

Le possibilità di aggiramento sono molto utilizzate persino nei paesi con regimi autocratici.

La realtà nei paesi con regimi autocratici

Vi sono paesi che si avvalgono molto della censura di internet. Ma anche essi si trovano di fronte a dei limiti con i blocchi di rete. In Iran sono ad esempio bloccate tutte le pagine che criticano l'ideologia religiosa dello Stato a profonda vocazione islamica. Gli iraniani più urbani e moderni sfruttano perciò i VPN e altri strumenti tecnici ad esempio per guardare film o la televisione occidentale come pure per leggere i giornali internazionali. In Russia è storia recente che lo Stato ha bloccato «Telegram», il diffuso servizio di messaggistica, poiché permetteva la cifratura delle comunicazioni e il servizio segreto non era in grado di decifrarla.

Le misure di blocco adottate dallo Stato russo nei confronti di Telegram hanno bloccato Google e Amazon, ma è stato possibile continuare a usare senza restrizioni il servizio di messaggistica in realtà oggetto del provvedimento. Questo a dimostrazione che anche negli Stati con regimi autocratici non è possibile bloccare con precisione chirurgica le offerte non gradite, sebbene in tali Paesi l'utilizzo di VPN venga regolarmente punito con gravi sanzioni.

Solo i Paesi come la Corea del Nord, che vietano di fatto alla popolazione di usare internet, possono garantire il controllo. Gli svantaggi sono evidenti: in tali Paesi l'economia digitale è inesistente e la libertà personale dei cittadini è notevolmente limitata. Eppure anche qui le persone trovano delle scappatoie: ad esempio con un mercato nero di chiavette USB e altri supporti di dati.

VPN (Virtual Private Network)

È possibile utilizzare un accesso VPN con software ottenibili in modo del tutto legale in Svizzera. E non è necessario essere uno specialista per questo. Basta caricare un'app sul proprio dispositivo o attivare un'estensione del browser. Il VPN cifra in seguito la connessione internet partendo dalla scheda di rete fino a

un server VPN. Una simile connessione è paragonabile a una galleria con cui il proprio dispositivo personale giunge fino a una casa di fiducia all'estero. Quando si naviga in internet, l'indirizzo della casa viene interpretato come origine dei movimenti. Vi sono numerosi offerenti di VPN, di regola a pagamento. Una panoramica dei VPN attualmente raccomandati si trova ad esempio all'indirizzo https://vpncreative.net/vpn-providers/.

Tor (The Onion Routing)

La rete Tor permette a tutti gli utenti finali di navigare in internet in modo anonimo. Tor sfrutta il principio del cosiddetto Onion routing per criptare i dati di connessione e di trasmissione di utenti in internet. In questo modo permette di navigare in modo anonimo e sicuro in internet. Per utilizzare Tor l'utente deve dapprima scaricare un client (software), chiamato in gergo «proxy». Questo software crea una connessione con la rete Tor e fornisce un elenco di tutti i server disponibili con cui l'utente può collegarsi. I server hanno una chiave pubblica per confermare la loro appartenenza autentica alla rete. Non appena l'utente ha ricevuto l'elenco sul proprio dispositivo, avviene una connessione scelta casualmente attraverso questo server Tor. Per motivi di anonimizzazione la rete non sfrutta solo un server, si collega bensì di regola con almeno tre server diversi. Dettagli al riguardo e un link per scaricare il proxy sono disponibili sul sito internet del progetto Tor:
https://www.torproject.org/projects/torbrowser.html.en

Preoccupazioni dal punto di vista giuridico

I blocchi di rete sono ingerenze non sottovalutabili nei nostri diritti e rappresentano dunque uno strumento preoccupante dal punto di vista dello Stato di diritto.

Ingerenza statale

Dal punto di vista giuridico, in molti casi i blocchi di rete vanno classificati come ingerenza sproporzionata dello Stato di diritto a seguito del loro carattere inadeguato ed eccessivo. Nel giudizio rientrano i punti seguenti:

- le possibilità tecniche e le relative possibilità di aggiramento;
- l'effetto indiretto dei blocchi di rete sugli utenti finali e i fornitori di servizi internet piuttosto che sugli autori delle violazioni (gestori dei siti web);
- la minaccia potenziale o la violazione parziale di importanti beni giuridici (diritti fondamentali);
- la protezione giuridica praticamente impossibile da configurare in modo irreprensibile dal punto di vista dello Stato di diritto (diritto di essere sentiti).

Alcuni esperti [1] vedono nei blocchi di rete una grave ingerenza nella libera comunicazione, tutelata da norme fondamentali. Di conseguenza i blocchi di rete richiedono in ogni caso una base legislativa. Per una relativa regolamentazione è perciò imperativa una base nella legge formale (art. 36 cpv. 1 Costituzione federale).

I blocchi di rete possono pregiudicare anche diversi diritti fondamentali.

Attacco ai diritti fondamentali

In seguito al rischio dell'overblocking e dell'ammissibilità, ad esempio, di giochi d'azzardo su piattaforme estere, i blocchi di rete devono essere giustificabili anche per le persone interessate dal blocco come terzi che svolgono attività legittime.

A seconda del caso, la libertà d'informazione, la libertà economica o la libertà personale – se i blocchi di rete sono legati all'analisi di pacchetti di dati – possono essere colpite con gradi diversi. In primo piano vi è il diritto alla sfera privata e all'autodeterminazione informativa (art. 13 Cost.).

Vanno inoltre osservate diverse garanzie procedurali, ad esempio le garanzie procedurali generali compreso il diritto di essere sentiti (art. 29 Cost.), il diritto al giudizio da parte di un'autorità giudiziaria (art. 29a Cost.) come pure standard minimi di una procedura giudiziaria (art. 30 Cost.): in particolare per l'impiego di liste di blocco che devono essere attuate dai fornitori di servizi internet è in discussione il rispetto del diritto di essere sentiti. La comunicazione della disposizione di blocchi di rete avviene infatti spesso nel Foglio federale e non attraverso comunicazione diretta a tutti gli interessati. I fornitori di servizi internet devono di conseguenza controllare autonomamente le liste di blocco sulle quali sono indicati i siti web da bloccare. Se tali liste vengono emanate senza sentire i proprietari dei siti web da bloccare è interessato il loro diritto di essere sentiti. Lo stesso vale per i titolari dei diritti che non hanno chiesto essi stessi l'emanazione di un blocco di rete.

Non è ancora accertata la conciliabilità di blocchi di rete svizzeri per offerte legali all'estero sotto l'aspetto degli accordi commerciali internazionali.

I blocchi di rete sono discutibili soprattutto nei casi in cui cercano di evitare un comportamento legale di utenti finali.

Legislazione contraddittoria

Una problematica particolare è rappresentata dai blocchi di rete che mirano di principio a ostacolare un comportamento legale di utenti finali. Se il comportamento che si intende bloccare non è punibile per legge, i blocchi di rete sono contraddittori. Un comportamento dei cittadini di per sé ammesso non può essere impedito od ostacolato. Il legislatore non può puntare sull'ammissibilità (giuridica) di un comportamento (ad es. giochi d'azzardo esteri su internet) e introdurre al contempo una regolamentazione per evitare (effettivamente) l'accesso a simili siti in internet. Sarebbe come se lo Stato non volesse vietare il transito su una strada ma intervenisse attivamente affinché la strada geli o vengano sparsi dei chiodi sulla carreggiata. Se il legislatore non vuole esporsi all'accusa del comportamento contraddittorio, rimangono solo due possibilità: può rimanere fedele all'attuale situazione giuridica e rinunciare all'introduzione di blocchi di rete oppure deve mettere le carte in tavola e con l'introduzione di blocchi di rete deve al contempo vietare anche le attività su piattaforme estere di gioco d'azzardo. Una via di mezzo tra queste due posizioni è di per sé contraddittoria.

Laddove si parla di reati sono possibili già oggi dei blocchi di rete – che avvengono di regola su base volontaria.

Collaborazione volontaria quale strumento efficace

Vi sono ambiti della vita quotidiana nei quali non possiamo a ragione ammettere una libertà assoluta in internet. Pensiamo ad es. alla lotta al terrorismo o alla pornografia infantile. Il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) collabora ad esempio a stretto contatto con i fornitori di servizi internet. Dal 2007 tra il SCOCI e i principali fornitori di servizi internet è stato siglato un accordo relativo al blocco di siti internet a carattere pedopornografico. Il blocco riguarda esclusivamente siti internet esteri che propongono il download di contenuti pornografici vietati con minori conformemente all'art. 197 cpv. 4 e 5 CP. I fornitori di servizi internet bloccano l'accesso a siti in virtù della propria etica aziendale e delle condizioni generali e reindirizzano successivamente l'utente a una cosiddetta «stop page». A questo proposito il SCOCI allestisce e gestisce un elenco costantemente aggiornato su cui figurano tra 700 e 1'000 siti web. Nel quadro di tale progetto, il SCOCI collabora a stretto contatto con INTERPOL. L'elenco allestito in Svizzera alimenta in gran parte la «worst of list» di INTERPOL su cui figurano i siti web che offrono contenuti pedopornografici. Il SCOCI cerca attivamente ogni giorno nuovi siti internet con contenuti a carattere pedopornografico e aggiorna costantemente l'elenco INTERPOL, gestito in collaborazione con altri Paesi. È discutibile se ancorando questa collaborazione a livello legislativo verrebbe creato un valore aggiunto. Poiché potrebbe generare una misura coercitiva statale, l'elenco dovrebbe essere assoggettato a un controllo statale da parte di un'autorità o di un tribunale. Non è però nell'interesse della collettività rendere di dominio pubblico un tale elenco.

Occorre rinunciare ai blocchi di rete

Motivi economici, sociali, tecnici e giuridici si oppongono all'introduzione di blocchi di rete.

Numerosi svantaggi

Un'analisi approfondita di blocchi di rete da una prospettiva economica, sociale, tecnica e giuridica mostra che sono un tentativo inadatto e pericoloso che estende i confini delle possibilità di ingerenza statale. I blocchi di rete danneggiano la nostra società libera, lo Stato di diritto e l'economia (su internet) in Svizzera.

Disturba in modo particolare il fatto che i blocchi di rete danneggino l'infrastruttura di rete e sono ciononostante semplici da aggirare. Inoltre, spesso è praticamente impossibile evitare un overblocking di contenuti web legali. I blocchi di rete sono contraddittori nei settori in cui vogliono limitare un comportamento di principio legale dei cittadini (come nel caso della legge sui giochi in denaro).

Internet e la libera circolazione dei dati sono la spina dorsale della nostra società ed è ormai impossibile immaginare la nostra vita quotidiana senza questo strumento, che non può quindi diventare la pedina di lobbisti di alcun tipo. Deve essere piuttosto liberamente accessibile ovunque. Rinomati esperti considerano inammissibile e sproporzionata l'introduzione di blocchi di rete nell'ambito del diritto d'autore. Le eccezioni devono essere ammesse esclusivamente per la protezione della sicurezza pubblica (protezione dal terrorismo, protezione dalla pedopornografia, ecc.).

Per questi motivi risulta chiaro che sulla base di riflessioni di principio occorre rinunciare all'introduzione di blocchi di rete.

I blocchi di rete nella legge sui giochi in denaro celano il pericolo di un effetto domino.

Legge sui giochi in denaro: si rischia di aprire una falla

Il 10 giugno 2018 il popolo svizzero sarà chiamato a votare sulla nuova legge sui giochi in denaro. Per proteggere le case da gioco con sede in Svizzera, la legge prevede dei blocchi dell'accesso – una novità assoluta in Svizzera – con cui in futuro dovrà essere vietato l'accesso a offerte di giochi in denaro estere in internet. Già oggi in Svizzera l'offerta di simili giochi è sì vietata, ma giocare è ammesso.

economiesuisse respinge la legge sui giochi in denaro a causa dell'introduzione di blocchi di rete e mette al contempo in guardia contro il cambiamento di paradigma. La rinuncia al libero accesso a internet potrebbe aprire una falla a favore della censura di internet. Una volta a disposizione i relativi strumenti, altri gruppi d'interesse troverebbero infatti rapidamente dei motivi per giustificare altri blocchi. Il segnale lanciato agli altri settori e alla nostra immagine a livello internazionale quale sede per aziende tecnologiche orientate al futuro sarebbe disastroso.

1. Florent Thouvenin, Burkhard Stiller, Peter Hettich, Thomas Bocek, Kento Reutimann in sic! 2017 pag. 701 segg.