

A Legislação sobre Internet no Brasil: Projetos, Leis e as Questões de Liberdade e Privacidade

Daniel M. G. de Moraes¹, Thiago C. Sousa¹

¹Programa de Pós-Graduação em Sistemas de Informação – Escola de Artes, Ciências e Humanidades – Universidade de São Paulo (USP) – São Paulo, SP – Brasil

{damorais, thiago.carvalho.sousa}@usp.br

Abstract. *This paper discusses the main law projects in Brazil about Internet and their rules of use, and also about crimes practiced through the network; from the perspective of privacy and individual freedom. Contextualizes it with the actions taken internationally, especially in the United States and European Union, world exponents in this matter.*

Resumo. *Este trabalho discute os principais projetos de lei brasileiros sobre a Internet e suas regras de uso, assim como crimes praticados através da rede, sob a ótica da privacidade e liberdade individuais. Contextualiza o assunto junto a medidas adotadas internacionalmente, principalmente nos Estados Unidos e União Européia, expoentes mundiais nesta questão.*

1. Introdução

Hoje, uma grande parcela da população brasileira tem acesso à Internet e, cada vez mais, este número tem aumentado, conforme pode ser observado no gráfico 1. Junto com este acréscimo no número de acessos, têm aumentado também o número de incidentes dos mais diversos tipos: crimes envolvendo roubo de senhas para acesso a contas bancárias, difamação, crimes de incitação ao ódio, entre outros [IBGE 2009]. Situações existentes no mundo real e que são, em muitos casos, muito mais graves no meio virtual, dada a velocidade com a qual a informação se propaga.

Não raro são noticiados pela mídia situações onde imagens íntimas de pessoas são divulgadas por terceiros, boatos negativos são espalhados e, a despeito de serem verdadeiros ou não, temos o prévio julgamento da sociedade, incitações a ódio racial são veiculados, escondidos atrás de um sentimento de anonimato e impunidade a qual se tem atrás de uma tela de computador.

Assim sendo, têm surgido discussões a respeito de como tratar estes crimes e o próprio papel da Internet, no âmbito de direitos e deveres do cidadão. Debate este que tem atingido as esferas legislativas brasileiras, entrando em pauta a discussão de projetos de lei, sendo eles os mais emblemáticos o projeto de lei 2126/2011 [Câmara dos Deputados 2011], conhecido como Marco Regulatório da Internet e o projeto de lei 84/1999 [Câmara dos Deputados 1999], conhecido como Lei Azeredo, em referência ao nome de seu relator.

Segundo Yves [Pouillet 2009], “é preciso estabelecer regras para proteger a privacidade e garantir a proteção da informação. Estas medidas são de fato necessárias, pois ajudam indivíduos a manter e desenvolver a capacidade de agir de forma independente, ou cooperar com os outros no seio da sociedade para que ela possa permanecer democrática, baseada no respeito mútuo de diferenças e ao livre desenvolvimento de

a proteção de direitos autorais, dando poderes legais para combate ao tráfego on-line de propriedade protegida e artigos falsificados [Kang 2011]. Segundo o projeto, usuários que compartilham conteúdo pirata poderiam ser presos; e sites poderiam ser fechados pela acusação de permitir ou facilitar a divulgação de conteúdos ilegais. O simples fato de um site ter ligação com outro suspeito de pirataria (como por exemplo, um *link* sugerido por um buscador), ou um usuário que poste uma informação de pirataria numa rede social, seriam motivos suficientes para que esses sites fossem fechados.

Logo, esse projeto de lei incitaria uma censura na internet, removendo a liberdade de ação e expressão dos seus usuários. Grandes gravadoras de músicas, estúdios de cinema e editoras de livros foram os principais apoiadores desta lei, alegando que são lesados pela livre distribuição de seus conteúdos na rede. Já as principais empresas e serviços da *Internet* (como *Google*, *Facebook* e *Twitter*) foram contrários ao projeto, incentivando seus usuários a protestarem contra.

O dia 18 de janeiro de 2012 foi marcado como o ápice das revoltas, quando diversos sites em todo o mundo se manifestaram contrários ao SOPA. Alguns, inclusive, interromperam seus serviços por 24 horas. T tamanha proporção das manifestações, até mesmo a Casa Branca se posicionou contra o projeto de lei.

No dia 20 de janeiro, um dos criadores e principais defensores do projeto, Lamar Smith, cedeu à pressão e suspendeu o projeto. [R7 2012].

2.2 PIPA

A sigla significa **PROTECT IP Act** (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*). Numa tradução livre, seria algo como Lei de Prevenção de Ameaças Reais Online à Criatividade Econômica e ao Roubo da Propriedade Intelectual.

Em síntese, o objetivo do projeto é dar ao governo dos EUA e aos detentores de direitos autorais ferramentas adicionais para conter o acesso a *sites* com conteúdos ilegais, especialmente aqueles que se localizam fora dos Estados Unidos. Segundo a lei, o Governo Americano poderia bloquear o acesso e inclusive fechar *sites* suspeitos de difundir a pirataria [McCullagh 2011].

A medida, proposta em maio de 2011 pelo senador Patrick Leahy, ganhou o apoio da Indústria do Entretenimento Cultural. Mas assim como o SOPA, não suportou as pressões populares e internacionais e foi arquivado [Weisman 2012].

2.3 Outras Legislações

A Câmara dos Deputados dos EUA aprovou em 26 de abril de 2012 o **CISPA - Cyber Intelligence Sharing and Protection Act** (Lei de Proteção e Compartilhamento de Cyber Inteligência), um projeto de lei apoiado por 100 membros do Congresso dos EUA. O CISPA pretende melhorar o poder dos EUA para combater crimes e ataques virtuais, promovendo e incentivando a troca de informações entre governo federal, agências de segurança e empresas privadas. A lei aprovada permite que provedores de internet, redes sociais e qualquer outra entidade privada repassem para o governo (e troquem entre si) informações que digam respeito a pessoas consideradas suspeitas de cometer crimes pela internet, sem a necessidade de ordem judicial [Idgnow 2012].

A *Mozilla Foundation* foi a primeira grande empresa que se posicionou contrária a Lei [Koebler 2012]. Representantes dizem que o CISPA fere a privacidade, e dá imunidade a empresas e ao governo para o uso indevido de informações. Críticos ainda argumentam que os conceitos que definem uma pessoa como “suspeita” são muito vagos, levantando uma discussão ética.

Ao contrário dos projetos de lei SOPA e PIPA, grandes companhias como *Facebook*, *Microsoft*, *Intel*, *IBM* e *Oracle* se declaram publicamente a favor da CISPA. Segundo reportagem do Diário Liberdade (2012), o principal motivo pelo qual as empresas estão apoiando o CISPA é porque ele tira a pressão das empresas privadas de regular os usuários. Transfere este papel e responsabilidade para uma entidade do governo. Efetivamente, ele faz com que a empresa não possa ser processada por passar as informações de um usuário para o governo.

O projeto do CISPA está sendo votado no congresso norte-americano. O projeto já foi aprovado pelos deputados, e agora depende da votação do Senado. O texto foi aprovado mesmo após a Casa Branca se posicionar contra a lei [Olhar Digital 2012].

3. Acordos de Ordem Mundial

3.1 A Convenção de Budapeste

A Convenção sobre o Cibercrime, também conhecido como Convenção de Budapeste, foi o primeiro tratado internacional elaborado buscando tipificar os principais crimes cometidos na Internet, harmonizar leis, aperfeiçoar as técnicas de investigação e aumentar a cooperação entre as nações [Souza e Pereira 2009].

Foi criada em 2001, na Hungria, pelo Conselho da Europa, e está em vigor desde 2004, após a ratificação de cinco países. Engloba mais de 30 países signatários, entre eles: Albânia, Armênia, Áustria, Bélgica, Bulgária, Croácia, Ilha de Chipre, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letônia, Moldova, Holanda, Noruega, Polônia, Portugal, Romênia, Espanha, Suíça, República Iugoslava da Macedônia, Ucrânia e Inglaterra. De países não-membros do Conselho Europeu, houve a adesão do Canadá, Japão, África do Sul e dos Estados Unidos [Council of Europe 2012].

Segundo o texto, a Convenção [Council of Europe 2001] prioriza “uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” e reconhece “a necessidade de uma cooperação entre os Estados e a indústria privada”. O Tratado possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente) e 48 artigos encorpados num texto de fácil compreensão, sobretudo porque não traz informações muito técnicas. Em 2006, foi incluído mais um protocolo sobre a criminalização de atos de natureza racista e xenofóbicos [Arias 2006].

A Convenção de Budapeste é o principal acordo internacional regulador de uma legislação para crimes na Internet. Ele dá diretrizes gerais, mas não fere a autonomia dos países signatários de criarem suas próprias leis para criminalizar os cibercrimes. Portanto, observamos na União Européia (que tem o maior número de países participantes) alguns países que têm legislações mais rígidas, enquanto outros são mais

tolerantes. Nos Estados Unidos, que também é signatário da convenção, foi criada dentro do Departamento de Justiça Federal a “Seção de Crimes do Computador e Propriedade Intelectual” (CCIPS, na sigla em Inglês), que legisla segundo as diretrizes do tratado.

O Brasil não aderiu à Convenção de Budapeste. Logo, o país ainda não conta com uma legislação específica para a *Internet* e cibercrimes. Foi proposto o projeto conhecido como Lei Azeredo, que segue os princípios da Convenção, mas é mais rígido. Trataremos sobre ele nos próximos capítulos.

3.2 ACTA

A sigla em inglês significa *Anti-Counterfeiting Trade Agreement*. Em tradução livre, “Acordo de Comércio Contra a Pirataria”.

O acordo foi assinado em Outubro de 2011 por Austrália, Canadá, Japão, Marrocos, Nova Zelândia, Cingapura, Coreia do Sul e Estados Unidos. O pacote prevê leis mais rígidas para defesa de direitos autorais e combate à pirataria [Foreign Affair and International Trade Canada 2012].

O ACTA estipula que os países signatários criem leis nacionais que garantam a retirada de conteúdo ilegal da internet. Para isso, a privacidade de usuários pode ser invadida e o infrator pode se ver obrigado a ressarcir parcelas de lucro, além de receber multas e penas legais [Demartini 2012].

Além da propriedade intelectual, este acordo também aumenta a gravidade de crimes como a gravação de imagens a partir de telas de cinema, ou a falsificação de medicamentos. A vigilância na distribuição física de conteúdo pirateado também seria intensificada.

A União Européia estuda a adesão ao ACTA. Entretanto, manifestações ocorridas em toda a Europa demonstram a insatisfação da população com tais medidas [Gaspar 2012].

4. A Legislação Brasileira

No Brasil não há um conjunto de leis prevendo a existência da Internet como a temos hoje. Segundo Vanessa Simões, coordenadora da promotoria de combate a crimes cibernéticos do Ministério Público de Minas Gerais, é possível assegurar que "para 50% dos inquéritos que hoje aportam na promotoria são, infelizmente, requeridos o arquivamento porque não existe tipificação para a conduta ali elencada." [Folha de São Paulo 2011].

Sendo assim, têm surgido o debate acerca da regulamentação da Internet e a definição de condutas litigiosas por meio da rede, assim como meios para controlar e encontrar eventuais contraventores. Foram propostos na Câmara dos Deputados dois projetos de lei neste sentido: O projeto de lei 84/1999 [Câmara dos Deputados 1999], também conhecido como Lei Azeredo devido ao relator da proposta, deputado Eduardo Azeredo, e o projeto de lei 2126/2011 [Câmara dos Deputados 2011], proposto pelo Poder Executivo, conhecido como Marco Regulatório da Internet.

4.1 O Marco Regulatório da Internet

O projeto de lei 2126/2011 foi proposto em agosto de 2011 pelo poder Executivo e tem por objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" e também determinar "diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios". Está dividido em cinco capítulos.

No primeiro capítulo são apresentadas as disposições preliminares do projeto de lei. Nele são apresentados os fundamentos e princípios que orientaram na confecção da lei, assim como os seus objetivos específicos. Também aqui são definidos os significados de cada um dos termos utilizados, como por exemplo, Internet, terminal e endereço IP, para o referido contexto.

O segundo capítulo trata dos direitos e garantias dos usuários. Têm destaque neste capítulo dois pontos de suma importância: o Inciso I do artigo 7º, no qual assegura ao indivíduo o direito à "inviolabilidade e ao sigilo de suas comunicações" sigilo este que pode ser quebrado "por ordem judicial, nas hipóteses e na forma que a lei estabelecer" e também o artigo 8º o qual estabelece a "garantia do direito à privacidade e à liberdade de expressão nas comunicações", disposição a qual vem reforçar através de lei específica o que é disposto e garantido pelo artigo 5º da Constituição Federal (1988).

O terceiro capítulo, intitulado "Da provisão de conexão e de aplicações de Internet", estabelece os deveres a serem cumpridos pelo provedor de Internet, principalmente sobre suas obrigações relativas à guarda de registros de acesso, manutenção da privacidade do usuário e quebra do sigilo, ocorrida por ordem judicial. Também expõe a não responsabilização do provedor de conexão sobre o conteúdo e operações efetuadas pelos usuários do serviço.

A atuação do poder público é tratada no quarto capítulo, onde são constituídas as "diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no Desenvolvimento da Internet no Brasil". O conteúdo deste capítulo está de acordo com as atribuições do poder público definidas na Constituição [Constituição da República 1988], principalmente no que tange à transparência do poder público, a participação do indivíduo no processo decisório no que tange a novas medidas e também o papel educacional, disposto neste projeto através do artigo 21, que estabelece o "dever constitucional do Estado na prestação da educação em todos os níveis de ensino" para "o uso seguro, consciente e responsável da Internet" [Câmara dos Deputados 2011].

Por fim, o quinto capítulo apresenta as disposições finais, sobre a utilização deste conjunto de leis para a defesa de direitos e interesses, e também determina a entrada em vigor, que ocorreria a partir da sanção presidencial.

Atualmente tal projeto de lei está sendo discutido na Câmara dos Deputados, tendo como última atividade a solicitação feita pelo Deputado Alessandro Molon, onde o mesmo pede a desapensação do conteúdo do terceiro capítulo, do restante; uma vez que este é o ponto de maior discussão sobre o projeto, e que, segundo o mesmo "não deveriam tramitar conjuntamente em função da diferença no escopo de atuação da sua propositura" [Câmara dos Deputados 2011].

4.2 A Lei Azeredo

Proposto em maio de 1999, pelo projeto de lei nº 84 / 1999 [Câmara dos Deputados 1999] teve sua redação alterada pelo emenda/substitutivo do Senado Federal nº 84/1999 [Câmara dos Deputados 2003] no qual o projeto de lei foi atualizado e algumas alterações em seu teor foram realizadas. Este projeto de lei tem por objetivo "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências", apresentando artigos a serem incorporados na Legislação Brasileira de forma a prever e punir uma série de condutas criminosas possíveis de execução por meios digitais.

Segundo o projeto de lei, serão incluídas no Código Penal as tipificações de crimes e respectivas punições às seguintes ações feitas por meio eletrônico:

- Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado;
- Obtenção, transferência ou fornecimento não autorizado de dado ou informação;
- Divulgação ou utilização indevida de informações e dados pessoais;
- Inserção ou difusão de código malicioso;
- Estelionato Eletrônico;
- Falsificação de dado eletrônico ou documento.

Além de alterações em leis já existentes como, por exemplo, o acréscimo do termo "Internet" na redação do artigo 241 da Lei nº 8069, de 13 de julho de 1990, que versa sobre a tipificação de crime e punições sobre a produção e utilização de material de pornografia infantil.

Um ponto importante nesta nova redação é a especificação de obrigações do provedor de acesso a Internet (artigo 22) com relação ao monitoramento da conexão a Internet por parte de seus consumidores. Segundo a nova redação, passa a ser obrigações do provedor de acesso:

- Manter o registro de informações de acesso relativas a origem, destino, data e horário de cada conexão recebida (Inciso I);
- Registrar informações adicionais, mediante requisição judicial, a serem usadas em investigações em curso, sendo então responsáveis pela guarda e inviolabilidade e confidencialidade de tais dados (Inciso II);
- Informar a autoridades competentes quaisquer denúncias recebidas nas quais contenham indícios de crime, ocorridos no âmbito da rede sob responsabilidade do provedor (Inciso III).

Atualmente (desde março de 2012), o projeto de lei encontra-se com um requerimento para a realização de uma audiência pública para a discussão do projeto na Câmara dos Deputados, onde se pretende discutir os pontos mais controversos deste projeto, para que então sejam realizados ajustes no texto e um novo encaminhamento para aprovação [Câmara dos Deputados 1999].

5. A Privacidade e as Leis Regulatórias Sobre o Acesso à Internet

Observando as legislações estudadas, vemos que a tentativa dos governos é proteger a propriedade, cada qual de acordo com os seus princípios constitucionais. Nos EUA e União Européia, onde a presença e acessibilidade à Internet entre a população já se dá há um longo tempo [International Telecommunication Union 2011], nota-se que o desafio está sendo a proteção à propriedade intelectual, a proteção aos direitos autorais, conforme é possível observar pela tentativa de proposição de leis como o SOPA e o CISPA.

Projetos como o SOPA e o CISPA não fogem muito do excessivo controle sobre a Internet. Apesar de não haver o monitoramento do indivíduo, é dado às autoridades o poder de bloquear completamente o acesso a determinado endereço da rede, bastando para tal a suspeita de irregularidades.

Apesar de terem sido elaborados com o intuito de dificultar a distribuição de conteúdo ilegal, vislumbrar desvirtuamentos na utilização desta medida, como forma de repressão e controle da informação. E isto não é um exercício complexo: vide o controle da Internet exercido por países com restrições severas a liberdade de acesso a informação e expressão, como a China e o Irã, onde tais restrições servem mais aos interesses do poder em atuação do que propriamente do indivíduo.

No Brasil, conforme evidenciado pelos projetos da Lei Azeredo e do Marco Regulatório da Internet o objetivo é definir o papel da Internet na sociedade, os direitos, deveres e responsabilidades de cada um dos componentes. Isto ocorre pela recente e acelerada expansão da importância da Internet na sociedade, cujo número de usuários em território nacional tem crescido de forma vertiginosa nos últimos anos.

Porém, nota-se um ponto comum em todos os projetos de lei: a questão do monitoramento do usuário e o poder dado às agências regulatórias em todos os âmbitos. Enquanto nos EUA o SOPA se propõe a dar poderes às agências regulatórias para bloquear o acesso a quaisquer dos sites, dados e usuários, independente de qualquer julgamento prévio, no Brasil temos o monitoramento acentuado do usuário final, na forma de registros de acesso pelos provedores, onde qualquer origem e destino são registrados e disponibilizados para quaisquer autoridades, para "fins de investigação", sem haver na legislação qualquer indicativo de situações onde poderia haver esta quebra de sigilo. Adiciona-se aí a possibilidade, segundo o projeto de lei 84/1999, de se "preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação" [Câmara dos Deputados 1999]: temos aí então um enorme poder de monitoramento pelas autoridades, não condizente com as liberdades previstas na Constituição Federal (1988).

Traçando um paralelo, é como se o cidadão, independente de ter cometido um crime ou não, tivesse um rastreador ligado ao seu corpo, o qual registrasse todos os seus movimentos e cujos dados estivessem à disposição, bastando para tal a autorização judicial. Ressalta-se que a mera suspeita já seria suficiente para a liberação de tais dados, uma vez que a liberação da permissão de acesso seria dada por um juiz, sem que seja necessariamente identificada a real culpa do indivíduo. Somente esta questão já se torna contraditória com um dos princípios orientadores na elaboração do Marco Regulatório, que é a "proteção da privacidade", conforme exposto no Inciso III do artigo 3º deste projeto de lei.

Ainda mais controverso se torna este monitoramento quando consideramos a sua real efetividade no rastreamento e punição de um eventual contraventor. Tomando como base que a "Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos computacionais através do mundo" [Kurose e Ross 2010], a atuação das autoridades com relação ao rastreamento de algum crime utilizando a rede é restrita ao âmbito nacional. Qualquer atuação fora disto depende de acordos internacionais, como a Convenção de Budapeste [Souza e Pereira 2009], o que é deveras limitante, uma vez que nem todos os países do mundo são signatários (incluindo aí o Brasil) e muitas vezes a obtenção de informações esbarra na legislação do país em questão. Visto que é simples burlar o acesso e mesmo o usuário dito comum (sem conhecimentos técnicos avançados) faz acessos que envolvem servidores nos mais diversos pontos do mundo, tal rastreamento se torna inócuo no sentido de rastrear a origem de um delito, enquanto que a exibição dos hábitos de acesso ficaria evidente. Mais uma vez, o contraventor, sabendo desta possibilidade de rastreamento, não faria acessos utilizando a parte brasileira da rede, disfarçando seu acesso a partir de algum país, possivelmente dentre aqueles que não fazem parte de nenhum acordo de cooperação na identificação de crimes.

Portanto a discussão ainda deve ser aprofundada, visando discutir o papel ético de tais medidas e até que ponto a proteção (e sua respectiva punição) contra crimes deve ser motivo para restrição da liberdade e privacidade do indivíduo inocente.

6. Considerações Finais

Este trabalho apresentou alguns aspectos atuais da legislação brasileira no que tange o acesso à Internet. Nota-se, pelo estudo o quão inicial é o estágio do trabalho dos legisladores no que competem estas questões. Mas também se evidencia o fato que mundialmente também é um assunto delicado e polêmico, principalmente pela tênue linha que separa a segurança do acesso a violações de liberdades individuais.

O caso brasileiro é bastante peculiar uma vez que nossa legislação não prevê uma série de variações de crimes, propiciadas pelo acesso à Internet. Mas o maior problema não está na legislação em si, já que os crimes como estelionato, violação de privacidade, calúnia e difamação, falsificação de documentos, entre outros, já são previstos em nosso código penal, sendo a Internet apenas um novo meio para a execução de tais delitos e, portanto, se configura como variantes de simples incorporação às leis. O maior problema está na detecção destes crimes, o que por si só já evidencia o porquê da existência de artigos tão polêmicos relativos ao monitoramento.

É necessário que o debate acerca do tema seja estendido, de forma que a segurança do cidadão não venha ao custo dos direitos a privacidade e a liberdade, e também que não seja dado poder suficiente ao Estado para que tal segurança desvirtue em censura. Também é importante que sejam envolvidos no debate especialistas técnicos, uma vez que mesmo que um mecanismo de rastreamento, como o proposto no Marco Regulatório e na Lei Azeredo, pode se mostrar inócuo diante das características técnicas da Internet.

7. Referências

- Arias, M. L. (2006) “Internet Law - The European Union Criminalizes Acts of Racism and Xenophobia Committed through Computer Systems”, https://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2422, acesso em maio, 2012.
- CCIPS (2006) “Prosecuting Intellectual Property Crimes”, <http://www.justice.gov/criminal/cybercrime/>, setembro, acesso em maio, 2012.
- Câmara dos Deputados da República Federativa do Brasil (2011), “Projeto de Lei 2126/2011”, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255> acesso em maio, 2012.
- Câmara dos Deputados da República Federativa do Brasil (1999), “Projeto de Lei nº 84/1999”, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>, acesso em maio, 2012.
- Constituição da República Federativa do Brasil de 1988 (1988), http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm, acesso em maio, 2012.
- Council of Europe (2001) “Convention on Cybercrime”, <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>, novembro, acesso em maio, 2012.
- Council of Europe (2012) “Chart of signatures and ratifications”, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>, acesso em maio, 2012.
- Demartini, F. (2012) “Fantasma do SOPA ainda vive, e agora se chama ACTA”, <http://www.tecmundo.com.br/pirataria/18311-fantasma-do-sopa-ainda-vive-e-agora-se-chama-acta.htm>, janeiro, acesso em maio, 2012.
- Diário Liberdade (2012) “EUA lançam nova lei de controle da internet”, <http://www.diarioliberalidade.org/mundo/comunicacom/26539-eua-lan%C3%A7am-nova-lei-de-controle-da-internet.html>, maio, acesso em maio, 2012.
- Folha de São Paulo (2011) “‘Lei Azeredo’ recebe críticas em audiência na Câmara”, <http://www1.folha.uol.com.br/poder/943026-lei-azeredo-recebe-criticas-em-audiencia-na-camara.shtml>, julho, acesso em maio, 2012.
- Foreign Affairs and International Trade Canada (2011) “Anti-Counterfeiting Trade Agreement (ACTA)”, http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/intellect_property.aspx?view=d, acesso em maio, 2012.
- Gaspar, J. (2012) “ACTA pode não chegar a lei na Europa”, <http://inforeflex.wordpress.com/2012/05/05/acta-pode-no-chegar-a-lei-na-europa/>, maio, acesso em maio, 2012.
- IBGE (2009) “De 2005 para 2008, acesso à Internet aumenta 75,3%” http://www.ibge.gov.br/home/presidencia/noticias/noticia_visualiza.php?id_noticia=1517, acesso em maio, 2012.

- Idgnow (2012) “Câmara dos EUA aprova Cispa, lei que pode ferir privacidade”, <http://idgnow.uol.com.br/internet/2012/04/26/congresso-dos-eua-aprova-cispa-lei-que-pode-ferir-privacidade/>, abril, acesso em maio, 2012.
- International Telecommunication Union (2011) “ICT Facts and Figures”, <http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf>, acesso em maio, 2012.
- Kang, C. (2011) “House introduces Internet piracy bill”, http://www.washingtonpost.com/blogs/post-tech/post/house-introduces-internet-piracy-bill/2011/10/26/gIQA0f5xJM_blog.html, outubro, acesso em maio, 2012.
- Koebler, J. (2012) “Mozilla Becomes First Tech Company to Slam CISPA”, <http://www.usnews.com/news/articles/2012/05/02/mozilla-becomes-first-tech-company-to-slam-cispa>, maio, acesso em maio, 2012.
- Kurose, J., Ross, K. (2010) “Computer Networking: A Top-Down Approach”. 5ª edição, Pearson, p. 2-9.
- McCullagh, D. (2011) “Senate bill amounts to death penalty for Web sites”, http://news.cnet.com/8301-31921_3-20062398-281.html, maio, acesso em maio, 2012.
- Olhar Digital (2012) “CISPA: Mozilla se posiciona contra o projeto”, http://olhardigital.uol.com.br/produtos/digital_news/noticias/cispa-mozilla-se-posiciona-contra-o-projeto, maio, acesso em maio, 2012.
- Pouillet, Y. (2009) “Data protection legislation: What is at stake for our society and democracy?”, In: Computer Law & Security Review 25, Elsevier.
- R7 (2012) “Principal defensor de lei antipirataria suspende o projeto nos Estados Unidos”, <http://noticias.r7.com/tecnologia-e-ciencia/noticias/principal-defensor-de-lei-antipirataria-desiste-do-projeto-nos-eua-20120120.html>, janeiro, acesso em maio, 2012.
- Senado da República Federativa do Brasil (2003), “Emenda/Substitutivo do Senado 84/1999”, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=405461> acesso em maio, 2012.
- Souza, G. L. M., Pereira, D. V. (2009) “A Convenção de Budapeste e as Leis Brasileiras”, <http://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf>, maio, acesso em maio, 2012.
- Weisman, J. (2012) “After an Online Firestorm, Congress Shelves Antipiracy Bills”, http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=2, janeiro, acesso em maio, 2012.
- Wikipedia (2012) “Stop Online Piracy Act”, http://pt.wikipedia.org/wiki/Stop_Online_Piracy_Act, acesso em maio, 2012.