Regulação da Internet como Administração da Privacidade

Internet Regulation as Governance of Privacy

Submetido(*submitted*): 13/12/2016
Parecer(*revised*): 14/01/2017
Aceito(*accepted*): 21/01/2017

Patricia Yurie Dias*

Resumo

Propósito – Análise dos elementos da teoria responsiva da regulação como mecanismos utilizados pelas empresas como administração do direito à privacidade na internet.
Metodologia/abordagem/design – Estudo da teoria responsiva de regulação de Ayres e Braithwaite e das normas e leis relacionadas com direito à privacidade e internet. Além disso, será abordado um caso jurídico e regulamentos dos Estados Unidos e União Europeia.
Resultados – A auto-regulação, o diálogo, a colaboração e a responsabilidade da regulação responsiva podem contribuir para a edição de padrões mínimos a serem seguidos pelas empresas ou regulados como administração da privacidade no âmbito da internet.

Palavras-chave: direito à privacidade, internet, regulação, marco civil da internet e regulação responsiva.

Abstract

***Purpose** – Analysis of the elements of responsive regulation as mechanism used by companies as a governance of the right to privacy on the internet.*
***Methodology/approach/design** – Study of the responsive regulation theory of Ayres and Braithwaite and the rules and laws related to the right to privacy on the internet. In addition, a legal case and regulations of the United States and European Union will be addressed.*
***Findings** – Self-regulation, dialogue, collaboration and accountability of responsive regulation can contribute to the edition of minimum standards to be followed by companies or regulated as a governance of privacy on the internet.*

Keywords: right to privacy, internet, regulation, Brazilian Civil Rights Framework for the Internet, responsive regulation.

Introdução

No Brasil, o marco civil da internet (MCI) ocorreu com a publicação da Lei nº 12.965/2014 que estabeleceu princípios, garantias, direitos e deveres para

*Analista em Ciência e Tecnologia desde 2010 no Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). Atualmente lotada na Coordenação-Geral de Assuntos Jurídicos de Comunicação (CGJC) da Consultoria Jurídica do MCTIC. Antes de ingressar no MCTIC, foi advogada na DATAPREV e analista na FUNASA. Graduada em Direito e Relações Internacionais pelo UniCeub e em Ciências Sociais pela UnB. Email: patriciaydias@gmail.com.

o uso da internet no Brasil. Contudo, quando ocorre uma violação ao direito à privacidade, em muitos casos a justiça brasileira encontra dificuldades em executar uma sentença judicial brasileira. Isso acontece, pois na maioria das vezes, não se identifica o violador ou a jurisdição brasileira não alcança o sujeito ou a empresa localizada em outro país, como por exemplo, a Google e o Facebook que possuem sede nos Estados Unidos. Este é um tema que tem sido discutido no âmbito da justiça brasileira, como pode ser visto no caso do RESP nº 712.456 interposto no STJ acerca da responsabilidade civil por conteúdo gerado na internet por terceiros. Dessa forma, tendo em vista que a internet é um fenômeno que abarca fronteiras transnacionais, a questão da regulação da internet é importante uma vez que se buscará estabelecer normas e princípios mínimos que protejam os direitos à privacidade em âmbito mundial.

O artigo utilizará a teoria responsiva de regulação de Ayres e Braithwaite a que sustenta que a regulação que o Estado pode proporcionar é limitada, por isso, propõe-se, uma auto-regulação dos entes privados com uma cooperação com diálogo entre os regulados em conjunto com uma regulação estatal na qual o Estado, por meio de leis e instrumentos normativos, estabelecerá punições casos haja transgressões legais. Ainda, o Estado também pode recompensar os regulados quando eles desempenharem comportamentos desejáveis. Com base nesta teoria, os regulados são motivados por um senso de responsabilidade onde os agentes são aptos a cooperarem. Para Braithwaite, dependendo de como o sistema regulatório se comporta, ele passa o sistema de normas para dentro do sistema de negócios. A pesquisa se utilizará de normas primárias (Constituição Federal e leis), bem como jurisprudência e doutrina, além da coleta de materiais disponíveis em sites de órgãos públicos nacionais e internacionais. Primeiro, serão abordados os principais conceitos teóricos da teoria de Ayres e Braithwaite e sua aplicabilidade na regulação da internet como administração da privacidade. Segundo, será analisado o direito à privacidade no âmbito da internet. Por fim, analisar-se-ão os instrumentos jurídicos existentes para a proteção do direito à privacidade na internet.

A estrutura do artigo será composta por: 1) Introdução; 2) Teoria responsiva de regulação de Ayres e Braithwaite; 3) Direito à privacidade; 4) Instrumentos normativos (leis e jurisprudência) relacionados à internet; e 5) Conclusão.

O enunciado da hipótese de pesquisa que se pretende comprovar no artigo é que o direito à privacidade potencialmente se beneficia dos resultados positivos de comportamento desejável quando a regulação da internet adota um desenho regulatório responsivo caracterizado pelos seguintes elementos: auto-regulação, diálogo, colaboração e responsabilidade.

Teoria responsiva de regulação de Ayres e Braithwaite

A teoria responsiva de regulação de Ayres e Braithwaite foi construída com base na ideia de quando se deve punir ou quando se deve persuadir os regulados de forma que eles adotem os comportamentos desejados pelos reguladores. A ideia é de que punir é caro, enquanto que a persuasão é mais barata, por isso, propõe-se a ideia de colaboração. Dessa forma, os autores criaram instrumentos regulatórios com base na pirâmide regulatória na qual a conduta do regulado irá determinar: se é preciso uma regulação mais ou menos intervencionista a depender de como a entidade age, se como um ator virtuoso, racional ou irracional. Ou seja, aumenta-se o grau de intervencionismo à medida que agrava as penalidades.

A pirâmide regulatória é formada basicamente com os seguintes elementos: auto-regulação (privada), auto-regulação forçada, regulação de comando com punição discricionária e regulação de comando com punição não discricionária (figura 1). A auto-regulação é a base da pirâmide, ou seja, é onde está maior parte das normas regulatórias que os regulados devem seguir sem serem coagidos por meios de punições. No topo da pirâmide estão os dispositivos legais que implicam infrações e punições no caso das entidades que não respeitaram as normas estabelecidas nas esferas abaixo do topo. Ayres e Braithwaite explicam que a base da pirâmide é ampla, pois é mais inclusiva, colaborativa e com uma abordagem regulatória baseada no 'diálogo'. Em cada um dos sucessíveis níveis a pirâmide tem cada vez mais 'intervenções punitivas', ou seja, se houver transgressões às normas tem que ter punições (AYRES e BRAITHWAITE, 1992, p. 39).

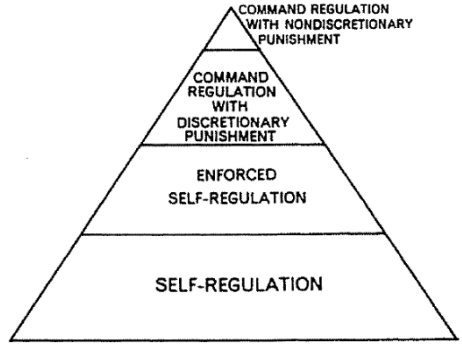

Figura 1

A ideia da pirâmide regulatória é desejável uma vez que classifica, em um primeiro momento, os regulados como sendo atores virtuosos, ou seja, eles são

considerados atores que agem de forma colaborativa com o setor que está sendo regulado. Somente se eles descumprirem as normas estabelecidas na base da pirâmide, o seu status de ator virtuoso vai sendo alterado para ator racional até ser considerado ator irracional. O modelo piramidal proposto por Ayres e Braithwaite busca aumentar a aderência dos regulados às regras e aos padrões mínimos, buscando favorecer o ator virtuoso, dissuadir o ator racional e incapacitar o ator irracional. Dessa forma, é preciso estabelecer punições caso a entidade não colabore com todo o sistema de regulação, e quanto mais se aproxima do topo, as punições vão ficando mais severas, até a pena máxima de cassação, ou seja, retirada da licença da entidade para atuar no setor regulado (BRAITHWAITE, 2006, p. 887).

Assim, verifica-se que Braithwaite apoia a auto-regulação, pois o melhor regulador é o próprio regulado, ou seja, é preciso proporcionar um ambiente onde os regulados atuam de forma própria. Contudo, o essencial na teoria da pirâmide regulatória é que gera a responsabilidade social uma vez que se busca construir um conjunto de normas no qual o sistema de normas funcionará, buscar-se-á uma construção das normas dentro da sociedade. Por isso, quando a regulação é mais legítima e justa, a aderência dos regulados à Lei é maior.

Por exemplo, considerando o contexto da regulação da internet como administração da privacidade, percebe-se que é possível que as empresas estabeleçam padrões mínimos que cada entidade precisa seguir para evitar que a privacidade dos cidadãos seja violada. As empresas podem criar manuais de procedimentos de forma que preservem mais as informações pessoais e protejam a privacidade dos seus usuários. De acordo com a teoria responsiva de regulação de Ayres e Braithwaite, esses padrões mínimos seriam a auto-regulação localizada na base da pirâmide, baseada no diálogo, na cooperação e na responsabilidade. Claro que, caso as empresas não adotem ou sigam tais padrões mínimos, os Estados, por meio de leis e normas, podem estabelecer regras de condutas básicas a serem seguidas e, se estas leis forem violadas, serão aplicadas as punições para cada caso.

No Brasil, o primeiro instrumento legal específico com relação a intervenção estatal na regulação da internet foi Lei nº 12.965, de 23 de abril de 2014, conhecida como marco civil da internet (MCI). Além disso, é importante notar que, apesar de o MCI ter sido a primeira lei específica sobre a rede mundial, antes já havia diversos instrumentos normativos que lidavam com o tema, a exemplo da Norma 004/1995[1], do Ministério das Comunicações – aprovada pela

[1]Norma 004/1995: "Uso de meios da rede pública de telecomunicações para acesso à internet aprovada por meio da Portaria MC nº 148, de 31 de maio de 1995 e publicada no Diário Oficial da União nº 104, seção 1, de 01/06/1995, p. 7875/7876.

Portaria nº 148 de 31/05/95 – e de Regulamentos da Anatel, como a Resolução nº 614/2013[2], que aprovou o Regulamento do Serviço de Comunicação Multimídia, mais conhecido como Internet fixa. A verdade é que o MCI foi o primeiro a estabelecer direitos para os usuários da Internet de forma clara e não esparsa, apesar de estes já terem proteção constitucional, a exemplo do direito à privacidade, neutralidade de rede – que é uma expressão do princípio da isonomia.

Direito à privacidade

Quando se trata de privacidade na internet, percebe-se que essa tecnologia tem permitido o monitoramento do comportamento das pessoas de forma contínua a um baixo custo. Um desafio constante aos formadores de políticas públicas é responder qual seria a quantidade de lei e tecnologia necessária para restaurar o nível adequado de controle da privacidade uma vez que esse nível deve equilibrar os interesses privados e públicos (LESSIG, 2006, p. 200).

A privacidade apesar de ser um conceito amplo, pode ser analisada a partir de dois aspectos, um voltado para o âmbito privado e outro para o público. No ambiente privado, a tradicional questão de "privacidade" está relacionada com o limite que a lei impõe para que uma pessoa ou governo possam invadir o espaço privado de outra; dessa forma, foram estabelecidas imposições legais como as leis e instrumentos normativos. No Brasil, a Constituição Federal de 1988 diz ser ilegal entrar na casa de alguém sem o seu consentimento. No espaço público a privacidade é vista mais no sentido de "vigilância", pois é o ambiente onde o indivíduo exerce relações sociais e atividades que são públicas. Geralmente, nesse ambiente não se tem proteção legal com relação à privacidade, pois, ao exercer as atividades rotineiras em âmbito público como caminhar, ir ao shopping, em tese, o indivíduo está renunciando o seu direito ao sigilo, uma vez que os outros conseguem monitorar e/ou controlar suas atividades que estão sendo realizadas no espaço público (LESSIG, 2006, p. 201).

Como o direito à privacidade não é absoluto, caso uma pessoa sinta que houve a violação de algum direito é possível ajuizar ação de reparação de dano, seja no âmbito público ou privado. Quando se trata de internet, percebe-se que as pessoas têm recorrido ao Judiciário quando sentem que teve algum direito violado na rede, como pode ser verificado no caso do RESP nº 712.456 interposto no STJ, no qual o autor, sacerdote da Igreja Católica, foi vítima de falsário que criou e-mail e perfil falsos no Gmail e Facebook e divulgou mensagens inverídicas com afirmações enganosas, inclusive sobre seu engajamento em uma associação de promoção da homossexualidade. O autor, após verificar o fato, entrou em contato

[2]Resolução Anatel nº 614/2013, publicada no Diário Oficial da União nº 103, seção 1, de 31/05/2013, p. 86/90.

com as rés Google e Facebook para a remoção do perfil falso, contudo, não obteve êxito. Dessa forma, a desídia das empresas em bloquear os perfis falsos, contribuiu para que permanecesse sendo divulgado o conteúdo jocoso e inverídico, abalando a imagem do sacerdote perante a sociedade e seus superiores eclesiásticos. Na sentença, o juiz condena as rés ao pagamento de R$ 10.000,00, a título de indenização por dano moral.

Em que pese a justiça brasileira ter condenado a Google e o Facebook, a execução da sentença se torna mais difícil tendo em vista que as empresas têm nacionalidade estrangeira e, ainda, há casos em que as violações cometidas no âmbito da internet extrapolam os limites territoriais de um país, dificultando assim, a aplicação do princípio da territorialidade que dispõe ser aplicável a lei brasileira ao crime cometido no território nacional, conforme o art. 5º do Código Penal. Dessa forma, empresas sediadas em diversos pontos do mundo têm gerado impactos sobre direitos de pessoas fora de sua jurisdição, assim, seria mais interessante que as empresas adotassem padrões mínimos de preservação da privacidade como forma de evitar futuras ações judiciais internacionais.

É importante frisar que, geralmente, a privacidade tende a ser renegada frente a valores que envolvem segurança nacional, terrorrismo, eficiência ou empreendedorismo. De acordo com a teoria política liberal a privacidade é conceituada como uma forma de proteger a liberdade individual, mas para Cohen essa privacidade não existe. Contudo, a liberdade das práticas de vigilância pública ou privada é fundamental para a prática de informação e reflexão da cidadania. Ou seja, nos dias de hoje, as tecnologias das informações têm permitido o monitoramento das atividades pessoas para que as empresas e/ou governo manipulem as informações disponíveis ao público por meio da utilização de ferramentas de pesquisas, filtros, plataformas sociais e propagandas. Isto quer dizer, se a cidadania envolve votar, participar de debates públicos e opinar; estes direitos somente são exercidos de forma plena quando as informações disponíveis ao público não são manipuladas de acordo com determinado interesse público ou privado. Privacidade é uma característica estrutural indispensável dos sistemas político democrático liberal. O entendimento dos propósitos de privacidade demanda uma abordagem estrutural para a regulação da privacidade. A proteção efetiva da privacidade requer uma atenção compreensiva aos atributos das práticas de vigilância privada e pública, e os caminhos que a vigilância privada e pública suplementa e reenforça uma a outra. A regulação efetiva da privacidade deve render sistemas de vigilância pública e privada significantemente transparente e responsável (COHEN, 2012, p. 2).

Instrumentos normativos (leis e jurisprudência) relacionados à internet

Por muitos anos, os Estados Unidos e Europa têm estudado quais são as medidas necessárias para assegurar uma proteção adequada de privacidade aos cidadãos. Com base nestes estudos, por volta de 1998, o *Federal Trade Commission – FTC*[3], que é agência federal dos Estados Unidos responsável pela defesa do consumidor americano e por manter a competição do mercado, tem sido responsável pelas políticas de privacidade desde 1970. A FTC elaborou um Relatório no qual estabeleceu os cinco princípios básicos para a proteção da privacidade, tais princípios ficaram conhecidos como sendo o *Fair Information Practice Principles – FIPPs*.[4]

Enquanto o governo americano não apresenta a legislação de privacidade, o FTC urge que as indústrias adotem medidas de auto-regulação para garantir a proteção à privacidade dos consumidores. Com isso, ressalta-se que em 2012, o FTC elaborou o Relatório sobre *"Protecting Consumer Privacy in an Era of Rapid Change"*[5] apresentando as melhores práticas para as empresas protegerem a privacidade dos consumidores americanos e darem aos consumidores o controle sobre a coleta e uso dos seus dados pessoais por meio de escolhas simples e aumento da transparência. O Relatório é como se fosse um manual de boas práticas para as empresas comercias e também servirá de base para a formulação da legislação de privacidade pelo Congresso americano.

Segundo o Relatório dos FIPPs elaborado pela FTC, os cinco princípios básicos para a proteção da privacidade são: 1) Aviso/Conhecimento: conhecimento prévio das práticas utilizadas antes da coleta de qualquer informação (identificação da entidade que coleta os dados, qual será o uso dos dados, natureza dos dados, destinatário dos dados); 2) Escolha/Consentimento: dar ao consumidor as informações de como os dados são coletados e serão usados, mas sem se limitar, a "cláusulas de *opt-in/opt-out*" que são ações afirmativas realizadas pelos usuário para permitir ou para impedir o uso dos dados; 3) Acesso/Participação: possibilidade do consumidor ter acesso aos dados sobre ele

[3]Federal Trade Commission – FTC. Disponível em: https://www.ftc.gov/. Acesso em: 27/11/2016.

[4]Federal Trade Commission – FTC. Privacy Online: A Report to Congress – Junho 1998. Disponível em: https://www.ftc.gov/reports/privacy-online-report-congress . Acesso em: 27/11/2016.

[5]Federal Trade Commission – FTC. Protecting Consumer Privacy in an Era of Rapid Change. FTC Report – Março 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf . Acesso em: 20/11/2016.

e também contestar a exatidão dos dados, a qualquer momento e sem custo; 4) Integridade/Segurança: assegura a integridade dos dados, bem como protege contra a perda dos dados e acesso não autorizado, destruição, uso ou divulgação dos dados, além da "anonimização"; 5) Execução/Reparação: mecanismos efetivos para aplicação dos FIPPs e também a reparação ao uso indevido dos dados (CARLONI, 2013).

O Relatório dos FIPPs baseou-se nos princípios defendidos em outras jurisdições, como o *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)[6] da *Organization for Economic Cooperation and Development* (OECD) e o *European Union Directive on the Protection of Personal Data* (1995)[7].

A União Europeia utilizou, por muitos anos, a Diretiva de Proteção de Dados da União Europeia 95/46 EC (DPD) como instrumento composto por uma série de regras que fornecem aos cidadãos europeus o controle sobre seus dados pessoais. Em 2012, a Comissão Europeia propôs uma reforma às regras de proteção dos dados dentro da União Europeia e; em 2016, a referida Diretiva foi substituída pelo Regulamento da União Europeia 2016/679 e pela Diretiva (EU) 2016/680[8]. Enquanto o Regulamento entrou em vigor em maio de 2016, somente deverá aplicado maio de 2018. A Diretiva entrou em vigor em maio de 2016 e todos os Estados Membros da União Europeia deverão adotar as regras às leis nacionais até maio de 2018. Por fim, ressalta-se que a Diretiva 2002/58/CE que dispõe sobre o tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas no âmbito da União Europeia terá que ser revista a fim de assegurar a coerência com o Regulamento da União Europeia 2016/679.

Os Estados Unidos, apesar de não ter um regime único de privacidade como o Regulamento da União Europeia, têm diversas leis de privacidade estabelecidas por setores como saúde, finanças, educação. Essas leis setoriais são estabelecidas com base em princípios e regras do FTC. Ainda, os Estados têm suas próprias leis de privacidade e segurança (KALYVAS, 2015, p. 34).

---

[6]Organization for Economic Cooperation and Development (OECD). Disponível em: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf . Acesso em: 18/01/2017.

[7]European Commission. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML . Acesso em: 18/01/2017.

[8]European Commission. Disponível em: http://ec.europa.eu/justice/data-protection/ . Acesso em: 28/11/2016.

O último relatório da FTC é sobre *"Protecting Consumer Privacy in an Era of Rapid Change"*[9] e sugere que as empresas adotem as seguintes práticas, além das FIPPs: 1) Privacidade por design: construir a privacidade em cada estado do desenvolvimento do produto. A empresa deve adotar os princípios substantivos (segurança dos dados, limites razoáveis para coleta, sons para práticas de retenção de dados, precisão nos dados) e procedimentos para implementar a proteção. 2) Escolha simples: permitir que os consumidores decidam sobre o uso dos dados em qualquer tempo e contexto, incluindo o mecanismo de "não rastrear". De acordo com o Relatório, as práticas que não requerem o consentimento para coletar e usar os dados são aqueles voltados para o uso primário da transação ou requerida por lei. Contudo, quando se tratar de dados utilizados para fins diferentes daqueles coletados ou coleta de dados sensíveis para certos propósitos é necessário obter o consentimento expresso e afirmativo antes da utilização. 3) Transparência: práticas de coleta e uso transparentes. Os avisos de privacidade devem ser claros, curtos e mais padronizados; o consumidor deve ter o acesso aos dados que as empresas mantêm, além dos esforços em educar os consumidores sobre as práticas de privacidade acerca dos dados comercializados.

Com relação ao Brasil, a legislação dispõe sobre a proteção da privacidade de forma dispersa e não específica e pode ser encontrada nos seguintes instrumentos normativos: Constituição Federal; Código Civil; Política Nacional de Informática e marco civil da internet. Ressalta-se que, com relação aos "dados pessoais" está tramitando no Congresso Nacional o Projeto de Lei (PL) nº 5.276/2016[10] para regulamentar a matéria. Esse PL está apensado ao PL da Câmara nº 4060/2012 que dispõe sobre o tratamento de dados pessoais. Além desse PL, tem o PL do Senado nº 330/2013[11] que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais.

A Constituição da República (CF) incluiu a privacidade no rol dos direitos fundamentais, como pode ser visto a proteção de forma direta 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."

[9]Federal Trade Commission – FTC. Protecting Consumer Privacy in an Era of Rapid Change. FTC Report – Março 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf . Acesso em: 20/11/2016.

[10]Projeto de Lei nº 5.276/2016 – Câmara dos Deputados. Disponível em: http://www.camara.gov.br/. Acesso em: 17/01/2017.

[11]Projeto de Lei do Senado nº 330/2013 – Senado Federal. Disponível em: http://www25.senado.leg.br/web/atividade/materias/-/materia/113947 . Acesso em: 17/01/2017.

Outros direitos a privacidade também foram garantidos de forma indireta pela CF como: proteger a inviolabilidade do domicílio (artigo 5º, XI) e da correspondência e das comunicações telegráficas (artigo 5º, XII). Dessa forma, verifica-se que a Carta Maior contém dispositivos que visam proteger a privacidade pessoal, seja da vida íntima do indivíduo ou de suas comunicações. Assim, entende-se que tal entendimento deve ser estendido aos instrumentos normativos que tratem da privacidade no âmbito da internet.

O Código Civil brasileiro menciona, ainda que de forma ampla, que a vida privada é inviolável, conforme pode ser visto no art. 21 do Capítulo II – Dos direitos da personalidade:

> "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Ressalta-se que foi ajuizada uma Ação Direta de Inconstitucionalidade no Supremo Tribunal Federal – STF (ADI nº 4815), tendo em vista o aparente conflito entre princípios constitucionais: liberdade de expressão (art. 5º IV, IV, XIV; 220, §§ 1º e 2º) e inviolabilidade da intimidade (art. 5º, X). O STF no dia 10/06/2015 julgou procedente a ADI nos seguintes termos:[12]

> "O pedido formulado na ação direta para dar interpretação conforme à Constituição aos artigos 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, declarar inexigível o consentimento de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais, sendo por igual desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas)."

O interessante dessa decisão do STF é que demonstra que a proteção da privacidade não é absoluta, uma vez que existem outros direitos envolvidos que podem estar sendo violados como o direito de pensamento e a liberdade de expressão. No caso citado, o STF buscou proteger o direito à liberdade de pensamento ao permitir a publicação de obras biográficas sem o consentimento da pessoa biografada. Contudo, vale ressaltar que não foi excluído o direito à privacidade ou intimidade da pessoa, então, se o autor extrapolar seus limites na obra biografada e a pessoa biografada se sentir lesada, é possível buscar reparação judicial.

A Política Nacional de Informática dispôs no art. 43º que as matérias relacionadas aos direitos relativos à privacidade e direitos da personalidade serão

[12]ADI 4815. Relatora Min. CÁRMEN LÚCIA, Tribunal Pleno, julgado em 10/06/2015, PROCESSO ELETRÔNICO DJe-018 DIVULG 29-01-2016 PUBLIC 01-02-2016). Supremo Tribunal Federal. Disponível em: http://www.stf.jus.br/. Acesso em: 29/11/2016.

objeto de leis específicas, a serem aprovadas pelo Congresso Nacional. Além disso, estabeleceu no art. 2º os seguintes princípios:

> Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:
>
> (...) VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas;
>
> (...)
>
> IX - estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas; (...)"

Em que pese aos diversos instrumentos normativos brasileiros tratarem de forma genérica acerca dos direitos à privacidade; foi com o marco civil da internet (Lei nº 12.965/2014) que esse direito foi tratado de forma um pouco mais específica no ambiente da internet.

De acordo com os incisos II do art. 3º do MCI, são princípios ao uso da internet do Brasil: II - proteção da privacidade, na forma da lei.

Assim, as inovações trazidas pelo marco civil da internet podem ser encontradas no decorrer do seu texto legal. O art. 7º da Lei nº 12.965/2014, assegura aos usuários os seguintes direitos e garantias: inviolabilidade da vida privada e indenização pelo dano material ou moral; não fornecimento de dados a terceiros; informações sobre coleta, uso, armazenamento, tratamento e proteção; finalidade da coleta; consentimento expresso e exclusão definitiva dos dados pessoais.

Além disso, o art. 8º da Lei nº 12.965/2014 dispõe que a garantia da privacidade nas comunicações é condição para o pleno acesso à internet, sendo nulas de pleno direito as cláusulas contratuais que violem essa regra, tais como aquelas que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet.

A Seção II da Lei nº 12.965/2014 contém os arts. 10 ao 12 que dispõem acerca da "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", no qual trouxe dispositivos acerca do respeito à preservação da intimidade, da vida privada, da honra e da imagem na guarda e na disponibilização dos registros e de acesso; respeito aos direitos de privacidade, à proteção de dados e ao sigilo das comunicações privadas e dos registros em qualquer operação de coleta, armazenamento, guarda e tratamento de registros. A seção também trata das sanções cíveis, criminais ou administrativas no caso de violação das normas anteriores.

Vale frisar, que o art. 15 do MCI abriu uma brecha legal para monitoramento uma vez que permite a guarda de registros de acesso e aplicações de internet pelo prazo de seis meses ou mais, podendo ser estendidos em caso de pedido judicial. Para Silvio Rhatto, tal determinação respeita menos os limites de privacidade do que os já previstos na Lei do Grampo (Lei nº 9.296, de 24 de julho de 1996) uma vez que: "na balança dos direitos individuais 'versus' interesses supostamente coletivos, o ganho de agilidade em investigações civis e criminais seria muito baixo em comparação à gravidade da drástica diminuição da privacidade de toda a população do país". Para Eduardo Neger fixar um prazo para guarda de dados foi um avanço da legislação, pois muitos provedores guardavam logs de acesso por tempos maiores do que foi determinado pelo MCI (PASSOS, 2014).

O art. 21 da Lei nº 12.965/2014 dispõe sobre a responsabilidade de danos decorrentes de conteúdo que violem a intimidade; e o art. 23º aborda os casos de segredo de justiça, inclusive acerca dos pedidos de guarda de registro.

Dessa forma, percebe-se que o MCI, se por um lado, protegeu o direito à privacidade, estabeleceu direitos aos usuários e criou regras para o acesso aos dados pessoais e registros de comunicações; por outro, estabeleceu regras que permitem o monitoramento do registro de acesso na internet. Assim, de acordo com a teoria de Ayres e Braithwaite, essas normas poderiam ser classificadas como sendo aquelas localizadas no topo da pirâmide regulatória chamadas de comando e controle do Estado. Quando estas regras são descumpridas o Estado aplica as sanções.

Tendo em vista o conhecimento dessas normas e com o objetivo de preservar a privacidade dos indivíduos, as empresas poderiam criar padrões mínimos a serem seguidos por elas, se quiserem podem até incorporar essas normas legais dentro das regras da própria empresa. Se isso ocorresse, seria uma forma de auto-regulação criada a partir da colaboração e diálogo entre as empresas.

Por fim, verifica-se que tanto a União Europeia quanto os Estados Unidos estão buscando formas e princípios que resguardem mais a proteção da privacidade dos cidadãos. Contudo, muitas vezes, os Estados, em defesa da segurança nacional (como a guerra contra o terrorismo), buscam justificar a excepcionalidade no tratamento de direitos fundamentais como a vida, a liberdade e a privacidade. O caso Snowden, que envolveu o vazamento de informações acerca da espionagem global feita pela Agência Nacional de Segurança dos Estados Unidos, abarca a questão dos limites à invasão da privacidade na internet (PILATI e OLIVO, 2014, p. 282).

Por outro lado, o Brasil, apesar de ainda não ter um documento específico para a proteção da privacidade, tem esforçado em criar instrumentos normativos

com o objetivo de delinear os direitos e obrigações no âmbito da internet, como pode ser visto com o marco civil da internet.

Conclusão

Diante dos argumentos apresentados, após a exposição da teoria responsiva de Ayres e Braithwaite, do conceito de privacidade e dos instrumentos normativos, verificou-se que o direito à privacidade potencialmente se beneficia dos resultados positivos de comportamento desejável quando a regulação da internet adota um desenho regulatório responsivo caracterizado pelos seguintes elementos: auto-regulação, diálogo, colaboração e responsabilidade.

A teoria responsiva de Ayres e Braithwaite pode ser aplicada na regulação da internet como forma de administração da privacidade por meio da auto-regulação e normas de comando e controle. A auto-regulação, que é a base da pirâmide regulatória, pode ser encontrada em normas internas das empresas que visam estabelecer padrões mínimos para proteger a privacidade dos usuários. O diálogo é outra ferramenta que a empresa pode utilizar com o Estado ou outros atores envolvidos com a internet, com o objetivo de se criarem ambientes mais protegidos e que garantam uma maior privacidade aos usuários da rede. A colaboração é um importante instrumento para o funcionamento da regulação da internet uma vez que os atores que colaboram sofrem menos punições do Estado pelo descumprimento das leis, pois estão colaborando com todo o sistema da internet. A responsabilidade dos atores envolvidos com a proteção da privacidade no âmbito da internet leva a uma maior segurança jurídica na rede, uma vez que quando a regulação é mais legítima e justa, a aderência dos regulados à lei é maior. Por fim, por outro lado, se os elementos acima não resguardarem a proteção da privacidade dos indivíduos, o Estado, por meio das normas de comando e controle, também pode criar um conjunto de normas legais que estabelece condutas básicas a serem respeitadas e se elas não forem seguidas pelas empresas serão aplicadas as punições para cada caso.

Com relação ao direito à privacidade na internet, verificou-se que a tecnologia tem permitido o monitoramento e a vigilância das pessoas. Dessa forma, tendo em vista que o direito à privacidade não é absoluto e para evitar a violação desse direito, é necessário estabelecer padrões mínimos e instrumentos legais que visem conceder uma maior proteção à privacidade. As empresas e os governos precisam atuar de forma transparente e responsável no tratamento dos assuntos relacionados com a privacidade dos indivíduos na internet.

Por fim, no que tange aos instrumentos normativos, verificou-se que tanto os Estados Unidos como a Europa têm publicado Relatórios, manuais de boas práticas e documentos para que as empresas observem os princípios e as regras a

serem seguidos para proteger de forma mais efetiva questões ligadas a privacidade dos indivíduos no âmbito da internet. Além disso, esses instrumentos visam conceder aos indivíduos um maior controle sobre a coleta e uso dos seus dados pessoais. O documento mais atual é o Regulamento 2016/679 e a Diretiva 2016/680, ambos da União Europeia. Com relação ao Brasil, apesar de existir projetos de lei acerca da regulamentação dos dados pessoais na internet, hoje o instrumento normativo mais conhecido é a Lei nº 12.965/2014 que estabeleceu o marco civil da internet e criou direitos e garantias aos usuários de internet.

Referências Bibliográficas

ADI 4815. Relatora: Min. CÁRMEN LÚCIA, Tribunal Pleno, julgado em 10/06/2015, PROCESSO ELETRÔNICO DJe-018 DIVULG 29-01-2016 PUBLIC 01-02-2016). Supremo Tribunal Federal. Disponível em: http://www.stf.jus.br/. Acesso em: 29/11/2016.

AYRES, Ian e BRAITHWAITE, John. ***Responsive Regulation: Transcending the Deregulation Debate***. Oxford, UK: Oxford University Press, 1992.

BRAITHWAITE, John. ***Responsive Regulation and Developing Countries***. World Development 34(5): 884-898, 2006.

CARLONI, Giovana Louise Bodin de Saint-Ange Comnène. ***Privacidade e Inovação na Era do Big Data.*** Trabalho de conclusão de curso em Direito apresentado à FGV DIREITO RIO, 2013.

COHEN, Julie E. ***What Privacy Is For.*** 2013, Harvard Law Review, Vol. 126. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2175406 . Acesso em: junho de 2016.

COMMISSION, European. Disponível em: http://ec.europa.eu/justice/data-protection/ . Acesso em 28/07/2016.

COMMISSION, Federal Trade – FTC. Disponível em: https://www.ftc.gov/ . Acesso em: 27/07/2016.

COMMISSION, Federal Trade – FTC. Privacy Online: A Report to Congress – Junho 1998. Disponível em: https://www.ftc.gov/reports/privacy-online-report-congress . Acesso em: 27/11/2016.

COMMISSION, Federal Trade – FTC. Protecting Consumer Privacy in an Era of Rapid Change. FTC Report – Março 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf . Acesso em: 20/11/2016.

FOUNTAIN, Jane E. ***Building the virtual state : information technology and institutional Change***. The brookings institution, Washington, D.C., 2001, p. 205.

KALYVAS, James R.; OVERLY, Michael R***. Big Data – A business and legal guide.*** CRC Press, 2015.

LESSIG, Lawrence. ***Code and other laws of cyberspace.*** Basic Books, 2006.

PASSOS, Juliana. ***O que os dados podem dizer sobre nós***. ComCiência n.158, Campinas, 2014.

PILATI, José Isaac e OLIVO, Mikhail Vieira Cancelier de***. Um novo olhar sobre o Direito à Privacidade: caso Snowden e pós-modernidade jurídica***. Seqüência (Florianópolis), n. 69, p. 281-300, dez. 2014. Disponível em: http://www.scielo.br/pdf/seq/n69/12.pdf . Acesso em: 19/01/2017.

RUBINSTEIN, S. Ira. ***Big Data: The End of Privacy or a New Beginning?*** New York University School of Law, International Data Privacy Law, 2013, Working Paper nº 12-56, p. 74.