

**UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIA POLÍTICA
MESTRADO EM CIÊNCIA POLÍTICA**

SITUAÇÕES DE CONFLITO NO USO DA INTERNET: EMBATES E SOLUÇÕES

WILLIAN WASHINGTON WIVES

BRASÍLIA

2013

WILLIAN WASHINGTON WIVES

SITUAÇÕES DE CONFLITO NO USO DA INTERNET: EMBATES E SOLUÇÕES

Dissertação de Mestrado apresentada ao Instituto de Ciência Política da Universidade de Brasília para obtenção do título de Mestre em Ciência Política.

Orientador: Prof. Dr. Carlos Marcos Batista

BRASÍLIA

2013

WILLIAN WASHINGTON WIVES

SITUAÇÕES DE CONFLITO NO USO DA INTERNET: EMBATES E SOLUÇÕES

Dissertação aprovada em 28/07/2013, pelo corpo docente do curso de Ciência Política da Universidade de Brasília como requisito parcial para a obtenção do grau de Mestre em Ciência Política.

Carlos Marcos Batista
Professor Doutor Orientador da UnB

Cristiano Ferri Soares de Faria
Professor Doutor Examinador

Paulo César Nascimento
Professor Doutor Examinador da UnB

BRASÍLIA

2013

Reprodução permitida desde que citada a fonte.

WIVES, Willian Washington.

**Situações de conflito no uso da Internet: embates e soluções / Willian Washington Wives;
orientação Prof. Dr. Carlos Marcos Batista. Brasília, 2013. 82f.**

Dissertação de Mestrado em Ciência Política pela Universidade de Brasília (UnB).

- 1. Internet 2. Conflito 3. Censura**
- 4. Monitoramento 5. Democracia Digital**

CDU

DEDICATÓRIA
Aos meus pais.

AGRADECIMENTOS

*Agradeço aos meus pais, por terem me apoiado em toda
a duração do mestrado.*

*Agradeço à Suelen, por ter me ajudado em todos os
momentos.*

*Agradeço ao meu orientador, Professor Batista, por tudo
que me ensinou.*

RESUMO

Essa dissertação lida com as questões de conflitos causadas pela emergência da Internet. Particularmente conflitos entre governos e cidadãos, onde de um lado se colocam os governos tentando controlar a Internet e do outro os cidadãos tentando se expressar livremente nela. Para isso serão comparados cinco casos de países que restringem as liberdades online ou tentaram as restringir: EUA, França, Brasil, China e Irã.

Palavras-chave: Internet, conflito, censura, monitoramento, democracia digital

ABSTRACT

This dissertation deals with the new issues of conflict caused by the emergence of the Internet. Specifically with conflicts between governments and citizens, where on one side are the governments trying to regulate and control the Internet and in the other the citizens, using it to freely express themselves. For that purpose five countries that tried to restrict online liberties, or that effectively restrict it, will be compared: USA, France, Brazil, China and Iran.

Key-words: Internet, Conflict, censorship, monitoring, digital democracy, circumvention

SUMÁRIO

Introdução	11
1. Teoria	17
1.1 O espaço virtual e a política	17
1.2 Internet e representação	18
1.3 A Internet como modificadora da estrutura da poder	19
1.4 O discurso político.....	21
1.5 Democracia Eletrônica	22
1.6 Digital Divide	23
1.7 Privacidade e monitoramento	24
2. Objeto de Estudo	26
2.1 Direitos autorais e estratégias de controle	26
2.2 Censura	27
3. Metodologia	29
3.1 Modelo teórico.....	31
4. Estudos de caso	35
4.1 EUA	35
4.1.1 SOPA e PIPA	35
4.1.2 Reações ao SOPA/PIPA	39
4.1.3 Efeitos políticos e sociais	41
4.1.4 Outras considerações	43
4.2 França	44
4.2.1 Hadopi	45
4.2.2 Reações e críticas.....	47
4.2.3 Impactos e outras considerações.....	49
4.3 Brasil	51

4.3.1 Lei Azeredo	53
4.3.2 Marco Civil.....	54
4.3.3 O ‘SOPA’ brasileiro	56
4.3.4 Impactos e outras considerações.....	57
4.4 China.....	58
4.4.1 Histórico	60
4.5 Irã.....	61
5.Discussão e conclusão	64
5.1 Estados Unidos e França	64
5.2 Democracias e não democracias.....	65
5.3 Perspectivas brasileiras.....	65
5.5 Alternativas técnicas contra a censura na China e no Irã	66
5.5 Conclusão	68
5.5.1 A Ciência Política e o estudo da Internet	69
5.5.2 Palavra final.....	70
Bibliografia.....	73
Anexos	77

INTRODUÇÃO

Novas tecnologias causam situações de conflito. Essa afirmação pode ser aplicada, em escalas diferentes, para todas as mudanças de paradigma causadas por tecnologias de comunicação. O surgimento do livro impresso espalhou informações, religiões, ideologias e manifestações culturais de maneira muito rápida pela Europa. O surgimento do telégrafo aumentou essa velocidade ainda mais. Posteriormente o rádio e o cinema foram ferramentas políticas importantes para a ascensão do nazismo na Alemanha. Depois, a televisão modificou novamente as eleições dos países democráticos. Estudar os conflitos políticos gerados por cada uma dessas tecnologias é fundamental para se entender os desdobramentos delas na sociedade.

Nas duas últimas décadas a humanidade testemunhou o surgimento da internet como ferramenta imprescindível de compreensão do mundo. De uma ferramenta obscura utilizada por universidades e por militares norte americanos na década de 70, a Internet, a rede de redes, passou para primeiro plano das comunicações mundiais. Cada meio de comunicação anterior à Internet gerou sua própria ruptura, seus próprios conflitos, com a Internet não é diferente. Diversos setores que surgiram, cresceram e se beneficiaram no paradigma anterior se veem ameaçados pela mudança de paradigma, dessa maneira é natural que eles tentem se proteger. Nesses setores podem-se incluir os governos, inclusive os democráticos, pois se beneficiaram do impacto causado nos anos 50 pela televisão e cresceram se baseando nesse meio de comunicação, a Internet pode desafiar sua dominância já consolidada.

Fora do âmbito das democracias temos os países ditatoriais, como a China, que temem a internet, não por ela ser um novo meio, mas por sua arquitetura, por ela ser difícil de ser controlada¹. Aqui surgem os conflitos mais importantes da nossa década,

¹ “The vast potential and benefits of the Internet are rooted in its unique characteristics, such as its speed, worldwide reach and relative anonymity. At the same time, these distinctive features of the Internet that enable individuals to disseminate information in “real time” and to mobilize people has also created fear amongst Governments and the powerful. This has led to increased restrictions on the Internet through the use of increasingly sophisticated technologies to block content, monitor and identify activists and critics, criminalization of legitimate expression, and adoption of restrictive legislation to justify such measures.” (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2011, Human Rights Council, parágrafo 23) (obs.: as traduções das citações em língua estrangeira se encontram no Anexo I)

os conflitos que as ficções *cyberpunk* dos anos 80 e 90 de certa maneira previram². O controle da informação, dos fluxos de informação, da política da informação, isso gera conflitos, gera embates entre governos e cidadãos, de diversas maneiras. O controle da informação pode se mascarar em argumentos de proteção aos direitos autorais, ou ser mais explícito, como o bloqueio total da internet no Egito em 2011, ainda pode ser feito por meio de interpretações amplas de leis antigas, leis pré-internet que serviam para controlar os meios de comunicação existentes então.

Nesse trabalho pretende-se estudar algumas dessas situações de conflito, por meio de estudos de caso, estudos comparados e estudos bibliográficos. A partir desse estudo pode-se ver como os conflitos acerca do uso da internet estão acontecendo atualmente e quais soluções os cidadãos encontraram para lidar com isso, para evitar legislações abusivas, furar as barreiras impostas, ou para se expressar online sem medo de represálias.

Recentemente, os EUA passaram por um processo de discussão de uma nova legislação para combater a pirataria na Internet. Isso gerou uma situação de conflito que poderia alterar significativamente as relações de poder nesse país. As propostas SOPA(Stop Online Piracy Act) e PIPA(Protect Intellectual Property Act) foram legislações apoiadas pelas indústrias de conteúdo³ e criticada por setores importantes da sociedade civil, como a EFF (Eletronic Frontier Foundation), que viram nela o potencial de restrição das liberdades online. Nesse mesmo país, após os atentados de 11 de setembro, foi estabelecido o chamado Patriot Act que, dentre outras provisões, garantia um monitoramento online muito maior sobre os cidadãos americanos e sobre os inimigos dos Estados Unidos. Conflitos de interesses entre os cidadãos e o governo não demoraram a surgir, a mobilização contra o SOPA/PIPA foi intensa, e atualmente o governo Obama é ainda alvo de críticas por estender a duração do Patriot Act.

Outro país importante para o presente estudo é a França, que possui uma das legislações mais restritivas em se tratando de internet, chamada Hadopi. Por razões históricas é interessante se estudar esse país, com seu sistema Minitel ele foi um dos primeiros a ter uma rede compartilhada em escala nacional, o primeiro a ter uma rede pública fortemente controlada pelo governo. A sua legislação de internet é tão rigorosa a

² Obras como *Neuromancer* (Gibson, 1984), *Snow Crash* (Stephenson, 1992), *Ghost in the Shell* (Shirow, 1989).

³ Empresas e conglomerados de empresas que produzem filmes, músicas, literatura, etc...

ponto de estabelecer punições até mesmo para quem não fornece segurança suficiente à sua rede, isto é, deixando-a aberta para utilização não monitorada. A despeito da reação popular contra a medida ela foi aprovada, e o atual presidente, François Hollande, utilizou o sentimento popular contra a lei como um de seus pontos de campanha⁴.

As soluções encontradas por usuários mais experientes no uso da internet para ter uma navegação anônima e segura nesses casos é similar, utilizando ferramentas como servidores *proxy*⁵ eles podem escapar aos mecanismos de controle e tanto baixar conteúdos ilegais quanto disponibiliza-los para outros. Entretanto, isso adiciona um custo, tanto monetário quanto técnico, já que os servidores *proxy* não possuem a mesma velocidade da conexão normal do usuário e possuem uma barreira de entrada, nem todos sabem como utilizar essas ferramentas. Além disso, essas legislações implicam custo social, elas acarretam medo para usuários que continuam com os mesmos comportamentos anteriores. O sentimento de terror que as punições exageradas causam, multas grandes e até mesmo prisão, faz com que o usuário médio se sinta pressionado a seguir a legislação. Isso faz parte dos chamados *chilling effects*⁶, que diminuem a liberdade de expressão e também a criação de novas tecnologias, pelo medo causado pelo processo jurídico previsto pela legislação.

O Brasil passou por uma discussão recente acerca do Marco Civil da Internet. Essa legislação pretende estabelecer um marco regulatório para a internet. Ela foi feita com colaboração de usuários da internet e especialistas no assunto, que puderam dar suas opiniões acerca da legislação e discutir entre si utilizando as ferramentas propiciadas pelo governo. Também foram feitas diversas consultas públicas que

⁴ Após o início da campanha eleitoral francesa François Hollande propôs modificar a estrutura do Hadopi ao invés de trabalhar pela revogação da lei. (<http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/hadopi-comment-francois-hollande-pourrait-transformer-la-loi-07-03-2012-1438656_506.php> Acesso em 9/11/2012)

⁵ “Circumvention is the act of bypassing Internet censorship. There are many ways to do this, but nearly all circumvention tools work in approximately the same manner. They instruct your Web browser to take a detour through an intermediary computer, called a proxy, that is located somewhere that is not subject to Internet censorship has not been blocked from your location knows how to fetch and return content for users like you.” (Bypassing Censorship, disponível em <http://www.howtobypassinternet censorship.org/files/bypassing-censorship.pdf> consultado em 11 de janeiro de 2013)

⁶ “Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy. Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.” (“I’ve got nothing to hide’ and other misunderstandings of privacy”. Solove, D. J. Disponível em <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565> Acesso em 14 de junho de 2012.)

discutiram pontos específicos da legislação. Entretanto, o projeto, na época de elaboração desse trabalho, ainda não foi votado, já que existem muitas divergências entre a posição do governo e os poderosos *lobbies* das empresas de telecomunicações, que querem que a neutralidade⁷ seja modificada, retirada, para que ela possa cobrar mais por serviços como telefonia por internet e mensagens de texto de redes sociais.

Saindo do âmbito dos países democráticos, alguns países do oriente médio podem dar uma valiosa lição de como os governos temem a internet e seu uso. O Egito, durante os protestos da primavera árabe, teve suas conexões de internet totalmente interrompidas por um mês. O Irã passa por diversos debates internos, recentemente apontando para a criação de uma rede interna separada da Internet e totalmente monitorada pelo governo.

Outro exemplo importante é a China, que com o seu chamado *Great Firewall* bloqueia a conexão dos seus usuários a muitos sites. Para este país o controle político sobre a informação é importantíssimo, e recentemente vem sendo questionado por setores expressivos de sua sociedade.

Os conflitos estudados aqui são aqueles em que o governo tenta controlar a internet em desfavor de liberdades do cidadão. Governo deve ser entendido de forma ampla, em alguns desses conflitos partes diferentes do governo podem estar em lados opostos, como no caso das propostas de legislação SOPA/PIPA onde a Casa Branca escreveu uma carta contra a sua tramitação, mesmo ainda existindo apoio no congresso.⁸

Nesse estudo pretende-se entender de forma comparada os conflitos acerca da utilização da Internet. Pretende-se estudar os pontos controversos de algumas legislações e propostas de legislações que tem o potencial de diminuir a liberdade online ou causar conflitos políticos acerca de sua utilização. Com essa abordagem espera-se ter uma visão compreensiva dos conflitos recentes acerca da Internet, utilizando uma abordagem do ponto de vista da ciência política. Ainda, os estudos acerca desses

⁷ A neutralidade se refere à transmissão de pacotes de dados de maneira indiscriminada, isto é, sem um pacote receber vantagem sobre o outro, independentemente do conteúdo do pacote. Sem a neutralidade as empresas de Internet poderiam beneficiar pacotes em detrimentos de outros, beneficiando seus próprios conteúdos, por exemplo.

⁸ “While we believe that online piracy by foreign websites is a serious problem that requires a serious legislative response, we will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines the dynamic, innovative global Internet.” (Combating Online Piracy while Protecting an Open and Innovative Internet, Disponível em: <<http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy>> Acesso em 11 de janeiro de 2013)

assuntos podem guiar discussões; entendendo os fatores que levaram aos resultados de cada conflito passado, pode-se compreender os conflitos futuros.

No capítulo 1 será feita uma abordagem teórica acerca dos temas relevantes para a compreensão dos conflitos estudados, aqui espera-se esboçar os principais conceitos que guiam a discussão. No capítulo 2 será delineado o objeto de estudo. No capítulo 3 será detalhada a metodologia do trabalho, um modelo teórico será esboçado para guiar a discussão acerca das diferenças e semelhanças entre os casos. No capítulo 4 serão estudados os casos selecionados. Por fim no capítulo 5 serão discutidas as implicações dos conflitos de maneira comparada.

O papel da Internet

O que se espera da Internet em um país democrático, e em um país não democrático? Seria a resposta tão diferente a ponto de sermos obrigados a dividir a pergunta? Ou ainda poderíamos simplesmente perguntar: o que se espera da Internet em um país?

A Internet é uma ferramenta tecnológica que o mundo atual se vê dependente, não muito diferente da dependência gerada pela energia elétrica. A velocidade em que essa dependência surgiu foi muito grande, o paradigma de comunicação do mundo foi alterado de maneira radical. Da mesma maneira que o medidor de energia elétrica permitiu que empresas cobrassem pelo consumo, e conseqüentemente que ela fosse vendida, a abertura da Internet para fins comerciais permitiu a ela ser vendida, e subseqüentemente se infiltrar em quase todos os ramos da atividade humana. Após o período de rápida expansão dos anos 90 a humanidade passou a ser dependente das possibilidades de comunicação providenciadas pela Internet.

A política convencional, entretanto, demorou a se adaptar à Internet. Ainda hoje muitos parlamentares não utilizam em grande escala a Internet para suas campanhas, o tempo de televisão é o alvo principal de barganhas e disputas políticas. Apenas recentemente no Brasil a utilização eleitoral da Internet foi regularizada.

A política não convencional, por outro lado, aprendeu rapidamente a utilizar e a se beneficiar da Internet. Grupos de oposição em não democracias entenderam logo no

início da década de 90 que as comunicações por redes de Internet eram mais livres e mais seguras, e por muitas vezes a única possível. É após isso que os governos não democráticos passam a se preocupar com a Internet, a possibilidade de seus crimes virem à tona e de seus cidadãos se rebelarem é um fardo muito pesado a ser carregado, por isso começam as intervenções, as prisões e a censura online. Porém, quando esses governos passam a entender a Internet, a maioria já no final da década de 90 e início dos anos 2000, o mundo já se vê dependente dela, incluindo suas próprias economias, o que gera um dilema: como censurar sem diminuir consideravelmente a capacidade econômica de seu país? Alguns países tiveram a resposta desde o início, como a Coreia do Norte, que sacrificou a economia do seu país para ter controle total sobre as informações. Outros, como a China, não prescindiram dos benefícios econômicos, mas encontraram maneiras de censurar o uso político da Internet. Ainda outros resolveram ignorar por um tempo a Internet, como o Irã, mas eventualmente perceberam que era inútil censurar os meios internos de comunicação sem uma censura online concomitante.

O que falar das pressões geradas pela disseminação rápida de informações sobre os detentores de poder? Tanto em países democráticos quanto não democráticos é natural que os que governam desejem continuar governando, em alguns casos a Internet pode ser um entrave à concretização desse desejo. Assim surgem os conflitos políticos causados pelo uso da Internet, de um lado a vontade dos cidadãos de terem uma vida melhor, de outro o desejo dos governantes colherem os benefícios do poder. Em uma não democracia a resolução deste conflito é direta, tenta-se censurar ao máximo possível a expressão política na Internet. Em uma democracia essa censura explícita não é tolerada, mas os grupos detentores de poder frequentemente procuram maneiras sutis de inibir as manifestações contrárias aos seus interesses. Justificativas econômicas, como a proteção de direitos de autor, ou justificativas de segurança, como o combate ao terrorismo, são frequentemente utilizadas nessas tentativas sutis de controle, elas podem ter iniciativa governamental ou não, mas dependem do apoio de parlamentares eleitos para serem implantadas. Nas não democracias as leis de censura são feitas sem “entraves democráticos”, e com justificativas fracas, como “proteção da cultura local” ou defesa dos “interesses supremos do Estado”.

1. TEORIA

As Tecnologias da Informação e Comunicação (TICs) modificaram a paisagem política, cada uma tendo efeitos diferentes de acordo com suas características peculiares. Os estudos de comunicação política, e mais recentemente, de governo eletrônico e democracia digital analisam os variados impactos das TICs. Nessa parte teórica pretende-se dar uma breve introdução acerca dos aspectos importantes dos trabalhos que são mais relevantes para o objeto de estudo aqui tratado.

1.1 O espaço virtual e a política

Os meios de comunicação anteriores à internet consistiam de transmissão de informação “um para muitos”, a internet altera isso, tornando a comunicação “muitos para muitos”⁹. Cada cidadão pode ter suas ideias espalhadas para outros cidadãos, em uma escala muito maior em relação aos meios anteriores de expressar as suas opiniões, além disso cada usuário da rede tem acesso a informações e conhecimentos que seriam impossíveis de serem conhecidos anteriormente¹⁰.

A mudança que essa capacidade causa é o que Bimber (1998, 2011) chama de “pluralismo acelerado”, que se define pela possibilidade de criação rápida de grupos para atuar em temas específicos. Com a internet uma questão pode ser levantada e, se atrair número suficiente de pessoas, pode ser levada ao debate público, assim que a questão é resolvida, ou abandonada, o grupo pode se dissolver, com a possibilidade de seus membros participarem de outros grupos por outras questões completamente distintas da questão anterior, inclusive em grupos antagônicos. A criação de grupos

⁹ A Galáxia Internet (CASTELLS, 2001).

¹⁰ “Very few if any developments in information technologies have had such a revolutionary effect as the creation of the Internet. Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as an interactive medium.(...) More generally, by enabling individuals to exchange information and ideas instantaneously and inexpensively across national borders, the Internet allows access to information and knowledge that was previously unattainable. This, in turn, contributes to the discovery of the truth and progress of society as a whole.” (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2011, Human Rights Council, parágrafo 19)

online tem baixo custo, por isso grupos podem surgir imediatamente assim que uma causa relevante é identificada.

A criação e a extinção de grupos do pluralismo acelerado não é um processo de soma zero. Os participantes dos grupos de pressão ganham conhecimentos e conhecem pessoas com interesses semelhantes, isso gera o chamado capital social. Esse capital se caracteriza por ser derivado de situações sociais, geradas através de redes sociais. A existência de capital social faz com que uma sociedade se organize mais facilmente para defender seus interesses. A Internet tem o potencial de gerar esse capital pela diminuição de custos de participação e de criação de grupos organizados.¹¹

A manifestação da criação de grupos online pode ser encontrada em diversos tipos de movimentos sociais. Por exemplo, protestos de rua, abaixo assinados, envio de emails a parlamentares. Uma das formas de ação política que surgiram na Internet é o chamado cyber ativismo, esse tipo de ação política utiliza largamente as ferramentas da Internet, sejam as redes sociais, os blogs, podcasts, fóruns, entre outros. Em protestos mais tradicionais, o espaço virtual se mescla com o real, frequentemente os protestos incluem um elemento online concomitante, na forma de microblogs ou *streaming* em tempo real de vídeos dos eventos.

Essa primeira análise da união do espaço virtual com a política necessita de uma discussão mais aprofundada acerca da estrutura da representação na Sociedade em Rede, segundo a terminologia e estudo de Castells (2001,2011).

1.2 Internet e representação

Existem três modelos reconhecidos de representação: mandato imperativo, representação fiduciária e representação espelho. Cada uma delas possui acepções diferentes sobre o ideal da representação. O desnível entre a existência de aspectos dos três modelos em uma sociedade pode gerar a crise de representação¹². A Internet não resolve os problemas da representação, mas ela pode ser considerada uma resposta na medida em que altera as relações de poder que a regem.

¹¹ Estudos estatísticos demonstram essa relação, para tal ver Pénard e Poussing (2010) e para os efeitos gerais da Internet sobre o capital social ver Wellman et al (2001).

¹² Dicionário de Política, Norberto Bobbio, verbete Representação.

Uma das relações de poder alteradas pela Internet é a dos partidos, que podem obter ganhos ou perdas de acordo com a sociedade em que se encontram e de acordo com a definição de seu papel. Por um lado eles podem ter sua mensagem transmitida sem a necessidade dos canais tradicionais de mídia¹³. Por outro, os partidos podem ter sua influência reduzida na proporção em que o candidato depende cada vez menos dele para transmitir sua mensagem, a ideia de partido como mediador entre eleitores e candidatos enfraquece. A representação, nesse aspecto, pode ser cada vez mais direta, com menos intermediários entre a mensagem e o público. A perda ou ganho depende da estrutura em que o partido se encontra, e do uso que ele faz das ferramentas da Internet.

Existem discussões sobre o fim da representação com a emergência de uma democracia direto eletrônica. Browder (2006) argumenta, entretanto, que a prevalência de aspectos de democracia direta, por meio de referendos online, pode causar desbalanço entre os interesses apoiados, principalmente pelos interesses que possuem mais recursos para sua promoção. Penã-Lopez(2011) argumenta que por mais que existam as ferramentas digitais isso não gera modificação por si só nas estruturas de governo, e que apenas o fortalecimento das instituições democráticas tradicionais é capaz de gerar avanços democráticos e de inclusão de tecnologias nos governos democráticos. Por isso ele acredita que a despeito da importância dada às ferramentas digitais só podem existir avanços com as instituições presentes no poder real, no mundo real e com conexões já existentes com o poder. A representação, para esse autor, deverá ser modificada por dentro antes de ser modificada por fora pelas novas tecnologias.

1.3 A Internet como modificadora da estrutura de poder

Para Castells (2011) o poder da sociedade moderna reside nas redes de comunicação. Em seu livro *Communication Power* ele argumenta que na sociedade em rede os controladores da comunicação são os verdadeiros detentores do poder, pois podem escolher e filtrar as mensagens que ganham repercussão, alterando os rumos da política, economia e da sociedade. Entretanto, as redes sociais na Internet colocam novas posições na sociedade em rede, o que ele chama de *gate-keepers*, os que filtram e controlam a informação, se multiplicam, tornando a paisagem comunicativa mais

¹³ Gibson, Nixon e Ward (2003) *Political Parties and the Internet, net gain?*

complexa. A informação, nesse contexto, tem a possibilidade de atingir uma audiência muito rapidamente, a despeito da influência dos *gate-keepers* tradicionais, isso é parte do fenômeno que Castells descreve como reprogramação de rede. Nesse fenômeno as redes são reconstruídas ao redor de um assunto polêmico, Castells dá diversos exemplos disso em seu livro. Entretanto, existem críticas ao papel que Castells delega à Internet em geral¹⁴, essas críticas argumentam que a mídia tradicional ainda tem uma audiência muito grande, e que as demonstrações que ficam apenas na Internet têm dificuldades em se transformar em ações no mundo real.

A influência do poder das comunicações é clara ao se tratar de conflitos de Internet. Com a multiplicação de *gate-keepers* o controle político enfraquece, já que a rede pode se reprogramar em torno dos pontos tradicionais de filtragem. Por outro lado as ferramentas de rede novas também podem ser usadas para o controle, para uma rede de censura mais eficaz, é o que se vê em casos de protestos coordenados online que fracassaram por terem sido infiltrados, ou apenas monitorados, por agentes do governo¹⁵.

Castells também ignora o fenômeno chamado de *digital divide*¹⁶¹⁷, que é a incapacidade de certos grupos de utilizarem efetivamente a Internet, seja por diferença econômica, incapacidade técnica ou falta de habilidade no uso das ferramentas digitais. Para essas pessoas a mídia tradicional, com seus *gate-keepers* tradicionais, ainda pauta os temas discutidos. Por outro lado pode-se argumentar que a tecnologia está cada vez mais presente, e que mesmo em meios com menor penetração da Internet a sua influência ainda existe, por meio de transferências culturais e sociais entre os que são excluídos digitalmente e os que não são.

O poder político que advém do controle da informação dilui-se com a emergência da Internet. Certos regimes ainda tentam se agarrar às velhas formas de controle, com graus de sucesso variados, como a China e outros regimes ditatoriais. O poder das redes fornadas pelas novas tecnologias, segundo Castells (2011), reside na velocidade de reprogramação e na capacidade de se atingir um número grande de pessoas pelo modelo do *mass self-communication*, a comunicação de massa feita por

¹⁴ Hindman (2008). The myth of digital democracy. Princeton NJ: Princeton University Press

¹⁵ Como na Bielorrússia em 2011.

¹⁶ Geralmente traduzido como “exclusão digital”.

¹⁷ Segundo o Prof. Jan A. G. M. van Dijk em revisão do livro disponível em <http://www.utwente.nl/gw/mco/bestanden/CastellsCommunicationPowerReview.pdf>

uma pessoa ou grupo com potencial global de dispersão de informação. Tendo isso em mente a sociedade em rede demanda uma nova forma de articulação política, o controle dos fluxos de informação já não é suficiente para garantir a estabilidade de um poder consolidado. Para que essas formas antigas ainda prevaleçam é necessário um controle absoluto, que só pode ser feito bloqueando-se completamente o acesso à Internet, porém isso implica custos enormes, como não participar efetivamente do comércio global. Poucos países atuam dessa maneira, sendo a Coreia do Norte o exemplo mais concreto disso.

1.4 O discurso político

Símbolos de linguagem guiam a discussão política¹⁸. Esses símbolos se baseiam na linguagem política da democracia, derivada da democracia liberal e dos preceitos da declaração Universal dos Direitos do Homem e do Cidadão da revolução francesa. Entretanto, ao se tratar de novas tecnologias na política termos modernos são adicionados aos jargões consolidados: livre acesso, circunvenção¹⁹, ciber-ativismo, democracia digital. A estes se adicionam termos já antigos da ciência política, mas com conotações e interpretações modernas: acesso à informação, *accountability*, transparência. E também termos que resgatam diretamente à Declaração Universal dos direitos do homem e do cidadão, também com conotações novas: liberdade, igualdade, respeito.

Em alguns dos casos aqui estudados se mostra claro o discurso como justificativa em si mesmo. Assim se justificam as propostas de legislação e a censura estatal. Como argumental Dahl (2001) a imprensa livre e a discussão livre são essenciais para a democracia, já que dessa maneira é possível se expor as contradições do discurso. Em uma democracia plena existem diversas arenas de discussão, a mais importante delas sendo a legislativa, mas ela só pode ser completa com *inputs* fornecidos pela discussão pública livre. Com a discussão livre os legisladores podem conhecer as aspirações dos cidadãos, o que é naturalmente desejável para as

¹⁸Lasswell (1982), em introdução ao livro “A Linguagem da Política” define bem o papel da linguagem, do discurso e dos termos para a discussão política.

¹⁹ Tradução livre e resignificação da palavra em inglês *circumvention* que significa o ato de passar por um bloqueio *online*, como um *firewall*, com o objetivo de acessar conteúdos censurados. A palavra “circunvenção” existe em português, mas com outro significado.

democracias, e os cidadãos podem julgar os diferentes discursos e decidir se eles justificam ou não as propostas e os atos em questão.

Os termos do discurso têm implicações imediatas para a discussão política, por exemplo, o uso da palavra roubo (*theft*) para descrever violações de direito autorais ou direitos de cópia. As se copiar um conteúdo protegido por direitos autorais não está de fato se subtraindo algo, nem se utilizando de violência, são crimes de categorias e impactos muito diferentes. Porém, as indústrias de conteúdo chamam as violações de direito autoral de roubo, com o objetivo de enquadrá-las em uma mesma categoria analítica no imaginário dos cidadãos. Ao se transformar uma infração de baixo potencial ofensivo em um crime violento essas indústrias desejam angariar apoio para suas causas por meio do discurso. Em um ambiente de discussão livre isso pode ser questionado nas arenas de discussão, e a discussão na arena legislativa pode ser feita se levando em consideração as contradições dos discursos dos atores.

1.5 Democracia Eletrônica

Os estudos iniciais de democracia eletrônica tendiam a ver as ferramentas digitais apenas como replicadoras de instrumentos já existentes da democracia, como o voto. Entretanto, os estudos recentes já verificam a existência de fenômenos novos, comportamentos advindos exclusivamente das TICs.

Dahl sugere a utilização das TICs para se fomentar o surgimento de um “público atento”, para controlar as decisões das elites políticas²⁰. Pode-se argumentar que esse público atento surgiu naturalmente a partir das ferramentas da Internet, principalmente da Web 2.0, que permite a criação de conteúdo de maneira simplificada. Nesse sentido, o controle das elites proposto por Dahl leva a conflitos de interesses, que leva a

²⁰ “Dahl sugere que a nova tecnologia de comunicações podia ser útil para deslocar o processo político da poliarquia II para a poliarquia III. De modo pragmático, Dahl conclui que devíamos ‘abandonar a perfeição filosófica dos princípios substantivos do bem comum e procurar em lugar disso a perfeição prática dos processos para alcançá-lo’. Especificamente, ele mira a opinião pública, sugerindo que o uso criativo da nova tecnologia de comunicações poderia resultar em novas instituições construídas para assegurar o desenvolvimento e a existência continuada de um maior ‘público atento’. Este público poderia criar um controle sobre essas elites ‘influenciando as decisões governamentais, não só diretamente mas também indiretamente, através da sua influência sobre as opiniões das massas e da elite’. Em qualquer caso, uma nova tecnologia pode ser usada de várias maneiras danosas à democracia, “sem um esforço consciente” para usar nova tecnologia de comunicações ‘em nome da democracia’”(A democracia Eletrônica, Cadernos da Escola do Legislativo, Aikens, p. 83)

conflitos sobre a própria utilização da Internet e a tentativas de controle por parte dessas Elites.

Penã-Lopez (2011) argumenta que a despeito das novas tecnologias darem poder ao cidadão individual elas o retiram dos intermediários de governo, resultando em um aumento da distância entre os cidadãos e as grandes decisões políticas. Isso acontece porque os cidadãos podem atuar diretamente em problemas específicos e locais, passando ao largo das instituições que tratariam desses problemas, por isso essas instituições teriam seu escopo de atuação e influência diminuído e perderiam relevância. Entretanto, essas instituições seriam necessárias para a existência de atuação em instâncias maiores, supranacionais, onde o indivíduo não tem capacidade de atuar, dessa maneira diminuindo o intermediário. As ferramentas de democracia digital seriam então causadoras de um paradoxo, ao dar maior poder ao indivíduo elas reduziriam o intermediário, dando mais poderes às instâncias mais altas, inalcançáveis aos cidadãos isoladamente.

1.6 Digital Divide

O fenômeno da exclusão digital é sempre presente nos estudos de democracia digital. O trabalho mais importante acerca do tema, e o que atraiu atenção para o assunto, é o livro *Digital Divide* de Pippa Norris (2001). Nesse trabalho a autora chama atenção para a diferença da penetração da Internet entre os países desenvolvidos e os subdesenvolvidos (*global divide*), além disso outros fenômenos de exclusão são importantes, como a diferença de acesso entre as classes sociais (*social divide*) e a diferença de utilização para fins democráticos ou não (*democratic divide*). Estudos mais recentes (Mossberger et al (2003)) também apontam para a exclusão técnica, ou a incapacidade de utilizar as ferramentas de Internet e de democracia digital.

O controle sobre o uso da Internet pode se traduzir em uma ampliação dos abismos digitais apontados pelos autores. A estrutura da censura dos países ditatoriais como a China torna crime a utilização da Internet para fins políticos. De maneira semelhante, nos países democráticos o bloqueio de conteúdos, uma vez generalizado, pode-se tornar ferramenta para bloqueio de opiniões políticas. Dessa maneira

estabelecendo uma dimensão global para o *Democratic Divide* definido por Norris (2001).

1.7 Privacidade e monitoramento

Um dos pontos chave de conflito acerca da Internet é a questão da privacidade. A discussão da privacidade é repleta de clichês que são difíceis de serem abolidos, até mesmo no âmbito acadêmico. Como argumenta Solove (2008), a questão da privacidade é difícil de ser colocada em termos concretos. O dano causado pela falta de privacidade advém do desbalanço de poder, e não de um dano físico ou psicológico. Em seu artigo o autor demonstra diversos casos de violações de privacidade que foram desconsiderados pelas cortes de justiça dos EUA por não resultarem em dano de fato. Além disso, o autor analisa as concepções mais comuns acerca da privacidade, como o argumento de que não há problema em monitoramento quando não se tem nada a se esconder. Esse argumento parte do pressuposto errôneo de que a privacidade serve apenas para esconder coisas erradas.

O desbalanço de poder é um fator importante ao se estudar os conflitos advindos da utilização da Internet. As legislações e propostas de legislação que visam controlar a Internet nos EUA e na França colocam provisões que falham em fornecer alternativas legais factíveis contra abusos. A legislação francesa Hadopi requer um pagamento para apelar contra as notificações, o que envolve também um processo burocrático e sem prestação de contas prevista na legislação. As propostas SOPA e PIPA dos EUA previam a remoção de sites antes que fosse possível apelar contra a decisão, tendo assim o potencial de alterar as relações de poder sem punições para potenciais abusos que fossem cometidos.

A privacidade reflete esse desbalanço de poder. Como argumenta Solove (2008) a utilização de dados coletados sobre indivíduos para propósitos diferentes dos quais eles foram coletados inicialmente demonstra a incapacidade desses indivíduos de controlarem a utilização das informações acerca deles, mesmo que dessa utilização não seja possível estabelecer um dano direto. O reconhecimento da existência desses meios de coleta de informações leva aos *chilling effects*, que são prejudiciais para a liberdade de expressão por terem o potencial de reduzir a discussão e a transmissão de ideias

livremente sobre determinados assuntos. Esses efeitos são difíceis de mensurar, pois apontam para um problema estrutural na sociedade, que é o do monitoramento aliado à impossibilidade de controle por parte dos indivíduos sobre o processo.

A questão da privacidade é fundamental para se entender os conflitos aqui estudados. Os conflitos acerca da internet apontam para um desejo de monitoramento por parte dos governos, e uma conceituação fraca de privacidade por parte de setores da sociedade que aceitam esse monitoramento.

2. OBJETO DE ESTUDO

Conflitos surgem naturalmente nas sociedades²¹, é papel da ciência política estudar os conflitos de natureza política. Segundo o Dicionário de Política (Bobbio et al) “(...)Conflito é uma forma de interação entre indivíduos, grupos, organizações e coletividades que implica choques para o acesso e distribuição de recursos escassos.” (Gianfranco Pasquino, Dicionário de política, p. 227). Essa primeira definição estabelece um conjunto de análise que pauta o estudo dos conflitos, em primeiro lugar deve-se identificar qual é o recurso escasso em questão. Em segundo lugar, quais são os grupos ou indivíduos que participam do conflito.

Os conflitos podem ser regidos por regras aceitas pelas partes, nesse caso diz-se que eles são institucionalizados, geralmente esse é o caso dos países democráticos. Nesse caso é mais fácil identificar os atores envolvidos e os recursos escassos em jogo. Os conflitos podem não ter um fim nas instituições, nem todos os grupos envolvidos podem se contentar com o resultado e partir para soluções não institucionais, nesse caso tem-se a desinstitucionalização do conflito, que pode o levar para outras esferas públicas ou privadas onde ele será debatido.

O objetivo deste trabalho é entender essas situações de conflito no âmbito da Internet. Especificamente as relacionadas ao controle governamental da rede, seja por meio de censura governamental explícita ou bloqueio a conteúdos disponibilizados na Internet por justificativas econômicas ou sociais.

2.1 Direitos autorais e estratégias de controle

Nos países onde os conflitos acerca da Internet são institucionalizados o controle geralmente é feito por mecanismos com justificativas econômicas ou de segurança. Essas duas justificativas são exemplificadas, nos EUA, pelo *Patriot Act* e pelas propostas de legislações de defesa de direitos autorais na Internet, como o SOPA/PIPA.

²¹ “(...) todas as sociedades produzem constantemente em si antagonismos que não nascem casualmente nem podem ser arbitrariamente eliminados”(Dahrendorf (1976), como citado em Dicionário de Política, Bobbio, p. 227)

De acordo com o Meyer (2012), essas tentativas de controle da rede veem no sentido de dar mais poder de governança da Internet, e não apenas de controlar a difusão de conteúdos ilegais:

“(...)copyright is used as leverage for more control in the Internet governance debate. Much of the democratic and societal use of the Internet (for example, free speech writing or community building) depends on its open, cooperative, flexible, and decentralized nature. However, these very same characteristics are contested for economic or political reasons such as fighting piracy, and there are increasing calls for more and tighter regulation of the Internet.” (Meyer, T. Graduated Response in France: the clash of copyright and the Internet. 2012, Journal of Information Policy 2, pag. 108)

Isso implica que para defender a propriedade intelectual se reduz o potencial democrático da rede. As estratégias de defesa dos direitos autorais na internet criam pontos de controle, em contradição com a natureza difusa da Internet²². Entretanto, a abertura e descentralização são essenciais para a proteção da liberdade de expressão na rede, para a manutenção da segurança de expressar ideias, e em se tratando de países não democráticos é muitas vezes a única maneira possível de liberdade de expressão segura.

2.2 Censura

Nos países não democráticos a censura geralmente se justifica por meio de apelos sociais. Na China a principal justificativa para a censura estatal é diminuir a influência cultural do ocidente e combater práticas sociais indesejadas, como pornografia, sites de apostas online e rumores²³. Em países islâmicos a justificativa é

²² “(...)Many enforcement efforts directly target the architecture of the Internet, creating centralized points of control in the flow of information over the network. An answer is increasingly sought in altering the rationales and functioning of the Internet, with consequences that reach far beyond the problem of online piracy. Indeed, although copyright enforcement may not directly impact a citizen’s ability to find a job, fill out an online tax form, or gather information on upcoming elections, it fits within a wider trend of controlling access to information. There is little room for reflection on the value of widespread access to information and privacy for democratic purposes within an approach that advocates strong property rights and tampering with the architecture of the Internet.” (Meyer, T. Graduated Response in France: the clash of copyright and the Internet. 2012, Journal of Information Policy 2)

²³ Essa é a justificativa oficial, mas diversos estudos apontam para o real motivo: “ The Communist Party of China (CPC) has led China since 1949, and as a one-party authoritarian state, control over the dissemination of information is considered essential for stability. Because the Internet offers multiple ways to connect, share knowledge and broadcast messages, it threatens this monopoly over the

religiosa, tanto para defender a religião quanto seus praticantes. Entretanto, as justificativas são de pouca relevância para este trabalho, o aspecto político delas é que importa. As consequências políticas da censura são visíveis e geram conflitos entre os grupos que apoiam o governo e os cidadãos que querem utilizar livremente a Internet. Esses conflitos serão estudados de maneira comparada para se caracterizar as semelhanças e as diferenças entre os países democráticos e os países não democráticos em se tratando de conflitos acerca da Internet.

dissemination of information. As a result, the government has a heavy hand in Internet functionality in China. Not only is it highly regulated, but it is also policed by an incredibly sophisticated censorship architecture that monitors citizens' online usage and ensures they only see only what is deemed acceptable." (China in the Information Era: Can it Maintain Controls Over the Market Sector, Appease the Globally Connected Social Networking Community and Still Attract Foreign Direct Investment?, By Samantha M. Novick and C. Roe Goddard, Ph.D. Thunderbird School of Global Management)

No *Freedom on The Net 2012 Report* da Freedom House também é especificado a estrutura de justificativa da censura chinesa: "The CCP's content-control strategy consists of three primary techniques: automated technical filtering, forced self-censorship by service providers, and proactive manipulation. These techniques mutually reinforce each other to create a highly manipulated information landscape and one notably isolated from international news flows. The purported goal is to limit the spread of pornography, gambling, rumors, and other harmful practices, but web content related to sensitive political or social topics is targeted at least as forcefully." (Freedom on The Net 2012, pag. 131, disponível em <http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report.pdf> acessado em 10 de janeiro de 2012)

3. METODOLOGIA

A metodologia seguida nesse trabalho é a de estudos de caso. Os casos aqui apresentados terão como foco conflitos advindos do uso da Internet entre governos e cidadãos. Serão estudados os motivos que levaram ao conflito e as respostas e possíveis soluções encontradas pelos afetados pelo conflito. Além disso, a análise será dividida em países democráticos e não democráticos, dessa maneira poderão ser comparados os tipos de conflitos existentes em cada um deles. Cada seção do capítulo seguinte do trabalho será dedicada a estudar um país com um conflito específico. Nos casos em que legislações ou propostas de legislações façam parte importante do estudo elas serão analisadas de acordo com suas repercussões, não apenas no âmbito legal, mas no âmbito político e social.

A seleção dos casos foi feita se considerando a sua repercussão e a disponibilidade de material para seu estudo. Outro fator levado em conta foi a possibilidade de comparação entre eles, não só do ponto de vista das atitudes dos governos que geraram o conflito, mas também da similaridade das soluções encontradas pelos cidadãos.

O método de estudo de caso foi escolhido por três motivos principais: a heterogeneidade dos casos, o reduzido número deles e a falta de dados coletados por outras instituições acerca deles. Estudando cada caso com profundidade pode-se ter a possibilidade de se identificar os mecanismos causais que governam o fenômeno em questão. No caso deste presente estudo pode-se verificar como cada embate se desenrolou, quais foram as soluções encontradas e qual foi o resultado final. Esses mecanismos podem então serem comparados entre os casos e os pontos discordantes podem ser utilizados para se identificar as diferenças nos resultados. Os casos mais emblemáticos a serem aqui comparados serão o caso francês e o americano, legislações restritivas que sofreram rejeição popular, mas que tiveram resultados diferentes, uma foi aprovada e a outra não. Os estudos dos casos permitem verificar o mecanismo que levou a rejeição do SOPA/PIPA e a aprovação final do Hadopi. A diferença entre os dois pode ser importante para se entender esse resultado.

A heterogeneidade dos casos também requer um estudo mais aprofundado. Os embates acerca da internet no Brasil ainda estão em um processo inicial, no momento de

elaboração desse trabalho as principais legislações em tramitação ainda não foram votadas. Entender como o processo ocorreu em outros países pode ser comparado a como o processo está de fato ocorrendo no Brasil. Dessa maneira pode se comparar os casos e se tirar conclusões de interesse para esse estudo.

Ao se tratar dos embates acerca da internet não se pode excluir os países não democráticos, já que são exemplos importantes de conflitos atuais. Aqui os casos são ainda mais heterogêneos e entender cada caso individual é importante para se encontrar pontos de possibilidade de comparação. Esses casos podem ser comparados com os dos países democráticos em um nível mais elevado, as macro estruturas que governam os conflitos dos países não democráticos podem ser comparadas às macro estruturas dos conflitos dos países democráticos. Por exemplo, o desejo de controle das informações disseminadas na internet, todos os conflitos estudados aqui podem ser comparados nessa dimensão, a motivação do desejo de controle é que muda. Um país não democrático, como no caso da China, quer se manter no poder controlando as informações que o seu povo tem acesso - menos informação se traduz em menos possibilidades de dissidência política²⁴. Entretanto, a mesma motivação de controle pode ser encontrada em um país democrático, mas em uma escala menor, um partido pode querer se manter no poder evitando que determinadas informações sejam disseminadas. Aqui nesse estudo vê-se que a motivação do controle da internet nos países democráticos é largamente econômica, indústrias de entretenimento desejam cobrar mais pelo acesso à sua produção e criminalizar quem o acessa de maneira gratuita na rede. Em todos esses casos existe o desejo de controle, de restrição de liberdade, e esse desejo, juntamente com os métodos empregados por cada regime, pode ser comparado.

²⁴ “China’s Internet regulations and legislation are guided by the principle of “guarded openness”- seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination and the use of the Internet by domestic or foreign groups to coordinate anti-regime activity.” (China’s golden shield: corporations and the development of Surveillance Technology in the People’s Republic of China, International Centre for Human Rights and Democratic Development, 2001, pag. 9)

3.1 Modelo teórico

Para se entender os casos trabalhados nos países onde predomina a democracia é necessário entender a motivação e os fatores por trás das escolhas de seus parlamentares. A análise começará a partir de certos pressupostos, que se desenvolverão em um modelo para se entender os casos estudados.

Partindo das premissas de Downs(1957) um parlamentar é racional e tentará maximizar apoio político. No modelo aqui exposto duas variáveis serão importantes para se estudar os casos, financiamento e expectativa do eleitorado. Financiamento são os recursos que o parlamentar necessita para angariar votos e apoio político em geral, eles provem de financiadores que, por suas posições privilegiadas, possuem informação quase completa sobre a atuação do parlamentar, esses recursos são tanto financeiros quanto políticos. A expectativa do eleitorado é a visão que os eleitores têm daquele parlamentar, porém o eleitorado não tem informação completa e depende de fontes de informação para decidir suas expectativas. Entretanto o financiamento serve também para modificar as expectativas do eleitorado, trabalhando sobre essa questão informacional. Inicialmente, apoio total de um parlamentar j (A_j) ($j:1...n$) é igual a financiamento total (F) mais expectativa total dos eleitores (E) mais outros fatores (ε):

$$A_j = F + E + \varepsilon$$

Onde.

A expectativa total dos eleitores é representada pelo somatório das expectativas individuais de cada eleitor (E_i):

$$E = \sum E_i$$

A expectativa individual acerca do parlamentar j é função da percepção que o eleitor i tem da sua atuação política (P_j) e da informação (I_j) que ele dispõe acerca da atuação daquele parlamentar:

$$E_j = f(P_j; I_j)$$

A informação depende também do financiamento do parlamentar, e de outros fatores, que tem seu peso tanto maior quanto maior for a exposição das questões relevantes por meios não derivados do financiamento:

$$I_j = F_j + \varepsilon$$

A percepção da atuação parlamentar (P_j) depende do parlamentar atuar de acordo com o que seu eleitor potencial espera dele. O financiamento de campanha serve, dentre outras coisas, para o parlamentar informar ao seu eleitor sobre sua atuação, e também para dar o enquadramento desejado a determinada informação. Entretanto, o financiamento vem de financiadores, que pode ser apenas o próprio partido, mas frequentemente também existem financiadores privados. Esses financiadores possuem uma agenda, que pode ser igual ou não a do eleitorado do candidato, ao aceitar financiamento um parlamentar se compromete minimamente a trabalhar em favor da agenda do financiador.

A quantidade de financiamento total (F) de um parlamentar depende do somatório das expectativas de seus financiadores (B_k): (expectativa por si só não gera financiamento, mas gera possibilidade de financiamento, neste modelo implica que quem tem expectativa também é quem tem possibilidade de financiar, já que quem não é um financiador em potencial não é importante para o modelo)

$$F = \sum B_k + \varepsilon$$

A expectativa dos financiadores depende da percepção da atuação do parlamentar, e, segundo os pressupostos, o financiador é plenamente informado acerca do parlamentar que ele apoia:

$$B_k = f(T_j)$$

O problema nos casos estudados existe quando o desejo político do financiador está no lado oposto ao desejo político dos eleitores. Se o parlamentar espera que a quantidade de apoio político ganho por apoiar o financiador seja maior do que a perda por não apoiar o eleitorado ele vota com o financiador (equação I), se as expectativas forem iguais ele decide como quiser (equação II), se forem menores ele vota com o eleitorado (equação III). A expectativa do eleitorado também depende do financiamento, entretanto o peso dela é tanto menor quanto for maior a importância

dada às questões pelo eleitorado, isto é, em uma questão que outros fatores sejam mais importantes para a informação o peso da variável percepção da atuação parlamentar (P_j) vai ser muito maior do que a capacidade do financiamento de influenciar a informação, e os outros fatores (ε) terão peso maior sobre a questão informacional. Questões que colocam financiadores e eleitores em lados opostos tendem a ser desse tipo.

- I. $A(B_k) > A(E_i)$
- II. $A(B_k) = A(E_i)$
- III. $A(B_k) < A(E_i)$

A agenda dos financiadores é conhecida, entretanto a perda de apoio por não adotá-la pode ser variável, isto é, financiadores têm limites diferentes para retirar o financiamento caso o parlamentar não implemente sua agenda. A posição do eleitorado pode ser de difícil conhecimento, a incerteza tem seu papel na decisão do parlamentar. A apreensão do eleitorado tem níveis muito diferentes ao longo do tempo e das questões, uma questão polêmica pode não ter muito impacto, pois a apreensão acerca dela é baixa. É importante também notar a assimetria entre financiadores e eleitores, os primeiros possuem informação sobre os parlamentares enquanto os segundos dependem de outros para obter informações, inclusive dos financiadores que fornecem recursos para as campanhas eleitorais. Para os estudos de caso aqui citados é suficiente entender a relação entre financiamento, atuação parlamentar e apoio político. O caso da França e dos EUA demonstram, respectivamente, as situações descritas pelas equações I e III, e o caso brasileiro pode também ser analisado por essas equações.

Os países não democráticos podem ser comparados utilizando esse modelo, entretanto, as estruturas de incentivos são diferentes, e as informações acerca das motivações parlamentares são de difícil acesso. Uma decisão de um parlamentar racional envolve um cálculo, que em uma não democracia envolve fatores diferentes das democracias, como, por exemplo, a perseguição estatal e o medo de ir contra um desejo político do poder central a despeito da impopularidade dela entre os cidadãos. O modelo aqui exposto utiliza informações acerca das expectativas dos eleitores e informações de transparência dos financiamentos. Em uma não democracia essas informações não existem ou são muito pouco confiáveis.

O modelo teórico será aplicado nos estudos de caso dos Estados Unidos e da França, onde as informações referentes às variáveis do modelo são mais evidentes. Além disso, os casos são emblemáticos, pois demonstram conflitos semelhantes em que os resultados foram diferentes, pretende-se explicar essa diferença com a aplicação do modelo teórico esboçado. No caso brasileiro será estudado o processo, já que ele ainda não demonstra um resultado final. De fato nenhum dos países em questão tem um resultado final em relação aos conflitos de Internet, entretanto, ao se isolar casos específicos, as legislações em questão neste estudo, pretende-se demonstrar que a análise é possível e que os resultados obtidos podem demonstrar a validade do modelo para sua utilização futura.

Os conflitos dos países democráticos têm a característica de serem primariamente institucionalizados, ao contrário dos países não democráticos. Nesses países o jogo político possui menos regras aceitas por ambas as partes do conflito, e as estruturas de incentivo das democracias, como a reeleição e a *accountability* em geral, tem pouca ou nenhuma relevância para a manutenção do poder. O estudo desses países tem como objetivo a comparação com os países democráticos, para que a partir das diferenças possa-se entender o potencial dos conflitos relacionados à Internet. Os extremos a que chegam os países ditatoriais demonstram como os conflitos pelos recursos de poder são fundamentais para as sociedades, a democracia institucionaliza os conflitos, que poderiam chegar a esses extremos sem as instituições aceitas pelos atores envolvidos.

4. ESTUDOS DE CASO

Segue-se agora ao estudo dos casos selecionados. Pretende-se entender cada situação de conflito de maneira comparada, a fim de se obter um conhecimento sobre o surgimento, o desenvolvimento e a conclusão, caso exista, de cada caso. Os EUA, a França e o Brasil terão como foco de análise algumas de suas legislações e propostas de legislação acerca da regulação da Internet. O Irã e a China terão uma abordagem mais voltada para a compreensão das suas estruturas de censura, as legislações dos países não democráticos não são de grande importância, pois elas não são discutidas em um ambiente institucionalizado e democrático, elas são aprovadas independentemente dos desejos e das pressões da sociedade.

4.1 Estados Unidos

Duas legislações foram foco de conflitos recentes nos Estados Unidos, SOPA (Stop online piracy act) e PIPA (PROTECT IP Act). Elas foram colocadas em espera (*hold*) pelo congresso, devido aos protestos e reações de setores extensos da sociedade.

As legislações SOPA e PIPA tiveram amplo apoio das indústrias de conteúdo, que argumentam que a pirataria reduz suas vendas²⁵. Apesar de ter um foco comercial as legislações teriam gerado um clima maior de insegurança entre os usuários da internet, já que previam punições extensas aos infratores e alterariam a arquitetura da rede ao permitir explicitamente a censura de sites.

4.1.1 SOPA (Stop Online Piracy Act) e PIPA (Protect IP Act)

A proposta de legislação SOPA (*Stop Online Piracy Act*) foi introduzida em 26 de outubro de 2011 pelo congressista Lamar S. Smith. A proposta PIPA (*Protect IP Act*) foi introduzida no Senado dos EUA pelo congressista Patrick Leahy em maio de 2011.

²⁵ Uma lista de congressistas que apoiaram as medidas e receberam financiamento das indústrias de conteúdo está disponível em <<http://www.opencongress.org/bill/112-s968/money>> e <<http://www.opencongress.org/bill/112-h3261/money>>, acesso em 7.mai.2013.

O foco dessas propostas era de combater a pirataria online (defesa dos direitos de cópia e propriedade intelectual) e a venda de produtos falsificados. Mais detalhadamente, tornar ilegal um site facilitar de qualquer modo a operação de sites criminosos, inclusive com a presença de links para esses sites. Também tornava ilegal empresas americanas fornecerem receita de anúncios para sites criminosos e tornava obrigatório para os provedores de acesso à internet bloquear sites considerados ilegais pelo judiciário. Outras provisões tornavam ilegal o *streaming* de conteúdos não licenciados. Algumas penas propostas chegavam a cinco anos de prisão e multa. A proposta visava combater sites estrangeiros que praticam esses atos, de certa maneira isolando a internet norte-americana.

Um das críticas é que as provisões eram muito abrangentes, incluindo qualquer tipo de facilitação como passível de receber medidas legais. Se aprovadas as propostas também iriam acabar com os servidores *proxy* e VPN(*Virtual private network*) dos EUA, redes essas que são muito utilizadas por pessoas em regimes opressivos para escapar à censura local da internet, muitas das empresas que operam as VPNs e servidores *proxy* estão baseadas nos Estados Unidos. Alguns projetos importantes de anonimização e encriptação de dados na rede são patrocinados ou foram patrocinados pelo governo, como o projeto TOR(*The Onion Router*) e o projeto que garante servidores *proxy* para iranianos acessarem a Internet sem restrições. Esses projetos também poderiam ser considerados ilegais segundo a proposta.

A proposta SOPA estabelece claramente que sites estrangeiros considerados infratores devem ser bloqueados nos Estados Unidos, de acordo com o seguinte parágrafo:

“IN GENERAL.-A service provider shall take technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site (or portion thereof) from resolving to that domain name’s Internet Protocol address.(...)” (Stop Online Piracy Act Bill H. R. 3261, pag. 14)

Segundo esse parágrafo os sites internacionais dados como infratores não devem ter seu *hostname* resolvido, ou seja, o endereço digitado na barra do navegador não apontaria para o site desejado. Segundo um parágrafo posterior os buscadores, como o Google, também devem remover o site de seus resultados de busca:

“INTERNET SEARCH ENGINES.-A provider of an Internet search engine shall take technically feasible and reasonable measures(...) designed to prevent the foreign infringing site that is subject to the order, or a portion of such site specified in the order, from being served as a direct hypertext link.” (Stop Online Piracy Act Bill H. R. 3261, pp, 15 e 16)

Em relação aos servidores de VPNs e servidores *proxy* a proposta os tornaria ilegais, sob o argumento que eles facilitariam os bloqueios previstos. De acordo com a seguinte subseção:

*“(4) ENFORCEMENT OF ORDERS.-
(A) IN GENERAL.-To ensure compliance with orders issued pursuant to this section, the Attorney General may bring an action for injunctive relief-
(...)
(ii) against any entity that knowingly and willfully provides or offers to provide a product or service **designed or marketed for the circumvention or bypassing of measures described in paragraph (2) (...)**” (Stop Online Piracy Act Bill H. R. 3261, pag. 19, grifo do autor)*

Mais especificamente a proposta define as capacidades de tal serviço:

*“(D) DEFINITION.-(...) a product or service that is designed or marketed to enable a domain name described in such an order-
(i) to resolve to that domain name’s Internet protocol address notwithstanding the measures taken by a service provider under paragraph (2) to prevent such resolution; or
(ii) to resolve to a different domain name or Internet Protocol address that the provider of the product or service knows, reasonably should know, or reasonably believes that is used by an Internet site offering substantially similar infringing activities as those with which the infringing foreign site, or portion thereof, subject to a court order under this section was associated.” (Stop Online Piracy Act Bill H. R. 3261, pp. 20 e 21)*

Esse parágrafo torna ilegal os serviços de *proxy servers* e VPNs, que servem para passar por bloqueios de sites. Esses serviços que estariam baseados nos Estados

Unidos teriam sido tornados ilegais, e seriam fechados ou teriam que mudar de país para continuar suas operações²⁶.

A proposta também prevê que os provedores podem tomar ações voluntárias contra sites infratores, sem necessidade de ordem judicial, caso ele acredite que o site esteja tomando parte em algumas das ações consideradas ilegais pela proposta. De acordo com a seguinte seção:

“SEC.104. IMMUNITY FOR TAKING VOLUNTARY ACTION AGAINST SITES DEDICATED TO THEFT OF U.S. PROPERTY.

*No cause of action shall lie in any Federal or State court or administrative agency against, no person may rely in any claim or cause of action against, and no liability for damages to any person shall be granted against, a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for taking any action described in section 102(c)(2), section 103(d)(2), or section 103(b) with respect to an Internet site, or otherwise **voluntarily blocking access to or ending financial affiliation with an Internet site**, in the reasonable belief that—*

(1) the Internet site is a foreign infringing site or is an Internet site dedicated to theft of U.S. property; and

(2) the action is consistent with the entity’s terms of service or other contractual rights.”

(Stop Online Piracy Act Bill, pag. 48, grifo do autor)

Nos parágrafos expostos acima se encontra boa parte dos motivos das controvérsias em relação ao SOPA. Os pontos de debate levantados pelas discussões acerca do tema apontam que a proposta daria muito poder para as indústrias de conteúdo, já que muitas vezes também possuem provedores de acesso que poderiam tomar as medidas voluntárias sem ordem judicial contra conteúdos.

A utilização do termo “roubo de propriedade dos EUA” (*theft of U. S. property*) indica a moldura que o legislador deseja aplicar aos conceitos em questão. A cópia de conteúdos não pode ser caracterizada de maneira igual ao roubo, pois não há subtração de um bem, entretanto se deseja utilizar a linguagem política (como definido por Laswell, 1982) como justificativa em si mesma da possibilidade de remoção de conteúdo.

²⁶ O governo dos EUA mantém serviços desse tipo para garantir utilização de Internet para usuários em países onde o acesso é restrito, como o Irã. Para mais informações ver: http://www.theregister.co.uk/2003/08/29/us_sponsors_anonymiser_if_you/ consultado em 12 de janeiro de 2013.

Após as primeiras críticas a proposta sofreu uma primeira emenda, na qual ela se direcionava apenas aos sites não baseados nos Estados Unidos e continha provisões menos ambíguas em relação à censura de sites. Entretanto, essa emenda também foi criticada, pois ainda mantinha muitas das provisões iniciais.

A proposta PIPA foi baseada em uma proposta anterior, COICA (*Combating Online Infringement and Counterfeits Act*), que falhou em ser aprovada em 2010. O PIPA foi introduzido no Senado em 12 de maio de 2011. Essa proposta era similar ao SOPA, por isso os protestos foram unificados, contra ambas as propostas.

4.1.2 Reações ao SOPA/PIPA

Após cobertura da mídia e reações por parte de participantes de redes sociais grandes empresas de internet passaram a se colocar publicamente contra a proposta. No dia 18 de janeiro de 2012 a Wikipédia tirou seu site do ar e colocou uma mensagem em seu lugar criticando a proposta:

“Imagine a world without free knowledge. For over a decade, we have spent millions of hours building the largest encyclopedia in human history. Right now, the U.S. Congress is considering legislation that could fatally damage the free and open Internet. For 24 hours, to raise awareness, we are blacking out Wikipedia.” (Disponível em <http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA> acesso em 20.fev.2013)



FIGURA 1 - Banner no site wikipedia.org, disponível em <http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA>

Outros sites participaram nesse mesmo dia do *blackout* contra o SOPA/PIPA, retirando seus conteúdos do ar e colocando mensagens contra a proposta. Alguns sites também colocaram mensagens, mas sem retirar seus conteúdos do ar, como o Facebook, Twitter e o Google.

O co-fundador da Google, Sergey Brin, publicou uma carta aberta ao congresso americano, na qual criticava a proposta SOPA e a proposta PIPA (Protect IP Act). Nela ele comparava a proposta dos EUA à censura praticada no Irã, na China, e na Malásia, países onde a censura à internet é muito criticada e tolhe as liberdades individuais. Na carta ele enumera os principais problemas da proposta:

*“*Require web services, like the ones we helped found, to monitor what users link to, or upload. This would have a chilling effect on innovation
 * Deny website owners the right to due process of law;
 * Give the U.S. Government the power to censor the web using techniques similar to those used by China, Malaysia and Iran;
 and
 * Undermine security online by changing the basic structure of the Internet.” (An Open letter to Washington, Sergey Brin)*

Os protestos atingiram proporções grandes após a atenção pública gerada por grandes sites colocarem mensagens em suas páginas. Estima-se que 115000 sites participaram dos protestos e que mais de 3 milhões de cidadãos norte-americanos mandaram emails aos congressistas dos EUA²⁷.

Uma crítica importante à proposta é a de que ela foi feita sem consulta a especialistas ou a entidades que defendessem os direitos dos usuários. A maneira da qual ela estava redigida, e os tipos de bloqueios que ela previa, quebrariam a arquitetura da rede, e ultimamente a modificariam de maneira a diminuir a sua segurança²⁸. A seguinte citação demonstra como o processo de elaboração da proposta careceu de sugestões dos próprios usuários da Internet e de especialistas:

“At the House Judiciary Committee hearing on SOPA, no technical expert testified (...) Representatives of Pfizer, the pharmaceutical company, and the Motion Picture Association of America (MPAA) testified on behalf of intellectual property

²⁷ Segundo o NY times.

²⁸ Como visto na carta aberta de engenheiros contra as propostas SOPA/PIPA em <https://www.eff.org/sites/default/files/Internet-Engineers-Letter.pdf>

owners. Representatives of Google and Mastercard testified on behalf of the online intermediaries whose business practices the bills sought to regulate. A representative of the AFL-CIO testified on behalf of the copyright industries' rank-and-file union members. (Remember that the bills were put forward as job-saving.) Nobody, however, testified on behalf of Internet engineers or Internet users.”(Bridy, A. Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA. 2012, pag. 11)

Na elaboração da proposta vê-se que os interesses dos produtores de conteúdo estavam sendo priorizados em relação aos usuários. Antes das demonstrações públicas de rejeição às propostas a tramitação da proposta se assemelhava ao descrito pela equação I do modelo, o interesse dos financiadores prevaleceria. Entretanto, as demonstrações contrárias resultaram na percepção dos parlamentares que a perda de apoio político seria menor ao se apoiar os eleitores, resultando na situação descrita pela equação III.

Entretanto, a despeito das críticas ao conteúdo e a elaboração da proposta, o processo pode ser considerado como legítimo e democrático. A comoção pública gerou efeitos legislativos, o apoio à proposta caiu após algumas semanas de protesto e até mesmo a Casa Branca se colocou contra ela. Existiu um diálogo entre os legisladores e os cidadãos. Em outros processos, como o ACTA (*Anti-Counterfeiting Trade Agreement*) a discussão foi feita a portas fechadas, e sem possibilidade de diálogo, esse tipo de procedimento vai contra a argumentação da legitimidade procedimental de Habermas²⁹, onde o diálogo entre os legisladores e os cidadãos é fundamental para a legitimidade.

4.1.3 Efeitos políticos e sociais

A partir das evidências do estudo desse caso pode-se verificar que existe espaço para a participação popular no Congresso Americano, as influências para a elaboração das propostas de legislação foram suplantadas pelos protestos. Os protestos online tiveram duas facetas importantes, os coordenados pelas empresas de internet e os

²⁹ HABERMAS, Between facts and norms: contributions to a discourse theory of law and democracy. Como citado em BRIDY, A. Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA. 2012.

coordenados pelas pessoas utilizando as redes sociais. As mensagens passadas por sites como o Google e a Wikipédia foram suficientes para aumentar a apreensão do público quanto ao assunto, mas as assinaturas desse público por meio de diversas petições online mostraram aos congressistas o suporte de base que o movimento tinha. Ao ver essa pressão o congresso cedeu, as propostas nem chegaram a ser votadas, elas foram colocadas em espera (*hold*), e qualquer outra proposta no mesmo sentido teria que ser completamente reescrita para ter alguma tramitação no congresso. O medo dos congressistas das possíveis represálias nas urnas fez com que o apoio às propostas acabasse, dando um exemplo prático para os estudos de *accountability*.

O apoio social necessário para a resolução desse conflito gera capital social, propostas futuras podem ser comparadas ao SOPA/PIPA para que suporte contra elas seja angariado entre o público. Os laços criados pelas comunidades em torno do tema podem ser considerados como fracos, segundo os argumentos de Bimber(1998), entretanto, uma vez o tema já sendo de conhecimento público, novas comunidades podem surgir para se organizar para a resolução de outros conflitos. É a ideia de poliarquia aplicada à Internet, grupos *ad hoc* surgem de acordo com temas relevantes, os participantes desse grupo só se unem em relação a determinada causa e após ela ser resolvida o grupo se desfaz, deixando como legado o aprendizado acerca do tema e a possibilidade de reunião futura caso a questão seja levantada novamente.

Por outro lado os congressistas defensores de tais propostas podem tentar de diversas maneiras a sua aprovação, já que é mais fácil propor nova legislação do que se unir contra a legislação proposta. O apoio popular custa, em termos organizacionais e de exposição midiática. Os lobbies das indústrias de conteúdo fornecem apoio monetário às campanhas³⁰ de alguns congressistas, e isso é um peso importante nas decisões dos congressistas e das propostas que eles apresentam e apoiam.

Essa situação de conflito legislativa foi resolvida pelos cidadãos com pressão popular coordenada por grandes empresas interessadas em barrar a legislação, como o Google. O questionamento que pode ser feito é se no momento em que uma legislação desejável para essas empresas e ao mesmo tempo indesejável para os cidadãos for proposta ela terá uma comoção pública tão grande quando teve o SOPA/PIPA.

³⁰ Segundo dados pesquisados pelo opensecrets.org, disponível em <http://maplight.org/us-congress/interest/C2400> (acessado em 15/10/2012)

O caso francês, a ser estudado na seção seguinte, não teve o mesmo resultado. A capacidade de organização do público não foi o suficiente para bloquear a legislação. A percepção dos parlamentares franceses se aproximou da situação descrita pela equação I do modelo.

4.1.4 Outras considerações

Segundo o modelo esboçado da metodologia desse trabalho a explicação para o fracasso dessas legislações residiu no balanço da oposição dos interesses. Os interesses que apoiaram o SOPA/PIPA estavam em desacordo com uma parcela significativa do eleitorado. Esse desacordo surgiu com uma campanha maciça de informação aliada à demonstração popular. Essa campanha foi patrocinada por atores importantes, empresas e entidades que utilizaram de seu capital, tanto econômico quanto social, para atrair a atenção do público.

O resultado desse conflito é importante para o restante do mundo, legislações posteriores e semelhantes a essa em outros países, como no Brasil³¹, tiveram uma discussão pública melhor informada.

Por outro lado, os interesses motivadores da proposta encontraram outras maneiras de impor sua agenda. Por meio de acordos internacionais, secretos e discutidos a portas fechadas, provisões semelhantes ao SOPA/PIPA podem ser impostas, com nenhuma discussão pública³². As próprias operadoras de internet nos EUA também estão tomando medidas para defender os interesses das grandes produtoras de conteúdo, no novo esquema conhecido como *six strikes*³³, semelhante à legislação francesa, mas feita de maneira unilateral pelos provedores de acesso e sem discussão na esfera pública.

³¹ Ver seção 4.3.3 deste trabalho.

³² O *Anti Counterfeiting Trade Agreement* (ACTA), um possível acordo internacional que trata de temas semelhantes ao SOPA/PIPA, foi levado a conhecimento do público apenas por vazamentos de informação, *leaks*.

³³ <http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/>

4.2 França

A França possui um histórico de acesso de redes antes mesmo da utilização da Internet e da criação dos protocolos de rede modernos. Em 1982 na França foi introduzido comercialmente o sistema Minitel, que consistia em uma rede de computadores nacional que distribuía informações e possibilitava interação entre seus usuários. Foi um precursor da rede global de computadores e permitiu um nível alto de interação entre os cidadãos franceses muito antes do surgimento da internet global. Esse sistema perdurou até 2012, quando foi desativado.

Por outro lado, esse sistema atrasou a adoção da internet pelo público na França. Em 1997 foi atingido o pico de usuários desse sistema, com 9 milhões de pessoas conectadas. Entretanto, logo seguiu-se o declínio, a internet já fazia sucesso no mundo, e o sistema Minitel era restrito ao público francês e ultrapassado em termos de velocidade de acesso e de ferramentas disponíveis, principalmente pelo seu rígido controle pelo governo Francês, controle esse que diminuiu muito após a adoção em larga escala da internet em substituição ao Minitel³⁴.

Bruce Bimber(1998) caracterizou o sistema Minitel como criador de comunidades fracas, no sentido de vagamente conectadas entre si. No final dos anos 80 o sistema era largamente utilizado para propósitos recreacionais, apesar de existirem diversos fóruns de discussão e de uma grande quantidade de comércio eletrônico. Para Bimber esse sistema não era eficaz em criar laços fortes que pudessem se transformar em ação política, ao contrário de outros sistemas que ele analisa em seu trabalho. Ainda, a internet segundo ele deve ser entendida como uma ferramenta que fortalece o pluralismo, sem erodir a influência dos grupos já dominantes e nem criar comunidades fortes com capacidade de ação política. A política em redes fracas tenderia a se organizar através de questões específicas, sendo que a ação política só aconteceria em casos específicos e acerca de questões da agenda política. Para Bimber um novo meio

³⁴ “(...)Julien Mailland argues that a precedent of seeking to centrally control a communication network can be found in the French approach to the Minitel. France long resisted the development of the Internet, as it had introduced its own alternative communication network technology called the Minitel in the 1970s. The infrastructure supporting this videotex technology was centralized and restricted to France, and content on the Minitel network was strongly regulated by the French government.(...) Considering the national precedent set by the Minitel, the proactive approach of France to policymaking in general and the fact that the cultural industries in France are among the largest in Europe, it is not surprising that graduated response legislation was adopted in the country.” (Meyer, T. Graduated Response in France: the clash of copyright and the Internet. 2012, Journal of Information Policy 2)

de comunicação não altera a disposição de participar das pessoas, apenas altera a distribuição de informação.

4.2.1 Hadopi

A legislação Hadopi (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*) (*Loi Création et Internet*) é considerada umas das mais rígidas em relação à utilização da internet. Ela prevê punições após o terceiro aviso sobre infrações online, a chamada resposta gradativa (*riposte graduée*). A legislação cria uma instituição, o próprio Hadopi, que tem como objetivo administrar o seu cumprimento. Além de estabelecer a resposta gradativa a legislação também tem como objetivo incentivar a distribuição de conteúdo de maneira legal.

Essa legislação teve a tramitação em duas partes, a primeira parte foi promulgada em 12 de junho de 2009, a parte não promulgada foi considerada inconstitucional pela Corte Constitucional Francesa³⁵, já que previa a desconexão de usuários de internet sem o devido processo judicial³⁶. Para manter o aspecto punitivo da primeira lei foi introduzido a *Loi relative à la protection pénale de la propriété littéraire et artistique sur internet*, também conhecida como Hadopi 2, que colocava a punição por um processo acelerado, mas ainda passando por um juiz. Essa segunda parte foi aprovada em 15 de setembro de 2009. O Decreto nº2009-1773 estabelece a criação do Hadopi, a autoridade que regula a aplicação da lei. Segundo a legislação a Alta Autoridade (Hadopi) tem como objetivo:

“1° Une mission d’encouragement au développement de l’offre légale et d’observation de l’utilisation licite et illicite des oeuvres et des objets auxquels est attaché un droit d’auteur ou un droit voisin sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;

³⁵ Decisão 2009-580, disponível em: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf

³⁶ “In France, for example, after an initial administrative scheme, known as HADOPI, was held to be unconstitutional by the French Constitutional Council, a new system was introduced which requires a full criminal proceeding for disconnection for periods up to one year” (Suzor and Fitzgerald, The legitimacy of graduated response schemes in copyright law. Disponível em: <http://nic.suzor.net/wp-content/uploads/2011/08/Suzor-Fitzgerald-2011-Graduated-Responses-UNSW.pdf> acesso em 22/10/2012)

*« 2° Une mission de protection de ces oeuvres et objets à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;
 « 3° Une mission de régulation et de veille dans le domaine des mesures techniques de protection et d'identification des oeuvres et des objets protégés par un droit d'auteur ou par un droit voisin. » (Projet de Loi favorisant la diffusion et la protection de la création sur internet, adopté le 13 mai 2009, Art. L. 331-13, Senat)*

Por esses parágrafos vê-se que a legislação também tem como objetivo favorecer a difusão de conteúdos legais na internet, e que isso também seria papel da Hadopi.

A resposta gradual é definida no artigo L. 331-26. Na primeira ocorrência identificada o responsável pela conexão é notificado por email sobre o crime, na segunda ocorrência ele é notificado por carta registrada e na terceira ocorrência ele tem a sua internet cortada.

As punições previstas na proposta inicial do Senado foram criticadas pela Corte Constitucional Francesa, o seguinte parágrafo do relatório indica os argumentos principais:

“11. The parties contend that by giving an administrative authority, albeit independent, the power to impose penalties in the form of withholding access to the internet, Parliament firstly infringed the fundamental right of freedom of expression and communication, and secondly, introduced patently disproportionate penalties. They also argue that the conditions for imposing such penalties introduce a presumption of guilt which patently infringes the rights of the defence.” (Decision n° 2009-580 of June 10th 2009, parágrafo 11)

O argumento aqui explicitado é de que o corte do acesso à Internet viola o direito de expressão e comunicação, que as penalidades não são proporcionais ao delito e que elas ferem o princípio de presunção de inocência. Nos parágrafos seguintes o relatório detalha esses argumentos. No parágrafo 12³⁷ ele cita a declaração dos Direitos do Homem e do Cidadão para sustentar a tese de que o bloqueio ao acesso à internet

³⁷ “12. Article 11 of the Declaration of the Rights of Man and the Citizen of 1789 proclaims : "The free communication of ideas and opinions is one of the most precious rights of man. Every citizen may thus speak, write and publish freely, except when such freedom is misused in cases determined by Law". In the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services”(Decision n° 2009-580 of June 10th 2009, parágrafo 12)

viola o direito básico de expressão. No parágrafo 16³⁸ ele utiliza o mesmo princípio da Declaração para comparar a dicotomia entre a proteção dos direitos autorais e a liberdade de expressão, o primeiro não pode se sobrepor ao segundo. No parágrafo 18³⁹ ele detalha o princípio de presunção de inocência, como a prova de que o crime não foi cometido recai sobre o acusado isso seria contrário à disposição do artigo 9⁴⁰ na Declaração dos Direitos do Homem e do Cidadão. O Conselho também questiona o direito à privacidade dos cidadãos. Esses problemas foram sanados na lei chamada Hadopi 2, que coloca um procedimento diferente para as sanções, que passa por um juiz de direito.

4.2.2 Reações e críticas

As reações ao Hadopi vieram de diversos setores da sociedade francesa e da comunidade internacional. Entretanto, possivelmente pela natureza mais local da legislação, grandes corporações não se envolveram nos protestos como no caso do SOPA/PIPA. Blogs franceses, como o *quadrature du net*⁴¹, cobriram o processo legislativo e repassaram informações ao público, enquanto outros organizaram protestos de rua e coordenaram ações online⁴².

³⁸ “16. The powers to impose penalties created by the challenged provisions vest the Committee for the protection of copyright, which is not a court of law, with the power to restrict or deny access to the internet by access holders and those persons whom the latter allow to access the internet. The powers vested in this administrative authority are not limited to a specific category of persons but extend to the entire population. The powers of this Committee may thus lead to restricting the right of any person to exercise his right to express himself and communicate freely, in particular from his own home. In these conditions, in view of the freedom guaranteed by Article 11 of the Declaration of 1789, Parliament was not at liberty, irrespective of the guarantees accompanying the imposition of penalties, to vest an administrative authority with such powers for the purpose of protecting holders of copyright and related rights;” (Decision n° 2009-580 of June 10th 2009, parágrafo 16)

³⁹ “18. In the case in hand, under the provisions referred for review, the commission of an infringement of copyright at the address of the registered subscriber constitutes, according to the terms of the second paragraph of Article L 331-21 "the material ingredients of the breach of duty defined in Article L 336-3". Solely the party to the internet access contract may be the object of the penalties introduced by the provisions referred for review. In order to avoid the imposition of such penalties it is incumbent upon him, under Article L 331-38, to adduce evidence that the infringement of copyright or related rights was due to fraud perpetrated by a third party. Thus by reversing the burden of proof, Article L 331-38, introduces, contrary to the requirements deriving from Article 9 of the Declaration, a presumption of guilt on the part of the internet access holder such as to entail the imposition of penalties restricting or depriving him of his rights.” (Decision n° 2009-580 of June 10th 2009, parágrafo 18)

⁴⁰ “Artigo 9º- Todo o acusado se presume inocente até ser declarado culpado e, se se julgar indispensável prendê-lo, todo o rigor não necessário à guarda da sua pessoa, deverá ser severamente reprimido pela Lei.” (Declaração dos Direitos do Homem e do Cidadão de 1789)

⁴¹ <http://www.laquadrature.net>

⁴² La Bataille Hadopi, 2009.

Pesquisas feitas pela autoridade Hadopi mostraram que a legislação mudou o comportamento dos internautas franceses. Enquanto alguns passaram a não baixar mais conteúdos ilegalmente outros procuraram alternativas técnicas para burlar a lei, como a utilização de VPNs.

As críticas mais recorrentes nos protestos contra o Hadopi são acerca da implementação da lei e dos princípios que a regem. A seguir uma lista das principais críticas⁴³: a identificação apenas pelo endereço IP; a presunção de culpa; a personalidade da pena penal; o corte do acesso à internet; o aspecto pedagógico.

A identificação do autor do delito pelo endereço IP é um problema já que os endereços de IP não representam necessariamente uma pessoa. É prática comum as operadoras de internet reutilizarem os números de IP que elas tem disponíveis, então, para se identificar de onde foi feito um determinado download ilegal não basta o endereço IP, mas também o horário exato da conexão, isso obriga as operadoras a manterem registros de acesso. Esse registros contém a lista de todos os sites acessados pelo usuário, o que gera problemas de privacidade. Além disso, o endereço IP identifica apenas a conexão e não cada usuário individual que esteja partilhando da conexão. A lei Hadopi responsabiliza o assinante da internet por qualquer download que seja feito a partir de sua conexão, não importando quem individualmente fez o download.

A presunção de culpa se refere ao fato de que no processo de apelação contra um possível corte dos serviços de internet o usuário é que tem que provar que não praticou o delito e não a autoridade acusadora que deve provar o crime. Isso foi questionado também pela Comissão Constitucional na primeira versão do Hadopi, mas permaneceu na segunda versão sob um aspecto diferente. A punição na versão final é análoga a um tipo de punição expressa da legislação francesa para crimes de trânsito.

A legislação prevê punições para não fornecer segurança suficiente para sua rede. Um crime cometido online por outra pessoa pode então gerar punições para o assinante da linha de acesso.

O corte de acesso à internet é um ponto polêmico. A punição, segundo as críticas, é exagerada em relação ao delito praticado. O acesso à internet foi considerado

⁴³ Como enumerado em Loi Création et Internet. (2012, octobre 19). Wikipédia, l'encyclopédie libre. Consultado em 31 de outubro de 2012 em http://fr.wikipedia.org/w/index.php?title=Loi_Cr%C3%A9ation_et_Internet&oldid=84319859.

como direito humano essencial segundo relatório da ONU⁴⁴. Nesse relatório a punição de desconexão da internet por violações de direitos autorais foi considerada desproporcional e violadora dos direitos humanos⁴⁵. Nesse sentido a desconexão proposta na legislação Hadopi é desproporcional e fere os direitos básicos de comunicação e acesso a informações públicas do cidadão.

Por fim o aspecto pedagógico da lei é criticado por ser incapaz de educar de fato. As mensagens enviadas são genéricas e não demonstram exatamente a infração que o usuário cometeu. Ainda, a legislação criminaliza comportamentos que são considerados normais por boa parte da população⁴⁶, então poderia ser questionado como se tratar de um aspecto pedagógico se não há uma discussão aprofundada acerca do tema, já que ele vai contra o senso comum.

4.2.3 Impactos e outras considerações

A legislação Hadopi da França teve um desfecho diferente da legislação SOPA/PIPA nos EUA. Enquanto nos EUA as legislações foram engavetadas, na França elas foram aprovadas a despeito dos protestos e das críticas. As reações contra o SOPA/PIPA foram muito mais globais, com atores políticos e econômicos importantes participando dos protestos contra ela. O impacto do SOPA/PIPA poderia ter sido grande no mundo, já que boa parte da infraestrutura da internet se localiza nos EUA, e sua legislação poderia ser copiada como exemplo por muitos outros países. A legislação francesa tem um impacto mais localizado na Europa, e pela sua estrutura não poderia alterar o funcionamento da rede global.

⁴⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Disponível em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

⁴⁵ “(...)The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, **including on the grounds of violating intellectual property rights law**, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights.” (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2011, Human Rights Council, parágrafo 78, grifo do autor)

⁴⁶ Segundo as estatísticas elaboradas pela autoridade Hadopi 49% dos usuários declara já ter baixado algum conteúdo ilegal da internet. Segundo os relatórios disponíveis em www.hadopi.fr

A despeito das críticas, as primeiras estatísticas demonstram que a pirataria diminuiu e a venda de músicas de maneira legal aumentou⁴⁷. A redução da pirataria tem duas faces, a primeira é o medo causado pela legislação e pelas punições, a segunda é a capacidade técnica de burlar a fiscalização, como a forma de monitoramento é conhecida é fácil utilizar alternativas técnicas para escapar a ela. Usuários de internet mais experientes que desejem continuar burlando a lei não encontram problemas nisso, utilizando VPNs e outras ferramentas de anonimização. Entretanto, ao demonstrar que a legislação está tendo o efeito esperado os apoiadores ganham um argumento forte para a manutenção dela. Por outro lado os custos operacionais do Hadopi estão muito acima do esperado, e cortes no seu orçamento estão sendo discutidos na França⁴⁸.

A organização *Reporters Without Borders* classifica a França como um país potencialmente inimigo da internet⁴⁹. Além da lei Hadopi a organização identifica outras formas de repressão na internet na França, como bloqueio de sites, intimidação a jornalistas e violações ao princípio da neutralidade⁵⁰. Essas outras manifestações de repressão demonstram que os conflitos na internet na França não se limitam ao aspecto legislativo. No âmbito político vê-se que as legislações propostas são reflexos de conflitos mais profundos, advindos do desejo de controle das autoridades aliada ao descaso pelas declarações da ONU que classificam a Internet como direito básico⁵¹.

Um dos problemas do tipo de medida adotado pela França é que ela tem um escopo limitado de monitoramento de atividades na Internet, nesse caso são monitorados os compartilhamento de arquivos por redes P2P (Ponto a ponto), mas não outras formas de compartilhamento. A solução para os usuários é utilizar outras formas, como *streaming* e downloads diretos, além disso eles podem utilizar *servidores proxy* e VPNs localizados em outros países para burlar o monitoramento. Isso foi chamado de

⁴⁷ The effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France (Danaher, B., Smith, M. D., Telang, R., Chen, S.)

⁴⁸ http://www.theregister.co.uk/2012/08/06/hadopi_under_fire/ acessado em 11/09/2012

⁴⁹ Internet Enemies Report 2012, France (Reporters Without Borders, 2012, disponível em http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf, acessado em 9/11/2012)

⁵⁰ “The government has taken the exact opposite course from the one laid out in recente court rulings and international recommendations that condemn filtering and cut off Internet access, and has done so in a contexto of increased pressure on journalists to reveal sources.” (Internet Enemies Report 2012, France, pag. 46, Reporters Without Borders, 2012)

⁵¹ “French Foreign Minister, Alain Juppé, has in fact refused to endorse the UN declaration recognizing Internet access as a fundamental right, conditioning his signature on the recognition of intellectual property as a right equivalent to freedom of expression.” (Internet Enemies Report 2012, France, pag. 49, Reporters Without Borders, 2012)

“corrida armamentista tecnológica”⁵², onde o governo tem ferramentas de monitoramento de um lado e os usuários têm ferramentas de circunvenção do outro. Entretanto, argumenta-se por outro lado que o usuário de Internet mediano não possui a capacidade técnica necessária para utilizar essas ferramentas, e que dessa maneira a lei pode ser considerada eficaz.

4.3 Brasil

O Brasil presenciou a discussão recente acerca do Marco Civil da Internet. Essa legislação pretende estabelecer um marco regulatório para a utilização da Internet. Ela foi feita com colaboração de usuários da internet e especialistas no assunto, que puderam dar suas opiniões acerca da legislação e discutir entre si utilizando as ferramentas propiciadas pelo governo no site <<http://edemocracia.camara.gov.br/web/marco-civil-da-internet>>. Também foram feitas diversas consultas públicas que debateram pontos específicos da legislação com especialistas e com o público em geral.

As novas TICs permitem a participação e a disseminação da informação política em tempo real. A discussão acerca do Marco Civil da Internet aponta no sentido de abrir as portas para a participação popular na elaboração das leis. Isso retira a prevalência dos “acordos secretos” e a discussão a portas fechadas das leis, e coloca a discussão nas mãos dos interessados nela. Pode-se argumentar que o poder final de fato ainda está nas mãos dos parlamentares, principalmente do relator que tem a prerrogativa de acatar ou não as sugestões, mas com a existência desse canal o foco do trabalho legislativo de base é trocado.

⁵² “Technological arms race. The French Government introduced HADOPI 1 and HADOPI 2 to control Internet piracy and deter users from downloading copyright material. However, the laws may already be outdated as Internet users use new technology to circumvent their requirements. For example, Internet pirates can mask their identity with relative ease by using an anonymous proxy or a VPN server that conceals the end user’s IP address, allowing copyrighted content to be downloaded without leaving a trace. New means and measures will have to be adopted to fight this type of Internet piracy. However, HADOPI 1 and 2 should still deter the average Internet subscribers, which is their main objective.” <<http://www.linklaters.com/Publications/Publication1403Newsletter/20091016/Pages/FranceTheHadopiLaw.aspx>> Acesso em 16 de Janeiro de 2013.

Habermas(1996) argumenta que a produção legislativa deve se pautar em um diálogo entre os produtores de legislação e os seus receptores, os cidadãos⁵³, não em uma abordagem fechada e interna, mas externa, voltada aos cidadãos. A discussão do Marco Civil pode se aproximar dessa ideia, entretanto, o seu resultado final é importante, já que ela ainda pode sofrer modificações que vão de encontro ao que foi dialogado em seu período de discussão.

Outra legislação que foi recentemente discutida é o PL 2793/11(também chamado Lei Dickmann, agora lei nº 12735 de 30 de novembro de 2012) que tipifica crimes digitais. Essa legislação foi criticada por setores da sociedade por ter uma tramitação considerada muito rápida (172 dias na câmara) e ir contra o que foi dito no início da discussão sobre o Marco Civil, onde se propunha a começar a regular a internet não pelos crimes, mas pelos direitos dos usuários.

Na discussão brasileira existem duas frentes, a criminalizatória e a regulatória. A primeira foi a abordagem constante desde o início da discussão acerca da internet no Brasil. A abordagem regulatória é a do Marco Civil, que visa estabelecer direitos e as diretrizes iniciais para a regulação futura da rede. Os conflitos brasileiros acontecem nas duas frentes. Inicialmente as legislações que visavam estabelecer os crimes eram muito abrangentes e sofreram duras críticas da sociedade, com o tempo elas foram ficando mais razoáveis, culminando com a aprovação atual do projeto de lei que tipifica os crimes digitais (PL 2793/11). Entretanto, o Marco Civil sofre pressões contrárias de outros segmentos, notadamente das empresas do setor de telecomunicações, que veem seus potenciais lucros serem diminuídos ao serem obrigadas a fornecer certos direitos aos usuários, como serviços de qualidade superior a atual e impossibilidade de certas cobranças pelo princípio da neutralidade da rede. Alguns setores também criticam a falta da discussão acerca dos direitos autorais, propondo que a legislação brasileira seja tão restritiva quanto a legislação francesa.

O ponto mais polêmico da lei é acerca da neutralidade. Na proposta inicial do Marco Civil a neutralidade não é modificável, a não ser por questões técnicas. Entretanto, as empresas de telecomunicação não concordam, pois isso impediria a cobrança por serviços específicos de internet, e impediria a priorização do próprio conteúdo em relação a outros.

⁵³ Como citado em Bridy, A. Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA. 2012.

4.3.1 Lei Azeredo e lei de crimes digitais

A proposta de lei brasileira que mais gerou polêmica foi a chamada lei Azeredo (PL 84/99). Inicialmente ela foi proposta pelo Deputado Luis Piauhyllino, em 2011 o Deputado Eduardo Azeredo foi designado relator. A primeira versão proposta pelo deputado Piauhyllino foi fruto de uma discussão iniciada pela apresentação em 1996 da primeira proposta de legislação sobre o tema, de autoria do Deputado Cassio Cunha Lima (PL 1713/96).

Após o relatório do Deputado Eduardo Azeredo o PL 84/99 possui 23 artigos, muitos deles polêmicos e que geraram protestos e manifestações online. O ponto mais discutido foi o da necessidade de registro de *logs* do provedor de acesso, por três anos, o que acarretaria custos altos aos provedores, segundo o seguinte artigo do PL 84/99:

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial; (Projeto de Lei 84/99 da Câmara dos Deputados, substitutivo do Senado, disponível em <<http://www6.senado.gov.br/mate-pdf/114841.pdf>> acesso em 15 de janeiro de 2014)

Outro ponto discutido foi o da amplitude, certos pontos da proposta poderiam se aplicar a muitas situações por não estarem bem definidos, como os seguintes artigos:

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço. (Projeto de Lei 84/99 da Câmara dos Deputados, substitutivo do Senado, disponível em <<http://www6.senado.gov.br/mate-pdf/114841.pdf>> acesso em 15 de janeiro de 2014)

Segundo argumentação dos críticos esses artigos citados poderiam ser utilizados para punir certos comportamentos como downloads e até mesmo desbloqueio de celular⁵⁴.

Após diversas críticas, inclusive do presidente Lula⁵⁵, o projeto foi sendo modificado e chegou a forma final aprovada, com apenas quatro artigos. Algumas das práticas tornadas crime pelo projeto de lei original e pelo substitutivo do Senado foram mais detalhadas e incorporadas no PL 2793/11, a lei de crimes digitais. O artigo que detalha o crime de violação de sistema informatizado detalha claramente que se trata sobre dispositivo alheio:

*“Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (...)”
(Pag. 1 seção 1. Diário oficial da União de 03/12/2012. Disponível em <<http://www.jusbrasil.com.br/diarios/43878749/dou-secao-1-03-12-2012-pg-1>> acesso em 15 de janeiro de 2013.)*

4.3.2 Marco Civil da Internet

A proposta de legislação brasileira conhecida como Marco Civil da Internet (PL 2126/11) foi inovadora no sentido de horizontalizar a discussão acerca de um projeto de lei. O PL foi apresentado pelo poder Executivo e relatado pelo Deputado Alessandro Molon. Através do site e-democracia os cidadãos puderam dar suas opiniões e ideias acerca da proposta, e discutir entre si e com especialistas por meio de fóruns.

⁵⁴ <<http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/200020-CRIMINALIZACAO-DE-PRATICAS-COTIDIANAS-E-GUARDA-DE-DADOS-RECEBEM-CRITICAS.html>> acessado em 15 de janeiro de 2013.

⁵⁵ <<http://www1.folha.uol.com.br/folha/informatica/ult124u587048.shtml>> acessado em 15 de janeiro de 2013.

FIGURA 2 - Página da discussão do marco Civil da Internet, disponível em <http://edemocracia.camara.gov.br/web/marco-civil-da-internet/inicio>

A proposta teve um substitutivo apresentado pelo relator, incorporando diversas sugestões dos participantes da discussão, de especialistas e de provedores de serviços de acesso a Internet. Entretanto, a votação na Câmara foi adiada seis vezes até dezembro de 2012. Isso se deve à polêmica causada por provedores de acesso que se colocam contra o artigo 9º, que garante a neutralidade da rede⁵⁶. Como expresso no seguinte artigo do projeto:

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo vedada qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação. (PROJETO DE LEI Nº 2126, DE 2011, Câmara dos Deputados)

⁵⁶<http://www1.folha.uol.com.br/opiniaio/1210926-tendenciasdebates-marco-civil---por-uma-internet-livre.shtml> acesso em 15 de Janeiro de 2013.

Associações culturais⁵⁷ também se colocam contra o projeto, por entenderem que a necessidade de mandado judicial para a remoção de conteúdos ilegais atrapalhe sua luta contra a pirataria. Segundo o substitutivo apresentado pelo relator ao artigo 15:

“Art. 15. Com o intuito de assegurar a liberdade de expressão e evitar a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. Parágrafo único. A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.” (PROJETO DE LEI Nº 2126, DE 2011, Câmara dos Deputados)

4.3.3 O ‘SOPA brasileiro’

No dia 6 de abril de 2012 o deputado Walter Feldman (PSDB/SP) apresentou no plenário da câmara uma proposta muito semelhante à proposta de legislação SOPA, ainda que simplificada. Nesse projeto de lei (PL 3336/2012) são conceitualizados termos semelhantes ao projeto dos EUA, inclusive com distinção entre sites domésticos e estrangeiros. Da mesma maneira que na proposta SOPA sites poderiam ser bloqueados, sem necessidade de intervenção judicial, apenas com a classificação do sistema de registro brasileiro do site como “infrator”.

“Art. 4º A Autoridade de Registro de Internet poderá, de ofício, com fundamento na notificação de que trata o artigo anterior, ou mediante determinação judicial, declarar um sítio de Internet doméstico ou estrangeiro como “Sítio de Internet Infrator”.

Art. 5º Os provedores de acesso à Internet e servidores de nome de domínio em operação no Brasil adotarão todas as medidas técnicas necessárias para:

I – bloquear o acesso dos usuários de seus serviços ao Sítio de Internet Infrator;

II – bloquear a resolução do Nome de Domínio em Endereço IP do Sítio de Internet Infrator;

III – suspender o funcionamento dos sítios de Internet domésticos que forem classificados como Sítio de Internet Infrator;” (PROJETO DE LEI Nº 3336, DE 2012, Câmara dos Deputados)

⁵⁷ <<http://g1.globo.com/tecnologia/noticia/2012/11/entidades-culturais-pedem-revisao-de-de-projeto-de-marco-civil-da-internet.html>> acesso em 15 de Janeiro de 2012.

Esse projeto previa o mesmo tipo de bloqueio de sites da proposta SOPA, por DNS (*domain name system*). Além do bloqueio os buscadores online teriam de bloquear os resultados que apontassem para o site infrator (art. 6º) e os sites de pagamentos deveriam bloquear os pagamentos direcionados ao site (art. 7º).

A repercussão do projeto foi muito ruim, o deputado retirou a proposta 14 dias após apresentá-la, dando como justificativa os argumentos contrários que recebeu⁵⁸. A repercussão do caso deve-se em grande parte à semelhança com a proposta SOPA dos EUA, dessa maneira foi fácil transpor os argumentos para serem utilizados contra a proposta brasileira.

4.3.4 Impactos e outras considerações

A discussão brasileira acerca da regulamentação Internet se caracteriza por conflitos institucionalizados, com atores e arenas de discussão bem definidas. Nos casos aqui analisados o Congresso Nacional se mostrou como principal arena de discussão. Por outro lado existem outros tipo de conflito, principalmente relacionado à liberdade de expressão política. A organização Freedom House, em seu relatório Freedom on the Net 2012 entende como a principal restrição brasileira à liberdade na Internet a judicialização de casos de expressão política, notadamente a censura de opiniões em plataformas sociais acerca de políticos⁵⁹.

Pode-se ver semelhança com o caso francês e o estadunidense, entretanto as legislações e propostas de legislação brasileiras são mais razoáveis no ponto de vista de garantir liberdades e impedir abusos. A legislação americana, com as provisões da legislação DMCA (*Digital Millennium Copyright Act*) prevê a retirada de conteúdos

⁵⁸ O deputado inclusive colocou em seu site pessoal um pedido de desculpas. (<http://www.walterfeldman.com.br/?p=322>)

⁵⁹ “The Brazilian government does not employ any technical methods to filter or otherwise limit access to online content. In 2011, the main restrictions to online expression came from civil defamation suits and legal action by the judiciary and government officials following an ongoing trend in which private litigants and official bodies sue internet service providers (ISPs) and other internet companies and send takedown notices to blogging and social networking platforms. Google’s Transparency Report recorded Brazil as having the highest number of government requests to remove content among the countries assessed in 2011.” (Freedom on The Net 2012, pag. 100, disponível em <<http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report.pdf>> acessado em 10 de janeiro de 2012)

online sem a necessidade de mandado judicial, com responsabilidade civil para os provedores de conteúdo que não retirem conteúdos infratores de seus sites após mera notificação dos donos do conteúdo. No Brasil caminha-se para garantir a imunidade dos intermediários, que só seriam responsabilizados caso não acatassem alguma ordem judicial expressa para a retirada de determinado conteúdo.

4.4 China

A Internet na China foi muito importante para seu desenvolvimento econômico recente. O governo chinês incentiva seu uso econômico, ao mesmo tempo em que tenta bloquear sua utilização para fins de mudança social e política. Para o bloqueio do uso político e manutenção do uso econômico diversas técnicas sofisticadas são utilizadas. O principal projeto de monitoramento de uso foi chamado pelo governo chinês de *Escudo dourado (Golden Shield)*, as técnicas de bloqueio são jocosamente chamadas de *Great Firewall of China (GFW)*(termo cunhado em 1997 pela revista *Wired*)⁶⁰. Para além da censura o governo também bloqueia grandes sites ocidentais, como o Facebook, o Twitter e o Google, e incentiva a criação de cópias nacionais, como o *Weibo* e o *Baidu*. A existência desses serviços nacionais possibilita um controle rígido por parte das autoridades governamentais, ao mesmo tempo em que permite aos cidadãos chineses se beneficiar da utilização dessas ferramentas. Por fim, o governo chinês emprega uma grande quantidade de pessoas para guiar as discussões online a favor do governo, chamado de *50 cent party*(partido de 50 centavos (de *yuan*, o equivalente a 8 centavos de dólar)), que seria a remuneração por postagem eletrônica de defesa ao governo.

A censura chinesa visa evitar a utilização da Internet para fins de manifestações políticas e protestos. Entretanto, não é meramente a expressão de opinião política que é censurada, os maiores alvos da censura são as postagens que incitam a ação fora da rede. O medo das autoridades chinesas é que a indignação expressada no mundo *on-line* seja levada ao mundo *off-line*, em uma possível repetição dos protestos da praça da Paz Celestial de 1989, onde redes de telefone e fax foram utilizadas para a organização dos protestos. Em certos momentos a censura tem como alvo inclusive protestos a favor do

⁶⁰ Em referência à Grande Muralha da China (*Great Wall of China*) e a uma ferramenta de segurança e bloqueio de acessos chamada *Firewall*.

governo, o objetivo é evitar a ação coletiva que possa causar qualquer desequilíbrio na ordem social vigente.⁶¹ Um possível receio do governo é que esses protestos a favor possam se transformar em protestos contra, na medida em que seus organizadores adquiram conhecimento sobre a organização desses eventos e criem redes de relacionamento fiéis a si e a seus ideais.

As técnicas utilizadas no *Golden Shield* e no *Great Firewall of China* são múltiplas, complementares e com diversos níveis de complexidade. O principal bloqueio de grandes sites externos, como o Facebook e o Twitter, é feito por DNS(*Domain Name System*) e bloqueio de IP(*Internet Protocol*), isso impede um site de ser requisitado ao servidor pelo usuário, seja digitando o nome de domínio do site quanto diretamente o endereço de IP. Sites de menor expressão não são bloqueados manualmente, mas sim por uma lista de palavras e frases banidas, como “liberdade de expressão” e “direitos humanos”, essa lista pode ser atualizada rapidamente, respondendo a eventos que o governo deseja esconder ou impedir a discussão. Nas redes sociais chinesas e sistemas de e-mail também existe uma lista de palavras censuradas, quando um usuário tenta escrever um conteúdo com alguma palavra dessa lista o sistema não permite, ou em certos casos, ele direciona a postagem para análise posterior de um censor humano. Os provedores de acesso também estão sujeitos à censura, que deve ser praticada primeiramente pelos próprios provedores para evitar punições, a chamada auto-censura. Ciber-cafés devem por lei exigir identificação dos usuários, possuírem câmeras de segurança com gravação das atividades dos usuários, registro total dos sites acessados e a instalação de um software governamental de monitoramento de alto custo⁶². Caso um ciber-café não disponha de algum desses mecanismos obrigatórios de censura o seu dono pode sofrer punições, multas e prisão⁶³.

Existem algumas alternativas contra os sistemas de censura, a maioria deles depende do redirecionamento do tráfego de rede para outras partes do mundo, o que torna a conexão segura, porém lenta. Entretanto, essas conexões também são

⁶¹ “Our central theoretical finding is that, contrary to much research and commentary, the purpose of the censorship program is not to suppress criticism of the state or the Communist Party. Indeed, despite widespread censorship of social media, we find that when the Chinese people write scathing criticisms of their government and its leaders, the probability that their post will be censored does not increase. Instead, we find that the purpose of the censorship program is to reduce the probability of collective action by clipping social ties whenever any collective movements are in evidence or expected.” (How Censorship in China Allows Government Criticism but Silences Collective Expression. Gary King Jennifer Pan Margaret E. Roberts. American Political Science Review)

⁶² Segundo a publicação Internet Enemies Report 2012, Reporters Without Borders, China.

⁶³ Segundo as pesquisas feita na publicação “Access Contested” (OpenNet Initiative, 2011, China Profile)

monitoradas e bloqueadas assim que descobertas, gerando uma corrida entre a criação de novas conexões e o bloqueio delas⁶⁴.

4.4.1 Histórico

Em 1993 o governo chinês editou a primeira regulação temporária sobre a Internet, estabelecendo poderes sobre o seu desenvolvimento, necessidade de registro para uso e possibilidade de punições por crimes digitais⁶⁵. Segundo pesquisadores⁶⁶, a rapidez da regulação da Internet, que estava ainda em seus primórdios em 1993, advém dos protestos da praça da Paz Celestial em 1989, onde os manifestantes utilizaram tecnologias como fax e redes de telefone para transmitir as informações acerca dos protestos para outros potenciais protestantes e para a mídia internacional. Essa primeira regulação torna ilegal a criação de conexões internacionais à Internet por indivíduos ou empresas, com exceção de quatro empresas estatais de telecomunicações. Em 1994 é editada a segunda regulação, tipificando crimes na Internet, punições e possibilidade de fechamento de determinadas redes⁶⁷.

Em 1995 a Internet começa a estar disponível comercialmente na China. A estrutura de censura se organiza a partir deste ano, com diversos níveis entre os oficiais do partido e os usuários. Os alvos iniciais são os BBS (*Bulletin Board System*), sistemas de comunidades online semelhantes às atuais redes sociais, que concentravam as discussões online públicas no início da Internet comercial. A criação de páginas pessoais e blogs ainda não eram comuns, e a necessidade de servidores locais para os BBS tornava fácil a censura. Com o começo da comercialização registram-se os primeiros casos de conflito, em setembro de 1996 o primeiro serviço de BBS é fechado

⁶⁴ How China is Blocking TOR. (LINDSKOG, Stefan, WINTER, Philipp. Karlstad University. Disponível em < <http://arxiv.org/pdf/1204.0447v1.pdf>> Acesso em 29.abr.2013.)

⁶⁵ “China in the information Era: Can It Maintain Controls Over the Market Sector, Appease the Globally Connected Social Networking Community and Still Attract Foreign Direct Investment?” Novik, S. M. e Goddard, R. C., Thunderbird School of Global Management, 2012.

⁶⁶ Ver nota 65.

⁶⁷ “Virtual Censorship in China: Keeping the Gate between the Cyberspaces” Qiu, Linchuan Jack. International Journal of Communications Law and Policy, Issue 4, Winter 1999/2000

permanentemente, após incitar protestos nacionalistas contra o Japão⁶⁸. Diversos outros serviços de BBS são alvos de censura nos anos seguintes.

Em 2003 começa o projeto Escudo Dourado⁶⁹ (*Golden Shield*). Junto com o *Firewall* simples o governo passou a empregar técnicas e pessoal especializado para monitorar as atividades online. No ano seguinte começam os primeiros registros das atividades do *50 cent party*⁷⁰.

As relações da China com sites estrangeiros piorou nos últimos anos. Em 2009 o Facebook, o Twitter e o Youtube tiveram seu acesso bloqueado na China. O site de pesquisa do Google começou suas operações na China em 2005 e terminou em 2010, posteriormente redirecionando seus usuários para o seu site de Hong Kong. Os conflitos advindos desses bloqueios são diminuídos, pelo fato de existirem alternativas nacionais para esses sites, a despeito delas serem consideradas de qualidade inferior e serem alvos de maior censura.

Em 2012 a organização *Reporters Without Borders* classificou a China como um país inimigo da Internet⁷¹. A bibliografia sobre outros aspectos da censura chinesa é escassa, entretanto, alguns estudos analisam os tecnicamente impactos diretos da censura, como a velocidade de remoção de conteúdo e a inclusão de novas palavras censuradas (CRANDALL et al, 2012)(KING et al, 2012).

4.5 Irã

A censura à Internet no Irã começou de maneira gradual. Inicialmente ela foi ignorada pelo governo, entretanto, com a ascensão ao poder de Ahmadinejad em 2005 regulações mais rígidas e punições mais severas começaram a ser implantadas. Essa

⁶⁸ “This BBS, formerly renown for zealot political discussions, has been closed for nearly three years since September 1996 when it mobilized a nationalist protest movement against Japan regardless of official objection.” “Virtual Censorship in China: Keeping the Gate between the Cyberspaces” Qiu, Linchuan Jack. *International Journal of Communications Law and Policy*, Issue 4, Winter 1999/2000

⁶⁹ Segundo a referência da nota 65, outros citam o início mais cedo(1998) ou mais tarde (2006).

⁷⁰ Infelizmente a maioria dos links originais e oficiais que descrevem o *50 cent party* não estão mais online. Segundo fontes secundárias: “Their main duty is to closely monitor public opinion appearing on the internet, provide information and carry out targeted publicity network planning and Internet opinion guidance.” (retirado de <http://chinadigitaltimes.net/2008/05/chinese-bloggers-on-the-history-and-influence-of-the-fifty-cent-party/> acessado em 28 de novembro de 2012)

⁷¹ Internet Enemies Report 2012 (Reporters Without Borders, 2012, disponível em http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf, acessado em 9/11/2012)

censura começou de forma violenta, com prisões e até penas de morte para dissidentes que publicavam suas ideias na Internet. Atualmente o foco está mudando, com a instalação de capacidades técnicas ampliadas. Novas legislações também foram adotadas recentemente para facilitar a censura, o monitoramento e as prisões de dissidentes políticos⁷². Além da censura institucionalizada o Irã emprega hackers para monitorar as redes de comunicação⁷³.

Devido a o aumento da capacidade técnica e das repressões políticas aos dissidentes o Irã está assim se aproximando da China, com diversas modalidades concomitantes de filtragem, censura e repressão⁷⁴.

Assim como na Coréia do Norte o regime Iraniano planeja publicamente a implantação de um sistema de Internet fechado⁷⁵, uma Intranet, acessível apenas para os iranianos e apenas com conteúdos aprovados pelo governo. Ao contrario da China, o Irã demonstra assim sua preferência para o controle político ao invés da necessidade de abertura econômica.

A censura no Irã visa combater a dissidência política em primeiro lugar, em segundo lugar reforçar os preceitos islâmicos. Na campanha presidencial de 2009 diversos sites de conteúdo político foram bloqueados, gerando manifestações de revolta e protestos por liberdade. Dissidentes políticos foram presos e diversos blogs e sites de oposição foram bloqueados.

⁷² “The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. The 2009 Computer Crime Law (CCL) identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage ‘public morality’ or to be a ‘dissemination of lies.’ Punishments mandated in the CCL are severe. They include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions.” (Freedom on The Net 2012, pag. 273, disponível em <http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report.pdf> acessado em 10 de janeiro de 2012)

⁷³ “(...)IRGC commanders have explicitly welcomed hackers willing to ‘work for the goals of the Islamic Republic’.”(Freedom on The Net 2012, pag. 277)

⁷⁴ Segundo o relatório Freedom On the Net 2012 a censura Iraniana é a maior do mundo, superando inclusive a chinesa. (Freedom on The Net 2012, pag. 262)

⁷⁵ “Alongside the expansion of existing controls, in July 2011, the Iranian authorities began referring to the creation of a National Internet. Iran’s fifth development plan from June 2010, which the government is obliged to implement, provides for the establishment of a ‘National Information Network,’ although the plan does not specify the objectives of creating it. According to the Minister of ICT, the objectives include protecting the exchange of data within the country from security breaches, monitoring emails, and creating a ‘safe internet.’ The particular technical specifications of the plan remain unclear and officials have used various names to describe the initiative, including a “Halal” or “Clean” internet, while others have issued conflicting statements about the project’s end result. Media coverage and public discussions have often described the National Internet as a national intranet that, upon its launch, would cut off users inside Iran from the global internet.” (Freedom on The Net 2012, pag. 269)

A despeito da similaridade com as técnicas chinesas, a estrutura da censura iraniana é mais simples, consistindo de filtragem de conteúdo, ameaças de sanções, como prisões e torturas e monitoramento online por unidades de polícia. Recentemente tem-se verificado a existência de apoiadores pagos pelo governo, de maneira similar ao *50 cent party* chinês⁷⁶.

Assim como na China os efeitos das técnicas de censura se demonstram na diminuição do uso político aberto da Internet. Diversas alternativas técnicas são encontradas pelos usuários para burlar a censura, entretanto, o governo frequentemente encontra maneiras de bloquear essas alternativas. Leis foram implantadas para criminalizar as ferramentas para burlar a censura e a utilização de determinados sites, como o Facebook.

A censura no Irã começou de maneira gradual, enquanto na China a Internet foi fortemente regulada e censurada desde sua chegada. Na China, mesmo com a censura e as punições, os protestos e as atividades políticas online continuaram fortes. No Irã a diminuição da expressão online foi maior, pois a Internet deixou de ser uma plataforma livre para uma plataforma reprimida nos anos 2000.

⁷⁶ “Efforts to control online speech by the Iranian government have relied primarily on large-scale Internet filtering and the threat of targeted legal action. The declaration of a spokesman from the Revolutionary Guard to launch ten thousand blogs written by members of the Basij, a volunteer Iranian paramilitary force under the authority of the Iranian Revolutionary Guards, hints at the adoption of a different strategy for shaping online information: a government-backed war of words on the Internet.” (Open Net Initiative, Internet Filtering on Iran, 2009, disponível em <https://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf> Acesso em 5.mai.2013)

5. DISCUSSÃO E CONCLUSÃO

Nessa sessão segue uma breve discussão comparada acerca dos casos estudados. Inicialmente com a França e os EUA, que são os países que se encaixam no modelo exposto na sessão de metodologia deste trabalho. Em seguida com a discussão sobre o caso brasileiro com a perspectiva fornecida pelo estudo desses casos. Depois, uma breve introdução às alternativas técnicas contra a censura nos países não democráticos. Por fim a conclusão e os pensamentos finais acerca do tema.

Os países não democráticos forneceram uma oportunidade para se entender como a Internet funciona em situações de baixos níveis de democracia. Em uma perspectiva comparada pode-se estudar como os casos do Irã e da China são diferentes dos casos dos EUA, França e Brasil. Ao mesmo tempo, quais ações dos países democráticos indicam o mesmo desejo de controle que é explícito nos países não democráticos.

5.1 Estados Unidos e França

O mais notável a se verificar no estudo desses países é a diferença de resultados. Nos EUA as legislações restritivas não foram aprovadas, enquanto na França elas foram. Segundo o modelo de explicação exposto na metodologia pode-se argumentar que os parlamentares da França se encaixam na situação exposta pela equação I, onde a perda de apoio político teria sido maior caso eles tivessem votado com o eleitorado. Nos EUA, as percepções dos parlamentares acerca da opinião de seus eleitores os fizeram tomar o rumo inverso, a perda de apoio político seria maior do que votar com os financiadores, a situação descrita pela equação III.

O apelo contra as legislações SOPA e PIPA foi global, já que as consequências da aprovação delas teriam sido sentidas globalmente. Diversas grandes empresas de Internet se localizam nos EUA, como o Google, e essa legislação teria trazido impactos mensuráveis sobre suas operações. Já na França o impacto é muito mais localizado. É interessante notar que o histórico francês de lutas populares, ainda assim isso não foi suficiente para se atrair a atenção de um público grande o suficiente para protestar

contra a medida. A atuação das grandes empresas de Internet nos EUA canalizou a reação pública, na França isso não aconteceu, dando espaço para a aprovação da legislação.

5.2 Democracias e não democracias

Nas não democracias o controle político da Internet é muito fácil de ser exercido. As ferramentas técnicas de censura estão cada vez mais baratas e simples de serem instaladas, além disso a repressão aberta pode ser exercida sem grandes consequências para o regime. Nas democracias o processo político emperra a criação dessas barreiras e a utilização da repressão. Apesar disso, diversas táticas tem sido utilizadas nas democracias para imitar o controle das não democracias, como ameaças de penas altas, multas altas e a instalação de barreiras com fins específicos, mas com capacidade de aplicação geral. Recentemente o ativista de direitos humanos Aaron Swartz foi preso por baixar ilegalmente artigos científicos da plataforma JSTOR, o procurador geral dos EUA pediu uma pena de 50 anos de prisão por violação de termos de uso. O ativista acabou se suicidando pelas pressões. Isso não é muito diferente da repressão aberta que existe nas não democracias, utilizar um caso como exemplo para os demais é uma maneira fácil de criar auto-censura, medo e *chilling effects* sobre a liberdade de expressão.

A instalação de mecanismos técnicos de controle, como no caso francês, imita a técnica de controle de censura dos países não democráticos. Monitoramento constante sobre os comportamentos online dos cidadãos pode ser utilizado para vigilância política. Ainda que esse não seja a utilização original prevista o mecanismo existe e pode ser utilizado para tal.

5.3 Perspectivas brasileiras

O Brasil se encontra em uma posição instável do ponto de vista do controle sobre a Internet. Por um lado existe uma moldura legal sobre a manutenção de direitos pelo Marco Civil da Internet. Por outro lado associações culturais e retrógradas, como a

Ordem dos Músicos do Brasil, desejam ter controle sobre os conteúdos online para poder aumentar suas fontes de captação de recursos. Conglomerados de mídia, como a rede Globo, tem interesses específicos também, como a não manutenção da neutralidade da rede, para poder lucrar com priorização de pacotes de dados específicos.

Ferramentas como o site e-democracia da Câmara dos Deputados apontam para uma abertura do processo de criação das leis. Isso pode ser considerado como uma evolução natural dos processos de legislação participativa, com um impacto nacional e possibilidades de discussão ampliadas. A Internet reduz o custo de participar, ao invés das audiências públicas com horário e locais definidos a discussão online no e-democracia pode ser feita independentemente da conveniência de horário dos participantes. Isso democratiza o acesso e permite interações entre atores que poderiam nunca se encontrar para a discussão pelos paradigmas de participação anteriores. Por outro lado essa plataforma ainda é pouco divulgada e pouco utilizada, e isso pode ser utilizado como argumento para demonstrar sua pouca relevância. Entretanto, não é de se estranhar o pouco uso, as discussões políticas são complexas, e nem todos tem interesse em analisar profundamente os argumentos e dar suas opiniões.

O Brasil pode resolver de maneira democrática seus conflitos acerca da Internet, e se mostrar como um exemplo para o restante do mundo, ou acatar as pressões de certos setores da sociedade que querem aumentar suas possibilidades de lucro utilizando a Internet, sem se importar com a diminuição das liberdades online. As legislações restritivas, como a lei Azeredo, têm sido rechaçadas pelos parlamentares, mas elas sempre têm sido propostas, de maneira que o público deve sempre ficar atento para que elas não sejam aprovadas e se transformem em fontes de restrições e censura.

5.4 Alternativas técnicas contra a censura na China e no Irã

Pela natureza técnica da Internet é possível passar pela maioria das barreiras impostas. Existem serviços variados para cada tipo de censura, com graus variados de sucesso e com riscos diferentes associados a cada um deles⁷⁷.

⁷⁷ As técnicas contra a censura são também muito utilizadas nos países democráticos, principalmente as que possibilitam maior privacidade nas comunicações. As capacidades de privacidade são utilizadas

Segundo o manual online “Circumvention tools”⁷⁸ existem diversas ferramentas disponíveis para o acesso de sites bloqueados. *Web proxies* são sites que disponibilizam um servidor *proxy* sem a necessidade de instalação de software adicional. Existem ferramentas instaláveis que também acessam servidores *proxy*, mas com mais compatibilidade por estarem fora do navegador, como por exemplo o HotSpot Shield e o Ultrasurf. A ferramenta TOR(The Onion Router) além de providenciar um servidor *proxy* também utiliza um protocolo de anonimização, que já foi extensivamente testado por autoridades independentes de segurança online. Outras ferramentas são as VPN(Virtual Private Network) que podem criptografar em tempo real o conteúdo que é transmitido através delas. O maior problema em relação ao Irã é a baixa velocidade de transmissão de dados, todas as ferramentas descritas diminuem a velocidade da conexão, o que torna complicado a utilização delas. As mais simples seriam as mais úteis, por usarem menos recursos de rede, como as *web proxies*, entretanto, também são as menos seguras e mais suscetíveis de serem bloqueadas pelo governo. A questão chinesa mais importante é o monitoramento físico, que é obrigatório em ciber cafés e estabelecimentos que fornecem serviços de Internet.

O governo dos Estados Unidos patrocina um programa de distribuição de instruções sobre como acessar servidores *proxy* no Irã⁷⁹, através de rádio são repassadas as informações na língua local sobre como acessar o servidor. A partir desse servidor os iranianos podem acessar a internet global sem monitoramento nem censura do governo iraniano.

As soluções para a censura encontradas no Irã são de natureza semelhante às soluções chinesas, entretanto existem diferenças. A velocidade da Internet residencial no Irã é do no máximo 128kbps, o que é lento, e praticamente impede o acesso a vídeos e conteúdos dinâmicos. Na China o acesso residencial também não é de alta qualidade, porém o maior gargalo são com as conexões externas, existem poucos pontos de conexão entre a Internet chinesa e o resto do mundo, o que limita a velocidade de conexão com servidores VPN localizados em países sem censura.

principalmente por criminosos que temem vigilância, corporações que temem a espionagem industrial e indivíduos que desejam ter maior privacidade em sua navegação online.

⁷⁸ Disponível em <http://www.howtobypassinternet censorship.org/files/bypassing-censorship.pdf>, acesso em 20/01/2013.

⁷⁹ “US Sponsor Anonymiser – if you live in Iran” disponível em http://www.theregister.co.uk/2003/08/29/us_sponsors_anonymiser_if_you/ acessado em 14 de janeiro de 2013.

5.5 Conclusão

Os conflitos acerca do uso da Internet estão acontecendo em diversos países. Não importa se o país é democrático ou não, se ele é desenvolvido ou não, a capacidade de utilização livre da Internet pode ser ameaçada pelo governo. Por outro lado, conflitos podem ser democráticos, como no caso da discussão do Marco Civil da Internet no Brasil. A diferença reside nas ferramentas as quais os diversos grupos de poder, e de pressão, têm para influenciarem os rumos da discussão política.

Foram aqui estudados cinco países diferentes, casos heterogêneos, mas que demonstram algumas das diversas facetas dos conflitos acerca da Internet. Na França a legislação Hadopi se demonstrou ineficaz na luta contra a pirataria, sendo alvo de críticas nos últimos dias por seus gastos excessivos e poucos resultados. No Brasil, uma versão esvaziada da lei de crimes digitais foi aprovada e a discussão do Marco Civil da Internet, apesar de ampla e democrática, não resultou ainda na aprovação da lei.

Do ponto de vista do estudo acadêmico pode-se considerar o período aqui estudado como um de transição. A primeira e a segunda década da Internet comercial (considerando a partir de 1988) foram marcadas pela pouca regulação, agora, em meados da terceira década, que os governos tentam criar regulações mais específicas a esse meio. Uma solução preferencial ainda não foi encontrada e os diversos segmentos do público interessado tentam moldar as propostas de legislações a seu favor. Na França foi clara a vitória das indústrias de conteúdo na aprovação do Hadopi, entretanto, com sua ineficácia, essas indústrias podem procurar outras formas de proteger seus interesses no futuro. No Brasil, as indústrias equivalentes tentam barrar a aprovação do Marco Civil, mas com os escândalos recentes da questão da espionagem na Internet existe uma força significativa de opinião pública para a aprovação do projeto.

O período de transição está longe do fim. Com tecnologias novas de monitoramento surgem novas tecnologias de circunvenção, a “guerra armamentista tecnológica”. Com regulações de comportamentos online surgem novos comportamentos não regulados. Como no caso do Hadopi, o monitoramento de redes P2P fez surgir uma demanda maior por Downloads diretos e por VPNs, novos comportamentos e novas tecnologias de circunvenção.

Espera-se que os casos estudados nesse trabalho tenham demonstrado as possibilidades que os conflitos apresentam para as garantias civis e a liberdade. Casos extremos como a China e o Irã demonstram como um ambiente de Internet monitorado em uma não democracia pode ser até mesmo fatal para os usuários que expressem suas ideias. Já os conflitos institucionalizados dos países democráticos apontam no sentido de que a discussão pode se dar de maneira democrática, mesmo que o resultado final seja a restrição de liberdades, como no caso da França. E mesmo assim, a despeito de a legislação Hadopi ter sido aprovada, ela vem sendo discutida de maneira ampla na França, diferentemente da China e do Irã, onde se posicionar contra uma lei pode ser considerado um crime contra o Estado.

5.5.1 A ciência política e o estudo da Internet

As instituições políticas tradicionais não existem em uma forma estanque, imutável e incapaz de absorver as mudanças de paradigma da sociedade. Com o surgimento de cada nova tecnologia da informação as instituições políticas responderam, inicialmente por meio de utilização delas e posteriormente por meio de regulação. As diferenças principais da Internet em relação às tecnologias anteriores são sua abrangência, a velocidade de adoção pelo mundo e a facilidade de comunicação de massa fornecida para cada usuário individual da rede. A ciência política não pode ignorar o efeito que isso teve nas instituições, que hoje se debruçam sobre essa nova tecnologia para tentar entendê-la e regulá-la do ponto de vista político.

Os governos lutam para regular a Internet de maneira favorável a si. Os cidadãos, por outro lado, lutam para manter a Internet livre e sem regulações. Entretanto, essa afirmação dicotômica é muito simples em relação aos conflitos atuais. Mesmo com as capacidades de comunicação de massa da Internet os custos da ação coletiva não são possíveis de serem ignorados. A redução dos custos de participação não implica custo zero de participação. As legislações americanas requereram uma enorme mobilização para serem barradas. Os protestos franceses não atraíram número suficiente de pessoas para barrar a legislação Hadopi. Muitos usuários não se preocupam com as regulações e preferem que outros lutem pelos seus direitos, no típico problema do carona.

Os dilemas da ação coletiva não deixaram de existir com o surgimento da Internet. A redução de custos para a participação e para a organização de grupos de pressão não implica um pretense novo surgimento da participação como tal, mas apenas de novas categorias de participação. Categorias essas que podem ser questionadas quanto a sua eficácia, mas que possuem resultados práticos inegáveis, como a luta contra o SOPA/PIPA. Outros exemplos de participação derivadas das ferramentas de Internet são as manifestações que ocorreram no Brasil em junho de 2013, sendo as redes sociais o principal mecanismo de mobilização.

5.5.2 Palavra final

Além da regulação e do controle, nas democracias é também fonte de conflitos a questão do monitoramento e espionagem. Nos últimos dias de finalização desse trabalho foi denunciado o caso de espionagem online em larga escala feito pela agência de segurança NSA dos EUA, o programa chamado PRISM. Segundo os documentos revelados por Edward Snowden, as principais companhias responsáveis por serviços online, como o Google, Facebook, Yahoo e a Microsoft são obrigados a fornecer diversas informações acerca de seus usuários à agência, como comunicações, sites visitados, endereços de IP e outros. Este fato gerou respostas pelo governo dos EUA, o Senado americano questionou o diretor da NSA acerca dos fatos e investigações começaram quase imediatamente após o vazamento dos dados. Na Internet a resposta foi também quase imediata, diversas organizações começaram protestos e as companhias citadas nos documentos deram respostas evasivas acerca do monitoramento.

O monitoramento das agências de segurança implica questões sérias de privacidade. Apesar de necessitar de um mandado judicial para espionar em detalhes cidadãos americanos as agências de inteligência podem coletar diversas informações sem a necessidade desse mandado. Informações conhecidas como metadados, dados acerca dos dados⁸⁰, podem revelar a localização e o contexto de determinadas atividades e servir como monitoramento, a NSA argumenta que não necessita de um mandado para

⁸⁰ Como, por exemplo, para quem um e-mail é enviado, mas não o conteúdo em si dele. Fotos públicas também podem conter metadados, como localização onde foram tiradas e informações do aparelho que tirou a foto.

coletar esses metadados em larga escala. Outro país que possui a capacidade de coletar esses dados em larga escala é a China, que possui capacidade de monitorar seus cidadãos de maneira similar. Como argumenta Solove (2012) os programas de monitoramento implicam um desbalanço de poder, não só o cidadão é monitorado como ele não sabe da extensão dessa capacidade pelo poder público, isso se torna evidente nesse episódio por se tratar de um monitoramento secreto e pervasivo.

As companhias citadas nos documentos rapidamente providenciaram respostas. Facebook, Apple, Dropbox e outros responderam que não tinham conhecimento do programa. O Google, além disso, requisitou à uma corte de justiça dos EUA (*Foreign Intelligence Surveillance Court*) a capacidade de revelar detalhes dos pedidos de dados feitos pela NSA. A natureza dessas ordens das agências de segurança impede que a própria ordem seja revelada, adicionando ainda mais à dimensão de desbalanço de poder, como explicado por Solove (2012). De acordo com essa impossibilidade de se admitir a existência das ordens o Google forneceu sua resposta no seu blog oficial:

“(...)First, we have not joined any program that would give the U.S. government—or any other government—direct access to our servers. Indeed, the U.S. government does not have direct access or a ‘back door’ to the information stored in our data centers. We had not heard of a program called PRISM until yesterday.

Second, we provide user data to governments only in accordance with the law. Our legal team reviews each and every request, and frequently pushes back when requests are overly broad or don’t follow the correct process. Press reports that suggest that Google is providing open-ended access to our users’ data are false, period. Until this week’s reports, we had never heard of the broad type of order that Verizon received—an order that appears to have required them to hand over millions of users’ call records. We were very surprised to learn that such broad orders exist. Any suggestion that Google is disclosing information about our users’ Internet activity on such a scale is completely false.(...)” (Disponível em <<http://googleblog.blogspot.com.br/2013/06/what.html>>)

As respostas das outras companhias foram similares, entretanto a existência dessas respostas demonstra que as denúncias feitas por Snowden não são produto de uma invenção, no mínimo elas geraram uma percepção de que a espionagem pode existir em larga escala, e pode existir em um país plenamente democrático, a despeito das instituições que deveriam proteger as liberdades individuais. No momento em que essas denúncias chegaram ao público pode se perceber o conflito, as pessoas esperaram

por respostas, tanto das empresas quanto do governo. Rapidamente as reações contra o programa PRISM se espalharam pela Internet, e grupos de pressão foram criados, em um exemplo de atividade do pluralismo acelerado de Bimber (1998, 2011).

As denúncias também resultaram em reações por parte de empresas e governos não envolvidos. Empresas de computação em nuvem passaram a colocar como um de seus pontos de venda o fato de não estarem localizadas em território dos EUA, e sim em países com definições melhores de privacidade, como a Suíça. O governo da Alemanha questionou o programa de vigilância. No Brasil a discussão do Marco Civil da Internet foi reativada, junto com a discussão de outros projetos que visam a proteção de dados dos usuários de Internet (como o PL 3558/12 e o PL 4060/12).

O futuro pode ser de uma Internet restrita e fechada ou aberta e livre, depende de como cada país discutir suas políticas acerca desse meio. Conflitos são inevitáveis, e tentativas de restrição sempre existirão, mas nas democracias existe espaço para a discussão, e com pressão popular aliada a parlamentares honestos essas restrições podem ser evitadas. Cabe a ciência política estudar esses conflitos, identificar os atores relevantes e as arenas de discussão, sendo também ferramenta de manutenção dos direitos, garantias e liberdades que se personificam na capacidade de acesso livre e na livre expressão de ideias, seja na Internet ou fora dela.

BIBLIOGRAFIA

AIKENS, Geoffrey S. **A democracia Eletrônica**. *Cadernos da Escola do Legislativo*, Belo Horizonte, jul/dez 1998. Pp 41-101.

ANTI, Michael (Zhao Jing). **Behind the firewall of china**. TED talk. Disponível em: <http://www.ted.com/talks/michael_anti_behind_the_great_firewall_of_china.html> acessado em 23/11/12>

BATISTA, Carlos Marcos. **ICT's and Good Governance: The Contribution of Information and Communication Technologies to Local Governance in Latin America**. Brasília: Núcleo de Pesquisa em Políticas Públicas – Universidade de Brasília, 2003. Disponível <<http://www.unesco.org/webworld/e-governance>>. Acessado em 15/11/2011.

BATISTA, Carlos Marcos . **TIC e participação cidadã na América Latina um estudo dos legislativos locais**. In: CUNHA, Maria Alexandra; FREY, Klaus; DUARTE, Fábio. (Org.). Governança local e as tecnologias da informação e comunicação. 1 ed. Curitiba: Champagnat, 2008.

BOBBIO, Norberto. **Dicionário de Política**. Brasília: Editora Unb, 2010.

BRIDY, A. **Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA**. 2012. Disponível em <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042787>. Acesso em: 21.dez.2012.

BROWDER, Rebekah K. **Internet Voting with Initiatives and Referendums: Stumbling Towards Direct Democracy**. Seattle university School of Law. 2006

CASTELLS, Manuel. **La Galaxia Internet**. 1ª Edição. Barcelona: Areté, 2001.
_____. **Communication power**. Oxford University Press, 2009.

CRANDALL, R. J. **The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions**. 2012. Disponível em <<http://arxiv.org/ftp/arxiv/papers/1303/1303.0597.pdf>> Acesso em 28.abri.2013.

DAHL, R. A. Poliarquia. São Paulo: Edusp, 1997.

DANAHER, B., SMITH, M. D., TELANG, R., CHEN, S. **The effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France**. 2012. Disponível em <<http://ibercrea.es/wp-content/uploads/2012/01/HADOPI-FINAL.pdf>> Acesso em 21.dez.2012.

ECONOMIST, The. **Democracy index 2012. Democracy at a standstill**. Intelligence Unit. 2012. Disponível em <<http://pages.eiu.com/rs/eiu2/images/Democracy-Index-2012.pdf>> Acesso em 13.maio.2013.

EUA. **PIPA (PROTECT IP Act) Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011.** 112th Congress. Disponível em: <<http://www.govtrack.us/congress/bills/112/s968>>. Acesso em 16 de janeiro de 2013.

EUA. **SOPA (Stop online piracy act) To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes.** H.R. 3261. 112th Congress. Disponível em: <<http://www.govtrack.us/congress/bills/112/hr3261/text>>. Acesso em 16 de janeiro de 2013.

ELDEMAN, Benjamin e ZITTRAIN, Jonathan. **Empirical Analysis of Filtering in China.** Berkman Center for Internet & Society. Harvard Law School. 2003. Disponível em <<http://cyber.law.harvard.edu/filtering/china/>> Acesso em 21.dez.2012.

FARIA, Cristiano F. S. **O Parlamento aberto da era da internet, pode o povo colaborar com o Legislativo na elaboração das leis?** Centro de Documentação e Informação. Edições Câmara. Brasília, 2012.

FRANÇA. **Decision n° 2009-580 of June 10th 2009.** Conseil Constitutionnel. Disponível em: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf> Acesso em 11.jul.2012.

FRANÇA. **Projet de Loi Favorisant la diffusion et la protection de la création sur internet.** Sénat. 2009 Disponível em <<http://www.senat.fr/leg/tas08-008.pdf>>. Acesso em 5.jul.2012.

FRANÇA. **Projet de Loi Relatif a La Protection Penale de La Propriete Litteraire et Artistique Sur Internet Etude d'Impact.** 2009. Disponível em <<http://tempsreel.nouvelobs.com/file/718941.pdf>> Acesso em 21.dez.2012.

GIBSON, R. NIXON, P. WARDS, S. **Political Parties and the Internet, net gain?** Routledge, 2003.

GOODIN, Robert E. **The oxford handbook of political Science.** Oxford University Press, 2009.

HINDMAN, Matthew. **The myth of digital democracy.** Princeton NJ: Princeton University Press, 2008.

HYDE, A. et al. **Circumvention Tools Bypassing internet censorship.** Disponível em <<http://www.howtobypassinternet censorship.org/files/bypassing-censorship.pdf>>. Acesso em 11.jan.2013.

KING, Gary, PAN, Jennifer, ROBERTS, Margaret E. **How Censorship in China Allows Government Criticism but Silences Collective Expression.** American Political Science Review. 2012. Disponível em <http://faculty.haas.berkeley.edu/neil_thompson/DSI_Seminar/Papers/censored.pdf> Acesso em 29.abr.2013.

KELLY, Sanja, COOK, Sara, TRUONG, Mai. **Freedom on The Net 2012**. Freedom House. 2012. Disponível em: <<http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report.pdf>> Acesso em 10 de janeiro de 2012.

LASSWELL, Harold D.. **A Linguagem da Política**. Brasília Editora Universidade de Brasília, 1982, 2º edição.

LINDSKOG, Stefan, WINTER, Philipp. **How China is blocking TOR**. Karlstad University. Disponível em < <http://arxiv.org/pdf/1204.0447v1.pdf>> Acesso em 29.abr.2013

MEYER, Trisha. **Graduated Response in France: the clash of copyright and the Internet**. Journal of Information Policy 2, 2012.

MOSSBERGER, K.; TOLBERT, C. J.; STANSBURY, M. **Virtual Inequality: Beyond the Digital Divide**. Washington: Georgetown University Press, 2003.

NAN, Lin. **Building a network theory of social capital**. *Connections* 22. 1999. Disponível em: <[http://web.archive.org/web/20080308005741/http://www.insna.org/Connections-Web/Volume22-1/V22\(1\)-28-51.pdf](http://web.archive.org/web/20080308005741/http://www.insna.org/Connections-Web/Volume22-1/V22(1)-28-51.pdf)> Acesso em 21.dez.2012.

NOVICK, Samantha, M. GODDARD, Roe C. **China in the Information Era: Can it Maintain Controls Over the Market Sector, Appease the Globally Connected Social Networking Community and Still Attract Foreign Direct Investment?** Thunderbird School of Global Management. 2012. Disponível em: < <http://files.isanet.org/ConferenceArchive/bf64d50e4b044df8a8d7091dad0b93b3.pdf>> Acesso em 21.dez.2012.

NORRIS, P. **Critical Citizens**. Oxford University Press, 1999.

_____. **Digital Divide - Civic Engagement, Information Poverty, and The Internet Worldwide**. Cambridge University Press, 2001.

_____. **Public sentinel, news, media & governance reform**. The world Bank. 2010. Disponível em: <<http://siteresources.worldbank.org/EXTGOVACC/Resources/PublicSentineleBook.p>> Aceso em 21.dez.2012.

PASQUINI, Mathieu (editor) et al. **La Bataille Hadopi**. InLibro Veritas. 2009.

PEÑA-LOPEZ, Ismael. **The disempowering *Goverati*: e-Aristocrats or the Delusion of e-Democracy**. **Open University of Catalonia**. 2011 Disponível em < www.jedem.org/article/view/50/69> Acessado em 3.mar.2013.

PÉNARD, Thierry e POUSSING, Nicolas. **Internet Use and Social Capital: The Strength of Virtual Ties**. Journal of Economic Issues, n 44. Disponível em <

<http://perso.univ-rennes1.fr/thierry.penard/biblio/PenardPoussingSocialCapital.pdf>>
Acesso em 21.dez.2012.

PÉNARD, Thierry, POUSSING, Nicolas e SUIRE, Raphael. **Does the Internet make people happier ?**, Economics Working Paper Archive (University of Rennes 1 & University of Caen) Center for Research in Economics and Management (CREM), University of Rennes 1, University of Caen and CNRS.2011.

QIU, L. J. **Virtual Censorship in China: Keeping the Gate between the Cyberspaces** International Journal of Communications Law and Policy, Issue 4, Winter 1999/2000 Reporters Without Borders. **Internet Enemies Report 2012**. 2012. Disponível em: <http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf> Acesso em 9.nov.2012.

ROSENSTONE, S. J.; HANSEN, J. M. **Mobilization, Participation and Democracy in America**. Pearson Education, 1996.

SOLOVE, D. J. **I've got nothing to hide' and other misunderstandings of privacy**. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565>. Acesso em 14 de junho de 2012.

STABILE, M. **Democracia Eletrônica para quem? Quem são, o que querem e como os cidadãos avaliam o portal da Câmara dos Deputados** BRASÍLIA 2013. Dissertação (Mestrado). Instituto de Ciência Política, Universidade de Brasília, Brasília.

UNITED NATIONS. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue**. 2011. Disponível em <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> Acesso em 20.jul.2012.

WALTON, G. **China's golden shield: corporations and the development of Surveillance Technology in the People's Republic of China**, International Centre for Human Rights and Democratic Development, 2001. Disponível em: <http://web.archive.org/web/20110716063126/http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF> Acesso em 21.dez.2012.

WELLMAN, Barry et al. **Does the Internet Increase, Decrease or Supplement Social Capital? Social Networks, Participation, and Community Commitment**. *American Behavioral Scientist*, Vol 45(30), Nov. 2001. Disponível em: <<http://www.chass.utoronto.ca/~wellman/publications/index.html>> Acesso em 21.dez.2012.

SUZOR, Nicolas, FITZGERALD, Brian. **The legitimacy of graduated response schemes in copyright law**. 2011. Disponível em: <<http://nic.suzor.net/wp-content/uploads/2011/08/Suzor-Fitzgerald-2011-Graduated-Responses-UNSW.pdf>> acesso em 22/10/2012> Acesso em 22.out.2012.

ANEXO I – TRADUÇÕES

Traduções

Nota 1 – página 10: O vasto potencial e benefícios da Internet estão enraizados em suas características únicas, como sua velocidade, alcance global e relativa anonimidade. Ao mesmo tempo, essas características distintivas da Internet que possibilitam aos indivíduos disseminar informação em tempo real e mobilizar pessoas também criaram medo dentre os Governos e os poderosos. Isso tem levado ao aumento das restrições na Internet pelo uso de tecnologias cada vez mais sofisticadas para bloquear conteúdo, monitorar e identificar ativistas e críticos, criminalização de expressão legítima e adoção de legislação restritiva para justificar tais medidas.

Nota 5- página 12: Circunvenção é o ato de trespassar a censura na Internet. Existem muitas maneiras de se fazer isto, mas quase todas funcionam aproximadamente da mesma maneira. Elas instruem seu navegador da Web a fazer um desvio por um computador intermediário, chamado de proxy, que está localizado em algum lugar que não está sujeito a censura na Internet, não foi bloqueado de sua localização e sabe procurar e retornar o conteúdo para usuários.

Nota 6 – página 12: Vigilância pode criar efeitos congelantes na livre expressão, livre associação e outros direitos da Primeira Emenda essenciais para a democracia. Até mesmo vigilância de atividades legais pode inibir pessoas de as fazerem. O valor da proteção contra os efeitos congelantes não é medido simplesmente por focar nos indivíduos particulares que são impedidos de exercer seus direitos. Efeitos congelantes prejudicam a sociedade, pois, dentre outras coisas, eles reduzem a amplitude de pontos de vista expressos e o grau de liberdade com os quais se participa da atividade política.

Nota 8- página 13: Enquanto nós acreditamos que a pirataria online de sites estrangeiros é um problema sério que requer uma resposta legislativa séria, nós não iremos apoiar legislação que reduz a liberdade de expressão, aumenta o risco de segurança cibernética, ou diminua a Internet global dinâmica e inovadora.

Nota 10- página 16: Muito poucos desenvolvimentos nas tecnologias da informação tem tido um efeito tão revolucionário como a criação da Internet. De maneira diferente de qualquer outro meio de comunicação, como o rádio, a televisão e as publicações impressas baseadas em transmissão de informação de mão-única, a Internet representa um salto a frente como um meio interativo(...) De maneira mais geral, ao habilitar os indivíduos a trocar informações e ideias instantaneamente e com baixos custos através de fronteiras nacionais, a Internet permite acesso a informação e conhecimento que era anteriormente inatingível. Isso, por sua vez, contribui para a descoberta da verdade e progresso da sociedade como um todo.

Página 26 – corpo do texto: (...) direitos autorais são utilizados como uma alavanca para mais controle no debate acerca da governança da Internet. Muito do uso democrático e social da Internet (por exemplo, liberdade de expressão escrita ou construção de comunidade) depende da sua natureza aberta, cooperativa flexível e descentralizada. Entretanto, essas mesmas características são questionadas por razões econômicas ou políticas, como o combate a pirataria, e existem pressões para regulações da Internet maiores e mais restritivas.

Nota 22- página 26: (...) Muitos esforços de controle tem como algo diretamente a arquitetura da Internet, criando pontos centralizados de controle no fluxo de informações sobre a rede. Procura-se uma resposta em alterar a racionalidade e as funções da rede, com consequências que se estendem além do problema da pirataria online. Na verdade, embora a proteção de direitos autorais podem não impactar diretamente a habilidade de um cidadão de encontrar um emprego, preencher um formulário de impostos online, ou ter informações sobre as próximas eleições, ela se encaixa dentro de uma tendência ampla de controle de acesso à informações. Existe pouco espaço para a reflexão do valor do amplo acesso à informação e privacidade para propósitos democráticos dentro de um pensamento que advoga fortes direitos de propriedade e a alteração da arquitetura da Internet.

Nota 23- página 26: A estratégia de controle de conteúdo do partido comunista chinês consiste de três técnicas primárias: filtragem técnica automatizada, auto-censura forçada por provedores de serviço de acesso, e manipulação proativa. Essas técnicas se reforçam mutuamente para criar uma paisagem de informação altamente manipulada e notadamente isolada do fluxo de notícias internacionais. O objetivo proposto é limitar a disseminação de pornografia, jogos de azar, rumores e outras práticas danosas, mas o conteúdo na rede relacionado a tópicos políticos sensíveis ou tópicos sociais é tão alvo quanto.

Nota 24 – página 29: As regulações e legislações da Internet na China são guiadas pelo princípio de ‘abertura vigiada’ – procurando preservar os benefícios econômicos da abertura para a informação global, enquanto protegida contra dominação econômica estrangeira e o uso da Internet por grupos domésticos ou estrangeiros para coordenar atividades anti-regime.

Página 35- corpo do texto: EM GERAL- Um provedor de serviço deve tomar medidas tecnicamente factíveis e razoáveis desenhadas para prevenir acesso pelos seus assinantes localizados dentro dos EUA ao site estrangeiro infrator (ou uma porção dele) de resolver para aquele nome de domínio o endereço de IP.

PROVEDORES DE PESQUISA DA INTERNET: Um provedor de pesquisa da Internet deve tomar medidas tecnicamente factíveis e razoáveis desenhadas para impedir o site estrangeiro infrator que é sujeito da ordem, ou a porção do site especificada na ordem, de ser servido como um hyperlink direto.

Página 36 – corpo do texto: EXECUÇÃO DAS ORDENS-

(A) EM GERAL- Para garantir conformidade com as ordens emitidas nessa seção, o Advogado Geral pode fazer uma ação de medida cautelar (...)

(ii) contra qualquer entidade que conscientemente e deliberadamente provê ou oferece para prover um produto ou serviço desenhado ou comercializado para a circunvenção das medidas descritas no parágrafo (2) (...)

Página 36 – corpo do texto: (D) DEFINIÇÃO.- (...) um produto ou serviço que é desenhado ou comercializado para habilitar um nome de domínio descrito em tal ordem-

(i) resolver para aquele de nome de domínio ou endereço de protocolo de Internet mesmo tendo em vista as medidas tomadas por um provedor de serviço de acesso sob o parágrafo (2) prevenir tal resolução; ou

(ii) resolver para um nome de domínio ou endereço de protocolo de Internet que o provedor do produto ou serviço saiba, razoavelmente deva saber, ou razoavelmente acredita que é utilizado por um site oferecendo atividades infratoras substancialmente similares as quais o site infrator estrangeiro, ou uma porção dele, sujeitas a uma ordem judicial sob a qual esta seção foi associada.

Página 37 – Corpo do texto: SEC. 104. IMUNIDADE POR TOMAR AÇÕES VOLUNTÁRIAS CONTRA SITES DEDICADOS AO ROUBO DE PROPRIEDADE DOS EUA.

Nenhuma causa de ação deve recair em nenhum corte Federal ou Estadual ou agência administrativa contra, nenhuma pessoa pode ser causa de ação contra, e nenhuma indenização por dano para nenhuma pessoa deve ser garantido contra o provedor de serviço, provedor de rede de pagamento, serviço de propaganda na Internet, propagandista, provedor de busca na Internet, registrador de nomes de domínio por tomar quaisquer ações descritas na seção 102(c)(2), seção 103(d)(2), ou seção 103(b) com respeito a um site de Internet, ou voluntariamente bloquear acesso ou finalizar afiliação financeira com o site, na crença razoável de que-

- (1) O site é um site estrangeiro infrator ou é um site dedicado ao roubo de propriedade dos EUA; e
- (2) A ação é consistente dentro dos termos de serviço da entidade ou outros direitos contratuais.[]

Página 38 – Corpo do texto: Imagine um mundo sem conhecimento livre. Por mais de uma década, nós gastamos milhões de horas construindo a maior enciclopédia da história humana. Agora mesmo, o congresso dos EUA está considerando legislação que poderia danificar fatalmente a Internet livre e aberta. Por 24 horas, para aumentar a atenção, nós estamos tirando do ar a Wikipédia.

Página 39 – corpo do texto:

*Requerer serviços web, como os que ajudamos a fundar, a monitorar o que os usuários linkam, ou fazem upload. Isso teria um efeito congelante na inovação.

*Negar aos donos de websites o devido processo legal.

*Dar ao governo dos EUA o poder para censurar a web utilizando técnicas similares às utilizadas pela China, Malásia e Irã; e

*Diminuir a segurança online modificando a estrutura básica da Internet.

Na discussão do comitê Judiciário da Casa acerca do SOPA, nenhum especialista técnico falou (...) Representantes da Pfizer, a companhia farmacêutica, e da MPAA testemunharam a favor dos detentores de propriedade intelectual. Representantes do Google e da Mastercard testemunharam a favor dos intermediários online que a proposta desejava regular. Um representante do AFL-CIO testemunhou a favor das indústrias dos membros das indústrias de conteúdo. (lembe-se que as propostas foram colocadas como salvadoras de empregos). Ninguém, entretanto, testemunhou a favor dos engenheiros da Internet ou de seus usuários.

Nota 34 – Página 43: (...) Julien Mailland argumenta que um precedente da busca de controle central de redes de comunicação pode ser encontrado na postura francesa em relação ao Minitel. A França resistiu por muito tempo ao desenvolvimento da Internet, pois havia introduzido sua própria tecnologia de redes de comunicação alternativa chamada Minitel nos anos 70. A infraestrutura de suporte dessa tecnologia de vídeo-texto era centralizada e restrita à França, e o conteúdo da rede Minitel era fortemente regulado pelo governo francês. (...) Considerando o precedente nacional feito pelo Minitel, a abordagem proativa da França em construção de políticas em geral e o fato de que as indústrias culturais na França estão entre as maiores da Europa, não é surpresa que a legislação de resposta gradual foi adotada no país.

Página 44 – Corpo do texto:

1 – uma missão de incentivo ao desenvolvimento da oferta legal e da observação da utilização lícita e ilícita das obras e dos objetos aos quais esteja associado um direito de autor ou um direito autoral ou um direito conexo nas redes de comunicações eletrônicas utilizadas para o fornecimento de serviços de comunicação online ao público;

2 – uma missão de proteção dessas obras e objetos em relação às tentativas de violação a esses direitos cometidos nas redes de comunicação eletrônicas utilizadas para o fornecimento de serviços de comunicação online ao público;

3- uma missão de regulação e de cuidado no campo das medidas técnicas de proteção e de identificação das obras e dos objetos protegidos por um direito de autor ou por um direito conexo;

Nota 36 – Página 44: Na França, por exemplo, depois de um esquema administrativo inicial, conhecido como HADOPI, foi considerado como inconstitucional pelo conselho constitucional francês, um novo sistema foi introduzido que requer um precedente criminal completo para a desconexão por períodos de até um ano.

Página 45 – Corpo do texto: 11. As partes concordam que em dar a uma autoridade administrativa, mesmo que independente, o poder de impor penalidades na forma de retirar acesso à Internet, o Parlamento primeiro infringe o direito fundamental de liberdade de expressão e comunicação, e segundo, introduz penalidades patentemente desproporcionais. Eles também argumentam que as condições para impor tais penalidades introduzem uma presunção de culpa, que patentemente infringe os direitos de defesa.

Nota 37 – página 45: 12. O artigo 11 da Declaração dos Direitos do Homem e do Cidadão de 1789 diz: ‘A comunicação livre de ideias e opiniões é um dos direitos mais precisos do homem. Todo cidadão pode então falar, escrever e publicar livremente , exceto nos casos em que essa liberdade é mal utilizada nos casos determinados pela Lei. No corrente estado dos meios de comunicação e dado o desenvolvimento geral dos serviços de comunicação online pública e a importância disso na participação na democracia e expressão de ideias e opiniões, esse direito implica liberdade de acesso a esses serviços.

Nota 38 – Página 45: 16. Os poderes para impor penalidades criadas pelas provisões contestadas dá ao Comitê a proteção do direito de cópia, que não é uma corte de lei, o poder de restringir ou negar acesso à Internet por usuários e às pessoas as quais elas

disponibilizam acesso à Internet. Os poderes fornecidos a esta autoridade administrativa não são limitados a uma categoria específica de pessoas, mas estendidas a toda a população. Os poderes deste Comitê então podem levar à restrição do direito de qualquer pessoa para exercer o seu direito de se expressar e se comunicar livremente, em particular de sua própria casa. Nessas condições, sob o ponto de vista da liberdade garantida pelo artigo 11 da Declaração de 1789, o Parlamento não tem liberdade, a despeito das garantias acompanhadas pela imposição de penalidades, de dar a uma autoridade administrativa tais poderes para o propósito de proteger detentores de direitos de cópia e direitos relacionados.

Nota 39 – Página 45: 18. No caso atual, sob as provisões referidas para revisão, o cometimento de uma infração de direito de cópia no endereço do usuário registrado constitui, de acordo com os termos do segundo parágrafo do Artigo L 331-21 ‘o ingrediente material da quebra de dever definida no Artigo 336-3’. Apenas o contratante do acesso à Internet pode ser objeto das penalidades introduzidas pelas provisões referidas para revisão. Para evitar a imposição de tais penalidades é obrigado a ele, sob o Artigo 331-38, coletar evidência que a infração de direito de autor ou direitos relacionados foi alvo de uma fraude de uma terceira pessoa. Então, ao reverter o ônus da prova, o Artigo 331-38, introduz, contrariamente aos requisitos derivados do Artigo 9 da Declaração, uma presunção de culpa da parte contratante do acesso à internet para lhe impor penalidades restringindo ou deprivando-o de seus direitos.

Nota 45 – Página 47: (...)O Repórter Especial considera o corte de usuários do acesso à Internet, independentemente da justificativa, incluindo a de violação de leis de direitos de propriedade intelectual, como desproporcional e portanto uma violação do artigo 19, parágrafo 3, do Pacto Internacional de Direitos Civis e Políticos.

Nota 50 – Página 49: O governo tomou o curso exatamente oposto do dito recentemente em cortes e recomendações internacionais que condenam filtragem e corte de acesso à Internet, e o tem feito em um contexto de aumento de pressão sobre os jornalistas para revelar fontes.

Nota 51 – Página 49: O ministro das relações exteriores francês, Alain Juppé, tem de fato negado o apoio à declaração da ONU reconhecendo o acesso à Internet como direito fundamental, condicionando sua assinatura ao reconhecimento do direito de propriedade intelectual como um direito equivalente à liberdade de expressão.

Nota 52 – Página 49: Corrida armamentista tecnológica. O governo francês introduziu o HADOPI 1 e o HADOPI 2 para controlar a pirataria online e deter os usuários de baixar matérias protegidos pelo direito de cópia. Entretanto, as leis podem ser consideradas já ultrapassadas, já que os usuários utilizam novas tecnologias para a circunvenção dos requerimentos. Por exemplo, os piratas de Internet podem mascarar suas identidades facilmente utilizando uma proxy anônima ou um servidor VPN que esconde o IP do usuário final, permitindo assim o download de conteúdos protegidos pelo direito de cópia sem deixar traços. Novas meios e medidas terão de ser adotados para lutar contra esse tipo de pirataria na Internet. Entretanto, o HADOPI 1 e o HADOPI 2 devem ainda impedir o usuário de Internet mediano, o que é o objetivo principal deles.

Nota 61- Página 57: Nosso achado teórico central é que, ao contrário de muitas pesquisas e comentários, o propósito do programa de censura não é suprimir o criticismo do Estado ou do partido comunista. Na verdade, a despeito da censura ampla das mídias sociais, nós encontramos que quando o povo chinês escreve críticas abertas

de seu governo e de seus líderes, a probabilidade de que sua postagem será censurada não aumenta. Em vez disso, nós encontramos que o propósito do programa de censura é reduzir a probabilidade de ação coletiva ao cortar os laços sociais em qualquer momento em que movimentos coletivos estão em evidência ou são esperados.

Nota 69 – Página 59: Esse BBS, anteriormente reaberto por intensas discussões políticas, foi fechado por quase três anos desde setembro de 1996 quando ele mobilizou um protesto nacionalista contra o Japão a despeito da objeção oficial.

Nota 70 – Página 59: O seu principal dever é monitorar de perto a opinião pública na Internet, provendo informações e planejamento público de publicidade direcionada e guia de opiniões de Internet.

Nota 72 – Página 59: A lei de imprensa de 2000, por exemplo, proíbe a publicação de ideias que sejam contrárias aos princípios islâmicos ou ruins aos direitos públicos, nenhum dos quais é definido claramente. O governo e o judiciário invocam regularmente isso e outras legislações fracamente definidas para criminalizar opiniões críticas. A Lei de Crimes de Computador de 2009 define punições para espionagem, atividades hacker, pirataria, calúnia, e publicação de materiais considerados como danosos à ‘moral pública’ ou serem ‘disseminadoras de mentiras’. As punições da legislação são severas, com sentenças de prisão longas, multas absurdas, e penalidades para provedores de serviços que falharem em aplicar as restrições de conteúdo do governo.

Notas 73 – Página 60: (...) os comandantes da IRGG tem explicitamente aceitado hackers que estejam dispostos a ‘trabalhar pelos objetivos da república islâmica’.

Nota 75 – Página 60: Junto com a expansão de controles existentes, em Julho de 2011, as autoridades iranianas começaram a se referir à criação de uma internet nacional. O quinto plano de desenvolvimento do Irã de Junho de 2010, o qual o governo é obrigado a implementar, provê o estabelecimento de uma ‘Rede de comunicações nacional’, entretanto o plano não justifica os objetivos de sua criação. De acordo com o ministro das tecnologias da informação, os objetivos incluem proteger a troca de dados dentro do país de brechas de segurança, monitorar e-mails e criar uma ‘internet segura’. As especificações técnicas do plano continuam não claras e oficiais utilizaram variados nomes para descrever a iniciativa, incluindo ‘Halal’ ou Internet ‘Limpa’, enquanto outros deram informações conflituosas em relação ao resultado final do projeto. A cobertura da mídia e a discussão pública tem frequentemente descrito a Internet Nacional como uma intranet nacional que, com o seu lançamento, iria cortar os usuários dentro do Irã do acesso à Internet global.

Nota 76 – Página 61: Esforços para controlar a expressão online pelo governo do Irã tem dependido em larga escala de filtragem de Internet e ameaça de ação legal. A declaração do porta voz da Guarda Revolucionária para lançar dez mil blogs escritos por membros da Basij, uma associação iraniana voluntária paramilitar, indica uma adoção de estratégias diferentes para modificar a informação online: uma guerra de palavras apoiada pelo governo na Internet.