REGULAÇÃO DA INTERNET NO BRASIL, EUA E UNIÃO EUROPEIA: modelos, caminhos e impactos sobre os direitos civis [1]

INTERNET REGULATION IN BRAZIL, THE USA AND THE EUROPEAN UNION: models, approaches and impacts on civil rights

Sivaldo Pereira da Silva [2]

***Resumo**: Este paper analisa o atual cenário regulatório da Internet e seus principais impactos nos direitos civis. O trabalho se concentra em dois temas-chaves: (a) Privacidade e (b) Neutralidade de Rede e busca compreender como estes debates estão ocorrendo nos Estados Unidos, União Europeia e Brasil. O estudo foi baseado na revisão de leis, resoluções, relatórios, documentos governamentais, decisões judiciais e outras publicações. Os resultados demonstram que, quanto à privacidade, há cenários distintos: regulação fraca nos EUA; em implementação no Brasil e regulação mais consolidada na Europa. Já sobre a neutralidade de rede, os resultados apontam uma tendência geral de adoção deste princípio, porém através de mecanismos distintos: força de lei no Brasil; normas infralegais nos EUA e diretrizes-regulatórias na União Europeia.*

***Palavras-Chave:** Regulação da Internet. Privacidade. Neutralidade de rede.*

***Abstract**: This paper presents a study on the current Internet regulation debate and its impacts on civil rights. More precisely, the work focuses on two key topics: (a) Privacy and (b) Network Neutrality. It describes how these debates have been developed in the United States, the European Union and Brazil. The methodology was based on the intersection of information obtained from laws, resolutions, reports, governmental documents, court decisions and other publications, as well, literature review. The findings demonstrate that exist a set of disparities regulatory situations: a weak regulation in the US; a young regulation in Brazil and a strong traditional regulation in Europe. About net neutrality, the results show a common trend of this principle but through different mechanisms: the force of law in Brazil; agency action in the US and official guidelines in the European Union..*

***Keywords:** Internet regulation. Privacy. Net Neutrality*

[1] Trabalho apresentado ao Grupo de Trabalho Políticas de Comunicação do VI Congresso da Associação Brasileira de Pesquisadores em Comunicação e Política (VI COMPOLÍTICA), na Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), de 22 a 24 de abril de 2015.

[2] Sivaldo Pereira da Silva é Doutor em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia. É professor do Curso de Jornalismo da Universidade Federal de Alagoas (UFAL) e do Programa de Pós-Graduação em Comunicação da Universidade de Brasília (UnB). E-mail: sivaldop@yahoo.com

1. Introdução

O desenvolvimento da comunicação digital nas últimas décadas e o crescimento da Internet em sua importância social, política e econômica estão repercutindo em novas legislações nacionais que buscam sanar vácuos regulatórios e dirimir conflitos iminentes. Em todos os casos, é possível afirmar que o estabelecimento dessas normatizações quase nunca tem sido pacíficas e são marcadas por tensões entre os interesses de empresas, governos e indivíduos (seja no âmbito do consumo, seja no campo dos direitos). Embates recentes como a guarda de *logs* na aprovação do Marco civil da Internet no Brasil, a disputa entre a FCC e as empresas de telecomunicações nos EUA em torno da neutralidade de rede ou a polêmica na decisão da Corte Europeia de Justiça sobre o "Direito de ser esquecido" na Internet são apenas alguns exemplos neste cenário.

Embora possamos elencar uma série de elementos que estão no fundo dessas disputas, é possível identificar duas preocupações recorrentes que atravessam boa parte desses embates: (a) a concentração de poder econômico dos *players*, principalmente corporações comerciai e (b) a proteção de direitos fundamentais dos indivíduos, principalmente quando à liberdade de expressão, direito à informação e privacidade.

Tendo esta tensão como premissa, a pergunta central que move este *paper* pode ser resumida nos seguintes termos: como está o atual cenário regulatório da Internet e seus principais impactos nos direitos civis ? Mais especificamente, o trabalho se concentra na análise de dois temas-chaves: (a) Privacidade e (b) Neutralidade de Rede, buscando caracterizar como essas duas frentes estão sendo tratadas em três contextos: Brasil, Estados Unidos e União Europeia. A escolha desses três âmbitos se deu em função de suas respectivas importâncias geopolíticas e por representarem, atualmente, palcos de significativa atividade regulatória nos últimos anos.

Do ponto de vista metodológico, além da revisão de literatura, o estudo se baseou em análise de legislações, normas infralegais, decisões judiciais, diretivas multilaterais, posicionamentos de organizações civis, comerciais e governamentais.

Para responder ao objetivo proposto, o *paper* foi organizado em duas seções: no primeiro momento delineia-se uma compreensão geral dos dois debates-chaves: Privacidade e Neutralidade de Rede. Com o entendimento conceitual posto, a segunda seção analisará como esses temas estão sendo tratados nos três contextos políticos em análise (EUA, União Europeia e Brasil), que opções e modelos regulatórios estão se configurando; quais os caminhos e impactos sobre os direitos civis se desenham nestes cenários.

1. Dois debates-chaves: Privacidade e Neutralidade de Rede

Se tivermos como pano de fundo a preocupação em compreender os impactos da regulação da Internet sob os direitos civis nos últimos anos, dois temas podem nos dar uma boa visão. O primeiro é a Privacidade, considerada historicamente um direito individual, que traz questões como autonomia dos sujeitos, mercantilização de informações pessoais, direito ao anonimato, vigilância, guarda de dados. O segundo é o que vem sendo chamado de Neutralidade de Rede, considerada um princípio histórico sob o qual foi erguida a Internet, que impacta em direitos coletivos, liberdade de expressão, concentração de mercado e tráfego de dados.

Nesta seção, o objetivo será delinear conceitualmente cada uma dessas discussões para podermos, na seção posterior, compreender o seu lugar nas políticas de regulação. Comecemos pela privacidade.

1.1 Privacidade: do direito à solidão à mercantilização dos bits

Embora rejuvenescida pelos recentes debates sobre proteção de dados e vigilância digital, a concepção jurídica de privacidade tem suas origens no século

XIX. Ergueu-se nesta época como uma reação à expansão da indústria de mídia impressa (jornais, revistas etc.) que passava a se interessar por informações pessoais (principalmente de personalidades ilustres) como parte de seu repertório de produtos-narrativos (SEVIGANI, 2013; FERNBACK;PAPACHARISSI, 2007; WOO, 2006). O artigo de Samuel Warren e Louis Brandeis, publicado em 1890 pela *Harvard Law Review*, é considerado um dos primeiros documentos que delineia os aspectos centrais da ideia de privacidade como foi concebida desde então. Como explica Woo (2006)

> […] Warren and Brandeis (1890) co-authored a famous article entitled 'The Right to Privacy', defining privacy as 'the right to be let alone'. [...] Warren and Brandeis (1890) argued that news articles and the press invaded people's private and domestic lives, an argument probably motivated by Warren's distress at the publicity surrounding his daughter's wedding (DeCew, 1997) (WOO, 2006, p. 951).

Esse "direito à solidão" deve ser compreendido dentro de um contexto histórico específico: a emergência de uma sociedade liberal que carregava consigo princípios como a universalidade do indivíduo; o temor da ditadura da maioria e do Estado vigilante-opressor; a distinção entre vida pública e vida privada. Ao mesmo tempo, também marca o início do processo de mercantilização de dados pessoais como matéria-prima para indústria da informação. Neste caso, sob a força industrial da *penny press* (TRAQUINA, 2005; BRIGGS; BURKE, 2006) e uma cultura de massa emergente.

Se a concepção moderna de privacidade nasce do "direito de ser deixado sozinho" ou "direito de ser deixado em paz" isso não significa que privacidade seja sinônimo de intimidade. Privacidade trata da relação da intimidade com o exógeno. Ou melhor, das fronteiras desta relação. Por isso, a privacidade vai além de um direito calcado na guarnição da vida privada dos olhos do grande público. Consiste em uma questão relacional: trata das trocas entre o "eu" e o "outro, dos limites dessas trocas simbólicas (DeCEW, 1997; WOO, 2006; BUCHMANN et al, 2013). Consiste em uma questão social, um fenômeno que está nas bordas das relações entre o indivíduo e aquilo que lhe é externo:

> Privacy, however, is not synonymous with the private sphere, but also encompasses the freedom of self-presentation in public whilst maintaining concealment of other aspects of one's self, i.e. there is an inherent tyranny in demanding that any self should totally reveal who they are, and in many contexts anonymity must be safeguarded in public intercourse such as commerce (BUCHMANN et al, 2013, p. 20).

Sendo uma questão social tem seus efeitos políticos. Com o desenvolvimento das democracias modernas percebeu-se que privacidade e autonomia estão umbilicalmente ligadas. Por envolver as fronteiras entre o indivíduo e o que lhe é externo na construção da sua identidade, a privacidade carrega em si uma questão de poder: a autonomia individual só pode ser garantida se os limites dessa intervenção do poder externo (o olhar vigilante de entes potencialmente opressores como público, governos e instituições como a mídia) sobre a intimidade do indivíduo forem devidamente estabelecidos.

Em regimes democráticos, resguardar a autonomia do indivíduo contra esse olhar externo afeta questões como (a) a liberdade de escolhas do indivíduo de acordo com a sua consciência (evitando a ditadura da maioria); (b) a qualidade da participação política que precisa ser exercida sem coerção (como nos caso do voto secreto em eleições); (d) a promoção da pluralidade democrática, garantindo exercício do direito à livre associação (através do compartilhamento privado de opinião entre grupos políticos, culturais e religiosos); (c) a autodeterminação do sujeito frente às forças potencialmente opressoras (ao estabelecer fronteiras entre esse poder externo e o *self*). (BUCHMANN et al, 2013; PHILLIPS, 2004)

É justamente por se tratar de uma questão relacional que a privacidade envolve processos de comunicação. Deste modo, ao olharmos para o cenário digital do século XXI, perceberemos que a "datificação" da vida em todos os seus âmbitos (MAYER-SCHONBERER; CUKIER, 2013) afeta diretamente a privacidade pois altera as bases da produção, coleta e circulação de informação pessoal. Em um contexto de crescente poder das corporações que tem em suas mãos um enorme volume de dados pessoais digitalizados:

> […] the accumulated power of Internet corporations (financial, network-making, discursive) enable Internet privacy crises that are

> driven by surveillance-based business models. Privacy is either declared to be obstructive or it must take the form of a commodity to fit into the corporate Internet. The latter implies that personal data are perceived as private property that is exchangeable for certain benefits (SEVIGNANI, 2013, p. 735).

A mercantilização de informação pessoal pela indústria da informação não é algo novo: como vimos, isso já era feito pelo *mass media* no final do século XIX. Porém, em tempos de Internet, o foco não é a mais obtenção de dados pessoais para ser publicado e consumido como um produto-narrativo midiático. A ênfase atualmente é distinta: os dados pessoais se transformaram em *commodities* (valorizadas sob o título de informação estratégica valiosa para outras corporações) que são obtidas pelas empresas através da cessão voluntária de dados pessoais por um benefício básico: o uso da ferramenta. Na prática, o cidadão abre mão da sua privacidade em troca do próprio acesso à plataforma, gerenciadas em sua maioria por grandes corporações privadas (PHILLIPS, 2004; WOO, 2006). Até porque não lhe restaria mais do que duas opções simples: ou aceita-se os termos de privacidade colocados pelo serviço ou não se pode utilizá-lo.

Paradoxalmente, ao mesmo tempo que há uma crescente valorização dos dados pessoais como *commodity* no mercado (Phillips, 2004) há também uma tendência de desvalorização da noção de privacidade como direito individual, uma vez que seu valor de troca se nivela ao simples uso do produto.

Além da "barganha" (ou da simples troca da privacidade pelo uso da ferramenta) as empresas também tem buscado convencer os usuários em ceder seus dados pessoais sob a justificativa de obter uma melhor experiência com o serviço:

> The discourse about cookies is framed in terms of convenience to the user; deleting them will result in a less streamlined, less personal and less productive MSN web experience. This statement also serves, rhetorically, to comfort the user that cookies are not dangerous (i.e. they do not deliver viruses), although they are used to monitor consumer online activity (Lipschultz, 2001).Whatever privacy concerns might be raised by the notion that monitoring devices are placed on the user's computer are mollified discursively by the emphasis on convenience. Thus the consumer is positioned to make a choice between privacy and convenience (FERNBACK; PAPACHARISSI, 2007, p. 724).

Para Woo (2006) a sujeição voluntária à vigilância não parece constituir um "invasão" do espaço pessoal por forças externas a ponto de violar o "*right to be alone*". Por isso, para o autor, conceito tradicional de privacidade - baseado na invasão unilateral do espaço pessoal por forças externas - e a subsequente produção de políticas com esta visão - não funcionam mais neste cenário. Ele explica que a autonomia do indivíduo, neste contexto de poderosas e onipresentes tecnologias digitais de monitoramento, só poderia ser garantida se passarmos a compreender a noção de privacidade não mais como o "direito de ser deixado em paz" e sim como o "direito de não ser identificado".

Percebendo estas várias dimensões, Phillips (2004) aponta quatro ênfases que se erguem nas preocupações com privacidade em sua relação com as novas tecnologias: (a) proteção contra intrusão; (b) negociação entre o publico e o privado; (c) gerenciamento de identidade e (d) proteção contra vigilância.

Tendo em vista esta característica multidimensional e observando o crescimento do poder de diversos *players* neste campo, a solução proposta por Fernback e Papacharissi (2007) seria tratar a privacidade como um bem público:

> Because privacy encompasses both social and economic dimensions, the concept of privacy itself can be regarded as a public good. Public goods such as parks, postal services or universal education contribute to the well-being of a society without any determinable material price, value, ownership or structure for compensation […]Therefore, conceiving of privacy as a public good is a useful foundation for providing recommendations for a democratic internet privacy policy (p. 731).

Olhar a privacidade como bem público parece razoável e requer priorizar padrões regulatórios com base em princípios normativos bem delimitados. Ao mesmo tempo, isso requer levar em conta pensar a noção de privacidade para além do foco no indivíduo. Como aponta Poritz (2007), em geral as leis vigentes reconhecem algum nível de proteção à privacidade individual (em diferentes graus e ênfases), mas poucas versam de fato sobre a privacidade coletiva.

No mundo, há hoje um intenso debate sobre os modelos e caminhos regulatórios para a privacidade no ambiente digital. Porém, ainda há pouca

regulação específica recentemente consolidada e, em muitos contextos, ainda não há ainda um efetivo controle das empresas sobre o uso comercial de dados pessoais.

1.2 Neutralidade de rede: um princípio histórico e seus efeitos

Além da privacidade, um segundo debate-chave que nos coloca diante de uma série de outras questões que impactam nos direitos civis, é aquilo que se convencionou chamar de *neutralidade de rede*. Para compreendermos devidamente este tema seria preciso (a) contextualizar o seu lugar na origem e evolução da Internet e (b) situar o seu impacto no atual contexto de intenso tráfego de dados e avançadas tecnologias de controle e monitoramento.

Historicamente, a internet foi concebida para funcionar através de camadas (camada física, camada lógica, camada de aplicações etc.) e para o bom funcionamento do tráfego de dados nessas camadas foram estabelecidos protocolos e princípios. Dois deles são basilares e fundamentais pois determinam a dinâmica do fluxo de dados: a transmissão de informação ocorre no formato ponto-a-ponto ("*end-to-end*"), isto é, descentralizado (diferente do modelo tradicional de comunicação cêntrica); e a transmissão de informação ocorre através do livre fluxo de datagramas (unidades de informação) pela rede sem a certeza de que o dado chegará ao seu destino final mas que será feito o "melhor esforço" ("*the best effort*") para sua entrega (CLARK, 2004; MARCUS, 2014). Estas duas características traziam de fundo a ideia da rede como livre caminho por onde os datagramas poderiam trafegar, sendo igualmente tratados no melhor esforço possível de entrega. Para alguns autores, isso implica que:

> […] the Internet's end-to-end design allows parties operating at the edge of the network to introduce their innovations to large audiences with great speed and low barriers to entry, inducing survival-of-the-fittest competition that determines which innovations succeed or fail based purely on their own merits (Lemley and Lessig 2001; Lessig 2006; Werbach 2005; Wu 2003; Wu and Lessig 2003) (COOPER, 2013, p. 29).

A neutralidade de rede está baseada justamente neste princípio: a concepção da rede aberta por onde os dados trafegam de forma neutra, igualitária, sem distinção.

Esta concepção ficou relativamente estável e manteve-se preponderante enquanto a internet crescia. Porém, com o aumento exorbitante do fluxo de informação nos últimos anos e com a evolução das ferramentas de checagem e gerenciamento de "pacotes de dados"[3] as empresas de telecomunicações (provedores de acesso) passaram a contar com a possibilidade real e concreta de quebrar a neutralidade e estabelecer diferenciações entre os dados que trafegam na rede.

Como explica Shelanski (2007), os defensores da quebra da neutralidade de rede argumentam que o investimento e a inovação no setor iriam diminuir com o tempo, a menos que as operadoras das redes pudessem cobrir os custos resultantes do crescente tráfego de dados no ambiente digital. Nesta perspectiva, afirmam que os provedores de aplicativos e conteúdos (*sites*, mídias socais, *apps* etc.) deveriam arcar com parte destes custos e as operadoras deveriam ter o direito de cobrar tarifas específicas: criando vias mais rápidas e mais caras; cobrando mais ou menos a depender do tipo de conteúdo (vídeo, voz, texto etc.). Algo que também se aplicaria aos usuários: poderia haver diferenciações entre aquele que acessa a Internet de modo moderado e aquele que a utiliza de modo mais intenso e ativo (que posta vídeos, baixa mp3 ou envia mais dados).

Para analistas como Lessig e McChesney (2006), a quebra da neutralidade de rede colocaria fim ao que a Internet tem de mais promissor, a possibilidade de qualquer um inovar sobre ela a partir de condições relativamente isonômicas para os desenvolvedores. Citando Timothy Wu, os autores afirmam que a quebra da neutralidade de rede favoreceria um "modelo de negócios à moda de Tony Soprano", uma vez que "extorquindo dinheiro por proteção de cada website – desde o menor *blog* até o Google – as operadoras de redes teriam imensos lucros" (Lessig e McChesney, 2006, *online*).

[3] Que possuem atualmente uma eficiente capacidade de identificar, classificar, retardar e acelerar todos os tipos de conteúdos trafegados na rede.

Além da garantia de um ambiente livre para inovadores de aplicativos e conteúdos, a defesa da neutralidade de rede também recai sobre as liberdades individuais. O direito de ir e vir e a liberdade de expressão estariam ameaçados pelo poder das empresas que teriam a possibilidade de criar hierarquias para o tráfego de dados ou tratar usuários de forma diferenciada durante o processo de comunicação.

A incorporação ou não da ideia de neutralidade como princípio em novas legislações nacionais é uma guerra ainda em andamento, com algumas batalhas perdidas pelas empresas de telecomunicações nas Américas e na Europa, como veremos na próxima seção. Uma das características desta disputa é o intenso *lobby* que as corporações têm produzido sobre a esfera política. O objetivo é impedir que o princípio seja textualizado em lei e garantir brechas jurídicas para que as empresas possam ter o direito de intervir no tráfego de dados e obter divisas financeiras a partir desse gerenciamento.

Ao mesmo tempo, o próprio crescimento da Internet também impõe ao princípio de neutralidade exceções, diante da inevitável atividade de gerenciamento do tráfego de dados para que a rede funcione de forma adequada. O aumento contínuo de todo tipo de conteúdo trafegando *online* é uma realidade que obriga a existência de algum nível de gerenciamento do tráfego. Por exemplo, quando a rede está congestionada o tempo de espera para que todo um conjunto de dados seja transmitido aumenta significativamente. Ocorre que, alguns tipos de dados são menos sensíveis ao *delay* que outros. Por exemplo, 10 segundos para que um *e-mail* saia de sua origem e chegue ao seu destino é quase imperceptível para usuário. Porém, 10 segundos em uma transmissão ao vivo de vídeo ou VoIP (Voz por IP) significa um longo tempo e gera problemas na experiência dos usuários. Nestes casos, seria necessário priorizar o tráfego de uma transmissão ao vivo em detrimento do conteúdo de um *e-mail* para que o *delay* deste primeiro seja o menor possível, minimizando o problema da sensibilidade quanto ao tempo. O que é geralmente aceito pelos defensores da neutralidade, é que esta regra deve ser vista como um princípio geral inviolável, com exceções mínimas e justificáveis (que não signifiquem ceder poder às operadoras para ditarem todo o tráfego da rede).

Por fim, um último obstáculo enfrentada pela neutralidade de rede é a sua exequibilidade. Ainda que seja transformada em lei e que as exceções sejam devidamente regulamentadas há ainda pouca estrutura de fato eficiente para garantir o monitoramento das empresas de acesso. Para isso, os entes reguladores precisariam se remodelar e investir em ferramentas e tecnologias de controle capazes de detectar possíveis violações, além de sustentar poder de *enforcement* para fazer cumprir a lei.

2. Regulação da internet nos EUA, União Europeia e Brasil: dois temas e seus impactos nos direitos civis

Com as bases conceituais delineadas sobre os dois debates-chaves na seção anterior, neste momento passaremos a observar como esses temas (privacidade e neutralidade de rede) estão sendo tratados em cada um dos três contextos em estudo (EUA, União Europeia e Brasil).

A análise ocorrerá buscando identificar minimamente (a) qual o quadro regulatório que prevalece em cada contexto e sob que *background* legal; (b) qual o cenário e ocorrências com possíveis impactos nos direitos civis atualmente; (c) quais as perspectivas e caminhos.

2.1 Privacidade *online* e neutralidade de rede nos EUA

Nos EUA, há hoje quatro principais leis que tratam da privacidade e proteção de dados pessoais frente às corporações: (1) o *Children's Online Privacy Protection Act* (COPPA) de 1998; (2) *o Telecommunications Act de 1996*; o (3) *Health Insurance Portability and Accountability Act* (HIPAA) de 1996; e o (4) Gramm-Leach-Bliley Act (GLB) de 1999[4].

A GLB diz respeito principalmente a informações financeiras. A HIPAA lida com as regras sobre o armazenamento de dados de identificação como nome,

[4] Em outro campo de análise, isto é, na regulação da privacidade do indivíduo frente ao Estado existem o Privacy Act de 1974 e também o Patriot Act of 2001.

idade, número de telefone, número de seguridade social etc. Nestes dois casos, ambas as leis dedicam apenas trechos delimitados para tratar de privacidade. No caso do *Telecommunications Act* têm-se importantes parágrafos sobre as obrigações de privacidade dos operadores da rede, dos *common carriers*. Por fim, a normatização mais concentrada no tema privacidade é a COPPA que dita as normas e proibições sobre coleção e disseminação de informação pessoal sobre crianças de até 13 anos. Nota-se que o país ainda não possui uma lei específica sobre privacidade digital recém elaborada. O principal ente regulador de temas que envolvem dados pessoais e privacidade frente às empresas é a *Federal Trade Commission* (FTC): uma agência federal de proteção ao consumidor e de políticas de competição de mercado.

No país, prevalece um modelo de regulação caracterizado pelo pouco rigor no controle de possíveis violações. Os princípios são geralmente vagos e o ente regulador tem baixa intervenção. O que coloca as empresas comerciais em uma posição confortável para lidar com os dados pessoais produzido pelos indivíduos *online*:

> The privacy statement formula follows in the tradition of self-regulation prevalent in the USA, which is founded on a lack of government involvement in regulating consumer privacy (with the exception of the Children's Online Privacy Protection Act of 1998 (COPPA)).The adequacy of privacy statements as protective measures is arguable; attorneys frequently draft online privacy statements to include catch-all stipulations that permit flexibility regarding uses of consumer information (Fausett, 2001) (FERNBACK; PAPACHARISSI, 2007, p. 719).

Na prática, isso tem resultado em um cenário de pouca proteção à privacidade. Fernback e Papacharissi (2007) apontam que um estudo da FTC revelou que apenas 20 % dos *websites* estadunidenses haviam implementado a diretrizes da Agência para práticas informacionais adequadas. Como sinetiza Phillips (2004):

> In summary, these rules permit data-holders to do anything they want with information derived from and produced by individuals, provided that they de-link the data from the individual's indexical identity. The actions of individuals may be used to describe and model them in any way that the data-holder wishes, provided the data-holder cannot

> actually contact, locate, point to or act upon the individual thus described. They are, again, informed by an understanding of 'privacy' that is closely related to the protection of the individual from unwanted intrusion (p. 701).

Atualmente, há projetos de lei sobre privacidade no Congresso americano, como *Online Personal Privacy Act* ou ainda propostas de leis que abordam privacidade e vigilância, como o *Cybersecurity Information Sharing Act (CISA) e Cyber Threat Sharing Act.* Porém, todos sem avanço efetivo na tramitação. Para alguns analistas, os EUA permanecem como "the only major trading nation which has not adopted comprehensive privacy protection legislation" (FERNBACK; PAPACHARISSI, 2007, p. 719).

Já no que diz respeito ao tema da Neutralidade de Rede, o país tem quadro diferente: embora também não haja legislação específica tratando da questão, nos últimos anos o órgão regulador das comunicações no país (a FCC - *Federal Communications Comission*) tem desenvolvido ações buscando a garantia deste princípio, basicamente legislando através de normas infralegais. A última delas, a resolução aprovada no dia 26 de fevereiro de 2015 (por 3 votos a favor e 2 contra, entre os membros da Comissão) [5], reforçou as regras sobre neutralidade de rede e enquadrou os provedores de acesso como Título II, isto é, esses *players* passaram ser submetidos a normas mais rigorosas.

A aprovação desta resolução se deu após alguns precedentes: (a) a existência de denúncias e ocorrências de ações discriminatórias praticadas pelos provedores americanos de acesso (como Verizon, Comcast) ao intervir ou retardar conteúdos de usuários e aplicações por interesses comerciais; (b) a edição de resoluções anteriores que tentaram dirimir essas violações (c) a disputa nos tribunais em ações movidas pelas empresas que conseguiram até então invalidar as resoluções estabelecidas pela FCC (MARCUS, 2014). Um dos principais argumentos das corporações nos tribunais, acatado pelos juízes, era que a FCC não sustentava competência para impor as regras sobre neutralidade pelo fato dos provedores de conexão estarem classificados como "serviço de informação" (Título I, sujeitos a

[5] Ver uma síntese em < http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0204/DOC-331869A1.pdf > acesso 10 março 2015.

menos regramentos do agente regulador). Por esta razão, a estratégia da Comissão foi justamente re-enquadrar os provedores como “serviço de acesso” (Título II, que implicaria automaticamente em maiores responsabilidades perante a FCC)”, tornando-os totalmente sujeitos a um novo conjunto de obrigações.

A nova resolução marca uma guinada importante na política americana, principalmente no que diz respeito à neutralidade de rede pois tenta estipular regras claras e coloca o agente regulador em uma posição ativa no processo. Um cenário distinto da regulação da privacidade no mesmo país, marcada pela preponderância do *laissez-faire* e por uma presença regulatória tímida neste campo.

Embora a resolução de fevereiro de 2015 seja hoje a mais importante base para a neutralidade no país, não significa que há o estabelecimento definitivo de regramento pró-neutralidade. Trata-se de uma guinada relevante, mas provisória sobre o tema. Embora a ordem tenha efeito prático, trata-se de uma norma infralegal, sujeita a modificações por uma eventual nova gestão da Comissão ou por novas ações judiciais que podem contestar o reenquadramento dos provedores. No campo político, há ainda o *lobby* das empresas no congresso americano por onde pode tramitar projetos de lei sobre o tema buscando redimensionar, no plano legislativo, o que está estabelecido pela FCC atualmente.

2.2 Privacidade *online* e neutralidade de rede na União Europeia

Na Europa, os países em geral possuem leis mais rígidas quanto à privacidade, destoando do modelo que prevalece nos EUA. Ao contrário do caso americano, a legislação europeia dá maior atenção à proteção da privacidade de consumidores e as agências reguladoras agem de modo mais consistente neste campo (FERNBACK; PAPACHARISSI, 2007; BUCHMANN et al, 2013; BYGRAVE, 2015;).

A própria União Europeia estabelece normas comuns que tentam amarrar todos os países do bloco com diretivas a serem implementadas por cada estado membro (FRA, 2014). As duas principais diretrizes europeias sobre privacidade são

o *Data Protection Directive*, aprovada em 1995 e em vigor desde 1998 (a principal norma) e a *Directive on Privacy and Electronic Communications*, de 2002 (também conhecida como e "Telecoms Package", por lidar com o setor de telecomunicações e, dentro disso, traz algumas direções sobre privacidade).

Para visualizarmos a tendência europeia de maior ênfase na privacidade, o caso que vem sendo chamado de “O Direito de ser esquecido” serve como um bom parâmetro[6]. A história começa com um advogado espanhol, Mario Costeja Gonzáles, que foi obrigado a vender alguns de seus bens em processos de insolvência no final 1990. Um jornal espanhol (La Vanguardia) reportou sobre o processo na época. Gonzáles resolveu seus problemas financeiros. Porém, quando o jornal passou a disponibilizar toda sua base de conteúdo na Internet, as informações sobre o problema financeiro de Gonzáles se tornaram acessíveis para um grande público. Diante disso, em 2010, o espanhol pediu que o La Vanguardia removesse as informações e o Google retirasse os resultados para a busca com seu nome. A Agência Espanhola de Proteção de dados julgou o caso e considerou que o La Vanguardia não precisaria retirar o conteúdo publicado *online*, mas o Google foi obrigado a apagar do seu buscador o tema sobre a insolvência financeira do advogado espanhol. O caso foi parar na Corte Europeia de Justiça que confirmou a validade da decisão da Agência.

A decisão tem gerado polêmica tanto na Europa quanto do outro lado do Atlântico e demonstra claramente uma tendência europeia de maior rigidez com a proteção da privacidade. Nos EUA, o New York Times publicou editorial criticando a decisão e apontando seus eventuais efeitos sobre o direito à informação:

> The European position is deeply troubling because it could lead to censorship by public officials who want to whitewash the past. It also sets a terrible example for officials in other countries who might also want to demand that Internet companies remove links they don´t like[7].

[6] Embora seja nomeado de “Direito de ser esquecido” este tema ainda não se consolida como um direito em *strictu sensu*: trata-se ainda de um debate sobre o potencial direito de não ser identificado online, de não ser indexado pelas plataformas digitais sob a justificativa de que isso violaria o princípio da privacidade.

[7] O texto na íntegra está disponível em <:http://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html?_r=0 > acesso 4 fevereiro 2015.

Para Toobin (2014) a decisão também demonstra que o modelo europeu estaria priorizando a privacidade em detrimento da liberdade de expressão e que o modelo americano faria justamente o inverso. O autor explica que nos EUA já houve ação semelhante no Texas, por exemplo, mas que a Justiça deu ganho de causa para o Google. Ele acredita que “the American regard for freedom of speech, reflected in the First Amendment, guarantees that the Costeja [Gonzalez] judgment would never pass muster under U.S. law” (2014, *online*)

A tendência europeia, neste caso, também parece não fazer coro no Brasil. A nova lei brasileira sobre o tema (Marco Civil da Internet) não versa sobre o papel dos buscadores no "direito de não ser indexado". Em linhas gerais, estipula que a retirada de conteúdo *online* só pode ser feita por ordem judicial. Em casos que afetam a privacidade e intimidade, a lei também prevê a possibilidade do indivíduo atingido negociar a retirada diretamente com a empresa. A jurisprudência que tem prevalecido no país diverge da posição europeia. Em 2012 o Supremo Tribunal de Justiça (STJ) não acatou o pedido da apresentadora Xuxa Meneghel para que o Google retirasse os resultados de busca para termos como "Xuxa pedófila"[8]. Em 2014, o caso chegou ao Supremo Tribunal Federal (STF) que manteve a decisão do STJ. E assim, outros tribunais regionais tem seguido este mesmo posicionamento para casos similares[9].

Se por um lado a privacidade *online* e a proteção de dados pessoais está relativamente enfatizada na União Europeia, a neutralidade de rede pode ser considerada um pouco menos consolidada. Algo em torno “do meio do caminho”. Embora haja diretrizes da agência reguladora europeia - o BEREC (*Body of European Regulators for Electronic Communications*) - afirmando seu comprometimento com a internet aberta e com a neutralidade de rede, não há uma lei sobre o tema que se aplique a todos os estados-membros. Há um projeto de lei em tramitação no Parlamento Europeu e são poucos os países com legislação específica em vigor. Para entender este cenário, a explicação do BEREC no

[8] Veja íntegra da decisão no *site* do Superior Tribunal de Justiça <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201103079096&dt_publicacao=29/06/2012 >

[9] Como o caso da decisão do Tribunal de Justiça de Goiás: < www.conjur.com.br/2015-fev-19/google-nao-obrigado-excluir-nomes-sistema-busca-tj-go >

documento "*Summary of BEREC positions on net neutrality*" pode ser esclarecedora:

> BEREC is committed to the open Internet, and believes that the existing regulatory tools, when fully implemented, should enable NRAs to address net neutrality-related concerns. For the time being, the situation appears to be mostly satisfactory and problems are relatively rare, though this assessment should be nuanced, as the situation varies significantly between national markets. Having said that, the net neutrality debate is legitimate, since rapidly envolving practices make it credible - though not certain - that problems will arise more frequently in the future. NRAs will therefore continue to closely monitor the evolution of the market, including setting up measurement schemes for the quality of the IAS available, and are ready to act whithout hesitation if necessary. (BEREC, 2012, p. 10)

A baixa ocorrência de violação significativa se dá pelo fato do mercado europeu ser mais competitivo e menos concentrado (quando comparado ao mercado dos EUA) o que acaba diluindo o poder das empresas no setor. Além disso, a política europeia é caracterizada historicamente por um perfil mais ativo dos entes reguladores neste segmento (MARCUS, 2014).

Saindo do plano geral e indo para as realidades nacionais, A Tabela 1 (OLMOS; CASTRO, 2013) traz um panorama sobre como os países membros tem tratado o tema da neutralidade.

Tabela 1: A neutralidade de rede nos países da União Europeia (2013)

	Possui posição oficial pública sobre o tema	Possui norma, mas não na forma de lei	Possui Lei aprovada ou projeto de lei	Anunciou planos de mensuração
Austria	X	X		
Belgium	X		X	
Bulgaria				
Croatia	X			
Cyprus				
Czech Republic	X			
Denmark	X	X		X
Estonia	X			
Finland	X			X
France	X	X		
Germany	X			X
Greece				
Hungary	X			X
Ireland	X			

Italy	X			
Latvia	X			
Lithuania	X			
Luxembourg	X		X	
Malta				X
Netherlands	X		X	
Poland	X			
Portugal	X			
Romania	X			X
Slovakia				
Slovenia	X		X	
Spain	X			X
Sweden	X			
United Kingdom	X	X		

(OLMOS; CASTRO, 2013, p. 3)

Como podemos notar, a maioria dos países não possui ainda a neutralidade firmada em lei. Na verdade, apenas Holanda e Eslovênia têm hoje leis aprovadas mencionando textualmente a questão. Nos casos de Luxemburgo e Bélgica (também marcadas na mesma coluna da tabela 1) possuem projetos de lei ainda em tramitação nos respectivos parlamentos.

Importante ressaltar que a ausência legal do princípio da neutralidade nas legislações nacionais europeias e a indefinição ainda de uma norma supranacional não significa que há uma tendência contrária a este princípio. Na verdade, o tema ainda não se tornou um objeto de debate e disputa relevante no continente, que parece sustentar hoje um quadro de regulação incipiente e reativa em casos de possíveis violações da neutralidade. O primeiro país europeu a firmar a neutralidade de rede em lei foi a Holanda em 2011 justamente como uma reação a um horizonte de violação[10]:

> The Dutch law was a direct result of public outrage over announcements by the Dutch network operator KPN of its intention to introduce a 'chat charge' for users of IP messaging applications such as WhatsApp in order to mitigate the negative impact that these applications were having on KPN's revenues from traditional SMS services (MARCUS, 2014, p. 90).

[10] A título de informação complementar: o primeiro país a fixar a neutralidade de rede em lei foi o Chile em 2010. O segundo a Holanda em 2011. O terceiro a Eslovênia em 2012. O quarto, o Brasil em 2014.

Em 2014, o Parlamento Europeu pré-aprovou diretiva que busca assegurar a neutralidade de rede como princípio a ser adotado pelos países membros[11]. Até o início de 2015, esta norma ainda estava em tramitação. Se transformada em lei, pode significar um passo adiante neste campo no continente europeu.

2.3 Privacidade *online* e neutralidade de rede no Brasil

No Brasil, até o início desta década, a legislação sobre privacidade basicamente se resumia a alguns artigos da Constituição Federal de 1988 e do Código Civil (Lei nº 10.406, de 2002.). Com a inexistência de uma lei específica, os litígios sobre invasão de privacidade e proteção de dados *online* vinham sendo resolvidos através de jurisprudência. Ou seja, a Justiça acabava gerando decisões com base na escassa normatização e essas sentenças se tornavam parâmetros para julgamentos futuros.

Neste cenário, alguns Projetos de Leis que versavam sobre privacidade e crimes cibernéticos surgiram no Congresso Nacional. Em 2012, foi aprovada a Lei nº 12.737 (também conhecida como lei Carolina Dieckmann) que trata de invasão de dados pessoais e, indiretamente, lida com privacidade (embora a palavra "privacidade" não apareça no texto. Também surgiram outras proposições, como o Projeto de Lei 84/1999, de autoria do deputado federal Eduardo Azeredo chegou a ser aprovado na Comissão de Ciência e Tecnologia da Câmara em 2012, mas recebeu um conjunto de críticas por tratar o usuário *online* predominantemente do ponto de vista criminal sem respeitar liberdades e direitos individuais. Acabou não tendo sua tramitação avançada.

Em meio a esse vácuo jurídico, o Ministério da Justiça lançou em 2009 o projeto do *Marco Civil da Internet*: uma consulta pública para uma futura lei que versaria sobre os direitos civis dos cidadão *online*, incluindo uma seção sobre

[11] Ver em <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+AMD+A7-2014-0190+237-244+DOC+PDF+V0//EN>

privacidade digital. A Lei 12.965 foi aprovada em abril de 2014 e está desde então em processo de implementação.

Na prática, no Brasil é possível falar que a lei do Marco Civil traz avanços importantes sobre a privacidade *online* e estabelece algumas normas na relação entre consumidor e provedores, diminuindo assim a insegurança jurídica até então vigente. Porém, há algumas limitações relevantes nesta nova legislação que ainda precisariam ser superadas: (a) a lei está em processo de regulamentação de artigos importantes por isso ainda necessita de normas complementares para funcionar de fato; (b) a lei não trata de privacidade fora da internet e, por isso, será complementada por uma outra legislação específica sobre proteção de dados, ainda em processo de elaboração[12]; (d) permanece a lacuna do ente regulador para o tema, um reflexo das fragilidades do sistema regulatório no país.

Além desses obstáculos, a forma como a guarda de *logs* foi definida pela lei também tem sido objeto de críticas. A nova norma passou a exigir a manutenção compulsória de dados de conexão do usuário para "eventuais investigações" sob ordem judicial por um período de 12 meses no caso dos provedores de acesso e durante 6 meses no caso dos provedores de aplicações. Embora a norma deixe clara a inviolabilidade das informações e obrigue as empresas a mantê-las seguras, para algumas organizações e ativistas, esta determinação consiste em uma forma de "grampo" prévio a todo cidadão. Ou seja, na prática cada indivíduo passa a ser indiscriminadamente monitorado, invertendo o princípio constitucional da presunção de inocência[13]. As críticas também afirmam que não há garantias de que os provedores possam utilizar comercialmente os dados pessoais dos usuários a fim de amortizar os custos de manutenção desses registros.

Já no que diz respeito à Neutralidade de rede, o cenário brasileiro também tem no Marco Civil um divisor de águas. Em seu Artigo 3º a nova lei afirma textualmente a “preservação e garantia da neutralidade de rede”. No Artigo 9º define

[12] Em paralelo à consulta pública para regulamentar os artigos do Marco Civil, o Ministério da Justiça também abriu uma debate para elaboração da minuta do Projeto de Lei de Proteção dos Dados Pessoais. Este texto visa ir além de questões de privacidade na Internet e tratará, por exemplo, da proteção da privacidade junto a bancos, empresas telefônicas, seguradoras etc..

[13] Ver texto integral da carta em < http://marcocivil.org.br/cartamc/ > Acesso 5 mar 2015.

que somente em duas exceções poderá haver a discriminação ou degradação do tráfego: em caso de (1) requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e em caso de (2) priorização de serviços de emergência. Os parâmetros de execução dessas exceções serão regulamentados por decreto presidencial, ainda em processo de elaboração.

A neutralidade de rede foi sem dúvida um dos temas mais polêmicos no processo de aprovação da lei do Marco Civil e, não por acaso, gerou um intenso *lobby* dos provedores de acesso (empresas de telecomunicações) para barrar a textualidade do princípio. Embora tenha sido aprovada, esta pressão continua agora no processo de regulamentação.

Um dos principais desafios que a regulamentação enfrenta é estabelecer a com clareza a exceção estipulada Art. 9º, ou seja, dizer quando e como as exceções podem ocorrer sem que isso se configure como quebra do princípio da neutralidade. Um outro desafio é criar condições concretas para que haja fiscalização evitando que o princípio seja violado na prática pelas empresas uma vez que o acompanhamento requer a ação de um ente regulador eficiente.

Conclusão

Este *paper* teve como objetivo compreender o atual estágio de regulação da Internet e seus impactos nos direitos civis, frente ao poder dos *players* comerciais. A discussão foi baseada em dois temas-chaves: privacidade *online* e neutralidade de rede. O estudo se concentrou em três contextos geopolíticos: EUA, União Europeia e Brasil e tentou configurar um quadro analítico sobre cada uma dessas realidades.

No que diz respeito à privacidade, os resultados demonstram que há atualmente modelos regulatórios distintos nos contextos analisados. Nos EUA prevalece uma regulação fraca marcada pelo *laissez-faire* e empoderamento das empresas sobre os dados pessoais *online.* No caso brasileiro, a regulação recém aprovada traz avanços (como a proibição do comércio de dados pessoais; regras e obrigações na guarda de dados etc.) mas ainda está em processo de regulamentação e implementação. Já na Europa, o cenário é marcado por um

conjunto de realidades legislativas e jurídicas tradicionalmente mais comprometidas com o principio da privacidade, havendo assim um quadro regulatório mais denso quanto a este tema.

No caso do debate sobre neutralidade de rede, os resultados demonstram que existe hoje uma tendência de adoção deste princípio nas três realidades geopolíticas estudadas. Entretanto, esta tendência se materializa através de diferentes estágios regulatórios e mecanismos de regulação. No Brasil, a neutralidade está assegurada por lei e segue para ser regulamentada e operacionalizada. Nos EUA a neutralidade está sendo instituída no plano infralegal (no nível das resoluções da agência reguladora) em um ambiente caracterizado por um mercado concentrado e por disputas judiciais entre regulador e operadoras. Já na União Europeia, há um cenário de pouca violação e por isso o bloco tem apenas diretrizes em defesa do princípio e uma lei em tramitação no parlamento europeu. Além disso, apenas dois países (Holanda e Eslovênia) possuem leis aprovadas sobre o tema.

Todo esse quadro demonstra que a regulação da Internet é um processo que já está em andamento e, devido à sua complexidade, ocorre em velocidades distintas e em graus de desenvolvimento diferentes entre os países. No atual estágio regulatório, nota-se que há ainda escassas legislações específicas que tratem da proteção dos direitos civis na Internet. Essas poucas leis, como o Marco Civil brasileiro, foram aprovadas recentemente e encontram-se nos primórdios de suas implementações e suas efetivações ainda precisam ser colocadas à prova.

Referências

BEREC. Body of European Regulatores for Electronic Communications. **Summary of BEREC positions on net neutrality**. BoR (12) 146, 2014. Disponível em <http://berec.europa.eu/files/document_register_store/2012/12/BoR_%2812%29_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf> Acesso 18 de janeiro 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Disponível em: <www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso: 10 ago. 2013.

BRASIL. **Lei Nº 12.96**5, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso: 10 jan. 2015.

BRASIL. **Lei Nº 10.406,** de 10 de janeiro de 2002 (Código Civil Brasileiro). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso: 16 jan. 2015.

BRIGGS, Asa & BURKE, Peter. Uma **história social da mídia**: de Gutemberg à Internet. Rio de Janeiro: Jorge Zahar Editor, 2006.

BUCHMANN. Johannes et al. **Internet Privacy**: Options for adequate realisation. Berlim: Springer-Verlag Berlin Heidelberg, 2013.

BYGRAVE, Lee A. Law and Technology A Right to Be Forgotten? **Communications Of The ACM***,* 58(1), p. 35-37, 2015.

CLARK, David D. **An Insider's Guide to the Internet**. MIT Computer Science and Artificial Intelligence Laboratory (Version 2.0). Cambridge: MIT, 2004

COOPER, Alissa. **How Regulation and Competition Influence Discrimination in Broadband Traffic Management**: A Comparative Study of Net Neutrality in the United States and the United Kingdom. 2013. Tese de doutorado (Doutorado em Communication and the Social Sciences). University of Oxford, St. Catherine's College.

DeCEW. Judith W. **In Pursuit of Privacy:** Law, Ethics, and the Rise of Technology. Ithaca e Londres: Cornell University Press, 1997.

EUA. Estados Unidos da America. **Telecommunications Act** de 1996. Disponível em <http://transition.fcc.gov/Reports/tcom1996.pdf >

EUA. Estados Unidos da América. **HIPAA - Health Insurance Portability and Accountability Act** de 1996. Disponível em <http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf > acesso 14 novembro 2014.

EUA. Estados Unidos da America. **COPPA - Children's Online Privacy Protection Act** de 1998. Disponível em <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> acesso 13 novembro 2014.

EUA.Estados Unidos da América. **GLB - Gramm-Leach-Bliley Act** de 1999. Disponível em < http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf > acesso 14 novembro 2014.

FERNBACK. Jan; PAPACHARISSI, Zizi. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. **New Media & Society**, 9(5), p. 715–734, 2007.

FRA. European Union Agency for Fundamental Rights. **Handbook on European data protection law.** Luxembourg: Publications Office of the European Union, 2014. Disponível em <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law >. Acesso 4 de fevereiro 2015.

LESSIG , Lawrence; MCCHESNE Y, Robert W. No Tolls on the Internet. In: **Whashington Post**. 8 de junho de 2006. Disponível em <http://www.washingtonpost.com/wpdyn/content/article/ 2006/06/07/AR 2006060702108.html>. Acesso em: 27 jun. 2012.

MARCUS, Scott. **Network Neutrality Revisited**: Challenges and Responses in the EU and in the US. Bruxelas: Parlamento Europeu, 2014. Disponível em < http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf. >

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. ***Big Data***: A Revolution That Will Transform How We Live, Work, and Think. Nova York: HMHBooks, 2013

OLMOS, Ana; CASTRO, Jorge. **Net Neutrality in the EU** - Country Factsheets (Report). Brussel: Open Forum Academy, 2013. Disponível em <http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20-%20Country%20Factsheets%2020130905.pdf >

PHILLIPS, David J. Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. **New Media & Society,** 6(6), p. 691–706, 2004

PORITZ, J. Who searches the searchers? Community privacy in the age of monolithic search engines. **Information Society**, 23 (5), p. 383-89, 2007.

SEVIGNANI, Sebastian. The commodification of privacy on the Internet. **Science and Public Policy**, 40, p. 733–739, 2013.

SHELANSKI, Howard A. Network Neutrality: regulating with more questions than answers. **Journal on Telecommunications and High Technology Law**, 6, p. 23-40, 2007.

TOOBIN, Effrey. The Solace of Oblivion: In Europe, the right to be forgotten trumps the Internet. **Annals of Law - New Yorker**, 29, 2014 (online). Disponível em <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion >.

TRAQUINA, Nelson. **Teorias do Jornalismo:** porque as notícias são como são (vol I e II). Florianópolis: Insular, 2005.

UE. União Europeia. **Data Protection Directive** - Directive 95/46/EC of the European Parliament and of the Council de 24 de outubro de 1995. Disponível em < http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 > acesso 11 novembro 2014.

UE. União Europeia. **Directive on Privacy and Electronic Communications -** Directive 2002/58/EC of the European Parliament and of the Council , de 2002. Disponível em < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> acesso 9 novembro 2014.

WOO, Jisuk. The right not to be identified: privacy and anonymity in the interactive media environment. **New Media & Society**, 8(6), p. 949–967, 2006.