



UNIVERSIDADE DE BRASÍLIA - UnB
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

WILLIAM HIDEKI TASHIRO
MATRÍCULA 09/0135792

“DIREITO AO ANONIMATO NA INTERNET”

Brasília, DF

2015

WILLIAM HIDEKI TASHIRO

“DIREITO AO ANONIMATO NA INTERNET”

Monografia apresentada ao final do curso de graduação em Direito da Faculdade de Direito da Universidade de Brasília como requisito para obtenção do grau de Bacharel em Direito.

Orientador: Professor Doutor Alexandre Veronese

Brasília, DF

2015

WILLIAM HIDEKI TASHIRO

“DIREITO AO ANONIMATO: INTERNET E REGULAÇÃO”

Monografia apresentada ao final do curso de graduação em Direito da Faculdade de Direito da Universidade de Brasília como requisito para obtenção do grau de Bacharel em Direito.

Orientador: Professor Doutor Alexandre Veronese

Brasília, 8 de julho de 2015

Banca Examinadora:

Prof. Doutor Alexandre Veronese

Orientador

Prof^a. Doutora Christiana Freitas

Integrante da Banca Examinadora

Prof. Mestre Paulo Rená da Silva Santarém

Integrante da Banca Examinadora

Prof. Doutor Evandro Piza Duarte

Integrante da Banca Examinadora

À Keiyti,
Meu eterno professor.

Agradecimentos

Agradeço meus pais sem os quais eu não seria nada do que fui, sou, ou poderei ser na vida. Obrigado Sra. Mari por me educar tão bem e cuidar de mim em todos os momentos da minha vida. Obrigado Sr. Keiyti por ter me ensinado tanto mesmo depois de tanto tempo.

Agradeço à minha família que, mesmo distante, sempre me recebeu com carinho nas poucas oportunidades em que pude encontrá-los.

Agradeço à Juliana, que nunca saiu do meu lado nos meus momentos mais difíceis.

Agradeço aos meus amigos de infância, Lucas e Arthur, que são a definição de amizade leal e duradoura. Um obrigado em especial para Lucas, cujas conversas moldaram boa parte de quem eu sou.

Agradeço aos meus amigos Chico, Diogo, Few, Ganso, Gay, Guiga, Murilo, Máfia, Pips e Puff, por me fazerem vivenciar os momentos mais memoráveis da minha vida.

Agradeço aos meus amigos Abhner, Bruna, Davi, Fernanda, Dudu, Gisela, Guilherme, João, Jivago, Júlio, Luisa, Marcello, Mari, Rafael, Taísa e Victor, pela companhia durante aulas incríveis e aulas terríveis, e todos os momentos entre elas.

Agradeço aos meus amigos César, Dudu, Fuku, Henrique, Hide, Leo, Marcelão, Marquinhos, Paulinho, Piapi, Ricardo, Tsuzaki e Tutu por me ensinarem o que é ser em grupo.

Agradeço aos meus amigos Ramon, Waru, Diaslos, Tytee, Mateus, Metal, Lipe e Pex por me mostrarem que a derrota também é divertida.

Agradeço à Mimi, Ricky, Aki, Nicky, Yuki, Kira, Machão, Pretinho, Cotinha e Tinha, por me trazerem tanta alegria e me ensinarem a amar todos os animais.

“If all mankind minus one, were of one opinion, and only one person were of the contrary opinion, mankind would be no more justified in silencing that one person, than he, if he had the power, would be justified in silencing mankind.”

-John Stuart Mill

Resumo

O direito ao anonimato é desdobramento do direito à privacidade, e apresenta uma variedade abundante de efeitos, sobretudo se considerado em sua dimensão de grupo. Presente desde os primórdios da Internet, seu lugar na *web* e sua sobrevivência no mundo digital moderno tem sido colocada em cheque conforme a sociedade demanda por uma maior regulação do cyberspaço. Diante deste novo panorama digital, a melhor chance do direito ao anonimato é se articular para que seja lembrado o seu fundamental papel em uma sociedade democrática.

Palavras-chave: Internet, Anonimato, Regulação, Privacidade, Psicologia

Abstract

The right to anonymity is a development of the right to privacy, and displays a large array of effects, even more so considering its dimension in groups. Around since the start of the Internet, its place in the web and its survival in the modern digital world has been put in check as society demands for an increased regulation of the cyberspace. In wake of this new digital landscape, the best chance the right to anonymity has is to articulate itself to remind all its fundamental purpose in a democratic society.

Keywords: Internet, Anonymity, Regulation, Privacy, Psychology



"On the Internet, nobody knows you're a dog."

Sumário

Introdução	1
1. Sobre o Direito ao anonimato	4
1.1 O anonimato na Internet	5
1.1.1 Os principais grupos de defesa aos direitos digitais	6
1.2 Os efeitos positivos e negativos do anonimato na Internet.....	8
1.2.1 A hipótese de equalização e o efeito de desinibição online.....	9
1.2.2. A teoria do modelo de identidade social dos efeitos da desindividualização (SIDE)	11
1.3 O direito ao anonimato no Brasil.....	12
2. Sobre a regulação da Internet	17
2.1 Por que obedecemos às leis?.....	18
2.2 Lessig e a regulação do cyberspaço	21
2.2.1 A arquitetura da regulação	23
3. Perspectivas harmônicas para o anonimato no futuro	24
3.1 Anonimato Revogável	25
3.2 Sistemas de Listas Negras Anônimas	26
3.3 Modelo harmônico de Lessig.....	27
Conclusão	28
Referências bibliográficas	30

Introdução

A invenção do microcomputador pessoal aliada à criação da rede mundial de computadores foram os fatores determinantes para a consolidação da chamada sociedade da informação pós-moderna. Ainda que não haja consenso para uma acepção universal do termo, a definição geralmente aceita é de que a sociedade da informação é aquela que intensificou o uso da tecnologia da informação para transformações de ordem social, econômica, cultural e política. Parafraseando Lyotard: enquanto o modernismo é uma condição cultural caracterizada pela constante mudança em favor do progresso, o pós-modernismo é o ápice deste processo, no qual a constante mudança tornou-se *status quo* e a ideia de progresso tornou-se obsoleta.

A internet, aclamada hoje como o instrumento primordial de integração global, popularizou-se com força na década de 1990, oferecendo uma rede mundial de transmissão de dados que eliminaria as barreiras espaciais e temporais de interação. A ferramenta de informação, nascida para a guerra, cresceu para adquirir um grande potencial democratizador e contra-hegemônico, fomentando, com suas infinitas possibilidades, o que parece ser um ambiente ideal para intermediar debates deliberativos e estimular o envolvimento do público. O direito, entretanto, essencial em todo ambiente no qual ocorre interação humana, encontrou dificuldades em regular tal espaço, justamente em virtude de seu caráter descentralizado.

Com o crescimento do número de usuários da Internet e sua expansão generalizada a todos os setores da sociedade, a regulação da Internet acabou se tornando uma tarefa árdua, sobretudo quando se deve articular os direitos, garantias e deveres preexistentes dos indivíduos, agora apresentando-se também em uma dimensão de cidadãos-internautas. O aumento da velocidade/quantidade de transmissão de dados viabilizou a pirataria de propriedade intelectual com alta eficiência, gerando, em seu turno, a propositura de leis como a SOPA¹, PIPA², e ACTA³, todas em defesa do direito autoral e em oposição da liberdade de navegação, expressão e utilização da *web*. A introdução de projetos de lei que restringiriam a liberdade do usuário tinha sido até então inédita, e reuniu a comunidade internauta para protestar contra sua aprovação. Na figura

¹ Stop Online Piracy Act

² Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act

³ Anti-Counterfeiting Trade Agreement

do grupo *Anonymous*, ganhou força o hacktivismo, movimento que se utiliza da rede de computadores para, munidos de conhecimentos e ideologias típicos de *hackers*, promover o ativismo político, geralmente com o objetivo de apoiar a liberdade de expressão, os direitos humanos e a liberdade de informação. Outra figura proeminente no movimento hacktivista é a *WikiLeaks*, uma organização jornalística internacional e sem fins lucrativos que tem como objetivo publicar informações confidenciais de governos, consideradas sigilosas ou importantes.

Ao mesmo tempo, o mundo assistiu ao acontecimento da Primavera Árabe, a onda de protestos, manifestações e rebeliões democráticas que revolucionaram a ordem de poder e depuseram os líderes de países como Egito, Tunísia, Líbia e Iêmen, parcialmente em razão do vazamento pela *WikiLeaks* de documentos que evidenciaram a corrupção e autoritarismo desses governos. As mídias sociais tiveram um papel fundamental na organização, comunicação e disseminação de informações necessárias para a articulação das manifestações, uma vez que a imprensa e os meios de comunicação tradicionais estavam comprometidos pelo controle estatal, provando o caráter contra-hegemônico da Internet e seu valor como veículo de comunicação descentralizado.

Finalmente, em 2013, o então funcionário da NSA⁴ Edward Snowden vazou uma série de documentos que denunciaram programas de vigilância globalizada fundadas em tratados secretos, um sistema de espionagem massiva que possui capacidades intrusivas de comunicações eletrônicas em todo o mundo, e com alcance ilimitado. A revelação causou revolta na comunidade global e nos governos espionados, pondo em cheque a privacidade de todos os indivíduos e gerando o debate sobre o direito à privacidade na era digital. A Internet agora se revelara uma ferramenta perigosa, passível de ser manipulada para extrair os dados de cada indivíduo, se necessário, sob a justificativa de proteção da paz e do antiterrorismo.

Da criação da Internet e da comunidade internauta, até o amadurecimento de ambas, podemos ver como o panorama global tem mostrado cada vez mais a necessidade de regulações, prerrogativas e contramedidas. É precisamente nessa seara que pretendo realizar minha pesquisa. A partir daqui, portanto, surge um questionamento: como devemos articular os direitos e deveres do cidadão com a regulação da Internet? Existe espaço para o anonimato na Internet?

⁴ National Security Agency – Órgão de Inteligência americano

Para responder essas perguntas, realizarei um estudo comparativo entre o direito ao anonimato e seus horizontes no campo da regulação da Internet. Começo este trabalho com a explicação dos conceitos de direito à privacidade e direito ao anonimato. No capítulo primeiro, procuro explicar o impacto do anonimato na esfera digital e as teorias dominantes de seus efeitos em grupo. Após comentar a situação do direito ao anonimato no Brasil, prossigo para o capítulo seguinte, no qual investigo o porquê de termos uma consciência normativa tão fraca quando tratamos de Internet, e passo a analisar a proposta de Lessig para a regulação da Internet. Finalmente, encerro com a verificação da possibilidade de sistemas e modelos que valorizem o uso benéfico do anonimato e punam o uso prejudicial, harmonizando os conceitos de anonimato e regulação no âmbito da Internet.

Para a realização deste trabalho foi feita pesquisa de referências bibliográficas especializadas nos temas de direito digital, direito ao anonimato, direito à privacidade, psicologia do anonimato, psicologia comportamental, sistemas anônimos e governança digital. Foram consultados, ainda, artigos de periódicos, jornais e sites de notícias, todos referenciados. Todas as citações consultadas no original em língua estrangeira são apresentadas em tradução livre, acompanhadas do texto original em nota de rodapé.

Capítulo 1 - Sobre o Direito ao Anonimato

Primeiramente, devemos estabelecer o que é anonimato. O anonimato é condição na qual o nome de uma pessoa é desconhecido. Mais ainda, a pessoa é não-identificável, não-localizável e não-alcançável. O direito ao anonimato se relaciona intimamente ao direito à privacidade, e ao mesmo tempo em que é um desdobramento dele, também com ele se confunde de acordo com as interpretações do que é a privacidade e do que é o anonimato, como veremos a seguir.

O direito ao anonimato é aceito como um dos direitos de privacidade. A esfera da privacidade, por sua vez, se intersecciona com os conceitos de segurança e proteção de informação, e o direito a não ter a privacidade invadida se encontra elencado na Declaração Universal de Direitos Humanos, em seu artigo 12, que diz:

"Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques."

O direito à privacidade pode ser definido como “o direito a manter um domínio à nossa volta, que inclui tudo o que é parte de nós, como nosso corpo, lar, propriedade, pensamentos, sentimentos, segredos e identidade. O direito à privacidade nos dá a habilidade de escolher quais partes nesse domínio pode ser acessado por outros, e de controlar a extensão, maneira e tempo do uso dessas partes que escolhemos revelar.”⁵O direito à privacidade possui, ainda, uma miríade de dimensões, dentre as quais quatro são pertinentes para nosso estudo:

a) **o direito a ser deixado em paz**⁶: direito de uma pessoa a se isolar da atenção de outros se assim ela desejar, e o direito de estar imune ao escrutínio e de ser observado em ambientes privados, como o próprio lar;⁷

⁵ “The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.” (ONN et. al., 2005)

⁶ “Right to be let alone” (SOLOVE, 2008)

⁷ “right of a person to choose seclusion from the attention of others if they wish to do so, and the right to be immune from scrutiny or being observed in private settings, such as one’s own home” (SOLOVE, 2008) pp. 15-17

b) **a limitação de acesso**: se refere a habilidade de uma pessoa a participar na sociedade sem que outros indivíduos ou organizações colem informações sobre ela⁸;

c) **o controle sobre a informação**: a reivindicação de um indivíduo, grupo, ou instituição de determinar para eles mesmos quando, como e até onde a informação sobre eles é comunicada para outros;⁹

d) **o sigilo**¹⁰: um tipo seletivo de sigilo no qual indivíduos mantêm algumas informações secretas e privadas, enquanto escolhem tornar outras informações públicas e não-privadas.¹¹

Decorrente dessas dimensões do direito à privacidade, portanto, o direito ao anonimato seria a faculdade de isolar completa ou parcialmente, do público geral, o domínio com o qual um alguém se cerca, sob a justificativa de controle legítimo de sua vida privada, sua intimidade, sua honra e imagem. A privacidade, de forma ampla, pode ser entendida como a capacidade de existir na sociedade de forma anônima, o que demonstra o quão intimamente interligados são os conceitos de anonimato e privacidade.

1.1 O anonimato na Internet

Os direitos de privacidade, devido a sua natureza, estão inerentemente relacionados com a tecnologia da informação, de forma que os primeiros estudos sobre sua ligação se deram no início do século XX, com a popularização do telefone como meio de comunicação rápido e à longa distância, bem como a evolução da fotografia e do crescimento do jornalismo sensacionalista. Entretanto, com a chegada da Internet e as propriedades da *Web 2.0*, o engendramento entre estes elementos alcançou um horizonte ainda não explorado: o da privacidade informacional. Com o ingresso nas mídias sociais, no cadastramento em e-mails e em grupos de relacionamento, os internautas não possuem controle sobre o armazenamento, manipulação e exibição dos dados que escolhem revelar na Internet (bem como quem possuirá acesso a eles), anulando as dimensões de controle sobre informação e de sigilo seletivo do direito à privacidade. Mais ainda, o advento dos mecanismos de busca e o desenvolvimento das técnicas de mineração de dados, a

⁸ "Limited access refers to a person's ability to participate in society without having other individuals and organizations collect information about them". (SOLOVE, 2008) p. 19

⁹ "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (SOLOVE, 2008) p. 24

¹⁰ "secrecy" (SOLOVE, 2008)

¹¹ "selective kind of secrecy in which individuals keep some information secret and private while they choose to make other information public and not private" (SOLOVE, 2008) pp.22-23

limitação de acesso também se torna anulada. A única forma de manter o controle sobre a própria privacidade é se ausentar completamente de uma identidade online.

Este panorama, é claro, aumentou o interesse sobre a utilidade do anonimato na Internet, bem como os debates sobre o seu lugar no direito. Os conceitos de privacidade e de anonimato passaram a ser revistos sob a luz das novas técnicas e tecnologias de informação.

O cientista da informação Rainer Kuhlen concebe a privacidade em sua dimensão de autonomia informacional (*informationelle Selbstbestimmung*), “a capacidade de escolher e usar autonomamente o conhecimento e a informação em um ambiente eletrônico.”¹². Esta dimensão guarda similaridade com a definição do americano Eric Hughes, um dos fundadores do movimento *cypherpunk*¹³: “Privacidade não é segredo. Um assunto privado é algo que alguém não deseja que o mundo inteiro saiba, mas um assunto secreto é algo que alguém não deseja que ninguém saiba. Privacidade é o poder de revelar-se seletivamente para o mundo.”¹⁴

1.1.1 Os principais grupos de defesa aos direitos digitais

Os *cypherpunks* podem ser entendidos como a vanguarda do anonimato na Internet; o que há de mais extremo na defesa do anonimato e da criptografia como essenciais para uma sociedade digital. Os ativistas *cypherpunks* defendem o uso da criptografia como fio condutor de transformações sociais e políticas, acreditam que a privacidade é necessária na era digital, e que ela deve ser conquistada (e não esperada) por meio da criptografia. São contrários a qualquer tipo de regulação criptográfica, e são dedicados e construir sistemas anônimos. O meio para isso é a redação de código, publicados internacional e gratuitamente, independente da aprovação de terceiros (HUGHES, 1993). Um grande número de personalidades da indústria computacional são *cypherpunks*, dentre os quais pessoas como Jacob Appelbaum (criador do *Tor*¹⁵) e Julian Assange (fundador do *WikiLeaks*). Suas conquistas viabilizaram a criação da moeda

¹² “the capacity to choose and use autonomously knowledge and information in an electronic environment” (KUHLEN, 2004)

¹³ O *cypherpunk* é a junção do termo *cyberpunk*, no sentido do espírito do individualismo no ciberespaço, e da criptografia.

¹⁴ “Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.” (HUGHES, 1993)

¹⁵ Software de comunicação anônima

digital (ou virtual), como o *BitCoin*, bem como a criação do *CryptoParty*, um projeto global de conscientização para a prática e importância da criptografia.

Os *cypherpunks* possuem visões, no geral, extremistas, e devem ser entendidos como tal. Para eles, a criptografia e a privacidade ocupam o mais alto patamar de essencialidade no contrato social e em qualquer tipo de interação humana. É preciso limitar o escopo dessa filosofia para obtermos uma visão mais crítica do panorama geral. Uma sociedade ideal para os *cypherpunk*, por exemplo, existirá com um forte sistema criptográfico, o que certamente acarretará em riscos de segurança quando explorados pelo crime e pelo terrorismo. Apesar disso, vemos como acertada o ideal de que o discurso anônimo é vital para uma sociedade transparente e livre, assim como para uma genuína liberdade de expressão – a centralidade da filosofia *cypherpunk*.

John Gilmore, outro fundador do movimento cypherpunk, se juntou à John Barlow e Mitch Kapor para criar a ONG *Electronic Frontier Foundation*, em resposta a uma série de ações governamentais que demonstraram o nível de desinformação das autoridades sobre as formas de comunicação online (JONES, 2003), bem como a necessidade crescente de proteção dos direitos civis da Internet. A EFF rapidamente tornou-se uma aliada da defesa dos direitos digitais, providenciando fundos para defesa legal, participação como *amicus curiae*, defendendo indivíduos e tecnologias daquilo que considera ameaças legais sem fundamento, expondo condutas ilegais do governo, providenciando orientação a governos e tribunais, organizando ações políticas e correspondências em massa, apoiando a novas tecnologias que acredita preservar liberdades pessoais, mantendo um banco de dados e websites de notícias pertinentes, monitorando e confrontando leis em potencial que acredita poder interferir em liberdades pessoais e uso justo, e solicitando listas do que acredita ser abuso de patente para derrotar aqueles que consideram sem mérito.¹⁶ Dentre suas conquistas, a EFF recebeu \$1 milhão de dólares da Google como parte de um acordo de uma *class action* relacionada a assuntos de privacidade envolvendo a *Google Buzz*, mídia social atualmente extinta. A EFF

¹⁶“EFF provides funds for legal defense in court, presents amicus curiae briefs, defends individuals and new technologies from what it considers baseless or misdirected legal threats, works to expose government malfeasance, provides guidance to the government and courts, organizes political action and mass mailings, supports some new technologies which it believes preserve personal freedoms, maintains a database and web sites of related news and information, monitors and challenges potential legislation that it believes would infringe on personal liberties and fair use, and solicits a list of what it considers patent abuses with intentions to defeat those that it considers without merit.”
ELECTRONIC FRONTIER FOUNDATION. In: WIKIPÉDIA, a enciclopédia livre, Flórida: Wikimedia Foundation, 2015. Disponível em: < https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation>. Acesso em 30 de junho de 2015.

continua atuando como defensora dos direitos digitais, agindo como defensora dos direitos digitais e, em menor grau, dos ideais *cyberpunks*¹⁷.

Por último, o grupo *Anonymous* é a frente popular do hacktivismo. Originado em 2003 no fórum de imagens 4chan, o grupo se caracteriza pela organização anárquica, anônima entre si, e pelas atividades manifestações, campanhas e cyberataques coordenados e frequentemente em prol dos direitos digitais. Sua atuação é global e sempre a favor da liberdade de expressão e da pirataria.

1.2. Os efeitos positivos e negativos do anonimato na Internet

Para entender de maneira compreensiva os efeitos do anonimato nas interações em rede, devemos nos atentar em como o anonimato pode interferir na comunicação tanto em uma dimensão individual como em grupo. Uma das mais influentes teorias dos efeitos do anonimato no comportamento humano é controversa¹⁸ teoria de (ZIMBARDO, 1969) de desindividualização. Neste estado, os indivíduos em um grupo não são vistos como indivíduos propriamente ditos, mas, sim, percebidos como membros em um grupo, aumentando as chances para que diminuam seu autocontrole em campos como a culpa, vergonha, medo e comprometimento, levando a um comportamento que estaria, outrora, inibido. O anonimato, portanto, não quer dizer, necessariamente, que um indivíduo esteja invisível, bastando que outras pessoas não consigam identificar aquela pessoa como indivíduo para tanto. O conceito guarda similaridade com àquele de (LUNDBLAD, 2004) de *noise society*¹⁹, uma sociedade na qual os custos para a vigilância vão aumentar de acordo com a quantidade de informação pessoal criada. O ruído, entendido como tudo o que interfere a um terceiro de extrair informação privada, irá aumentar de tal forma a dificultar o processo como um todo, diminuindo a expectativa coletiva de privacidade, mas aumentando a expectativa individual de privacidade.

No campo do anonimato nas comunicações em rede, os efeitos positivos do anonimato podem ser generalizados na proteção de identidade, no aumento de eficiência de grupos de trabalho e no empoderamento de indivíduos marginalizados. Os

¹⁷“Esse é o tipo de sociedade que quero construir. Quero a garantia – com física e matemática, não com leis – que podemos dar a nós mesmos a real privacidade de comunicações pessoais.” Home Page de John Gilmore. Disponível em: <http://www.toad.com/gnu/>. Acesso em 1º de julho de 2015

¹⁸ Críticos da teoria afirmam que o estado de desindividualização não está necessariamente ligado ao ambiente, e sim a própria noção do indivíduo de autoconsciência (Christopherson, 2007)

¹⁹ “sociedade de ruído”

efeitos negativos podem ser generalizados em comportamento predatório sobre menores por meio de disfarce de identidade, intensificação de ódio racial, religioso ou de outra espécie e encorajamento de comportamento anti-normativo. (Christopherson, 2007)

Entretanto, no que toca o anonimato nas interações em grupo, são duas as teorias predominantes: A hipótese de equalização e a teoria do modelo de identidade social dos efeitos da desindividualização (SIDE²⁰, no inglês). Ainda que, atualmente, a teoria SIDE seja tida como a mais completa para explicar como o anonimato afeta as comunicações em rede, a hipótese de equalização é bem informativa no sentido de explicar quais os fatores tornam o internauta tão diferente de sua personalidade face-à-face. Ambas são explicadas a seguir.

1.2.1 A hipótese de equalização e o efeito de desinibição online

A hipótese de equalização considera as características da comunicação em rede para traçar a proposição de que neste ambiente o plano de comunicação se torna nivelado. Na visão desta pesquisa, o trabalho que melhor descreve as particularidades da interatividade online é o artigo de (SULER, 2004) sobre o efeito de desinibição online. É o efeito que ocorre quando há o relaxamento ou abandono de restrições sociais e inibições psíquicas em interações na internet, e que estariam presentes caso tais interações ocorressem face-à-face. Esta condição faz com que algumas pessoas exibam, enquanto online, certo comportamento de forma mais frequente ou mais intensa do que exibiriam pessoalmente. Alguns indivíduos podem demonstrar uma tendência a compartilhar sentimentos pessoais, revelar emoções, medos e desejos, assim como agir com incomum simpatia e generosidade. É a chamada desinibição benigna. Outros indivíduos, entretanto, podem agir ou se expressar de forma cruel, usando de xingamentos, críticas, raiva, ódio e até mesmo ameaças, sem que tenham medo de uma punição significativa. É o que Suler chama de desinibição tóxica.

O autor explora seis fatores que interagem entre si para criar esse efeito de desinibição: anonimato dissociativo, invisibilidade, assincronia, introjeção solipsista, imaginação dissociativa, e minimização de autoridade. Todos esses fatores são, por sua vez, influenciados pela personalidade única de cada indivíduo.

O anonimato dissociativo: é a própria noção de anonimato da internet. Quando as pessoas têm a oportunidade de dissociar seu comportamento de sua identidade

²⁰ "Social identity model of deindividuation effects" (Christopherson, 2007)

peçoal, elas se tornam menos vulneráveis para agir conforme desejam, sem que isso se ligue publicamente às suas vidas normais. Esse tipo de proteção permite que os usuários da internet se expressem sem precisar se inibir, mas, ao mesmo tempo, possibilita um comportamento antissocial sem qualquer prejuízo.

Invisibilidade: compartilhando de características do anonimato, a invisibilidade na internet se refere à remoção do físico nas interações online. Dessa forma, ainda que se saiba a identidade do interlocutor, retirando seu anonimato, a inibição diminui pelo simples fato de não ser possível ver, fisicamente, um ao outro. Isso se dá pela impossibilidade de percepção de sinais visuais ou sonoros, o que diminui, ou retira por completo, a preocupação com tais fatores de interação.

Assincronia: a assincronia da interação online permite que dois interlocutores conversem sem precisar de respostas em tempo real. Isso retira o fluxo constante de ações e reações, o que tenderia a fazer com que ambos agissem de acordo com o padrão das normas sociais. Na internet, onde há uma suspensão nesse tempo de reação, as pessoas podem pensar e escrever mais fielmente às suas verdadeiras emoções e pensamentos, sejam eles de natureza benigna ou tóxica.

Introjeção solipsista: na ausência de estímulos visuais, a mente humana irá atribuir características específicas para um indivíduo com quem interage na internet. A leitura da mensagem de outra pessoa pode criar um conjunto de imagens de como tal pessoa se parece, ou como soa, todas influenciadas pelo seu próprio conjunto cognitivo. A construção de uma personalidade que se projeta em outro pode transformar a realidade daquela pessoa em uma outra realidade criada pelo seu interlocutor.

Imaginação dissociativa: combinando a introjeção solipsista com a imaginação, produz-se um sentimento de escapismo no qual a internet se torna um refúgio, um universo diferente no qual não é preciso lidar com as responsabilidades e demandas do mundo real, separando, assim, o mundo online do mundo *offline*. Essa separação faz com que as pessoas acreditem que o mundo online é uma espécie de jogo, com regras e costumes que não se aplicam na vida real, podendo transitar entre ambos os mundos obedecendo cada conjunto de normas de forma separada.

Minimização de autoridade: no mundo virtual, o status social de determinado indivíduo não tem tanto impacto como na vida real. Fatores como vestimenta, linguagem corporal, e ambientação reduzem o impacto que seu status comanda. Na internet em geral, o plano de troca de ideias é igual para todos, o que significa que o poder de influência consiste, em grande parte, no poder de comunicação de um indivíduo

e na qualidade de suas ideias. Na mesma esteira, as pessoas não têm a relutância que teriam ao falar pessoalmente diante de grandes autoridades, pois na internet existe a sensação de equivalência, com qual as pessoas se sentem mais confortáveis para se expressar, bem ou mal.

A pesquisa de Suler é fundamental para que se entenda a dissociação que ocorre entre o mundo *offline* e o mundo online, no qual as regras e restrições sociais ficam temporariamente suspensas ou enfraquecidas. Dentre estes seis fatores, os que se apresentam como mais relevantes podem ser simplificados ao anonimato do usuário e à dissociação entre as regras do mundo real e sua importância para o mundo virtual. São regras sociais que não acompanham a transição do indivíduo entre o mundo real e o mundo virtual, da mesma forma que ocorre com as leis em geral, fazendo com que um indivíduo que obedeceria a lei no mundo real, transgrida-as quando passa a interagir em sua identidade online.

1.2.2. A teoria do modelo de identidade social dos efeitos da desindividualização (SIDE)

A teoria do SIDE é uma reinterpretação da teoria de (ZIMBARDO, 1969) de desindividualização, colocando ênfase nas variáveis específicas da situação em um cenário social. Ela possui o componente cognitivo e o componente estratégico.

O componente cognitivo diz que o anonimato nas comunicações em rede fortalece o impacto das normas sociais quando a identidade social (identificação com o grupo) do indivíduo é forte, ao passo que enfraquece o impacto das normas sociais quando a identidade pessoal (identificação com si próprio) é predominante. Dessa forma, as normas sociais são mais prováveis de serem seguidas quando o indivíduo tem um senso de identidade social mais elevado que um senso de identidade pessoal. Na mesma esteira, a teoria SIDE explica que quando todos os membros de um grupo são anônimos entre si, a importância do grupo aumenta e seus membros terão uma forte identidade conjunta. Entretanto, se todos os membros são identificáveis por um indivíduo, e aquele indivíduo permanece anônimo para o restante, esse único indivíduo anônimo terá uma forte identidade pessoal, e pode não agir de acordo com os objetivos do grupo (Spears & Lea, 1992). Em suma, a teoria sugere que, para que todos os membros do grupo trabalhem juntos para objetivos conjuntos, e não pessoais, todos os membros do grupo devem estar identificados visualmente, ou todos devem estar anônimos.

O componente estratégico da teoria SIDE explica que uma vez que as pessoas entendessem como o anonimato afeta a comunicação interpessoal na Internet,

elas passariam a utilizar esse conhecimento para usar o anonimato de forma estratégica para satisfazer seus próprios objetivos e necessidades de comunicação. (Spears & Lea, 1992) Um uso óbvio dessa dimensão do anonimato se mostra quando um grupo minoritário deseja expressar uma opinião controversa àquela da maioria, por exemplo. Outro aspecto relevante é o de gênero, sobre o qual (Flanagin et. al., 2002) pesquisou e descobriu a maneira como os homens tendem a reduzir a quantidade de anonimato nas comunicações em rede, ao contrário das mulheres, que preferem manter o anonimato presente na comunicação. Isso é um indício de que a mulher pode estar tentando reduzir o *gap* de poder sub-reptício geralmente presente na comunicação face-à-face, sendo estratégico o uso do anonimato na comunicação em rede para manter um nível de poder equiparado ao do homem.

O anonimato nas comunicações em rede possui tanto efeitos positivos como negativos, quase que simetricamente. Ao conferir eficiência na propagação do discurso da minoria, por exemplo, o anonimato pode conceder um pedestal sobre o qual o discurso de ódio pode ser vocalizado, tornando a organização pela Internet um meio pelo qual a harmonia social fique prejudicada. Por outro lado, se um grupo minoritário, como a parcela LGBT da população, conseguir se organizar pela Internet para fazer um *lobby* por direitos próprios, a efetividade de grupos anônimos poderia beneficiar a sociedade com um caráter emancipador. A ferramenta de empoderamento de setores marginalizados, afinal, é a mesma. A diferença reside no modo como será utilizado o componente estratégico da teoria SIDE, ou seja, como um grupo ou indivíduo irá se utilizar do anonimato para impactar a sociedade com um comportamento pró-social ou antissocial.

1.3 O direito ao anonimato no Brasil

O Brasil passou por um verdadeiro *boom* na quantidade de usuários e no tempo gasto online²¹, do início do milênio até os dias atuais. O fenômeno da Internet no Brasil, como tem sido chamado²², se deu de forma rápida e desenfreada, tornando a regulação da Internet mais difícil e mais caótica do que vista em países onde o

²¹Disponível em:

<<https://www.telegeography.com/products/commsupdate/articles/2004/05/25/brazilians-spend-the-most-time-on-the-internet/>> Acesso em: 30 de junho de 2015

²²Brazilian Internet phenomenon. In: WIKIPÉDIA, a enciclopédia livre, Flórida: Wikimedia Foundation, 2015. Disponível em <https://en.wikipedia.org/wiki/Brazilian_Internet_phenomenon>. Acesso em 30 de junho de 2015.

crescimento se deu naturalmente. Pelo mesmo motivo, a infraestrutura em nível nacional também encontrou dificuldades em se adaptar a um mercado que logo se tornou um dos maiores do mundo²³, atrasando enormemente a disponibilidade de um serviço consistente, veloz, e abrangente, tendo se equiparado a um padrão global apenas nos últimos anos.

Em razão de tudo isso, o direito informático sofreu um desenvolvimento retardado na academia brasileira. Ora, é natural que o interesse nas questões de direito da Internet cresça em razão de uma penetrabilidade ampla do serviço de Internet em todas as camadas da sociedade, o que antes não era possível; sobretudo quanto à regulação e controle de seu uso. Apesar disso, o direito digital, ainda é, infelizmente, uma área nova e pouco explorada na academia nacional. A relevância deste ramo do direito tem se provado gritante tanto no cotidiano do cidadão comum quanto no âmbito político, com a dicotomia entre dois projetos de lei: a Lei Azeredo e o Marco Civil. O primeiro restringe a liberdade em favor da regulação, e o segundo tem a neutralidade de rede²⁴ como princípio disciplinador da Internet. O Marco Civil foi aprovado em Senado e sancionado pela Presidenta Dilma Roussef em abril de 2014²⁵, enquanto o projeto da Lei Azeredo foi aprovado após ter sido alterado para conter principalmente a tipificação de delitos informáticos de invasão²⁶, muito menos polêmicos. O triunfo do Marco Civil, na forma como foi aprovado, marcou um passo importante na edificação de uma regulação informática em sintonia com os conceitos de neutralidade de rede, privacidade, e liberdade de expressão, ainda que represente apenas o começo de um longo trabalho de regulação.

Parece estranho, entretanto, falar de direito ao anonimato quando a Constituição Federal de 1998, em seu artigo 5º, IV, expressa que “é livre a manifestação do pensamento, sendo vedado o anonimato;”. A mesma vedação também aparece no texto da antiga na antiga Lei de Imprensa²⁷, em seu artigo 7º:

Art . 7º No exercício da liberdade de manifestação do pensamento e de informação não é permitido o anonimato. Será, no entanto, assegurado e respeitado o sigilo quanto às fontes ou

²³Disponível em:< <http://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries/>> Acesso em: 30 de junho de 2015.

²⁴A neutralidade da rede (ou neutralidade da Internet, ou princípio de neutralidade) significa que todas as informações que trafegam na rede devem ser tratadas da mesma forma, navegando a mesma velocidade. Neutralidade da rede. In: WIKIPÉDIA, a enciclopédia livre, Flórida: Wikimedia Foundation, 2015. Disponível em <https://pt.wikipedia.org/wiki/Neutralidade_da_rede>. Acesso em 30 de junho de 2015.

²⁵ LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

²⁶ LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

²⁷ LEI Nº 5.250, DE 9 DE FEVEREIRO DE 1967

origem de informações recebidas ou recolhidas por jornalistas, radiorepórteres ou comentaristas.

Fica patente, levando em consideração o tema deste trabalho, a necessidade de nos debruçar sobre esta seara e analisar esta vedação. Como já vimos, o direito ao anonimato é um desdobramento do direito à privacidade, que, por sua vez, possui uma diversidade de dimensões. O dispositivo constitucional, entretanto, se refere, claramente, ao anonimato no âmbito da livre manifestação de pensamento, e não ao anonimato como extensão do direito à privacidade. Impossível seria, nesse caso, pois a CRFB/88 tem o direito à privacidade como direito fundamental, insculpido no Art. 5º, X. "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

O anonimato em questão já foi alvo de discussão pelo STF no MS 24.369-DF, sobre a validade da delação anônima perante o Tribunal de Contas da União. Nele, pronunciou-se o relator Min. Celso de Mello:

O veto constitucional ao anonimato, como se sabe, busca impedir a consumação de abusos no exercício da liberdade de manifestação do pensamento, pois, ao exigir-se a identificação de quem se vale dessa extraordinária prerrogativa político-jurídica, essencial à própria configuração do Estado democrático de direito, visa-se, em última análise, a possibilitar que eventuais excessos, derivados da prática do direito à livre expressão, sejam tornados passíveis de responsabilização, "a posteriori", tanto na esfera civil, quanto no âmbito penal.

Essa cláusula de vedação - **que jamais deverá ser interpretada como forma de nulificação das liberdades do pensamento** - surgiu, no sistema de direito constitucional positivo brasileiro, com a primeira Constituição republicana, promulgada em 1891 (art. 72, § 12), que objetivava, ao não permitir o anonimato, inibir os abusos cometidos no exercício concreto da liberdade de manifestação do pensamento, viabilizando, desse modo, a adoção de medidas de responsabilização daqueles que, no contexto da publicação de livros, jornais ou panfletos, viessem a ofender o patrimônio moral das pessoas agravadas pelos excessos praticados, consoante assinalado por eminentes intérpretes daquele Estatuto Fundamental (JOÃO BARBALHO, "Constituição Federal Brasileira - Comentários", p. 423, 2ª ed., 1924, F. Briguiet; CARLOS MAXIMILIANO, "Comentários à Constituição Brasileira", p. 713, item n. 440, 1918, Jacinto Ribeiro dos Santos Editor).

Vê-se, portanto, tal como observa DARCY ARRUDA MIRANDA ("Comentários à Lei de Imprensa", p. 128, item n. 79, 3ª ed., 1995, RT), que **a proibição do anonimato tem um só propósito, qual seja, o de permitir que o autor do escrito ou da publicação possa expor-se às consequências jurídicas derivadas de seu comportamento abusivo**: "Quem manifesta o seu pensamento através da imprensa escrita ou falada, deve

começar pela sua identificação. Se não o faz, a responsável por ele é a direção da empresa que o publicou ou transmitiu.”²⁸
(grifo meu)

No voto, o Min. Celso de Mello é claro ao assinalar o propósito da vedação constitucional, qual seja, o de responsabilizar “aqueles que, no contexto da publicação de livros, jornais ou panfletos, viessem a ofender o patrimônio moral das pessoas agravadas pelos excessos praticados (...)”. O mesmo entendimento é encontrado também nos comentários da doutrina, inclusive sobre a Lei de Imprensa. Comenta o professor Celso Bastos:

Por isso mesmo, a Constituição estabelece um **sistema de responsabilidade** e o faz, proibindo o anonimato, que é a forma mais torpe e vil de emitir-se o pensamento. Lembre-se que o anonimato pode consistir, inclusive, em artigo assinado por pseudônimo desconhecido. A Lei de Imprensa cuida disso no §4, do art. 7º. A proibição do anonimato não significa necessariamente que debaixo de cada texto, figure o nome do autor, pois isso acabaria com a prática da edição de editoriais. **A Constituição demanda a existência de um responsável pela matéria veiculada**, não exigindo a correspondência deste nome com a do autor real do comentário.²⁹

Corroborando Manuel Alceu Afonso Ferreira:

Em ambos os preceitos, seja o da Constituição (art.5º, IV), seja o da Lei de Imprensa (art.7º, caput), as referências à vedação daquilo que neles se denomina “anonimato” tem, por objetivo [definir] sempre um responsável, sobre o qual recairá, se abusiva, a persecução civil ou criminal conseqüente. **Ou seja, por qualquer emissão intelectual, na forma de informação, comentário ou opinião, alguém, seja ou não o seu direto autor, responsabilizar-se-á.** (...) a proibição da anonimidade não significa embaraço a que as produções do intelecto possam não ter identificado o autor, mas, isto sim, impeditivo a que por elas não exista responsável.³⁰

E também Ives Gandra Martins:

Desta forma, tanto a vedação ao anonimato quanto ao sigilo de fontes são princípios da mesma hierarquia normativa, ou seja, são princípios constitucionais, devendo ambos nortear a atividade jornalística, vale dizer, é vedado o anonimato mas garantido o sigilo da fonte da informação sempre que necessário ao exercício da profissão. Ao nosso ver, os dois princípios não são conflitantes.³¹

²⁸MS 24.369-DF. Disponível em <http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm>>. Acesso em: 1º de julho de 2013.

²⁹ Artigo do Instituto Gutenberg sobre a interpretação do anonimato na Constituição e na Lei de Imprensa. Disponível em: <http://www.igutenberg.org/lei6.html>. Acesso em: 1º de julho de 2013.

³⁰ Artigo do Instituto Gutenberg sobre a interpretação do anonimato na Constituição e na Lei de Imprensa. Disponível em: <http://www.igutenberg.org/lei6.html>. Acesso em: 1º de julho de 2013.

³¹ Ibidem.

Diante do extraído, fica claro como a vedação do anonimato possui suas origens na Constituição de 1891 e na Lei de Imprensa, ambas preocupadas em inibir abusos da liberdade de expressão de pensamento. Percebe-se, com evidência, que a tradição civil do direito brasileiro não prioriza a livre manifestação de pensamento no ordenamento jurídico, relativizando-a em favor da facilidade em responsabilizar, diferente de países como os Estados Unidos, no qual é permitido, inclusive, o discurso do ódio (contanto que não provoque violência iminente) sob a proteção da Primeira Emenda.

De toda forma, o inferido da literatura jurídica brasileira é que a vedação ao anonimato se preocupava em evitar abusos contra o patrimônio moral das pessoas através de acusações ou imputações infundadas, com o objetivo de minar a imagem pública e a honra de um indivíduo ou organização. Principalmente na figura das denúncias anônimas falsas, entendeu o legislador que o anonimato causaria insegurança jurídica na falta de alguém para responsabilizar, caso ficasse provado que a denúncia havia sido realizada de má-fé. Mesmo a jurisprudência do STF, quanto a matéria de anonimato, discute a delação anônima e sua legalidade³², sem menção de direito eletrônico. Isso é, sem dúvida, reflexo das possibilidades jurídicas ainda não exploradas, bem como a academia nacional pouco desenvolvida quando dizem respeito aos direitos digitais.

Isso não quer dizer, entretanto, que o direito ao anonimato é mitigado na sua totalidade. Primeiramente, tanto pelo dispositivo constitucional em defesa à privacidade como a interpretação do STF de que a vedação “jamais deverá ser interpretada como forma de nulificação das liberdades do pensamento”³³, o direito ao anonimato como um dos direitos de privacidade está legitimamente protegido em nosso ordenamento. Em segundo lugar, os legisladores à época da Constituinte de 1988 certamente não antecipavam a opulência de informações da era digital, fazendo com que o direito ao anonimato, com todos os seus efeitos preocupações e possibilidades, não fosse enxergado, à época, no mesmo panorama que o atual. Por último, a adequação e o conceito de anonimato, na legislação, não é claro. Poder-se-ia argumentar em favor do uso de pseudônimos como alternativa ao anonimato, a capacidade de identificação por meio dos dados de IP³⁴, o uso do pré-estabelecido do anonimato em grupo, como fórum,

³² O entendimento atual, a propósito, é de que a delação anônima não obsta a abertura de inquérito.

³³ MS 24.369-DF. Disponível em

<http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm>>. Acesso em: 1º de julho de 2013.

³⁴ Internet Protocol

e a própria liberdade de expressão, conjugado com a necessidade de anonimato pelo medo de represália, ou interferência na vida profissional, entre outros. São todas possibilidades inexploradas e não discutidas em sede do Supremo Tribunal. Diante disso, a tendência de uma possível disputa legal quanto ao direito ao anonimato como realização da liberdade de expressão é otimista, mesmo com a letra fria da lei dizendo o contrário.

Perante esta conjuntura, fica manifesta a necessidade de uma regulamentação mais específica dos direitos digitais no ordenamento brasileiro. Somente no que toca o direito ao anonimato, são os abundantes os indícios de como está alheia esta seara. O cenário é otimista, entretanto, com um Marco Civil majoritariamente atento aos direitos digitais e a consulta pública para a redação do Anteprojeto de Lei para a Proteção de Dados Pessoais³⁵, nos mesmos moldes do que foi a discussão do Marco Civil.

Capítulo 2 – Sobre a regulação da Internet

Quando Habermas idealizou a conceito de esfera pública, em 1964, mencionou jornais, revistas, rádio e televisão como a mídia da esfera pública da época, onde se poderia transmitir informação e influenciar aqueles que a recebem. A internet, na forma como é hoje, é um meio de comunicação que transcende todas essas mídias, na medida em que as incorpora e, ao mesmo tempo, potencializa a eficácia de cada uma. Mais ainda, com o surgimento de fóruns, grupos de e-mail e redes sociais, o discurso social massificado é parte notória do mundo virtual e do cotidiano de seus usuários, sendo rotineira a livre discussão de assuntos que formam a opinião pública da sociedade. Para Habermas, a esfera pública é essa dimensão social que se situa entre a sociedade e o Estado, na qual todos os cidadãos têm potencial de acesso, e onde a opinião pública pode ser formada livre de interesses econômicos ou estatais. O corpo público toma forma quando os cidadãos conversam irrestritamente sobre qualquer assunto de seus interesses, com a garantia de liberdade de associação e de expressão. (HABERMAS, 1964)

A internet favorece a criação de comunidades multipartidárias e descentralizadas, na qual se encoraja o diálogo e a deliberação de todos aqueles que delas desejam participar. Dificilmente uma opinião que no mundo presencial seria marginalizada é sumariamente ignorada e isolada na *web*, contanto que o discurso seja razoavelmente compreensível e acessível a determinado público. Ademais, a redução nos

³⁵Disponível em: < <http://participacao.mj.gov.br/dadospessoais/>> Acesso em: 1º de julho de 2015

custos para se tornar um falante e emitente de opiniões possibilita que praticamente qualquer um consiga levar sua mensagem a um número considerável de pessoas, o que ampliou de maneira significativa o acesso de cidadãos comuns à esfera pública e à possibilidade de compor o corpo público. A desvantagem, porém, reside justamente na abundância de conteúdo; as opiniões e discursos agora, são tantas que os usuários podem ter dificuldade em aceitá-las com o mesmo nível de crítica e respeito. Poder-se-ia argumentar, entretanto, que tal fenômeno não é um defeito da internet como meio comunicativo, mas simplesmente um aumento da responsabilidade de seus usuários para discernir e selecionar qual o conteúdo de sua escolha, o que, ulteriormente, pode ser visto como uma melhora na autonomia dos agentes comunicativos.

De toda forma, percebemos, nessa esteira, que a Internet deve ser capaz de garantir a liberdade de expressão como requisito para que realize sua dimensão de espaço público. Obviamente, as ideias de censura e de seleção prévia de conteúdo são incompatíveis com a Internet, sob risco de inutilizar sua própria validade como espaço universal de discurso comunicativo. Dessa forma, qualquer regulação estatal deve ter a liberdade de expressão como pressuposto.

2.1 Por que obedecemos às leis?

Como já explicamos, as leis de internet possuem sua eficácia comprometida, em grande parte, devido aos próprios sujeitos legais, e pela forma como estes enxergam as leis quando encaradas por sua identidade virtual. O efeito de desinibição online afeta os usuários de internet de modo a dessensibilizar suas noções de empatia, respeito, convívio social e direitos humanos, tornando-os suscetíveis à prática de crimes cibernéticos – ou mesmo crimes comuns, só que praticados na *web* – sem que tenham a noção exata de que transgridam leis e de que estão sujeitos a suas devidas penas.

Em seu seminário³⁶, Wim Voermans explica o porquê das pessoas obedecerem às leis. Citando Lon Fuller, o professor explica que são necessários vários pressupostos para que os sujeitos legais obedeam às leis:

- a) O legislador deve pressupor a aceitação e a *compliance*³⁷ dos sujeitos legais.
- b) Os sujeitos legais devem pressupor que o Estado exerce a lei.

³⁶ Seminário realizado no Ciclo de Encontros do Projeto Pensando o Direito, realizado na Universidade de Brasília, em setembro de 2013. Disponível em: <<https://www.youtube.com/watch?v=do4v1wgASoE>>

³⁷ A tradução aproximada seria concordância/observância.

- c) A falha em quaisquer desses pressupostos ameaça o sistema como um todo.

Mais ainda, a falta de concordância é um efeito que se espalha, ou seja, influencia o comportamento de outros observadores. Leis e regras que não são observadas são, em sua essência, inúteis.

Para explicar a natureza humana do homem em sociedade, Voermans cita a obra de Steven Pinker, *Os anjos bons de nossa natureza*. Nela, Pinker introduz uma teoria diametralmente oposta à teoria do leviatã de Hobbes. Segundo ele, os humanos não são naturalmente violentos, tampouco precisam da violência como válvula de escape. Os humanos não são nem bons nem ruins, em sua natureza, mas nascem equipados de motivos que podem orientá-los para fora da violência e em direção ao cooperativismo e ao altruísmo. Sua tese é de que a violência diminuiu, assim como nossa tolerância para com ela. De acordo com Pinker, os humanos possuem cinco demônios internos (violência predatória/instrumental, dominância, vingança, sadismo e ideologismo) e quatro anjos bons (empatia, auto-controle, senso moral e razão). Enquanto os demônios se traduzem em características psicológicas que podem levar à violência, os anjos bons são motivos que podem orientá-los para longe dela. Em conclusão, a razão pela qual a violência diminuiu é que a humanidade passou por transformações históricas que favoreceram nossos motivos pacíficos e afastaram o crescimento da violência. (PINKER, 2011)

Segundo Voermans, a ameaça de punição, por si só, não funciona. É preciso demonstrar que regras são legítimas e necessárias: nós a aceitamos e a obedecemos porque acreditamos que devemos, e outros membros da sociedade ou do Estado nos lembram de fazê-lo. A tese central é de que a compreensão do porquê de as pessoas obedecerem a lei tem o condão de tornar mais eficiente sua execução. Voermans se alinha com a teoria construtivista de que a concordância depende do modo como as normas regulatórias se alinham com a convicção de seus destinatários. Nessa teoria, o principal motivador para a mudança de comportamento não é externo, mas, sim interno: se o regulador for bem sucedido em convencer os outros de que uma norma é boa, necessária, legítima etc, a concordância seguirá naturalmente. A internalização da norma e de sua *ratio* é o fator mais relevante para que as pessoas obedeçam a regras, e, por conseguinte, às leis em geral.

A lei, portanto, é um sistema de convicção³⁸. Nós a aceitamos e a obedecemos porque acreditamos que devemos, e outros membros da sociedade ou do Estado nos lembram de fazê-lo. De acordo com uma extensa pesquisa feita pelo professor Tom Tyler³⁹, as pessoas obedecem às leis apenas se pensam que são legítimas, e não por medo de punição. Logo, a punição não é um motivo forte para a concordância de leis⁴⁰.

Voermans acredita, portanto, que a melhor lógica, na afirmação das leis, é a motivacional. Ele traça 3 vertentes para a observância das leis:

Econômico-jurídica: Se as pessoas são racionais, elas podem fazer uma análise de custo-benefício da concordância de normas. Por outro lado, como defende Sunstein, o comportamento irracional, que é inato aos humanos, deve ser levado em conta para determinar que as pessoas não são boas em fazer tal análise.

Psicologia forense: Sanções são ineficazes para conformistas; sanções possuem um efeito indireto para identificadores (pessoas que querem pertencer a um determinado grupo); sanções são supérfluas para internalizadores; a visão da punição impede crimes futuros. Em conclusão, a punição efetiva afeta o domínio relevante de nossas mentes, e programa nossa vontade de concordância – o *Bandwagon effect*⁴¹ da concordância.

Psicologia: Em pesquisa, a maioria dos entrevistados indicam que não desobedecem às leis por motivos internos. (internalização). Os entrevistados, entretanto, acreditam que outros contenham-se por medo de punição. (externalização)

Sendo assim, Voermans conclui que o direito penal não contém seus sujeitos unilateralmente, e que o endurecimento de penas não ajuda. A ciência comportamental ensinou que os potenciais ofendedores não conhecem a lei, e, mesmo que a conhecessem, não poderiam usar esse conhecimento para seus próprios interesses, por influência de uma variedade de fatores sociais, químicos e pessoais. A *deterrence*⁴², por si só, não funciona⁴³. Ela deve se relacionar com os motivos internos de seus sujeitos e se aproveitar de suas convicções. Nessa esteira, o esforço administrativo para a observância das leis não se traduz em concordância por parte de seus sujeitos, e, da mesma

³⁸ “belief”

³⁹ (Tyler, 2006)

⁴⁰ “People obey the law only if they believe it’s legitimate, not because they fear punishment.” (VOERMANS, 2013)

⁴¹ “efeito Maria-vai-com-as-outras”

⁴² Dissuasão

⁴³ “Deterrence alone will not help – we also have to tie in with motives (nudges, communication, carrot stick, social stigma) – and capitalize on ‘beliefs’ (appeal to morality, educate)” (VOERMANS, 2013)

forma, a ameaça de punição não age diretamente como motivo para a concordância, mas, sim, indiretamente, como efeito reflexivo difuso nos sujeitos legais – o *Bandwagon effect*”. (VOERMANS, 2013)

Depreende-se que, se não houver esforço constante para a observância das leis, a chance de que ela não será seguida é alta. No nosso caso, as leis de informática não são nem claras, nem lembradas pelos membros da sociedade e do Estado. Não há espaço e/ou incentivo para internalização das normas, tampouco a chance para que elas se relacionem com os motivos e convicções individuais de cada pessoa. Por conseguinte, percebemos que, ao mesmo tempo em que a internet é um espaço público, ela não é tida como tal para efeitos de concordância e observância de leis.

Em adição a isso, como demonstrado no efeito de desinibição online, os sujeitos legais da internet não se comportam como o esperado pelo legislador, pois grande parte de seus usuários veem a Internet como um mundo à parte, com regras próprias e diferentes das que aplicam no dia-a-dia. Mais do que isso, as leis específicas de crimes cibernéticos são de difícil internalização. Um exemplo nacional é a edição da Lei Carolina Dieckmann⁴⁴ pioneira por tratar de crime especificamente informático: mesmo cientes do crime, os internautas continuam desinibidos para a distribuição de conteúdo privado.

2.2 Lessig e a regulação do cyberspaço

Em seu livro *Code 2.0*, Lawrence Lessig argumenta que o futuro da internet depende das ações que tomaremos para defini-la, e defende o aumento da regulação da Internet como forma de impedir a super regulação da mesma. Ele aponta quatro fatores que controlam como e de que forma o cyberspaço é regulado: a lei, as normas da sociedade, o mercado e a arquitetura (da Internet). Juntos, estas quatro limitações compõem a regulação. (LESSIG, 2006)

Estes quatro reguladores são distintos, porém interdependentes; cada um deles regula o comportamento no cyberspaço. A lei ameaça sanções frente a violações de direitos, levando o desafio da lei às suas consequências. As normas sociais são a etiqueta da Internet, um conjunto de convenções que têm o poder de tornar um indivíduo alienado pela comunidade. O mercado estabelece as restrições monetárias de acesso, e recompensa os sites mais populares. E finalmente, a arquitetura - o software e o

⁴⁴ LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

hardware que fazem da Internet o que ela é – condicionam o acesso do internauta. É esse último regulador que Lessig chama de código, e que defende ser a solução para a regulação mais eficaz do cyberspaço, como veremos adiante.

A Internet não é uma entidade soberana e desvinculada do sistema legal tradicional, livre de regulações externas, como se acredita em visões mais liberais, como a “Declaração de Independência do Cyberspaço” de Barlow⁴⁵. O mundo virtual é, sim, inerentemente diferente do mundo real, porém, ligado aos mesmos valores tradicionais relevantes da realidade. Para alguns valores a interpretação é a mesma em ambos os mundos. Entretanto, para outras, a passagem requer a adequada “tradução” de determinado valor, em um problema que Lessig chama de “ambiguidade latente”⁴⁶.

Uma das ambiguidades latentes do mundo virtual é o da privacidade. Quando do julgamento pela Suprema Corte dos Estados Unidos do caso *Olmstead*, em 1928, referente a utilização de escutas telefônicas sem mandado e sua relação com a Quarta Emenda da Constituição⁴⁷, o juiz Brandeis pronunciou um voto dissidente que é tido para Lessig como o modelo para os cyberativistas do futuro. Ao contrário do voto vencedor, que simplesmente afirmou que a Quarta Emenda não abarcava a utilização de escutas telefônicas como invasão de privacidade, Brandeis afirmou que esse tinha sido o caso apenas porque para a tecnologia da época, a invasão de propriedade era a única forma de invasão de privacidade. Preservando o significado da norma, o mais correto a se fazer seria interpretar a utilização de escutas telefônicas como uma invasão de privacidade, pois, desde então, a tecnologia havia mudado para que ela fosse considerada como tal. Brandeis, portanto, buscou preservar a proteção conferida pela Quarta Emenda, mesmo que isso significasse proteger mais do que literalmente escrito. Esta interpretação teleológica da norma neutraliza as transformações do tempo e seus desenvolvimentos tecnológicos para manter o propósito original da norma, situação na qual se encontra a

⁴⁵ Disponível em <<https://projects.eff.org/~barlow/Declaration-Final.html>> Acesso em: 1º de julho de 2015

⁴⁶ (LESSIG, 2006) p.170

⁴⁷ É a emenda que garante o direito à privacidade. Transcrito: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Disponível em: <http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html> Acesso em: 1º de julho de 2015

tradução das ambiguidades latentes da era digital. Este caso, entretanto, é um dos casos de fácil tradução, no qual os valores podem ser carregados sem muitas complicações.⁴⁸

2.2.1 A arquitetura da regulação

Se não há como saber quem alguém é, onde ele está, ou o que está fazendo, não há como regulá-lo. Seu comportamento será como ele assim desejar. (LESSIG, 2006) As palavras de Lessig preconizam todo o seu pensamento em relação a matéria de regulação na Internet. É indiscutível que, para o autor, a regulação deverá acompanhar o aumento na identificação do internauta, pois apenas assim, em sua visão, poderá haver a regulação. A ferramenta para tal mudança, é claro, é a arquitetura da web.

Lessig identifica a arquitetura como o único fator capaz de verdadeira regulação. Ora, a Internet não foi feita da pedra, não possui uma condição primal sem a qual não pode existir. Ela é um mero produto de seu design, e, portanto, está sujeita as mudanças provenientes de sua arquitetura. “A Internet poderia ser desenhada para revelar quem alguém é, onde esse alguém está, e o que esse alguém está fazendo. E se ela desenhada assim fosse, a Internet poderia se tornar o espaço mais regulável que o homem já conheceu.”⁴⁹

Atualmente, a arquitetura da Internet permite, como práticas comuns, o rastreamento de identidade pelo endereço IP e o armazenamento de dados em *cookies* para a identificação de um usuário. A facilidade com a qual o referido usuário pode se evadir de tais mecanismos, entretanto, é veemente. O cyberspaço, no geral, é muito falho na asserção de identidade, autenticação e credenciamento de um indivíduo, o que diminui a regulabilidade do cyberspaço. Diante disso, Lessig apoia a adoção de uma forma melhor de autenticação: um protocolo que habilita uma espécie de carteira de documentos virtual. Dessa forma, será introduzida uma camada de identificação na web, ao mesmo tempo em que confere controle ao usuário sobre quais informações específicas ele deseja revelar. Mais importante, os avanços na criptografia assimétrica permitem um aumento

⁴⁸ Os casos de difícil tradução, entretanto, – os que introduzem uma lacuna - têm duas respostas: a corte não se pronuncia e deixa o legislador decidir; ou articula questões de valor constitucional para conferir significado à palavra da Constituição. Lessing defende a segunda resposta, pois acredita que a discussão de valores constitucionais foi tomado pela Suprema Corte, tornando passivo o legislador nesses assuntos.

⁴⁹ “The Net could be designed to reveal who someone is, where they are, and what they’re doing. And if it were so designed, then the Net could become, as I will argue throughout this part, the most regulable space that man has ever known.” (LESSIG, 2006) p.53

de segurança na certificação do destinatário da veracidade de um fato revelado. De forma geral, o protocolo de autenticação tornará a Internet mais confiável, tanto para o usuário cidadão quanto para o governo e as empresas, diminuindo os problemas que emergem da falta de confiança. Esta mudança, juntamente com a implementação do novo IPv6, que garante uma melhor identificação no envio e recebimento de informação, tornará quase impossível o anonimato na Internet.

Lessig menciona a possibilidade da adoção de tecnologias que identifiquem o conteúdo dos pacotes de dados, por meio da adição de uma camada no protocolo TCP/IP para obter conhecimento de qual informação está sendo transmitida. Apesar de este método não imunizar o uso de tecnologias para o anonimato, como a criptografia, o público geral não se incomodará a fazê-lo, aumentando a regulabilidade da Internet.

Por último, a tecnologia *open source*⁵⁰ de mapeamento de IP permite, gratuitamente, que qualquer endereço IP seja ligado a uma localidade no mundo, localizando o usuário pertencente àquele IP. Embora o uso de *anonymizers*⁵¹ consiga evadir dessa tecnologia, o uso conjunto das chaves de autenticação supramencionadas aumenta substancialmente a eficácia do mapeamento.

Apesar de Lessig argumentar, nos capítulos posteriores, outras atitudes que podem ser tomadas pelo governo, pelo comércio e pela própria arquitetura para aumentar a regulabilidade da Internet, podemos extrair o mais importante para nosso estudo: a regulação da Internet deve ser acompanhada de um aumento na identificação do usuário, ou, se não for possível, na diminuição de comportamentos não-rastreáveis.

Capítulo 3 - Perspectivas harmônicas para o anonimato no futuro

O anonimato, como conceito, está frequentemente antagonizado com a segurança, no sentido de que um indivíduo verdadeiramente anônimo não possui *accountability*⁵² para responder a algum ato criminoso. Assim, a percepção geral costuma ser a de que o anonimato e a segurança se equilibram em pratos opostas de uma balança. Proponho, por outro lado, que o anonimato possa conviver com a *accountability*, bem como com uma regulação de Internet que aumente a confiança geral no sistema.

⁵⁰ Acesso universo via licença gratuita

⁵¹ Anonimizadores

⁵² A tradução próxima para o português seria responsabilização.

Para isso, a regulação da internet deve aumentar ao mesmo tempo em que fique assegurado o direito ao anonimato, e não em proporção inversa. A perda do anonimato público promove conformidade e uma sociedade opressora, ao passo que a garantia de anonimato promove liberdade de ação e uma sociedade aberta. (Slobogin, 2002) Mais do que isso, em alusão à figura do Panóptico, o mero conhecimento de que um indivíduo está sendo observado é suficiente para que seu comportamento mude, desvirtuando sua própria personalidade. O direito ao anonimato - ou a simples faculdade em exercê-lo - deve ser defendido sob todas as custas.

Em conformidade com essa visão, existem alternativas e caminhos que consideram a importância do anonimato na Internet sem deixar de punir o uso do anonimato para comportamentos antissociais.

3.1 Anonimato Revogável

Os avanços no campo do comércio eletrônico demonstraram como o anonimato incondicional pode ser abusado. A habilidade de revogar o anonimato é necessária para as organizações financeiras com o intuito de prevenir a fraude e/ou localizar pagamentos e saques suspeitos. Aplicando o conceito à comunicação em rede, o anonimato revogável parece equilibrar o direito a privacidade do usuário e as preocupações do governo e das organizações (Claessens et. al., 2003). Em teoria, o modelo de anonimato revogável garante o anonimato ao usuário com respeito a sua privacidade, sendo revogado apenas quando requerido pela força da lei, e sob justificativa fundamentada. A revelação da identidade do usuário será de conhecimento apenas da agência governamental que a requereu.

A palavra-chave para a análise da revogação de anonimato é proporcionalidade. Significa dizer que a revogação não deve ultrapassar o limite do necessário para que possa ser feita a identificação do usuário em questão, bem como a análise caso a caso de uma possível revogação. Uma vez incluídos no sistema tradicional de mandado, as revogações poderão ser analisadas com analogia a quebra de outros tipos de sigilo, como, por exemplo, o bancário. Dessa, forma apenas com o cumprimento de requisitos pré-estabelecidos é que poderia ser feita a revogação: ordem judicial fundamentada; existência de fundados elementos de suspeita; individualização do investigado e do objeto da investigação; obrigatoriedade de manutenção do sigilo em relação às pessoas estranhas ao procedimento investigatório; utilização dos dados obtidos somente para a investigação que lhe deu causa; etc. A ideia aqui é de equiparar a

revogação de anonimato com a quebra de sigilos tradicionalmente abarcados nos ordenamentos jurídicos, equiparando a seriedade e necessidade requeridas para que seja concedida.

Apesar da revogação de anonimato estar comumente associada à existência de sistemas com *backdoors*, o que em si significa uma quebra na confiança do sistema anônimo, alguns estudos têm pesquisado a possibilidade de implementar o anonimato revogável sem que seja preciso fornecer nada além do IP, por meio de técnicas avançadas de criptografia.⁵³ É importante ressaltar, neste caso, o lugar de destaque da arquitetura como regulador, em conjunto com a lei, o que torna a regulação mais eficiente e de fácil implementação.

3.2 Sistemas de Listas Negras Anônimas

O grande apelativo dos sistemas de *Anonymous Blacklisting* é o de não depender de um terceiro de confiança para a desanonimização de um usuário. Uma autenticação anônima com o provedor de serviço torna-o habilitado a anular o acesso de algum usuário que comportar-se indevidamente sem que seja revelada a sua identidade. O sistema funciona da seguinte maneira: o usuário que deseja ingressar no sistema anônimo realiza a autenticação com o provedor de serviço, que fornece a ela uma credencial identificadora, de conhecimento apenas do usuário. O provedor de serviço recolhe um *ticket* (extraído da transcrição de protocolo) da entrada daquela credencial, e, caso o usuário se comporte indevidamente, adiciona aquele *ticket* a lista negra. O portador da credencial mantém sua identidade anônima, porém não conseguirá ingressar no mesmo sistema.

O modelo de listas negras anônimas favorece o uso benéfico do anonimato, punindo apenas o mau comportamento. Extrapolado à todas as comunidades anônimas, significa dizer que o usuário que desejar ingressar em atividades anônimas antissociais será excluído de todas os sistemas anônimos, até que fique sem um ambiente anônimo para atuar ou pare de se comportar indevidamente. De uma forma ou outra, é um modelo que consegue manter os usuários anônimos benéficos e eliminar os prejudiciais, sem precisar desanonimizar.

⁵³ (Köpsell et. al., 2006)

3.3 Modelo harmônico de Lessig

O modelo harmônico de Lessig, na falta de nome melhor, é uma proposta minha em conceber o cyberspaço no estado regulado imaginado por Lessig coexistindo com o anonimato.

Como vimos, Lessig defende o aumento na especialização de credenciais para determinar com melhor precisão as qualidades de identificação, atividade e lugar do usuário, com o intuito de aumentar a regulação. Proponho, dessa forma, que seja emitida, por um órgão próprio, uma credencial para o uso anônimo da Internet. A credencial pode garantir desde um nível baixo de anonimato (anonimato de lugar) até um nível alto (anonimato completo), com a necessária fundamentação proporcional. O único dever para o usuário credenciado seria a de reportar os horários no qual usou a credencial ou não. Em cada uso, as credenciais de identificação teriam que ser autenticadas, para evitar fraude. As qualidades não anonimizadas continuariam sendo reguladas normalmente durante o uso.

Primeiramente, os usuários do anonimato para fins benéficos deixariam de ser afetados pelo aumento na regulação da Internet. Bastaria justificar o motivo pelo qual requer uma credencial de anonimato, podendo, inclusive, solicitar o sigilo da motivação. Todas os usos positivos do anonimato são suficientes para garantir um anonimato necessário para sua completa realização. O discurso anônimo na Internet, protegido em alguns países⁵⁴ como extensão do direito à liberdade de expressão, seria o suficiente para garantir a todos os cidadãos, sem necessidade de pedido, uma credencial de nível médio de anonimato, por exemplo.

Em segundo lugar, todas as funcionalidades cobertas pelo anonimato estariam devidamente especificadas no registro do usuário, o que impediria, por exemplo, de um indivíduo com a justificativa de ingresso em lista de e-mails de autoajuda possuir a habilidade de baixar arquivos de vídeo anonimamente. Com a adequada regulação, a possibilidade de fraude seria baixa, uma vez que o anonimato completo só seria concedido em casos excepcionais. Dessa forma, o governo continuaria tendo acesso a pelo menos um identificador do usuário comum. Pelo mesmo motivo, o governo diminuiria suas preocupações com atividades terroristas anônimas.

⁵⁴Legal Protection of Anonymity. In: WIKIPÉDIA, a enciclopédia livre, Flórida: Wikimedia Foundation, 2015. Disponível em <https://en.wikipedia.org/wiki/Anonymity#Legal_protection_of_anonymity> Acesso em: 4 de julho de 2015.

Se fosse fundada a suspeita de ato ilícito, o governo, mediante mandado judicial, poderia revogar a credencial e instaurar investigação, finda a qual, e sem provas de conduta ilícita, retornaria a credencial ao investigado. Todos os procedimentos seriam de total ciência do usuário.

Este modelo busca aliar as demandas de privacidade do usuário de Internet com as preocupações dos governos e organizações quanto aos perigos do anonimato. Parece, entretanto, ser razoável a regulação do anonimato por meio de credenciais destinadas para o uso benéfico, mantendo assim, a autonomia do usuário em relação a seus direitos de privacidade.

Conclusão

Desde os escândalos de vigilância global de 2013, o direito à privacidade na sociedade da Informação tem sido alvo de debates acerca de sua imprescindibilidade, em face à ameaça terrorista. A discussão encontra-se no âmbito de possibilidade de coexistência do direito à privacidade e a capacidade de agências governamentais acessarem os dados pessoais de cada cidadão. Diante de uma necessidade cada vez mais urgente de regulação, a comunidade científica e política se debruça para debater de que forma a regulação da Internet pode ser realizada com o respeito aos direitos e deveres dos internautas. Contudo, é necessário ter atenção e cuidado ao próprio funcionamento da internet como espaço público, assim como as características de seus usuários e suas práticas habituais. As particularidades dos internautas como sujeitos legais, tornam difícil a internalização de leis de Internet. Lessig ressalta a importância de uma regulação pautada na arquitetura da Internet, pois somente por meio dela que poderá haver um verdadeiro avanço. Ao mesmo tempo, preconiza o aumento da regulação se quisermos manter controle sobre o ritmo com o qual ela se dará.

Entre os debates surgidos pela vigilância global, o avanço da agenda antiterrorista, e o lobby da indústria de entretenimento para a proteção da propriedade intelectual, parece não haver espaço para o direito ao anonimato. Vimos, contudo, que o anonimato na Internet faz parte do próprio modo como as interações online se dão, e que é responsável por impactos benéficos para a ordem social, além de ser uma extensão de um direito fundamental do homem, o direito à privacidade. Mais do que isso, o anonimato deve continuar existindo, sem o qual estaremos em risco de nos tornarmos uma sociedade panóptica, sujeitos de nossa própria prisão.

O direito ao anonimato parece conflitar com a tendência da doutrina em aumentar as regulações da Internet. Entretanto, isso não quer dizer que o direito ao anonimato está prestes a ver seu fim - quer dizer apenas que ele deve saber seu lugar. O anonimato não mais poderá ser usado como manto para a ilegalidade, mas, sim, usado apenas para os fins benéficos para o qual ele é capaz. Assim, com o aumento das regulações de identidade no cyberspaço, o anonimato deverá ser usado com responsabilidade, como uma extensão ao direito à privacidade, e, portanto, protegido não só pela lei, mas também pela arquitetura da web.

Nessa sensível época de transição entre a Internet sem lei e Internet regulada, devemos nos atentar para não perdermos de vista a importância do anonimato e sua dimensão contra hegemônica. Ao mesmo tempo, a história da Internet até então deixou para muitos a percepção de que o anonimato faz parte da normalidade do comportamento na Internet. Se a lei, de repente, avançar no sentido de desanonimização sem que a sociedade esteja preparada para aceitá-la, correrá o risco de encontrar uma reação forte no sentido de fortalecer o anonimato perdido, o que poderá agravar ainda mais a tensão para articular os acontecimentos do mundo e a agenda da regulação da Internet. Devemos, portanto, equalizar o canal de diálogo entre governo e sociedade, buscando uma regulação inclusiva e participativa, pois, certamente, não será possível uma regulação unilateral sem que haja uma verdadeira ruptura no modo em como a sociedade e o governo veem o anonimato na Internet.

Referências Bibliográficas

CHRISTOPHERSON, Kimberly M. **"The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog".**" *Computers in Human Behavior* 23.6, 2007.

CLAESSENS, Joris, Bart PRENEEL, and Joos VANDEWALLE. **Anonymity Controlled Electronic Payment Systems.** In A. Barbé, E.C. van der Meulen, and P. Vanroose, editors, Proceedings of the 20th Symposium on information Theory in the Benelux, pages 109–116, May 1999.

CLAESSENS, Joris, Claudia DIAZ, Caroline GOEMANS, Jos DUMORTIER, Bart PRENEEL, and Joos VANDEWALLE. **"Revocable anonymous access to the Internet?."** *Internet Research* 13, no. 4 (2003): 242-258.

FLANAGIN, A. J., TIYAAMORNWONG, V., O'CONNOR, J., & SEIDOLD, D. R. **Computer-mediated group work: the interaction of member sex and anonymity.** *Communication Research*, 29, 66–93. 2002.

HABERMAS, Jürgen. **"The public sphere: an encyclopedia article"**, *New German Critique*, 1964. Disponível em <<http://www.socpol.unimi.it>>. Acesso em 10 nov. 2013.

HENRY, Ryan, and Ian GOLDBERG. **"Formalizing anonymous blacklisting systems."** *Security and Privacy (SP), 2011 IEEE Symposium on.* IEEE, 2011.

HUGHES, E. **A Cypherpunk's Manifesto.** (1993). Acesso em: 27 de junho de 2015, disponível em <<http://www.activism.net/cypherpunk/manifesto.html>>

JONES, S. **Encyclopedia of New Media.** Thousand Oaks: Sage Publications, 2003.

KÖPSELL, Stefan, WENDOLSKY, Rolf e FEDERRATH, Hannes. "Revocable anonymity." **Emerging Trends in Information and Communication Security.** Springer Berlin Heidelberg, 2006. 206-220.

KUHLEN, Rainer. **Informationsethik. Umgang mit Wissen und Information in elektronischen Räumen.** Universitätsverlag Konstanz, 2004, *apud* Privacy an intercultural perspective, por Rafael Capurro.

LESSIG, L. **Code Version 2.0.** New York: Basic Books, 2006.

LUNDBLAD, N. **Privacy in a noise society.** WHOLES Workshop: A Multiple View of Individual Privacy in a Networked World. Stockholm, 2004.

MILL, John Stuart. **On Liberty.** Editor by Edward Alexander. Ontário: Broadview Literary Texts, 1999. p. 29

ONN, Yael et. al., **Privacy in the digital Environment** (Haifa Center of Law & Technology, Niva Elkin Korem, Michael Birnhack, eds., 2005

PINKER, S. **The better angels of our nature: The decline of violence in history and its causes.** Penguin UK, 2011.

SLOBOGIN, C. **Public privacy: camera surveillance of public places and the right to anonymity.** Mississippi Law Journal, 2002.

SOLOVE, Daniel J. **Understanding Privacy.** Cambridge, Mass.: Harvard University Press, 2008.

SPEARS, R., & LEA, M. **Social influence and the influence of the “social” in computer-mediated communication.** In M. Lea (Ed.), Contexts of computer-mediated communication (pp. 30–65). London: Harvester-Wheatsheaf, 1992.

SULER, John. **The Online Disinhibition Effect.** *Cyberpsychology & Behavior*, New York, v. 7, n. 3, jul. 2004. Disponível em <<http://www.liebertpub.com/>>. Acesso em 2 out. 2013.

TYLER, T. R. **Why people obey the law.** Princeton University Press, 2006.

TSANG, Patrick P., et al. **"Blacklistable anonymous credentials: blocking misbehaving users without ttps."** *Proceedings of the 14th ACM conference on Computer and communications security.* ACM, 2007.

VERONESE, Alexandre, e Christiana Soares DE FREITAS. **"Segredo e Democracia: certificação digital e software livre."** Disponível em <http://www.ip.pbh.gov.br/ANO8_N2_PDF/artigo-segredo-e-democracia.pdf> Acesso em 15 de maio de 2015.

VOERMANS, Wim. Lecture. **O que faz as pessoas obedecerem leis?** In: CICLO DE ENCONTROS DO PROJETO PENSANDO O DIREITO, Universidade de Brasília, Brasília, DF, setembro de 2013. Disponível em <<https://www.youtube.com/watch?v=do4v1wgASoE>> Acesso em: 24 de junho de 2015

ZIMBARDO, P. G. **The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos.** Lincoln: University of Nebraska Press, 1969.