Universidade de Brasília – UnB
Faculdade de Direito

ANA CAROLINA HERINGER COSTA CASTELLANO

PRIVACIDADE E PROTEÇÃO DE DADOS ELETRÔNICOS: UMA ANÁLISE JURÍDICO-REGULATÓRIA DO MARCO CIVIL DA INTERNET SOB A PERSPECTIVA DAS TEORIAS DA REGULAÇÃO DO CIBERESPAÇO DE LESSIG E MURRAY

Brasília
2016

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

PRIVACIDADE E PROTEÇÃO DE DADOS ELETRÔNICOS: UMA ANÁLISE JURÍDICO-REGULATÓRIA DO MARCO CIVIL DA INTERNET SOB A PERSPECTIVA DAS TEORIAS DA REGULAÇÃO DO CIBERESPAÇO DE LESSIG E MURRAY

Autor: Ana Carolina Heringer Costa Castellano

Orientador: Prof. Dr. Márcio Nunes Iorio Aranha Oliveira

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília - UnB.

Brasília, ___ de _____ de ____.

FOLHA DE APROVAÇÃO

ANA CAROLINA HERINGER COSTA CASTELLANO

Privacidade e Proteção de Dados Eletrônicos: uma análise jurídico-regulatória do Marco Civil da Internet sob a perspectiva das teorias da regulação do ciberespaço de Lessig e Murray

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília - UnB.

Aprovada em: ___ de _____ de ____.

BANCA EXAMINADORA

_____
Prof. Dr. Márcio Nunes Iorio Aranha Oliveira
(Orientador – Presidente)

_____
Prof. Dr. Alexandre Kehrig Veronese Aguiar

_____
Prof. Doutorando Thiago Luís Santos Sombra
(Membro)

_____
Prof. Dr.
(Suplente)

AGRADECIMENTOS

A presente pesquisa é reflexo do mundo novo que descobri ao longo da graduação em direito. Conforme os estudos e leituras foram se aprofundando, a tecnologia e a informatização deixaram de ser meros interesses de uma mente curiosa para serem objeto de pesquisa e reflexão jurídica. Nessa estrada não foram poucos os que me apoiaram e incentivaram para permanecer sempre em busca do conhecimento acadêmico, profissional e pessoal. Logo, não poderia deixar de agradecer, ainda que em poucas palavras, às pessoas responsáveis por me auxiliarem nessa caminhada.

Em primeiro lugar, agradeço a Deus que me deu a vida e é o meu refúgio nos momentos de aflição e incerteza. Seu infinito amor me traz alegria e esperança e me faz confiar nas promessas divinas.

Aos meus pais, Lenise e Murilo, rochas inabaláveis que em momento algum me fizeram duvidar da minha capacidade e sempre me proporcionaram todo o tipo de apoio para que eu chegasse até aqui. Agradeço também à minha irmã Isabella pelas opiniões e revisões nesse trabalho que, ainda que sob coação, o ajudaram a chegar a esta conformação final.

Às minhas queridas amigas Artemisa, Adriana, Carolina, Jéssica e Natália, que conheci em meu primeiro ano da faculdade e me acompanharam até aqui. Vocês não somente foram brilhantes colegas de curso, que me incentivaram a ser uma acadêmica melhor, mas, sem dúvidas, foram pessoas essenciais em todos os momentos da minha vida, compartilhando juntas incertezas, dificuldades, sonhos e alegrias.

Ao meu orientador Márcio Iório Aranha pela sua admirável dedicação e compromisso com seus alunos, além da brilhante contribuição para o mundo jurídico e acadêmico.

Por fim, agradeço aos membros da banca que se mostraram prontamente solícitos diante do convite por mim realizado. As trajetórias acadêmicas traçadas por vocês servem como fonte de inspiração e me incentivam a continuar progredindo nessa nascente jornada acadêmica.

RESUMO

O presente trabalho tem como objetivo identificar e compreender as principais transformações que levaram a uma nova configuração social e econômica, pautada na informação, analisando, sobretudo a privacidade e a proteção de dados no ambiente digital. Com base nas teorias de Lawrence Lessig e de Andrew Murray, busca-se avaliar o cenário regulatório do ciberespaço e as diferentes proposições para limitar o comportamento na plataforma em rede, identificando os papeis do código e dos diversos atores da internet nesse processo. Outrossim, a partir desses substratos teóricos, o trabalho tem como escopo principal analisar as consequências da informatização para direitos fundamentais como privacidade e proteção de dados. Nessa esteira, indaga-se como as "pegadas digitais" deixadas no mundo virtual afetam não só as relações entre o indivíduo e as grandes empresas da internet, que fizeram da informação seu novo modelo de negócio, mas também a relação entre os cidadãos e o Estado, que, a partir do de seu papel ativo na produção de tecnologia vem realizando, cada vez mais, um processo conhecido como vigilância digital. Estabelecido esse cenário global, o presente trabalho pretende analisar a Lei nº 12.965/16, conhecida popularmente como Marco Civil da Internet, primeira legislação brasileira dedicada a disciplinar as relações digitais nacionalmente. Em seguida, entendido o contexto geral do instrumento normativo, pretende-se considerar de forma mais específica como a lei em comento trata os dados armazenados na rede, bem como o sigilo e inviolabilidade das comunicações online no Brasil. Por fim, analisar-se-á o decreto 8.771/16 que regulamenta a referida lei, especialmente no que concerne a proteção de dados e requisição judicial de informações, identificando os pontos de avanço e os pontos que ainda se encontram nebulosos e de difícil aplicação.

Palavras-chaves: Regulação do Ciberespaço; Privacidade; Proteção de Dados; Vigilância Digital; Marco Civil da Internet

ABSTRACT

The following research paper aims to identify and understand the main transformations that have led to a new social and economic setting, based on information, analyzing, mainly, privacy and data protection in the digital environment. Based on the theories of Lawrence Lessig and Andrew Murray, we try to evaluate the regulatory scenario of cyberspace and the different propositions to constrain human behavior in the network platform, identifying the roles of the code and the various actors of the Internet in this process. In addition, based on these schools of thought, the main purpose of this paper is to analyze the consequences of digitalization for fundamental rights such as privacy and data protection. In this regard, it is questioned how the "digital footprints" left in the virtual world affect not only the relations between the individual and the large Internet companies, which have made information their new business model, but also the interaction between citizens and the State, which, based on its active role in the production of technology, is increasingly engaging in a process known as digital surveillance. Once established this global scenario, the present research aims to analyze the Law 12.965 /16, popularly known as Marco Civil da Internet, the first Brazilian framework dedicated to disciplining digital relations nationally. With the understanding of the general context of the normative instrument, it is intended to consider in a more specific way in which the law in question treats the data stored in the network, as well as the secrecy and inviolability of online communications in Brazil. Finally, we analyse the Decree 8.771/16 that regulates said law, especially in what concerns data protection and judicial requisition of information, identifying the points of progresss and the points that are still cloudy and difficult to apply.

Keywords: Cyberspace regulation; Privacy; Data Protection; Digital Surveillance; Marco Civil da Internet

SUMÁRIO

INTRODUÇÃO

A informatização da sociedade alterou por completo, e em escala global, as relações interpessoais, resignificando conceitos essenciais como tempo e espaço. Essa nova configuração, que na teoria das ciências sociais é chamada *sociedade da informação ou do conhecimento*[1], foi alcançada por meio de duas grandes mudanças nas economias mundiais mais avançadas: (i) a transição para uma economia centrada na informação, na produção cultural e na manipulação de símbolos e (ii) o surgimento da internet (BENKLER, 2006). Assim, nos dias atuais, as formas de comunicação, entretenimento, compra e venda, prestação de serviços, enfim, todas as atividades inerentes à condição social humana podem ser traduzidas para essa nova linguagem computacional e encontram-se nesse território ainda incerto chamado ciberespaço.

Com a rápida ascensão da rede e do fenômeno da digitalização da informação, a sociedade deixou de depositar valor em átomos, ou seja, bens tangíveis, para reconhecer valor em "bits", que é a informação traduzida em dígitos binários (NEGROPONTE, 1995). Pode-se afirmar, portanto, que a informação se tornou a moeda de câmbio mais valiosa dos dias de hoje. Desta forma, a questão não está mais centrada em se o ciberespaço deve ser regulado ou não. Há um consenso quase que unânime entre os doutrinadores da área de que a regulação do mundo digital é imprescindível. O problema reside justamente em identificar quem deve ser o regulador e qual a melhor maneira de fazê-lo. Assim, os operadores do direito têm em suas mãos a complexa tarefa de reorganizar a estrutura jurídica de forma a adequar essas novas relações aos campos normativo e regulatório, trabalhando com fronteiras invisíveis, soberanias mitigadas e informações que mudam a cada segundo.

Dentro desse contexto, um questionamento recorrente e que vem desafiando os juristas é o que diz respeito aos dados e conteúdos armazenados na rede. Atualmente, é possível afirmar que a vida inteira de um cidadão está digitalizada e alocada em um servidor, que por sua vez pode estar localizado em qualquer parte do planeta. Como já destacado, a informação digital se tornou comercialmente mais rentável do que a informação analógica (MURRAY, 2016); consequentemente, ela é fortemente explorada pelos gigantes tecnológicos, isto é, grandes empresas, que, por dominarem a arquitetura da internet, fizeram do processamento de dados o

[1] Castells discorda desta terminologia, pois para ele, conhecimento e informação sempre foram elementos centrais em todas as sociedades historicamente conhecidas. A novidade reside no fato de ser uma sociedade baseada na microeletrônica, isto é, as relações sociais organizam-se por meio de redes tecnológicas. Por essa razão, ele cunhou o termo "Sociedade em rede". (CASTELLS, 2005)

caminho para lucros astronômicos.[2] Dessarte, é imperioso entender como são tratados estes dados, i.e, quem tem o direito de coletá-los, processá-los e armazená-los e quais os limites e responsabilidades legais para tanto, a fim de garantir direitos fundamentais como identidade e privacidade.

O Brasil, que não poderia escapar a essa nova realidade digital, em face aos desafios que vem enfrentando inerentes ao ambiente em rede, aprovou, em abril de 2014, o Marco Civil da Internet, nome popular da lei federal nº 12.965/14. Editada para ser uma "Constituição da Internet", estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil, essa legislação foi um divisor de águas no que concerne à regulação da internet em âmbito nacional, sobretudo ao que diz respeito à guarda de registros, privacidade dos dados e o conteúdo disponibilizado na Internet.

Embora seja uma legislação de vanguarda, o Marco Civil da internet apresenta diversas lacunas e impropriedades, abrindo espaço para um intenso debate nos cenários político, jurídico e acadêmico brasileiros. Essa insuficiência do diploma legal pode ser percebida ao analisar os recentes e polêmicos embates[3] entre o poder judiciário e o aplicativo de troca de mensagens WhatsApp, empresa pertencente ao Facebook, que levantaram questões essenciais como privacidade, criptografia e requisição judicial de informações. O objetivo da presente pesquisa, portanto, é analisar a legislação brasileira sob a perspectiva das grandes teorias da regulação do ciberespaço: a regulação por código de Lessig e o "network communitarianism" de Murray, avaliando os principais pontos de convergência e também de dissonância entre as duas e fazer um contraponto com o direito comparado, em especial o da União Europeia

Embasarão a presente pesquisa a teoria da regulação por código de Lessig, que vê na arquitetura do ciberespaço a chave para a regulação das relações digitais, isto é, para ele, aquele que detém o código é o regulador (LESSIG, 2006) e a teoria do "network communitarianism" de Andrew Murray, que acredita na existência de uma relação simbiótica e dinâmica entre os atores participantes da rede, isto é, entes públicos, privados e usuários (MURRAY, 2016). Com

[2] Segundo o mais recente estudo BrandZ realizado em junho de 2016 pela Millward Brown, empresa britânica mundialmente reconhecida pelas pesquisas de mercado, a empresa Google foi considerada, pela segunda vez em três anos, a marca mais valiosa do mundo, valendo $ 229.2bn (http://wppbaz.com/admin/uploads/files/BZ_Global_2016_Report.pdf)

[3] Em um espaço de tempo de menos de um ano, o aplicativo de troca de mensagens WhatsApp — com cem milhões de usuários no país — saiu do ar no Brasil por três vezes em razão de decisões judiciais. A polêmica é motivada pelo impasse entre a tentativa da Justiça de obter informações para subsidiar investigações criminais e a defesa da empresa, que alega não dispor dos dados devido ao seu sistema de criptografia ponta-a-ponta (STF derruba ordem de bloqueio do WhatsApp, disponível em http://oglobo.globo.com/economia/stf-derruba-ordem-de-bloqueio-do-whatsapp-19747680, acessado em 31/08/2016)

esses substratos teóricos, busca-se responder a seguinte pergunta de pesquisa: Como o tratamento da proteção de dados eletrônicos pelo ordenamento jurídico brasileiro e jurisprudência no período de 2014 até o momento atual se relaciona com as teorias de Lessig e Murray?

A Base empírica da pesquisa, ao enfrentar a pergunta proposta, se valerá do Marco Civil da Internet, da Constituição Federal, das normas de direito internacional, da jurisprudência norte-americana e da jurisprudência pátria a partir de abril de 2014.

Esse artigo será estruturado da seguinte forma: a) inicialmente, serão firmados os pressupostos teóricos que fundamentarão a pesquisa, tecendo uma análise mais aprofundada sobre as principais teorias da regulação do ciberespaço, quais sejam, a regulação por código de Lessig e o comunitarismo em rede (*network communitarianism*) de Andrew Murray; b) posteriormente, serão analisados os conceitos de privacidade e proteção de dados, buscando compreender como estes direitos estão situados no contexto informacional e como se adequam às duas teorias já destacadas; c) por fim, será feita uma pesquisa documental, analisando-se a legislação brasileira que trata sobre a internet, sobretudo o Marco Civil da Internet e o Decreto 8.771/16. Nessa esteira serão abordados dois temas disciplinados pela legislação: a proteção de dados e conteúdos armazenados na rede e o sigilo e inviolabilidade das comunicações, considerando-os sob a perspectiva da regulação por código e do comunitarismo em rede.

CAPÍTULO 1 – ECONOMIA DA INFORMAÇÃO EM REDE E REGULAÇÃO DO CIBERESPAÇO

> *Cyberspace was a consensual hallucination that felt and looked like a physical space but actually was a computer-generated construct representing abstract data.*
>
> Willian Gibson. Neuromancer, 1984.

Nesse capítulo serão abordadas as principais mudanças que levaram à configuração de um novo modelo de economia - a economia da informação em rede - e que ensejaram a criação de uma nova realidade virtual, conhecida como ciberespaço. Ademais, serão destacadas as principais teorias da regulação do ambiente em rede: ciberlibertarianismo, ciberpaternalismo e comunitarismo em rede, fazendo um paralelo entre essas duas últimas.

1.1 A ECONOMIA DA INFORMAÇÃO EM REDE

Informação, conhecimento e cultura sempre foram elementos centrais em todas as sociedades historicamente conhecidas (CASTELLS, 2005). É a forma como eles são produzidos e manipulados pelos indivíduos que diferencia os modelos de economia adotados e estabelece a configuração das relações interpessoais. Nesse cenário, a partir das diversas mudanças tecnológicas nas últimas décadas, foi possível notar uma série de adaptações econômicas, sociais e culturais que viabilizaram uma transformação radical do nosso papel como indivíduos autônomos, cidadãos e membros de grupos sociais nesse novo ambiente informacional (BENKLER, 2006).

Este processo de transformação é não só estrutural, uma vez que está relacionado aos próprios fundamentos de como mercados e democracias liberais se desenvolveram ao longo de quase dois séculos, como também é multidimensional, já que não é a tecnologia que determina a sociedade, e sim "a sociedade que dá forma à tecnologia de acordo com as necessidades, valores e interesses das pessoas que utilizam as tecnologias." (CASTELLS, 2005, p. 17).

Dentro desse contexto, podem-se destacar duas grandes mudanças nas economias mais avançadas, que ensejaram essa nova configuração da sociedade. A primeira delas é a transição para uma economia centrada na informação, i.e, a ascensão de áreas como finanças,

contabilidade e ciências; na produção cultural, como por exemplo a indústria da música e do cinema; e na manipulação de símbolos, ou seja, o valor é cada vez mais agregado a marcas em vez de aos produtos em si. A segunda foi a migração para um ambiente de comunicação erigido a partir de processadores de baixo custo e de alta qualidade, interconectados em uma rede ubíqua e global, isto é, o fenômeno hoje conhecido como "internet". Benkler (2006) denomina esse novo modelo de economia como "economia da informação em rede", que nas ciências sociais encontra seu reflexo na teoria da "sociedade em rede" de Castells, definida como:

> uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. (CASTELLS, 2005, p. 20)

Esse modelo teve início primordialmente nos Estados Unidos da América, que observou um aumento substancial na taxa de crescimento de sua produtividade no período entre 1996 e 2005. Segundo Castells (2005), o aumento da produtividade é o indicador empírico mais direto da transformação de uma estrutura produtiva. Desta feita, enquanto outros países investiam em uma economia de serviços, os norte-americanos, já em meados dos anos 1980, cunhavam um novo formato de mercado baseado em sistemas que permitem a coleta, o armazenamento e o processamento de informação.

Nesse cenário, cumpre destacar o papel fundamental do Estado, que atuou, e ainda atua, como protagonista no processo de informatização. Foi a partir dos riscos de investimento assumidos pelo Estado que novos mercados foram criados, abrindo espaço para um processo exponencial de inovação. Dessa forma, setores já consolidados e outros ainda emergentes, como os de tecnologia da informação e comunicação, farmacologia, biotecnologia, nanotecnologia e tecnologias verdes, tiveram o Estado como agente empreendedor, disposto em assumir os riscos das inovações mais radicais, incentivando a participação de atores econômicos e científicos[4]. (MAZZUCATO, 2014) Foi exatamente nesse contexto, propiciado pela atuação estatal, que os visionários do Vale do Silício acertadamente identificaram que o valor não está na informação

[4] Nesse sentido Mazzucato (2014, p. 133) afirma: "a Apple concentra seu talento não no desenvolvimento de novas tecnologias e componentes, mas em sua integração em uma arquitetura inovadora". Segundo a autora, grande parte das tecnologias incorporadas por essa gigante do Vale do Silício foram, na verdade, desenvolvidas sob esforços coletivos e cumulativos conduzidos pelo Estado. A empresa surfou a onda dos maciços investimentos públicos na informática e na internet. Sua habilidade reside no reconhecimento de tecnologias emergentes com grande potencial, aplicação de conhecimentos complexos em engenharia para integrar tecnologias de sucesso e priorização no desenvolvimento de produtos com foco no design. Ademais cumpre ressaltar que a Apple desfruta, ainda, de apoios tributários e contratos públicos nos Estados Unidos, além da proteção governamental da propriedade intelectual das empresas.

em si; ele está, na verdade, naquilo que as pessoas podem fazer com ela (MURRAY, 2016). Essa realização significou uma transição do valor econômico agregado às coisas, o que nos termos da física pode-se denominar átomos, para um valor econômico agregado à informação, que no ambiente digital denomina-se *bits* (NEGROPONTE, 1995).

A física Einsteiniana impõe contornos à matéria por meio de elementos como tempo e espaço, ou seja, ela está confinada por barreiras geográficas e temporais. O mesmo não ocorre no espaço virtual. Enquanto no mundo físico partículas portadoras de massa, como os átomos que compõem o corpo humano, se limitam a viajar em baixas velocidades, as partículas sem massa podem viajar a uma velocidade máxima de até 299.792.458 metros por segundo, o suficiente para ir quase que instantaneamente de um ponto a outro qualquer na superfície do planeta. É com essa a velocidade que os bits, i.e, a informação traduzida em dígitos binários, se deslocam por esse espaço virtual, conhecido como ciberespaço, cuja representação material são as redes de cabos e ondas eletromagnéticas que cruzam o planeta. Hoje, bits e átomos estão se tornando cada vez mais intercambiáveis: se no início o ciberespaço era um lugar onde trafegava apenas texto, hoje nele trafegam imagens em movimento e áudio. (VERLE, 1997)

A transição da informação analógica para a informação em bits se deu por meio de um fenômeno denominado digitalização. Digitalizar um sinal é extrair dele amostras, que se colhidas a pequenos intervalos, podem ser utilizadas para produzir uma réplica aparentemente perfeita daquele sinal (NEGROPONTE, 1995, p. 19). Esse processo é vantajoso por diversas razões, dentre elas: (i) a facilidade de se criar, manipular, transmitir e armazenar a informação; (ii) a diminuição do custo de coletar, manipular, armazenar e transmitir dados; (iii) o desenvolvimento de um valor intrínseco da informação eletrônica, o qual não pode ser encontrado na informação analógica devido à sua própria natureza; e (iv) a possibilidade que os padrões de operação de sistemas computacionais e de rede oferecem de criar informações digitais adicionais por meio de cópias de *back up e cache* (CATE, 1997).

Com o desenvolvimento das tecnologias de computação, comunicação e armazenamento e o consequente declínio de seus preços - uma das principais marcas da economia da informação em rede - os indivíduos passaram a assumir um papel mais ativo no processo de produção de informação. Isso significa que as barreiras físicas antes existentes, como imprensa, mídia e gravadoras, por exemplo, foram mitigadas, tornando a criatividade humana e a informação em si a base dessa nova economia. Andrew Murray (2016, p. 45) denomina esse fenômeno de “desintermediação”, no qual os “intermediários na cadeia de

produção são eliminados e os lucros resultantes dessa operação são divididos entre produtor e consumidor. ”

Alinhado com a desintermediação, está aquilo que Jonathan Zittrain (2008, p. 70) chama de “generatividade” (*generativity*), isto é, a “capacidade de uma tecnologia de produzir mudanças por iniciativa de uma larga, variada e descoordenada coletividade”[5]. O computador pessoal (PC), aliado à internet, desenvolveu-se de forma eminentemente generativa. Desde o início, ele foi arquitetado para fazer funcionar qualquer programa criado pelo distribuidor, pelo usuário ou por um terceiro remoto, tornando a criação de tais programas relativamente fácil. Quando essas máquinas, extremamente adaptáveis, são conectadas a uma rede com pouco controle centralizado, o resultado é uma matriz quase que totalmente aberta à criação e à rápida distribuição de inovação por usuários experts em tecnologia. Assim, a emergência e a participação ativa do indivíduo na rede montaram o cenário perfeito para um ambiente de compartilhamento e comercialização da informação: a Web 2.0

A Web 2.0 pode ser definida como “a segunda geração de serviços online e caracteriza-se por potencializar as formas de publicação, compartilhamento e organização de informações, além de ampliar os espaços para a interação entre os participantes do processo. ” (PRIMO, 2007, p. 2). Com o advento de empresas como Google, Amazon, Wikipédia, eBay, etc., o valor dos produtos digitais, que antes era majoritariamente facilitado pelos softwares, passou a ser, sobretudo, co-criado pela e para a comunidade de usuários. Desde então, novas plataformas, como Youtube, Facebook e Twitter, encontraram o sucesso na mesma fonte: a exploração da “inteligência coletiva”, *i.e*, a manipulação e a compreensão de enormes quantidades de dados gerados pelo usuário em tempo real. Assim, atualmente, os subsistemas do sistema operacional da internet são cada vez mais baseados em dados, tais como localização e identidade (de pessoas, produtos e lugares), e nas teias de significado que os conectam e lhes dão sentido (O’REILLY e BATTELLE, 2009).

A Web 2.0, portanto, não se trata apenas de uma combinação de técnicas informáticas. Ela é, principalmente, o marco de um período tecnológico, um conjunto de novas estratégias mercadológicas e de processos de comunicação mediados pelo computador. Esse novo formato de conexão em rede apresenta importantes repercussões sociais e potencializa processos de

[5] *Generativity is a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences.*

trabalho coletivo, trocas afetivas, produção e circulação de informações e construção social de conhecimento apoiada pela informática (PRIMO, 2007).

Diante do exposto, não restam dúvidas de que a utilização da informação digital é melhor e mais eficiente. Por meio de um processo simples e barato, "as pessoas passaram a integrar as tecnologias em suas vidas, conectando a realidade virtual com a virtualidade real e articulando essas duas esferas conforme as suas necessidades." (CASTELLS, 2005, p. 23). Contudo, à medida que os indivíduos passaram a transferir a maior parte de suas atividades para essa nova realidade chamada ciberespaço, diversos questionamentos foram colocados em pauta, especialmente no que diz respeito ao exercício das liberdades individuais (DONEDA, 2006).

Embora a linguagem e a plataforma em que as relações interpessoais ocorrem tenham mudado, os conflitos inerentes às relações humanas permanecem os mesmos. Nesse sentido, Negroponte (1995) já afirmava que apesar de vivermos em um mundo repleto de bits, ainda pensamos de acordo com uma lógica de átomos. A questão que se coloca diante dos operadores do direito, então, é: como regular um ambiente completamente desprovido de territorialidade e coesão social, que possui em seu seio diversas micro-comunidades, as quais estão interessadas em proteger apenas os próprios interesses? (MURRAY, 2011). Assim, para tentar dar uma resposta a essa indagação, surgiram diversas teorias sobre a regulação do ciberespaço, que pretendem pensar um sistema que assegure direitos individuais tanto online como offline, protegendo os valores e princípios eleitos pela sociedade como fundamentais.

1.2. TEORIAS DA REGULAÇÃO DO CIBERESPAÇO

1.2.1 Ciberlibertarianismo

Os primeiros teóricos da regulação do ciberespaço acreditavam que a realidade virtual era um mundo distinto para o qual os usuários se transportavam ao navegar na internet. Para eles, esse novo território, de soberania e jurisdição próprias, seria inatingível pelas leis dos Estados físicos, que estariam restritos às suas fronteiras naturais. Ademais, o fato de os indivíduos que navegam nesse ambiente virtual não possuírem corpos físicos e os bens digitais que detêm serem infinitos, tornaria impraticável qualquer tipo de sanção que se pretendesse aplicar (MURRAY, 2016).

Nesse sentido, John Perry Barlow, ex-lírico da banda Grateful Dead, co-fundador da *Eletronic Frontier Foundation* e conhecido ativista da internet, encapsulou essa ideia de

liberdade irrestrita do ambiente online em sua icônica Declaração de Independência do Ciberespaço:

> Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são benvindos entre nós. Vocês não têm a independência que nos une.
>
> Os governos derivam seu justo poder a partir do consenso dos governados. Vocês não solicitaram ou receberam os nossos. Não convidamos vocês. Vocês não vêm do espaço cibernético, o novo lar da Mente.
>
> Não temos governos eleitos, nem mesmo é provável que tenhamos um, então eu me dirijo a vocês sem autoridade maior do que aquela com a qual a liberdade por si só sempre se manifesta.
>
> Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer.
>
> [...]
>
> Seus conceitos legais sobre propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. Eles são baseados na matéria. Não há nenhuma matéria aqui.
>
> Nossas identidades não possuem corpos, então, diferente de vocês, não podemos obter ordem por meio da coerção física. Acreditamos que a partir da ética, compreensivelmente interesse próprio de nossa comunidade, nossa maneira de governar surgirá. Nossas identidades poderão ser distribuídas através de muitas de suas jurisdições.
>
> [...]
>
> Criaremos a civilização da Mente no espaço cibernético. Ela poderá ser mais humana e justa do que o mundo que vocês governantes fizeram antes. (BARLOW, 1996)

Esse manifesto, apesar de seu caráter utópico, resume as ideias de diversos teóricos, que mais tarde viriam a ser chamados ciberlibertários (JOHNSON e POST, 1996). Eles acreditavam que o ciberespaço estaria acima da realidade, uma vez que os governos do mundo físico não teriam legitimidade no território virtual em razão de sua natureza fluida e descentralizada. Em suma, esses doutrinadores sustentavam não só que o ciberespaço não deveria ser regulado, mas que este não *poderia* ser regulado, ele seria um território inevitavelmente livre por natureza (LESSIG, 2006).

1.2.2 Ciberpaternalismo

Com o desenvolvimento desse novo modelo de interação social e o uso cada vez mais constante da internet, ficou clara a necessidade de se exercer algum tipo de autoridade sobre o

ambiente virtual. Assim, uma nova escola doutrinária se desenvolveu; uma corrente que não partilha dos ideais libertários de que o ciberespaço estaria imune à intervenção regulatória do mundo real, mas que, diversamente, acredita na possibilidade e, sobretudo, na necessidade de se regular o ambiente em rede. Esses autores ficaram conhecidos como ciberpaternalistas.

1.2.2.1 A Regulação por Código de Lawrence Lessig

Lawrence Lessig (2006), um dos mais importantes teóricos da regulação do ciberespaço, sustenta que a liberdade nesse ambiente, tão prezada por seus antecessores, não vem com a ausência do Estado. Pelo contrário, para ele, se deixado às próprias custas, o ciberespaço se tornará uma ferramenta de controle, que pode acabar por suprimir direitos e liberdades fundamentais. Assim, essa nova realidade demanda uma reconfiguração do conceito de regulação para além do campo de aplicação tradicional do direito, i.e, além das leis ou normas. O ponto chave na obra de Lessig, portanto, é o reconhecimento de um novo e proeminente regulador: o código.

Lessig afirma que é o código – software e hardware[6] – que dita as regras da experiência online. É por meio de uma série de protocolos chamados TCP/IP[7], os quais permitem a troca de dados entre redes interconectadas, que se determina os padrões da internet, como por exemplo, quão fácil é proteger a privacidade ou quanto se pode limitar a liberdade de expressão na rede. É a arquitetura da internet que determina o acesso à informação e que, em última instância, atua como o legislador.

Inicialmente, essa troca de dados acontecia sem que os operadores envolvidos tomassem conhecimento do conteúdo da informação que está sendo transmitida ou quem é a pessoa responsável pelo envio dos dados – o código é neutro no que diz respeito a informação e ignorante quanto ao usuário. Esse design simplista não foi desenvolvido por acaso; ele reflete,

---

[6] O hardware é a parte física integrada por placas de vídeo, memórias, processadores, chips e tudo mais que o usuário pode tocar. É o chamado "corpo da máquina", e é aplicado tanto para computadores, notebooks, celulares, câmeras, robôs e mais. Já o software pode ser entendido como a "mente" que comanda a máquina, composta por elementos que não são palpáveis. Ele é formulado por meio de códigos e combinações para funcionar da maneira ideal. Então, os sistemas operacionais, como Windows, Mac OS, Android, iOS são softwares, cada um formulado à sua maneira. (Extraído de http://www.techtudo.com.br/noticias/noticia/2015/02/hardware-ou-software-entenda-diferenca-entre-os-termos-e-suas-funcoes.html)

[7] "O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI), onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas, estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração." (FERREIRA, 2013)

na verdade, uma decisão de manter a estrutura da rede elementar para que se possa operar o maior número de funções possível ao mesmo tempo. É o chamado princípio *end-to-end*, um dos fundamentos basilares da arquitetura da internet e um dos motivos cardeais para o sucesso e o crescimento dessa nova tecnologia. Foi precisamente em razão dessa natureza "neutra", que elementos que viabilizam e otimizam a regulação no mundo real, como identificação e autenticação, foram mitigados, tornando a regulação do ambiente em rede extremamente complexa.

Regulabilidade

Para fundamentar sua teoria, o autor desenvolve o conceito de "regulabilidade", definindo-a como a "capacidade de um governo regular o comportamento dentro de seu próprio alcance."[8] (LESSIG, 2006, p. 23). No contexto da internet, a regulabilidade estaria relacionada à capacidade de regular o comportamento dos cidadãos enquanto estiverem na rede. Ele sustenta que existem três elementos chaves para a regulação, que precisam, necessariamente, ser conhecidos pelo regulador: (i) quem é sujeito; (ii) onde ele está e (iii) o que ele está fazendo. O problema é justamente que, como já mencionado, a forma como a Internet foi originalmente desenhada não permitia conhecer de forma clara e precisa nenhum desses elementos.

A identidade – construída socialmente e formadora de escolhas políticas - sempre foi um importante elemento de uma comunidade. Ela pode ser definida como o conjunto de atributos ou facetas da personalidade, característicos ou únicos de uma pessoa, como por exemplo nome, caráter, voz, história de vida, etc., que são reconhecidos e respeitados pelos demais (ANDRADE, 2010). Em suas relações cotidianas, os indivíduos requerem certa dose de autenticidade para conferir confiança a essa identidade, especialmente no que diz respeito à ação estatal de restringir ou permitir certos comportamentos. Por essa razão, determinados elementos, como identificação, autenticação e credencial – chamados por Lessig (2006) de "Arquiteturas de Controle" - viabilizam e aperfeiçoam a ordem social.

No mundo real, algumas características da identidade podem ser averiguadas pessoalmente, sem qualquer informação adicional, como por exemplo, gênero, cor dos olhos, altura, etc. Todavia, outros elementos formadores da identidade, como idade, estado civil e profissão requerem substratos diversos que os confirmem, i.e, que os autentiquem. Esses outros elementos são chamados credenciais. Fundamentalmente a regulabilidade da vida no mundo real depende de certas arquiteturas de autenticação (identidade, placas de carro, carteira de

[8] *"Regulability" is the capacity of a government to regulate behavior within its proper reach.*

motorista, etc). Dessa forma, se for possível autenticar os anos de vida de alguém com certa facilidade, as leis baseadas na idade como, por exemplo, a legislação que disciplina o consumo de álcool, serão melhor aplicadas.

Na medida em que a vida se torna mais fluida, as instituições sociais passam a depender de outras tecnologias para conferir confiança a determinadas afirmações de identidade, como, por exemplo, as tecnologias biométricas (leitores de digitais, scanners de íris, etc.). As credenciais, portanto, se tornam uma ferramenta inevitável para assegurar essa autenticidade. O mesmo ocorre no universo digital. Conforme a internet foi amadurecendo e as pessoas passaram a utilizá-la na realização das mais diversas atividades, como compra e venda, transferências bancárias, relacionamento virtual, etc., o desenvolvimento de tecnologias que permitem ligar um comportamento online a uma identidade se fez indispensável.

Essas mudanças mostram, mais uma vez, o poder do código no ciberespaço. Foi a partir de uma série de demandas – especialmente do mercado - que alterações na arquitetura da internet passaram a ser implementadas, a fim de tornar as relações virtuais (em especial as relações comerciais) melhores e mais confiáveis. Elas fizeram com que a vida na internet se tornasse mais segura, e por consequência, mais regulável.

Desse modo, atualmente, ainda que seja possível tomar algumas medidas para não ser identificado na rede, esse anonimato exige uma certa dose de esforço. Para a maioria dos usuários, o uso da internet se tornou rastreável de diversas maneiras, como por exemplo por meio do endereçamento dos IPs – toda vez que alguém vista uma página na web, a rede sabe de onde vieram aqueles pedaços de informação; o computador, portanto, diz para o servidor onde um indivíduo está ao revelar o endereço do IP – e do uso de *cookies* - um protocolo que permite que o servidor, ao ser acessado, deposite uma pequena fração de informação no computador, tornando possível o reconhecimento do usuário, quando este navega para uma página diferente. Assim, Lessig afirma:

> A rastreabilidade dos endereços de IP e os cookies são o padrão na internet agora. Novamente, alguns passos podem ser seguidos para evitar essa rastreabilidade, mas a vasta maioria de nós não os segue. Felizmente, para a sociedade e para a maioria de nós, o que fazemos na Net não diz respeito a ninguém. Mas se o dissesse, não seria difícil nos encontrar. Nós somos pessoas que deixam migalhas por todo o lugar. (LESSIG, 2006, p. 49)[9]

[9] *The traceability of IP addresses and cookies is the default on the Internet now. Again, steps can be taken to avoid this traceability, but the vast majority of us don't take them. Fortunately, for society and for most of us, what we do on the Net doesn't really concern anyone. But if it did concern someone, it wouldn't be hard to track us down. We are a people who leave our "mouse droppings "everywhere.*

East Coast Code v. West Coast Code

Lessig defende, portanto, que assim como o mundo físico possui uma certa arquitetura – algumas características materiais do mundo, sejam construídas ou já existentes na natureza que restringem ou permitem comportamentos humanos[10] - o mesmo ocorreria com a internet. A diferença primordial é que, ao contrário do mundo físico, o ambiente em rede é um produto da mente humana que permite, por meio de uma linguagem diferenciada de 0s e 1s, alterar leis tradicionais da natureza, como tempo e espaço[11]. Por conseguinte, a regulação da internet deve ser imposta pelo mesmo código que governa esse ambiente:

> O que quer que seja que o ciberespaço tenha sido não há nenhuma razão pela qual ele tenha que se manter desta forma. A "natureza" da Internet não é a vontade de Deus. Essa natureza é simplesmente o produto do seu desenho. Esse desenho poderia ser diferente. (LESSIG, 2006, p. 38).

Portanto, assim como no mundo físico, algumas arquiteturas do ciberespaço são mais reguláveis e permitem um controle mais eficaz do que outras. Logo, a possibilidade de o ciberespaço, ou partes dele, ser regulado depende exclusivamente da natureza do código. Nesse sentido, ele afirma:

> Nós podemos construir, arquitetar ou codificar o ciberespaço para proteger valores que acreditamos serem fundamentais. Ou nós podemos construir, ou arquitetar, ou codificar o ciberespaço de forma a permitir que esses valores desapareçam. Não existe meio termo. Não existe nenhuma escolha que não

[10] Lessig define arquitetura como as barreiras físicas ou técnicas impostas às atividades que interferem positiva ou negativamente no comportamento humano. Nesse sentido: "*I cannot see through walls is a constraint on my ability to snoop. That I cannot read your mind is a constraint on my ability to know whether you are telling me the truth. That I cannot lift large objects is a constraint on my ability to steal. That it takes 24 hours to drive to the closest abortion clinic is a constraint on a woman's ability to have an abortion. That there is a highway or train tracks separating this neighborhood from that is a constraint on citizens to integrate. These features of the world - whether made, or found - restrict and enable in a way that directs or affects behavior. They are features of this world's architecture, and they, in this sense, regulate"* (LESSIG, 1998, p. 663)

[11] No ciberespaço pode-se estar em vários lugares ao mesmo tempo, ou seja, no mundo digital, várias coisas acontecem simultaneamente, cada uma em uma "janela". Podemos conversar com amigos, ler um romance, ver cotações da bolsa, calcular as despesas domésticas e jogar um jogo, tudo ao mesmo tempo. No ciberespaço o tempo encolhe. Se esperamos cinco minutos em uma fila do banco, achamos rápido. Em compensação, se tentamos nos conectar por computador ao mesmo banco e a operação demorar mais de cinco segundos, ficamos irritados. No ciberespaço o tempo que se leva para percorrer uma determinada distância não depende do comprimento, mas da largura da estrada. Para levar nossos átomos de Porto Alegre até o Japão demoramos várias horas. Para irmos até a sala vizinha no prédio demoramos alguns segundos. O tempo despendido nos dois deslocamentos vai depender, além do tipo de transporte utilizado, principalmente da distância entre os dois locais, ou seja, do comprimento da estrada. Já para levarmos nossos bits (digamos, nossa foto digitalizada) de um lugar a outro, o tempo gasto no deslocamento vai depender principalmente da largura de banda da conexão. No ciberespaço, a noção do tempo despendido em um deslocamento se altera. Os bits não se deslocam da mesma maneira que os átomos. A topologia do ciberespaço não coincide com a do mundo real. A Internet nega a geometria.(VERLE, 1997)

> envolva alguma forma de construção. O código nunca é descoberto; ele é sempre criado, e sempre criado por nós. (LESSIG, 2006, p. 6)[12]

Estabelecido esse cenário, Lessig apresenta o conceito dos códigos da Costa Leste e da Costa Oeste (*East Coast and West Coast codes*). Ele defende a existência de dois tipos de código. O primeiro seria aquele elaborado pelo Congresso, isto é, um conjunto de comandos que controlam o comportamento de indivíduos, companhias, entidades públicas, etc. Em resumo, seriam as leis, estatutos, diretivas, enfim, todo o trabalho legislativo do Estado, que, nos Estados Unidos da América, está concentrado em Washignton D.C, daí o nome "código da Costa Leste". O segundo código a que se refere são as instruções técnicas contidas nos softwares e hardwares que permitem o funcionamento do ciberespaço, o qual ele denominou "código da Costa Oeste", em razão da proeminência dessa atividade nessa região dos Estado Unidos, em especial no Vale do Silício.

Desde os primórdios de sua criação, a Internet foi orientada diversamente das outras formas de telecomunicação, como a telefonia, o rádio e a televisão, que não são redes programáveis pelo usuário, mas, pelo contrário, dependem de uma série de implementações feitas exclusivamente por seus administradores e estritamente reguladas pelo Estado. A finalidade da rede não era oferecer um conjunto de informações ou serviços. Na verdade, o objetivo principal era conectar as pessoas, sem se importar realmente com o que elas fariam com essa conexão. A rede simplesmente levava a informação de um ponto a outro (princípio *end-to-end*). (ZITTRAIN, 2008).

Conforme o código deixou de ser o fruto da mente de alguns estudiosos e *hackers* isolados e passou a ser um produto de grandes empresas que fizeram desse conjunto de informações seu meio de lucro, o poder do código da Costa Leste aumentou e a regulação se tornou mais simples - é muito difícil para o Estado monitorar indivíduos anônimos atuando isoladamente, no entanto, entidades comerciais, que são pessoas jurídicas sujeitas de direitos e obrigações, podem ser controladas com maior desembaraço.

Apesar dessa recém descoberta facilidade, o governo está sempre um passo atrás dos criadores de tecnologia – é o código da Costa Oeste que define o desenho do ambiente em que pretende atuar o código da Costa Leste, e, consequentemente, é o primeiro que determina a série

---

[12] *We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found; it is only ever made, and only ever made by us.*

de opções regulatórias disponíveis ao segundo. “Uma mudança na tecnologia pode alterar a dinâmica de poder entre aqueles que fazem as leis e aqueles que estão sujeitos a elas. ” (ZITTRAIN, 2008, p. 105)[13] . Assim, é a interação entre esses dois códigos que interessa ao estudo da regulação do ciberespaço, é o equilíbrio entre essas duas forças que permitirá o governo atingir o objetivo regulatório que pretende.[14]

Conclui-se, portanto, que a Internet não foi só um meio de construir uma rede generativa, mas também foi um meio de se estabelecer diferentes níveis de regulação e controle. O fato de usarmos a internet nos dias de hoje não é só uma escolha política, apesar de a intervenção do governo ser necessária em algumas instâncias. É na verdade uma consequência do *interplay* das forças do mercado e externalidades da rede (ZITTRAIN, 2008).

As quatro modalidades de regulação

Lessig (2006) apresenta, então, a sua célebre “Teoria das quatro modalidades de regulação”. Para explicar esse conceito, o autor descreve os indivíduos sujeitos da regulação como sendo “pontos patéticos” (*pathetic dots*), cujo comportamento é limitado por diferentes elementos, sendo os mais relevantes: a lei, as normas sociais, o mercado e a arquitetura. Nesse modelo, esses quatro fatores são independentes, mas se interconectam de forma que alguns se complementam e outros comprometem os demais. Em suma, qualquer mudança em uma das modalidades pode e vai afetar as demais.

O exemplo icônico que ele usa para explicar a teoria em destaque é o da regulação do cigarro. Supondo que um governo desejasse desencorajar o consumo de cigarros em um determinado país, poderia fazê-lo de diversas formas. Por meio da lei pode-se proibir totalmente o fumo ou apenas restringir o consumo em alguns locais específicos, impondo multas àqueles que fumem dentro de ambientes fechados, por exemplo. Por meio das normas sociais é possível influenciar a opinião pública com campanhas educativas que divulguem os malefícios do cigarro à saúde, criando uma conscientização coletiva contra o consumo desse item. O mercado também pode atuar como regulador, na medida em que se altera o preço ou a qualidade do

[13] *A change in technology can change the power dynamic between those who promulgate the law and those who are subject to it.*

[14] Para Lessig, um exemplo perfeito da interação entre os códigos das duas costas é o da China. Para dar cumprimento a seus ideais não tão democráticos, o governo Chinês impõe uma serie de determinações a provedores, como o Google, por exemplo, para que alterem seus algoritmos de modo a selecionar o conteúdo que será exibido aos usuários. Assim, os sites que o governo chinês deseja bloquear, por meio de uma configuração no código do buscador, não aparecem no campo de busca do Google. Nenhum sistema informa aos internautas que os resultados da pesquisa foram filtrados pelos censores chineses; para o usuário chinês aquela é a aparência “normal” do Google. (LESSIG, 2006)

produto. Se o mercado oferece uma variedade de cigarro com uma ampla gama de preços e qualidade, a habilidade de o indivíduo selecionar seu cigarro de preferência aumenta; aumentar a escolha é, portanto, reduzir as restrições. Por fim, pode se usar a arquitetura para regular o consumo de cigarro ao alterar elementos estruturais da tecnologia do produto, como por exemplo, estabelecer níveis máximos de nicotina ou a exigência do uso de filtros.

Assim, toda regulação é uma mistura de aspectos diretos e indiretos, sendo que a lei tem extrema importância neste mecanismo – é por meio dela que se pode exercer influência sobre as demais modalidades a fim de regular um comportamento:

> Em seu aspecto direto, a lei utiliza meios tradicionais para direcionar um objeto de regulação (quer seja o indivíduo regulado, as normas, o mercado ou a arquitetura); em seu aspecto indireto, ela regula esses outros reguladores de forma que eles regulem o indivíduo de formas diferentes. Assim, a lei usa ou agrega o seu poder regulatório para seus próprios fins. A regulação moderna é uma mistura desses dois aspectos. (LESSIG, 1998, p. 666-667) [15]

Criada a teoria, Lessig, então, propõe aplicá-la ao ciberespaço. Nesse sentido, ele sustenta que na internet: (i) a lei regula o comportamento ao impor sanções *ex post* pela violação de direitos online, como por exemplo, as leis que disciplinam o direito autoral, responsabilidade civil, pornografia infantil, etc.; (ii) a normas sociais regulam o comportamento por meio dos estigmas impostos pela comunidade digital a certas condutas no ambiente em rede[16]; (iii) o mercado regula o ciberespaço precificando as estruturas que possibilitam o acesso à rede e, por fim, e mais importante (iv) a arquitetura é o regulador por essência do ciberespaço; são os softwares e hardwares que compõem o ciberespaço que irão impor uma gama de limitações *ex ante* sobre o comportamento dos indivíduos.

Como já mencionado, diferentemente da arquitetura do mundo real, a arquitetura da internet é criada pelo código. É a partir de uma série de instruções técnicas e escolhas deliberadas de design, que se determinam quais comportamentos são possíveis ou impossíveis online[17]. Ocorre que esse código não é escrito por representantes eleitos democraticamente e, a

---

[15] *In its direct aspect, the law uses its traditional means to direct an object of regulation (whether the individual regulated, norms, the market, or architecture); in its indirect aspect, it regulates these other regulators so that they regulate the individual differently. In this, the law uses or co-opts their regulatory power to law's own ends. Modem regulation is a mix of the two aspects*

[16] Um exemplo está relacionado àqueles indivíduos que postam, com frequência, mensagens indesejadas – os chamados spams - em grupos de conversa e por consequência são retirados do grupo pelos demais participantes. (LESSIG, 2006)

[17] Note-se que aqui ou uso da palavra possível não tem um sentido deontológico, de "dever ser"; ela é utilizada em seu sentido literal, isto é *se preenche as condições necessárias para ser, existir ou realizar-se.*

princípio, não está sujeito a qualquer controle legal ou constitucional – são as grandes empresas privadas que desenham o código.

É evidente que, como se observa da experiência prática, muitas das leis do "mundo real" se aplicam a determinadas condutas no ciberespaço. Entretanto, deve-se perceber que este é também (se não principalmente) regulado pelos codificadores, a despeito da lei, que está sempre um passo atrás, visto que não consegue acompanhar o turbilhão de mudanças que acontecem no mundo tecnológico (EDWARDS, 2009). A maior preocupação de Lessig, portanto, era que a regulação ficasse nas mãos das grandes empresas privadas que produzem o código. Assim, se o comércio é quem define as arquiteturas emergentes do ciberespaço, não seria o papel do governo assegurar que aqueles valores que não são do interesse do comércio sejam igualmente protegidos dentro dessa arquitetura? Portanto, para esse teórico, a atuação estatal no sentido de regular o ciberespaço não só é possível, como ela é desejável.

1.2.3. Comunitarismo em rede *(Network Communitarianism)*

Como um contraponto ao ciberpaternalismo, especialmente à teoria de Lessig, surgiu o comunitarismo em rede **(***Network communitarianism)*, cujo maior proponente é Andrew Murray. Murray (2016) acredita que existe uma relação intrínseca entre o ambiente digital e o mundo real que funciona de maneira mais fluida do que o imaginado por aquele teórico. Nesse sentido, ele sustenta que os seus antecessores, tanto ciberlibertários quanto ciberpaternalistas, falham em perceber as complexidades do fluxo de informações encontrado nos modernos meios de telecomunicação, como a internet. Para embasar esse novo modelo de regulação, ele se apoia em duas doutrinas europeias: a Teoria do Ator-Rede, desenvolvida por Michel Callon e Bruno Latour e a teoria dos Sistemas Sociais de Luhmann e Gunther Teubner.

A Teoria Ator-Rede, também conhecida por ANT, é uma vertente da sociologia moderna que desconsidera o conceito de sociedade tradicional, abordando o social como sendo o coletivo de humanos e não-humanos que se associam formando redes, ou melhor, atores-rede, em um processo contínuo de transformação de interesses, denominado de "translação" ou "tradução" (LATOUR, 2005). Para os adeptos dessa teoria, as comunicações sociais são feitas de transações paralelas entre o material (coisas) e a semiótica (conceitos), que juntos formam uma única rede. Segundo Murray, essa conceitualização tem o potencial de ser particularmente poderosa quando aplicada à internet.

A internet é a maior rede de comunicação pessoa a pessoa existente. Ela permite que indivíduos realizem translações sociais no espaço e no tempo, possibilitando trocas entre pessoas com experiências comuns, mas que estão geograficamente distantes uma da outra e trocas entre pessoas com nenhuma experiência em comum, mas que estão geograficamente próximas. Assim, o potencial que novas redes têm de se formarem, reformarem e se dissolverem é enorme, o que faz com que a internet seja não só um meio de comunicação, mas também uma ferramenta cultural e social (MURRAY, 2016).

A Teoria dos Sistemas Sociais, por sua vez, pretende analisar e explicar o fluxo de informações dentro de sistemas complexos de comunicação social. Para explicar como a comunicação afeta as transações sociais, Luhmann (RODRIGUES e NEVES, 2012) define sistemas sociais como sendo "sistemas comunicativos". Nesse sentido, somente a comunicação teria um caráter estritamente social, uma vez que ela pressupõe o envolvimento de vários sistemas psíquicos; não pode haver comunicação individual. Ela é, ainda, autopoiética, pois só pode ser criada no contexto recursivo das outras comunicações, dentro de uma rede, cuja reprodução precisa da colaboração de cada comunicação isolada. Dessa forma, não é o ser humano quem comunica, mas o sistema social, daí a ideia de uma comunicação e de uma "sociedade sem seres humanos" (MELO, 2013).

Assim como a ANT, a Teoria dos Sistemas é uma tentativa de mapear e estudar o complexo processo de interações sociais no, cada vez mais complexo e conectado, ambiente da sociedade moderna. Enquanto a ANT versa sobre a evolução e formação das redes, a Teoria dos Sistemas Sociais se preocupa em estudar a filtragem do fluxo de informação no processo de tomada de decisão e a comunicação de ideias e conceitos entre sistemas (MURRAY, 2016). Apesar de suas diferenças, as duas teorias trazem uma nova perspectiva para o entendimento da comunicação e da interação social em um ambiente em rede como a internet, em que operam uma variedade de atores, tanto humanos quanto não humanos.

Nesse sentido, para Murray, o que Lessig não considerou em sua teoria é o fato de os indivíduos não serem passivos no processo de regulação. Na teoria ator-rede, o "ponto" a que se refere seria um nódulo na rede, enquanto na teoria dos sistemas, ele seria parte de um sistema. De qualquer forma, o "ponto" não é isolado; é, na verdade, uma matriz de pontos que se envolvem em uma relação simbiótica dentro da comunidade em rede, constantemente trocando ideias, crenças e opiniões. Na verdade, para os comunitaristas, três das quatro modalidades apontadas por Lessig – leis, normas e mercado, são processos essencialmente sociais e refletem um papel proativo no curso da regulação. Assim, é seguro afirmar que tais modalidades

regulatórias retiram sua legitimidade da comunidade e a ela prestam contas, ou seja, o processo regulatório é, por natureza, um diálogo e não uma série de limitações impostas externamente.

De forma sucinta, pode-se dizer que essa teoria acredita em uma regulação democrática e por consentimento. Logo, *accountability* seria uma palavra chave no processo de regulação do ciberespaço devido à própria natureza desse ambiente. Uma vez que a plataforma na qual as pessoas interagem é modificada, resta evidente que as formas de controlar esse espaço devem acompanhar essas mudanças. Em um ambiente marcado pela pluralidade seria irrazoável esperar que uma regulação unilateral apresente um resultado eficiente e satisfatório.

Nessas circunstâncias, Murray reconhece que a teoria de Lessig é inovadora em muitos sentidos, especialmente porque elaborou um mecanismo interativo de ciberregulação que identifica fatores além da lei para apresentar soluções efetivas à administração do comportamento online. No entanto, conforme apontam os comunitaristas, esse modelo falha em notar um aspecto muito importante e que tem impacto direto na experiência pratica da regulação do ciberespaço: o poder de determinar o ambiente regulatório não está apenas com o regulador. O domínio digital é uma complexa teia de atores – humanos e não-humanos – que interagem entre si e dão respostas imediatas a incentivos externos.

Para os teóricos do comunitarismo é importante levar em consideração, ainda, o fato de que os seres humanos são seres racionais que respondem a incentivos. Assim, o regulador deve descobrir quais os "botões certos que deve apertar", ou em outras palavras, quais incentivos receberão uma maior e melhor resposta da comunidade na rede. Um bom exemplo desse entendimento é a indústria de *streaming* na música. Uma pesquisa recente[18] demonstrou que, até março de 2016, o Spotify, um dos maiores serviços de streaming no mercado, possuía 30 milhões de usuários pagantes ao redor do globo, um grande avanço se comparado aos 20 milhões averiguados em junho de 2015. Isso demonstra que, enquanto as pessoas podem não se sentir compelidas obedecer a uma lei que proíba o download ilegal de músicas, elas estão cada vez mais inclinadas a pagar, mensalmente, uma quantia que consideram razoável por um serviço que oferece um produto de qualidade e de fácil acesso[19]. Por essa razão, agora é muito mais fácil regular o Spotify como uma companhia individual do que tentar controlar cada

[18] Number of paying Spotify subscribers worldwide from July 2010 to September 2016 (in millions), acessado em https://www.statista.com/statistics/244995/number-of-paying-spotify-subscribers/

[19] *Almost two thirds (62 per cent) of those who admit to illegally downloading, say using Spotify has encouraged them to reduce the amount they download illegally or kick the habit altogether.* Opinium Research carried out an online poll of 2,319 British adults between Friday 5th June and Tuesday 9th June 2009.

usuário online, o que traz benefícios não apenas para o regulador, mas também para os artistas, consumidores e para o mercado em geral.

Em resumo, para estes teóricos, o comunitarismo em rede seria o meio termo Aristotélico, isto é, o ponto desejável entre os ciberlibertários e os ciberpaternalistas. Essa nova escola doutrinária traz um elemento de realidade à teoria de Lessig. O mundo cibernético não é, de forma alguma, um espaço estático; ele é, na verdade, um organismo vivo no qual os participantes interagem em uma relação simbiótica. É preciso ter em mente que os atores são os mesmos: indivíduos, organizações privadas e governo, mas a arena mudou completamente.

***

Diante do exposto nesse capítulo, não restam dúvidas de que escolas que pregam a autorregulação e/ou a total abstenção do Estado sobre o ciberespaço já estão ultrapassadas. A regulação desse ambiente é indispensável, pois, como já observado, em um mundo em que a informação se tornou a moeda de câmbio mais valiosa e se apresenta como ponto de referência para um grande número de situações jurídicas, questões como o direito à privacidade e à identidade são trazidas à tona e precisam de soluções práticas e efetivas.

Para os operadores do direito, a internet se coloca, portanto, como uma questão de perspectivas: interna e externa. A primeira diz respeito à experiência do usuário que aceita o mundo virtual como uma construção legítima. Para ele, o computador, conectado à internet, proporciona uma janela para um mundo virtual que é análogo ao mundo físico e que o permite realizar diversas atividades. A segunda está relacionada ao funcionamento da rede no mundo físico, independentemente das percepções do usuário. Nessa perspectiva a internet é simplesmente uma rede de computadores ao redor do mundo conectados por cabos e fios. Por consequência, resultados legais dependem de fatos e os fatos da internet dependem de qual perspectiva será adotada. (KERR, 2003)

Partindo, então, de uma perspectiva interna, percebe-se que, para existir no mundo virtual, os indivíduos necessitam de dados *proxy* que os identifiquem - o que Lessig chamou em sua teoria de credenciais. Esse perfil eletrônico transforma-se numa verdadeira representação virtual do usuário, já que, muitas vezes, é o único aspecto visível a uma série de outros sujeitos, estando fadado a confundir-se com a própria pessoa. A partir do momento em que essa “metainformação” é a única parte de uma pessoa aparente a outrem, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição da esfera de liberdade (DONEDA, 2006).

Portanto, com base nas teorias expostas, nos próximos capítulos, pretende-se traçar o panorama da privacidade e da proteção de dados em rede, definindo conceitos essenciais como dados pessoais, vigilância digital e confiança. Ademais, busca-se entender como articular as forças públicas e privadas – códigos da Costa Oeste e da Costa Leste -, que estão em um embate constante pelo controle dessas informações, de modo a garantir direitos fundamentais, delineando papel do indivíduo regulado nessa equação.

CAPÍTULO 2 – PRIVACIDADE E PROTEÇÃO DE DADOS NO AMBIENTE EM REDE

If you want to keep a secret, you must also hide it from yourself.

George Orwell, 1984

As informações pessoais são a substância que compõe a identidade do homem moderno. As novas tecnologias emergentes, ao coletarem, cada vez mais, informações sobre os indivíduos, possibilitam um maior acesso a serviços, conveniências e benefícios extraordinários – destacando-se, dentre eles, a capacidade de manter um amplo círculo de relações através das mais recentes ferramentas de mídia social.

Os seres humanos são animais sociais e a necessidade de se conectar é inerente à essa condição. Contudo, a privacidade é igualmente um elemento essencial da condição humana. A preservação de espaços privados para permitir a reflexão, e desfrutar de momentos de solidão e intimidade, é tão relevante agora como sempre foi. Talvez, poderia até se afirmar que ela é mais acentuada e necessária agora, quando nossas vidas estão em rede, interconectadas e constantemente "ligadas." Destarte, o desejo de resguardar as esferas da vida privada não diminuirá – pelo contrário, ele tende a crescer. (CAVOUKIAN, 2013)

Assim, nesse capítulo, pretende-se abordar os temas da privacidade e proteção de dados no ambiente em rede, delineando alguns elementos essenciais para a concretização desses direitos, partindo da ótica das teorias da regulação do ciberespaço já apresentadas.

2.1 “PEGADAS DIGITAIS”

2.1.1 Big Data e Cookies de Internet

Conforme já delineado no capítulo anterior, com a informatização da sociedade, ocorreram algumas mudanças tectônicas que alteraram, fundamentalmente, a maneira como dados pessoais são coletados, armazenados e transferidos, quebrando paradigmas e desestabilizando mercados (WOODS, O'BRIEN e GASSER, 2016).

Deste modo, o fato de a informação ser processada por computadores representa, por si só, uma mudança nos efeitos de seu tratamento. Tais efeitos podem ser mensurados quantitativa ou qualitativamente. A primeira classificação refere-se à “força bruta”, isto é, o volume de informação processado (que é praticamente ilimitado) no menor intervalo de tempo possível e a segunda, por sua vez, diz respeito aos métodos, algoritmos e técnicas utilizados na digitalização da informação, que operam uma mudança qualitativa no escopo do tratamento de dados pessoais.[20] (DONEDA, 2006)

Nessa esteira, preços decrescentes na coleta, processamento, armazenamento e análise de dados, aliados aos avanços constantes da tecnologia, diminuíram as barreiras para que instituições dos setores público e privado passassem a manusear grandes quantidades de dados. Assim, à medida que os indivíduos se utilizam dessas novas tecnologias[21], suas “pegadas digitais”, isto é, informações pessoais deixadas na rede, como e-mails, mensagens, fotos, endereços e documentos passam a ser armazenadas em uma infraestrutura de propriedade do prestador do serviço por um período indeterminado de tempo. Essa configuração não é apenas conveniente para o usuário, mas tornou-se uma verdadeira *commodity* para os negócios na rede,

---

[20] Nesse sentido, Laura Schertel corrobora*:* “Desse modo, percebe-se que a informatização dos meios para o tratamento de dados pessoais afetou o direito à privacidade do indivíduo principalmente por duas razões: i) ao ampliar a possibilidade de armazenamento, tornando-a praticamente ilimitada; ii) ao possibilitar a obtenção de novos elementos informativos por meio da combinação de dados em estado bruto, a princípio, desprovidos de importância, a partir da utilização de novas técnicas, tais como o “profiling”, “data mining”, “data warehousing”, “scoring-system”, entre outros.” (MENDES, 2016)

[21] Impulsionada por essas mudanças nos custos e na tecnologia, surgiu a computação em nuvem, que oferece aos consumidores funcionalidades e conveniências antes inimagináveis. Agora, em razão de recursos computacionais avançados e de uma infraestrutura que se assemelha a um serviço “on-demand” na internet, os usuários não estão mais limitados pela capacidade de armazenamento de um dispositivo eletrônico; por meio de um serviço de armazenamento em nuvem, pode-se armazenar uma quantidade infinita de dados e acessá-los de qualquer lugar na rede. Aparelhos portáteis com microprocessadores de baixa potência podem alavancar a potência de milhares de servidores, redes neurais e algoritmos para fazer cálculos complexos, necessitando apenas de uma conexão de internet. *Essas características são geralmente harmoniosamente integradas numa pletora de produtos e serviços, dos quais, na maioria das vezes, o consumidor médio não conhece os pormenores técnicos – eles “apenas funcionam”.* (O'BRIEN, BUDISH, *et al.*, 2016, p. 4)

que minam e monetizam grandes quantidades de dados sobre os indivíduos. Nesse sentido, Lessig corrobora o entendimento de que os dados pessoais possuem grande valor na rede:

> Tudo o que você faz na rede produz dados. Esses dados, agregados, são extremamente valiosos, mais valiosos para o comércio do que para o governo. O governo (em circunstancias normais) apenas se importa que você obedeça a um certo conjunto de leis. O comércio, por sua vez, está interessado em descobrir como você quer gastar seu dinheiro, e os dados fazem exatamente isso. Com grandes quantidades de dados sobre você, sobre o que você faz e sobre o que você diz, torna-se cada vez mais possível comercializar você de uma maneira direta e efetiva. (LESSIG, 2006, p. 216)[22]

Essa posição central que o tratamento de informações pessoais possui em produtos e serviços oferecidos por companhias da internet - grande parte dos quais não apresentam custos ao consumidor - corrobora a importância dos dados pessoais no fundamento de seu modelo de negócios. Gradualmente, as empresas perceberam que as "pegadas digitais" deixadas pelos indivíduos após uma venda ou prestação de serviço, se analisadas agregadamente sob um método particular, podem revelar um significado maior que a simples soma de suas partes. Com essa enorme quantidade de dados, agora é possível extrair novas ideias e perspectivas sobre a realidade, as quais dão ensejo a criação de produtos e serviços inovadores, bem como a novas formas de desenvolvimento de políticas públicas e de regulação estatal. Essa nova maneira de analisar a realidade ficou conhecida como Big Data[23] e segue seu curso de desenvolvimento ao ritmo ditado quase que exclusivamente pelo interesse das empresas detentoras das bases de dados. (CRAVO, 2016)

Para exemplificar esse novo mercado, pode-se citar: (i) o uso pessoal de redes sociais para se conectar com a família e amigos e, em contrapartida, o uso comercial dessas plataformas para a entrega de serviços e propagandas personalizadas; (ii) o desenvolvimento de aplicativos para *smartphones* que oferecem informações customizadas e em tempo real aos usuários, enquanto permitem que companhias coletem fluxos de dados dos indivíduos; (iii) o uso de

---

[22] *Everything you do on the Net produces data. That data is, in aggregate, extremely valuable, more valuable to commerce than it is to the government. The government (in normal times) really cares only that you obey some select set of laws.But commerce is keen to figure out how you want to spend your money, and data does that. With massive amounts of data about what you do and what you say, it becomes increasingly possible to market to you in a direct and effective way.*

[23] Viktor Mayer-Schönberger e Kenneth Cukier (2013) definem o Big Data como a extração de novos insights ou a criação de novas formas de valor, em larga escala, a partir de uma pletora de dados que podem mudar mercados, organizações, a relação entre os cidadãos e o governo e muito mais. Em seu âmago, o Big Data está relacionado à previsão: é aplicar a matemática a uma quantidade enorme de dados a fim de inferir probabilidades: a probabilidade de que um email seja spam; a probabilidade que as letras digitadas "teh", signifiquem, na verdade, "the"; a trajetória e a velocidade de uma pessoa atravessando fora da faixa, conseguira chegar do outro lado a tempo, etc.

técnicas de modelagem de dados (*data modeling)*[24] em uma vasta gama de novos serviços, como avaliação de risco de crédito, empréstimos e ferramentas de finanças pessoais (WOODS, O'BRIEN e GASSER, 2016).

Grande parte desses dados espalhados pelo ciberespaço é biográfica e transacionável, incluindo informações como nome e sobrenome, endereço de email, endereço postal, número de telefone, registros de negócios, etc. Entretanto, uma crescente parcela desses dados pode ser descrita como comportamental e baseada em inferências, como gráficos sociais e relacionamentos do usuário, seus interesses, preferências pessoais, histórico de pesquisa, *clickstream*, localização geográfica e, até mesmo, a sua probabilidade de ficar doente.[25] (O'BRIEN, BUDISH, *et al.*, 2016). Assim, esse conjunto de informações passa a ser a nossa representação na rede; é a partir desse perfil eletrônico criado no ambiente virtual que os indivíduos são identificados e suas transações são validadas - há, portanto, um "divórcio" entre a identidade e a pessoa. (MURRAY, 2016)

Há que se ressaltar que, muitas das vezes, tais informações são coletadas por meio de *cookies*, isto é, pequenos arquivos no formato de texto utilizados para o armazenamento de dados, cujo objetivo principal é personalizar e otimizar o a experiência do usuário em um determinado site. Eles são instalados automaticamente no disco rígido do usuário no momento da visita de uma página na internet por meio de aplicações em flash ou através de cliques em banners publicitários, evitando que certos dados precisem ser fornecidos a cada vez que uma página é visitada. (SILVA, 2013). De um modo geral, estes pequenos programas são capazes de armazenar informações como as páginas que foram visualizadas no site, o tempo de duração do acesso, as preferências dos usuários, as compras realizadas, e em alguns casos, informações acerca das compras feitas como o cartão de crédito, endereço IP, além de informações técnicas como navegador utilizado, bem como o sistema operacional, os programas neles instalados, e o endereço e-mail do usuário (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

A princípio, se corretamente utilizados, "os cookies são absolutamente inofensivos, e têm por objetivo apenas auxiliar o usuário de Internet a personalizar sua experiência e facilitar

[24] Modelar significa criar um modelo que explique as características de funcionamento e comportamento de um software a partir do qual ele será criado, facilitando seu entendimento e seu projeto, através das características principais que evitarão erros de programação, projeto e funcionamento. É uma parte importante do desenho de um sistema de informação. Os modelos de dados são ferramentas que permitem demonstrar como serão construídas as estruturas de dados que darão suporte aos processos de negócio, como esses dados estarão organizados e quais os relacionamentos que pretendemos estabelecer entre eles. (DEBASTIANI, 2015)

[25] Ver: Shannon Petty piece, "Hospitals Are Mining Patients' Credit Card Data to Predict Who Will Get Sick," Bloomberg, July 3, 2014, http://www.bloomberg.com/news/articles/2014-07-03/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick.

a visitação a web sites." (LEONARDI, 2005, p. 84). Entretanto, como tudo na rede, existem algumas consequências negativas se utilizados de maneira maliciosa. De acordo com a Cartilha de segurança lançada pelo Comitê Gestor da Internet no Brasil (2012), os principais riscos relacionados ao uso de cookies são:

> a) Compartilhamento de informações: as informações coletadas pelos cookies podem ser indevidamente compartilhadas com outros sites e afetar a sua privacidade. Não é incomum, por exemplo, acessar pela primeira vez um site de música e observar que as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha.
> b) Exploração de vulnerabilidades: quando você acessa uma página *Web*, o seu navegador disponibiliza uma série de informações sobre o seu computador, como ˜ hardware, sistema operacional e programas instalados. Os cookies podem ser utilizados para manter referências contendo estas informações e usa-las para explorar possíveis vulnerabilidades em seu computador.
> c) Autenticação automática: ao usar opções como "Lembre-se de mim" e "Continuar conectado" nos sites visitados, informações sobre a sua conta de usuários ´ ao gravadas em ˜ cookies e usadas em autenticações futuras. Esta pratica pode ser arriscada quando usada em computadores infecta- ´ dos ou de terceiros, pois os cookies podem ser coletados e permitirem que outras pessoas se autentiquem como você.ˆ
> d) Coleta de informações pessoais: ˜ dados preenchidos por você em formulários *Web* também podem ser gravados em cookies, coletados por atacantes ou códigos maliciosos e indevidamente aces- ´ sados, caso não estejam criptografados.
> e) Coleta de hábitos de navegação: quando você acessa diferentes sites onde são usados cookies de terceiros, pertencentes a uma mesma empresa de publicidade, e possível a esta empresa determinar seus hábitos de navegação e, assim, comprometer a sua privacidade.

Em última instancia, a principal questão envolvendo a utilização de cookies diz respeito ao conhecimento do usuário de que seus dados pessoais estão sendo coletados e processados. Caso essa prática não seja informada ao internauta, este fica impossibilitado de exercer o controle e a autogestão sobre suas informações. Nessa toada, ao discorrer acerca da privacidade entre indivíduos e a coletividade e sobre o tratamento das informações pessoais, Stefano Rodotà, renomado jurista na área de direito e tecnologia, alerta:

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meio sofisticados para o tratamento de dados, podendo escapar ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. (RODOTÀ, 2007, p. 38)

É exatamente por causa dessa vulnerabilidade e ameaça à intimidade e a privacidade que muitos governos pretenderam regular o uso da internet a fim de estabelecer regras e

princípios para a proteção de direitos novos e dos já consagrados. Por conseguinte, busca-se proteger os dados dos usuários da rede e coibir eventuais crimes ou abusos comerciais praticados por setores públicos e privados. Nesse aspecto, destaca-se a Diretiva nº 95/46/CE, um grande avanço na proteção dos direitos à autodeterminação e proteção dos dados. Abaixo a transcrição de algumas diretrizes por ela proclamadas:

> Artigo 6º. 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> a) Objecto de um tratamento leal e lícito;
> b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;
> c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
> d) Exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou rectificados;
> e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.
>
> Artigo 7º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:
> a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou
> b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
> c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
> d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou
> e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou
> f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do no 1 do artigo 1. (UNIÃO EUROPEIA, 2003, p. 14)

Como se vê, a diretiva europeia se posicionou no sentido da defesa da privacidade de maneira a salvaguardar os direitos fundamentais de seus cidadãos. Os efeitos de tais regras foram percebidos na prática ao longo de tempo e vários sites europeus tiveram que adaptar às

novas regras acrescentando alertas claros e preciso sobre o uso de dados do usuário, explicando de forma explícita a sua finalidade, e antes de compartilhar as informações pessoais do internauta, obter o consentimento prévio para que este possa ter controle de seus dados. (SILVA, 2013)

Constata-se, também, que as mudanças trazidas pela informatização permitem um monitoramento incessante do comportamento em rede por um preço extremamente baixo (LESSIG, 2006). Em razão dos avanços das capacidades analíticas de alguns softwares, os riscos relacionados à privacidade de dados aumentam, colocando em questão abordagens tradicionais desse conceito, o qual será tratado com maior profundidade no próximo tópico. Para reforçar essa ideia, diversas pesquisas recentes demonstraram que é possível reidentificar ou conhecer detalhes sobre indivíduos descritos em *releases* de dados, mesmo em casos em que foram aplicadas técnicas para desidentificar a informação, gerando, a partir daí, estatísticas agregadas, das quais podem ser extraídos dados potencialmente sensíveis sobre o usuário – uma ameaça patente aos direitos de privacidade e autodeterminação informativa. [26]

Não bastasse a ascensão dos atores privados no tratamento de dados pessoais dos usuários, os rápidos avanços da tecnologia também afetaram e expandiram significativamente as capacidades de investigação de órgãos do Estado, com implicações diretas à privacidade dos indivíduos. Agora, agências do governo, em diferentes níveis, passam, cada vez mais, a coletar dados que influenciarão na tomada de decisões e na entrega de determinados serviços em áreas como segurança pública, saúde, infraestrutura e educação. Não obstante, junto a essas novas capacidades surgem questões jurídicas controversas, como a constitucionalidade da retenção de dados para fins de investigações, a extensão das prerrogativas de acesso a dados de comunicações**,** os limites das obrigações de assistência à polícia por parte de serviços protegidos por criptografia e os mecanismos de controle da atuação de órgãos de inteligência (ANTONIALLI e ABREU, 2016).

2.1.2 Vigilância Digital

A digitalização da informação não afeta apenas os dados que circulam na rede e sua utilização pelas empresas como subsídio de seus modelos de negócio. Ela também influencia

[26] Pesquisadores da Universidade do Texas demonstraram que históricos desidentificados de consumidores do Netflix foram reidentificados a partir de informações extraídas de outros sites como o Internet Movie Database, sendo possível desencobrir suas preferências políticas e outros dados potencialmente sensíveis (NARAYANAN e SHMATIKOV, 2008) Ainda nesse sentido uma pesquisa realizada pelos departamentos de ciências da computação de três grandes universidades dos Estados Unidos demonstrou que é possível utilizar o sistema de recomendação de produtos da Amazon para inferir informações sobre as transações de um usuário (CALANDRINO, KILZER, *et al.*, 2011).

diretamente em como a informação será coletada, processada e interpretada no mundo real pelas autoridades estatais. Como ressaltado por Mariana Mazzucato (2014), foi justamente o Estado o precursor de muitas das inovações tecnológicas hoje desfrutadas pela sociedade, portanto, é natural que a vigilância digital tenha se tornado a pedra angular da inteligência de sinais – SIGINT[27] e da exploração da computação em rede (CNE)[28] pelo governo.

Esse monitoramento pode tomar diversas facetas desde a interceptação, armazenamento e transmissão de comunicações digitais até o rastreamento de dispositivos, rastreamento biométrico e verificação de ameaças. Ao utilizar uma determinada seleção de ferramentas, é possível que governos ou até mesmo atores privados rastreiem indivíduos e monitorem seu comportamento e suas comunicações em rede, cujos dados podem ser utilizados para uma variedade de objetivos (MURRAY, 2016). Em resumo, pode-se dizer que a Vigilância Digital (*Digital Surveillance*) é o processo pelo qual algumas formas de atividade humana são analisadas por computadores de acordo com uma regra especifica. Essa regra pode ser: "sinalize todos os e-mails que falem sobre a AlQaeda" ou pode ser "sinalize todos os e-mails que falem mal do Presidente da República". Nesses dois casos, a característica principal é que um computador seleciona dados que serão posteriormente analisados por um ser humano (LESSIG, 2006).

Nunca houve dúvidas de que o Estado sempre possuiu a habilidade de interceptar comunicações, monitorar e rastrear comportamentos e obter dados de terceiros a partir de mandados judiciais. A princípio, ele o faz em prol da segurança nacional e paz social. Entretanto foi só a partir das revelações de Edward Snowden[29], funcionário da Agência de Segurança norte americana (NSA) em 2013, que foi possível perceber real dimensão desse monitoramento. É por essa razão que Lessig (2006, p. 210) afirma: "é preciso tomar cuidado com esse fenômeno

[27] SIGINT (acrônimo de *signals intelligence*) é o termo inglês usado para descrever a atividade da coleta de informações ou inteligência através da interceptação de sinais de comunicação entre pessoas ou máquinas.Ela é uma categoria de inteligência que compreende, individualmente ou em combinação, todas as inteligências de comunicação (COMINT), inteligência eletrônica (ELINT) e inteligência de sinais de instrumentação estrangeira, porém transmitida. (USA AIR FORCES, 1998)

[28] A CNE consiste, essencialmente, em técnicas de hacking por serviços de inteligência do Estado. (MURRAY, 2016)

[29] Edward Joseph Snowden é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA [1] que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana. A revelação deu-se através dos jornais *The Guardian* e *The Washington Post*, dando detalhes da Vigilância Global de comunicações e tráfego de informações executada através de vários Programas, entre eles o programa de vigilância PRISM dos Estados Unidos. (G1, 2013)

de “boas intenções”. Sistemas de vigilância são instituídos para um proposito, mas não são poucas as vezes que são utilizados para outros completamente distintos.”[30]

Nesse contexto, o referido autor chama a atenção para aquilo que ele denominou “ambiguidades latentes”, isto é, conflitos oriundos da tentativa de conciliar as normas do mundo físico com a arquitetura do mundo virtual. Ele cria a situação fictícia em que um código computacional (“verme”) é jogado na rede e se infiltra nos sistemas de contadores vulneráveis. Não é exatamente um vírus, pois esse código não se incorpora a outros programas, interferindo com o seu funcionamento; é apenas uma partícula adicional de código.

Em uma situação hipotética, o “verme” é usado pelo FBI para localizar um documento pertencente a Agência de Segurança Nacional norte americana, cuja posse sem a devida autorização é considerada ilegal. Para tanto, o “verme” se propaga na rede e se infiltra no disco rígido de um computador, escaneando todo o seu conteúdo. Se encontrar o documento, ele manda uma mensagem para o FBI e se não, ele se autodestrói. Não há qualquer tipo de suspeita que motive a busca; trata-se de uma busca generalizada de espaços privados pelo governo, que é feita, porém, sem qualquer interferência com o funcionamento da máquina ou sem que qualquer pessoa fique sabendo.

Lessig se pergunta, portanto, se esse “verme” seria inconstitucional, uma vez que a Quarta Emenda da Constituição norte americana[31], que prevê a proteção contra buscas e apreensões arbitrárias, foi instituída justamente como resposta aos abusos do *writ of assistance*, um tipo de mandado geral de busca emitido pelo governo colonial britânico e importante fonte de tensão na América pré-revolucionária. Ele argumenta que, apesar de ser uma tecnologia de busca, esse verme funciona de maneira diferente de uma busca e apreensão no mundo real. No mundo real, uma busca apresenta custos: os encargos da busca em si, a insegurança que venha a criar, a exposição dos agentes que conduzam uma busca além dos limites legais. O “verme”, ao contrário, aplaca esses custos. Todos os encargos são eliminados, a busca é praticamente invisível e a tecnologia utilizada é programada para encontrar apenas aquilo que é ilegal.

Essa situação traz à tona uma questão sobre como uma busca dessa natureza, que é eminentemente diferente de uma busca e apreensão no mundo atômico, deve entendida à luz

---

[30] We should also account for the “best intentions” phenomenon. Systems of surveillance are instituted for one reason; they get used for another.

[31] Emenda IV: O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas. (Embaixada dos Estados Unidos, Jul/2003.)

dos princípios constitucionais, e é exatamente esse dilema que Lessig denomina “ambiguidade latente”.

Para Lessig, a solução para o problema é entender o que se busca proteger com um “direito à privacidade”. Para tanto, ele elenca três conceitos de privacidade: (i) a primeira refere-se a uma concepção utilitária que entende a privacidade como uma proteção ao ônus injustificado de uma busca indiscriminada – aqui, refere-se às inconveniências sofrer tal perturbação; (ii) a segunda refere-se à privacidade como uma proteção à dignidade – mesmo que a busca não seja um fardo para qualquer pessoa, ou mesmo que a pessoa não perceba essa busca, essa concepção de privacidade entende que a própria ideia de busca é uma ofensa à dignidade. Esse interesse á dignidade só é assegurado caso o Estado possua uma boa razão para procurar, antes da busca em si. (iii) a terceira perspectiva não está relacionada nem à preservação da dignidade, nem a minimização de invasões. É, na verdade substantiva – privacidade como uma forma de limitar o poder do estado de regular.

Em um mundo pré-tecnológico, não havia ambiguidade, pois esses conceitos se confundiam: uma busca e apreensão que se pusesse como perturbação excessiva e injustificada configuraria uma violação da dignidade e vice e versa. Hoje em dia, não é mais assim. Com os avanços na informática essas três concepções podem levar a resultados completamente diferentes.

As tecnologias digitais contemporâneas oferecem ao governo, às corporações e a criminosos, uma capacidade de interferir com direitos do cidadão sem precedentes. A censura on-line, a vigilância em massa e direcionada, a coleta de dados, os ataques digitais contra a sociedade civil e a repressão resultante da expressão on-line forçam indivíduos de todo o mundo a buscar segurança para manter opiniões sem interferência e buscar, receber e transmitir informações e ideias de todos os tipos. Dessa forma, muitos encontraram a solução para essa invasão na criptografia e no anonimato, por meio de tecnologias sofisticadas para disfarçar sua identidade e sua pegada digital. Esses dois importantes veículos para a segurança on-line, proporcionam aos indivíduos meios de proteger sua privacidade, capacitando-os a navegar, ler, desenvolver e compartilhar opiniões e informações sem interferência e permitindo que jornalistas, organizações da sociedade civil ou membros de grupos étnicos ou religiosos ativistas, estudiosos, artistas e outros exerçam o direito à liberdade de opinião e expressão. (HUMAN RIGHTS COUNCIL, 2016)

Nesse sentido, cumpre destacar relatório inédito, realizado pela Electronic Frontier Foundation (EFF)[32], que compara práticas de vigilância e legislações em 12 países na América Latina. Na pesquisa foram analisadas leis e práticas publicamente disponíveis. Todavia, dada a cultura de sigilo profundamente arraigada em torno da vigilância nesses países, é muito difícil julgar até que ponto os Estados cumprem, de fato, as normas legais editadas. Garantir que a lei não só cumpre com os padrões de direitos humanos, mas realmente governa e descreve o comportamento real dos Estados é um desafio permanente.

O documento, conclui que a América Latina está um passo à frente do resto do mundo na existência de leis que protegem a privacidade. Porém, destacou que a maioria dos Estados não implementa esses direitos de maneira inteiramente compatível com os direitos humanos. Nesse sentido, as autoridades estatais e a sociedade civil devem tomar cuidado para que as normas escritas sejam, de fato, traduzidas em prática consistentes e que as falhas na defesa da lei possam ser descobertas e corrigidas. Isso levanta um segundo problema: a falta de supervisão pública adequada em toda a região. Esta é a principal razão pela qual mesmo as garantias positivas estabelecidas pela lei - e há muitos exemplos de boas normas de vigilância na região - simplesmente não funcionam. Estes só podem ser superados se a sociedade civil exigir transparência e responsabilidade da comunidade de inteligência e aplicação da lei.

Nessa esteira, cumpre destacar aqui dez importantes descobertas sobre a vigilância na América Latina:

> 1. As legislações sobre a vigilância são de má qualidade porque permitem interpretações arbitrárias pelas autoridades. É o caso de Brasil, Colômbia, El Salvador, Peru, Guatemala, Honduras, Chile, Paraguai e Uruguai.
> 2. As leis favorecem a proteção de alguns dados e não de outros. Os metadados não estão bem protegidos.
> 3. Não existem registros públicos para analisar os IMSI-catchers ou outras tecnologias de vigilância que estão em uso na região e não se sabe de que forma se usam as informações coletadas por eles.
> 4. Nem sempre é preciso de ordem judicial imparcial para acessar informações confidenciais.
> 5. Inexistem transparência, supervisão pública e direitos de reparação com relação às informações retidas pelos provedores de comunicação.
> 6. Não há suficiente precisão legal nem limites sobre as circunstâncias nas quais se autoriza a vigilância nas comunicações. Um exemplo disso é Honduras, que não limita o âmbito das atividades de vigilância.
> 7. Quando se trata de investigações criminais, a vigilância é tida como uma prática comum, não como último recurso, como deveria ser. Entre os 12 países do estudo, o Brasil é o único que tem uma lei especificando que um juiz não

[32] A Electronic Frontier Foundation – EFF é uma organização não-governamental pioneira na defesa de direitos digitais. A organização trabalha com tecnólogos, ativistas e advogados para defender a liberdade de expressão online, combater a vigilância ilegal e advogar em nome dos usuários e da inovação.

> pode autorizar a interceptação das comunicações quando “a prova puder ser feita por outros meios disponíveis”.
> 8. Em nenhum país o Estado tem a obrigação legal de notificar diretamente as pessoas afetadas pela vigilância.
> 9. Os serviços de comunicação não fazem relatórios públicos sobre a natureza e o âmbito de sua interação com governos e sua participação em atividades de vigilância. Apenas o México exige em sua Lei Geral de Transparência e Acesso à Informação Pública a transparência do governo quando se demandam dados dos provedores.
> 10. Não existem mecanismos de supervisão pública para controlar potenciais abusos de poder quando se trata da vigilância das comunicações. (CORREA e SIMÕES, 2016)

Em suma, não resta dúvidas de que a utilização cada vez mais ampla de informações pessoais para as mais diversas finalidades da vida em sociedade – identificação, classificação, autorização etc.– torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade, usufruindo de todas os benefícios proporcionados pela tecnologia. Entretanto, é preciso ter em mente que o tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco, tanto nas mãos de entidades privadas, como nas mãos do governo. Nesse sentido, Murray (2016) destaca dois dos principais perigos que podem derivar dessa prática: a fraude, isto é a utilização da informação por terceiros sem o conhecimento de seu titular e o mau uso dos dados pessoais, que se concretiza na possibilidade de exposição e utilização indevida ou abusiva das informações pessoais.

Portanto, ante o exposto, torna-se mister a criação de mecanismos que proporcionem ao indivíduo efetivo conhecimento e controle sobre seus próprios dados, os quais são expressão direta de sua personalidade. O desafio dos juristas, porém, é evitar que a resposta da lei diante dos desafios apresentados pela informatização seja elaborada em desordem, sob forma de regulamentações mal coordenadas, excessivamente minuciosas e muitas vezes fragmentadas, que, por tentarem acompanhar o progresso científico, sem uma base sólida de princípios e valores, tornam-se rapidamente obsoletas. (CATALA, 1998)

Assim, a pergunta que se coloca é: qual o misto de leis e tecnologia que pode estabelecer um nível adequado de controle que balanceie o interesse público e privado, protegendo direitos fundamentais e aos mesmo tempo criando um incentivo econômico para que novas tecnologias sejam desenvolvidas e aperfeiçoadas? É isso que se pretende analisar ao longo desse trabalho.

2.2 PRIVACIDADE

2.2.1 Contextualizando a privacidade

Escolher o valor a ser protegido pela sociedade com o direito de privacidade nunca foi uma tarefa fácil, tendo sido objeto de discussão para muitos teóricos. A privacidade não é apenas um conceito legal, ela também possui aspectos psicológicos, sociais, culturais e políticos (ONN, DRUCKMAN, et al., 2005). Assim, embora reconhecido universalmente, o direito à privacidade apresenta variações quanto à nomenclatura[33], conteúdo e extensão nas diferentes legislações, sendo objeto de diversas polêmicas jurídicas (MENDES, 2008).

Ao longo dos séculos, foram elaboradas diversas justificativas teóricas para o direito à privacidade, as quais, em última instância, podem ser divididas em duas grandes classes: a privacidade como um fim em si mesmo, isto é, um direito liberal que reflete, sobretudo, a liberdade; e a privacidade como o direito à dignidade humana. Essas justificativas explicam o direito mencionado como um meio de proteger a autonomia dos seres humanos, sendo uma ferramenta essencial para o seu desenvolvimento, construção de sua identidade, realização pessoal, criatividade e aprendizado (ONN, DRUCKMAN, *et al.*, 2005).

Quanto à positivação destes direitos, a privacidade é declarada e assegurada por normas internacionais, como a Declaração Universal dos Direitos do Homem (DUDH) e o Pacto Internacional dos Direitos Civis e Políticos (PIDCP) – ambos adotados pela ONU em 1948 e 1966, respectivamente, sendo, portanto, reconhecida como um direito humano fundamental:

> Artº 12º (DUDH): Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.
>
> Artº 17º (PIDCP): 1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação. 2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados.

No Brasil, o direito à privacidade está constitucionalmente inserido no artigo 5º, X da Carta Magna, que preconiza serem "invioláveis a intimidade, a vida privada, a honra e a imagem

[33] "Com relação à terminologia utilizada para designá-lo, encontram-se no direito americano expressões como "right to privacy" e "right to be let alone", enquanto no direito francês, encontram-se as expressões "droit a la vie privée" e "droit a la intimité". Na Itália, utilizam-se os termos "diritto alla riservatezza", "diritto alla segretezza" e "diritto alla rispetto della vita privatta", na Espanha fala-se de "derecho a la intimidad" e na Alemanha utiliza-se predominantemente a expressão "Recht auf informatiolelle Sebstbestimmung" (direito à autodeterminação informacional)" (MENDES, 2008, p. 18 e 19)

das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Ademais, o inciso XII do mesmo artigo garante a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Por este motivo, não resta dúvida que a privacidade é tida como direito fundamental, mais especificamente, de primeira dimensão, visto que constitui um direito civil individual de todo cidadão.

Ao encontro do quanto estipulado pela Constituição Federal, o Código Civil,[34] o Código de Defesa do Consumidor[35] e, mais recentemente, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet ("MCI") disciplinaram de forma mais específica referida proteção. Este último diploma, que será objeto de análise mais aprofundada no próximo capítulo, estabeleceu como um dos princípios do uso da internet no Brasil a proteção da privacidade e dos dados pessoais, conforme art. 3º, II e III[36], assim como, nos incisos do seu artigo 7º,[37] disciplinando os direitos

[34] Art. 21. 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.

[35] Estabelece regras relacionadas à formação de bancos de dados referentes a consumidores, conforme Seção VI, do Capítulo V, do Código de Defesa do Consumidor.

[36] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
(...)
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
(...)

[37] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
(...)
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
(...)

e garantias dos internautas e estabelecendo regras com o intuito de dar efetividade a referidas garantias (ALVES e VAINZOF, 2016).

Assim, o escopo desse trabalho não é traçar um panorama histórico da evolução dos conceitos de privacidade, que é longo e denso, nem debater as diversas nuances que o termo apresenta. O objetivo aqui é muito mais pragmático: é compreender as possíveis maneiras de tutelar o direito à privacidade do usuário na Internet, diante das tantas possibilidades de processamento de informações e vigilância digital.

***

Pelo exposto no tópico anterior, percebe-se que as tecnologias digitais fizeram com que o comportamento humano fosse muito mais "monitorável". A vida se tornou uma miríade de processadores paralelos – públicos ou privados - acessíveis a qualquer tempo para reconstruir eventos ou rastrear certas atividades. Enquanto no passado existia uma necessidade de proteger apenas as informações mais íntimas e sensíveis, hoje em dia, devido às mudanças tecnológicas, que permitiram o processamento de dados e a criação de perfis pessoais, constata-se que a privacidade também precisa ser protegida em relação aos fragmentos de informação biográficos, aparentemente inofensivos, como hábitos de consumo, nome, endereço, data de nascimento, estado civil, etc.

Inicialmente, muito se defendeu que, mesmo diante das características peculiares da Internet, os institutos normativos usados para interpretar e solucionar os conflitos gerados a partir da violação da privacidade na plataforma virtual deveriam ser os mesmos já existentes no ordenamento jurídico. Assim, os crimes já previstos no Código Penal e outras leis que disciplinam a violação da privacidade poderiam ser utilizadas pelos juristas em casos de transgressões no ambiente virtual. (MENDONÇA, 2014)

Uma das grandes defensoras dessa ideia é Helen Nissenbaum (2011), renomada doutrinadora sobre a privacidade e segurança no ambiente em rede. Para ela, falar em "privacidade online" sugere a ideia de que "online" seria um espaço distinto, uma realidade definida por infraestruturas tecnológicas e protocolos da rede, para o qual um novo conjunto de regras de privacidade pode ou deve ser criado. Ela rechaça esse entendimento, afirmando que não importa quão diferente seja a experiência no ciberespaço, este não constitui um domínio separado da "vida real" que mereça uma regulação distinta. Segundo a autora, a atividade online, mediada pela internet, está profundamente integrada na vida social, sendo radicalmente heterogênea e englobando múltiplos contextos sociais. Assim, os contornos da tecnologia

moldam o que você pode fazer, dizer, ver e ouvir online. Entretanto, mesmo que essas rupturas e transformações proporcionadas pela internet se apresentem como desafios em alguns contextos sociais, elas não ensejam legislações sui generis e determinadas pelo meio. Deve-se na verdade analisar essas transformações a luz de normas baseadas em uma ética geral e princípios políticos já existentes.

Todavia, é preciso ter em mente que, na época pré-informatizada, para coletar dados sobre pessoas ou monitorar suas comunicações era preciso dispender tempo e dinheiro – isto é, era necessária uma grande intervenção humana. Agora, com as novas tecnologias que propiciaram mudanças quantitativas e qualitativas no processamento da informação, o custo de controle é ínfimo e o procedimento é feito em questão de segundos, muitas vezes sem o conhecimento ou o consentimento do usuário. Percebe-se, portanto, que a utilização dos institutos já existentes não é mais suficiente para disciplinar o tema, uma vez que não amolda de forma plena todas as situações jurídicas apresentadas pela plataforma virtual.

Tradicionalmente entendido como o limite imposto pela lei à habilidade de terceiros penetrarem um espaço privado, o direito à privacidade não encontrava grandes dificuldades de ser aplicado em ambientes com razoável expectativa de intimidade. Essas restrições legais eram quase sempre complementadas por barreiras físicas: a lei pode dizer que é ilegal entrar em uma residência à noite, mas nem por isso as pessoas deixam de trancar suas portas e janelas.[38] Por essa razão, ao pisar na esfera pública, as pessoas tinham consciência de que abriam mão de seus direitos de esconder ou controlar aquilo que os demais pudessem vir a saber sobre elas (LESSIG, 2006). Entretanto, com o advento das tecnologias digitais, que hoje abarcam praticamente todos os aspectos da vida em sociedade, essa situação mudou.

Por viver em um contexto social, é evidente que nem tudo que diz respeito ao indivíduo pertence a sua vida privada - o direito à privacidade está relacionado a informações que afetam a independência e a habilidade de uma pessoa de exercer controle sobre suas relações íntimas e escolhas de vida (TRUDEL, 2009). A partir do momento que um indivíduo faz certas coisas que interessam a terceiros, a sua vida privada é necessariamente limitada pelos legítimos interesses daqueles. Nesse sentido corrobora o entendimento de Alan Westin:

> O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo

[38] No nosso ordenamento jurídico, essa ideia é claramente delineada na Constituição Federal que prevê a inviolabilidade do domicilio: **XI** - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; (Vide Lei nº 13.105, de 2015) (Vigência)

> está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive. O indivíduo o faz em face das pressões da curiosidade dos outros e dos processos de vigilância que toda sociedade necessita para a implementação de normas sociais. (WESTIN, 1970, p. 7)

Portanto, da mesma forma que diferentes âmbitos da vida são protegidos de diferentes maneiras no mundo físico, constata-se, também, que algumas interações na internet são consideradas públicas, enquanto outras pressupõem privacidade. Nesse sentido, os usuários podem, por exemplo, envolver-se em atividades que equivalem às transações cotidianas da vida pública, como a criação de perfis públicos em redes sociais ou a troca de dados pessoais por serviços, como *wi-fi*, download de arquivos etc. Em contraste, eles podem também praticar certas condutas na rede que devem, *a priori*, se manterem privadas, como por exemplo, a troca de mensagens ou as palavras-chave utilizadas em ferramentas de pesquisa.

A fim de estabelecer proteções que balanceiem todos os direitos fundamentais, é preciso levar em consideração o fato de que público e privado estão em um *continuum* no ciberespaço, o que torna os contornos do conceito de privacidade extremamente nebulosos. A existência de "lugares" diferentes na rede, aliada ao poder de processamento de dados das novas tecnologias, indica que o ciberespaço engendra riscos que precisam ser administrados, como por exemplo, os perigos decorrentes do processamento de informação e a capacidade crescente de algumas ferramentas de pesquisa (TRUDEL, 2009).

Isto posto, deve-se compreender que o arcabouço jurídico da internet pode ser analisado sob a perspectiva dos riscos que a tecnologia cria. O risco, como uma construção social, é avaliado de acordo com a conjuntura temporal, cultural, social e política. Nesse sentido, as ideias sobre os perigos e o potencial da tecnologia ajudam a construir percepções coletivas de privacidade, que, igualmente, variam com o contexto em que se encontram. Alinhado com esse entendimento, Schauer (1998) sugere que, apesar das transformações quantitativas e qualitativas no processamento da informação, não foi a internet que mudou as formas pelas quais a privacidade é invadida, mas sim é a própria concepção de privacidade da sociedade que está mudando.

2.2.2 O "Mercado de Limões" - Privacidade como instrumento de confiança

Atualmente, na vida cotidiana, as tecnologias de comunicação analógica têm sido cada vez mais substituídas por formas digitais: e-mails substituíram cartas, web sites substituíram jornais, e *e-books* passaram a competir com seus semelhantes de papel pelo mercado da literatura. Tais aparatos eletrônicos, incontestavelmente, melhoraram a vida do ser humano em diversos sentidos, expandindo tanto o acesso ao conhecimento como a liberdade de expressão. Entretanto, as novas tecnologias não vieram sem um custo: todas as vezes que compramos, lemos, falamos ou pensamos na rede, computadores criam registros dessas atividades, permitindo um monitoramento constante de hábitos de leitura, histórico de navegação, comunicações privadas etc.[39]

Assim, em resposta às novas tecnologias de monitoramento e à agressividade das grandes empresas na corrida por dados pessoais, a privacidade na concepção moderna adquiriu duas facetas de proteção: a da responsabilidade civil e a do controle. A privacidade como responsabilidade civil apresenta um comando substantivo: não cause danos ao processar dados pessoais. Já a privacidade como controle oferece um arcabouço jurídico procedimental para administrar a coleta e o fluxo de informações pessoais ancorado na oportunidade de os indivíduos estarem cientes que os seus dados estão sendo processados (RICHARDS e HARTZOG, 2015).

Ao mesmo tempo em que legislações de proteção de dados são úteis como um princípio organizador, paradoxalmente, elas têm se revelado como instrumentos de fragilização da privacidade. Isso ocorre porque, além de ainda serem incapazes de resolver determinados problemas relacionados a esse direito, essas normas estão centradas em um ideal de controle. Nesse entendimento, contanto que o usuário tenha autonomia para decidir quando abrir mão de

---

[39] Nesse sentido, a título de exemplificação, cabe destacar as condutas de *scanning* de e-mails e mensagens adotadas por empresas como Google Inc e Facebook Inc as quais, inclusive, foram alvo de diversas ações judicias por violação de privacidade dos usuários (United States v. Google Inc. (No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012); Corey et. Al v. Google Inc 5:16-cv-00473 (N.D. Cal. Jan. 27, 2016); Daniel Matera v. Google Inc. Case No. 15-CV-04062-LHK; Matthew Campbell, et al v. Facebook Inc. Case No. 13-cv-5996-PJH).
No caso da Google, a companhia oferece o serviço de correspondência eletrônica Gmail e faz um *scan* do conteúdo das mensagens para duas finalidades principais: oferecer anúncios personalizados e criar perfis dos assinantes a fim de aumentar os seus lucros.
Em todos os processos a empresa se mantém firme na alegação de que os argumentos levantados pelos requerentes são inválidos, uma vez que a prática em questão viabiliza os anúncios, que representam mais de 90% da sua renda e, consequentemente, permite que seja oferecido um serviço completamente isento de custos para o consumidor. A companhia sustenta, ainda que essa prática é um procedimento padrão, que ocorre no curso normal das atividades empresariais e, portanto, estaria protegida pelas leis federais e estaduais de interceptações de comunicação. Por fim, a Google postula o fato de que os usuários do Gmail, ao adquirirem o serviço, concordaram com os termos de privacidade, nos quais está expressamente descrita a prática de *scanning* de e-mails. (Motion to Dismiss. 06/13/2013.Case No. 5:13-md-02430-LHK)

certos direitos de privacidade, os processadores e controladores de dados estarão em conformidade com a lei.

Apesar desse modelo de notificação e escolha (*notice and choice*) estar bem arraigado em algumas das mais populares teorias sobre privacidade e também no sistema de regulação do mundo coorporativo, a pressuposição de que as pessoas podem fazer escolhas adequadas para proteger a sua informação é uma ilusão. Nessa esteira, em 2010, o FTC, Comissão Federal do Comércio norte-americana, emitiu um pronunciamento reconhecendo que

> Nos últimos anos, as limitações do modelo de "notificação e escolha" tornaram-se cada vez mais evidentes. Políticas de privacidade se tornaram mais longas, complexas e, em muitos casos, incompreensíveis para os consumidores. Muitas vezes, as políticas de privacidade são projetadas mais para limitar a responsabilidade das empresas do que para informar os consumidores sobre como suas informações serão usadas. Além disso, enquanto muitas empresas divulgam suas práticas, um número significativamente menor oferece, de fato, aos consumidores a capacidade de controlar essas práticas. Consequentemente, os consumidores enfrentam um fardo substancial de ler e compreender as políticas de privacidade e exercer as limitadas opções oferecidas a eles. (...) Além disso, a ênfase em "notificação e escolha" por si só não responde de maneira satisfatória a outras práticas largamente reconhecidas, como acesso a informações, limitação de coleta, especificação de propósito e garantia de qualidade e integridade dos dados.[40] (FTC, 2010, p. 19 e 20)

Para muitos críticos, o problema desse sistema de "escolha" está no regime de oferecer privacidade aos indivíduos baseado em um sistema "pegue ou deixe". Escolher significa deliberar e decidir livremente. Logo, a prática quase que universal de sistemas *opt-out*[41] não pode ser considerada um modelo ideal de escolha consciente do consumidor em um mercado competitivo. O argumento de que os indivíduos escolhem por livre e espontânea vontade pagar pelos serviços online na forma de dados pessoais[42] não merece ser sustentado em si mesmo,

---

[40] *In recent years, the limitations of the notice-and-choice model have become increasingly apparent. Privacy policies have become longer, more complex, and, in too many instances, incomprehensible to consumers. Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used. Moreover, while many companies disclose their practices, a smaller number actually offer consumers the ability to control these practices. Consequently, consumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered to them. (…) Additionally, the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity.*

[41] "Opt-out é o sistema de envio de mensagens eletrônicas, em que os destinatários dessas mensagens de marketing recebem-nas automaticamente, sem haver solicitação prévia. Apenas por meio de ação expressa do usuário, ele se libera do envio de mensagens. O sistema oposto é o opt-in, em que o usuário precisa fazer a opção para receber as mensagens." (HIRATA, 2014, p. 25)

[42] Esse argumento é recorrente nas diversas defesas apresentadas pela Google Inc. nos (muitos) processos em que é acusada de violação de privacidade. Citando o precedente Smith v. Maryland de 1979, a empresa sustenta que "uma pessoa não possui legitima expectativa de privacidade sobre as informações que entrega voluntariamente a terceiros". (Motion to Dismiss. 06/13/2013.Case No. 5:13-md-02430-LHK)

uma vez que o preço de não se envolver socialmente, comercialmente e financeiramente no ambiente em rede é demasiado alto, trazendo à baila o questionamento se essas escolhas são de fato livres (NISSENBAUM, 2011).

Nesse sentido pode-se dizer que o mercado para a privacidade no ciberespaço se encaixa no consagrado modelo econômico do "mercado de limões", apresentado por George A. Akerlof (1970). No exemplo original, compradores e vendedores interagem em um mercado com dois tipos de carros: carros usados em bom estado, que valem uma alta quantia e "limões", uma gíria do inglês que corresponde a carros usados ruins, sendo que apenas os donos sabem dessa condição. Nesse cenário, os compradores são incapazes de distinguir um bom carro de um "limão" e, por conseguinte, oferecem um preço menor do que seria esperado para um carro em bom estado, a fim de compensar as chances daquele automóvel estar depreciado. Como resultado, nenhum dono de carros bons vai desejar vender o seu veículo, deixando o mercado cheio de "limões".

Note-se que o problema se originou de um fato: os compradores, desconfiados, decidem que não há como saber se o carro é bom ou ruim, e os vendedores são incapazes de persuadi-los do contrário. Assim, os mercados são flagelados pela assimetria de informação, que ocorre quando a informação necessária para que compradores e vendedores cheguem ao "equilíbrio" não está igualmente distribuída entre todos os participantes de mercado. (ANDERSON, 2013)

Aplicando esse modelo à privacidade, é possível pensar em um consumidor escolhendo dentre os sites que respeitam a sua privacidade e aqueles que a ignoram, sem qualquer maneira de determinar, de antemão, qual é qual. Assim, percebe-se que a privacidade em web sites se parece com o "mercado de limões". A linguagem ofuscada empregada nas políticas de privadas de muitos provedores de aplicação deliberadamente privam o consumidor da informação adequada sobre que tipo de proteção está sendo de fato oferecida, impedindo que os sites compitam entre si no quesito privacidade. Em outras palavras, pelo fato de os usuários terem tanta dificuldade em acessar a política de privacidade de um site, as empresas têm menos incentivos para fornecer boas funcionalidades e o mercado passa a ser dominado por "limões". (VILA, GREENSTADT e MOLNAR, 2004)

Em geral, o custo de oportunidade de coletar informações é mais alto no ambiente online do que no mundo físico. Se analisarmos quão pequena é a escala em que se dão muitas das transações na internet, como, por exemplo, a compra de um livro ou uma simples visita a um site, ler e compreender uma política de privacidade extensa se torna muito menos palatável do que buscar informações ao comprar uma casa ou realiza um procedimento cirúrgico, por

exemplo. Em outras palavras, durante o tempo que você precisa para ler e compreender a política de privacidade da Amazon, você pode ir até a livraria e comprar o livro. (VILA, GREENSTADT e MOLNAR, 2004).

Desse modo, resta claro que a abordagem tradicional da privacidade, tanto na perspectiva da responsabilidade civil, como do controle, é quase sempre um conceito negativo - um dano a ser evitado ou um consentimento a ser obtido. Segundo Richards e Hartzog (2015) é esse enfoque pessimista que tem causado um pensamento desnecessário, incompleto e fixado em consertar danos, ao invés de agregar real valor ao direito de privacidade. Destarte, os autores apresentam uma nova concepção de privacidade, muito mais adequada aos tempos contemporâneos: a privacidade como instrumento de confiança.

A confiança é um ingrediente essencial para relações saudáveis e, consequentemente, sociedades bem-sucedidas. Existe uma vasta literatura sobre esse conceito, que permeia diversas áreas acadêmicas, desde as ciências sociais até campos mais inusitados como medicina e administração. Para além dos aspectos éticos e morais, a confiança se consubstancia em uma necessidade do próprio modelo jurídico e do contexto social contemporâneos, exercendo a lei um importante papel de pacificação social. Assim, uma boa definição geral é aquela que encara a confiança como

> um estado de espírito que permite que um indivíduo esteja disposto a se colocar em uma posição de vulnerabilidade perante outrem – isto é, a depender de outra pessoa apesar do risco positivo dela agir de uma maneira que pode prejudicar aquele que confia. (HILL e O'HARA, 2006 apud RICHARDS e HARTZOG, 2015, p. 22)[43]

Embora permeada por diversas nuances e graduações, a confiança é uma necessidade social. Na vida cotidiana, os sujeitos aderem a relações jurídicas específicas em virtude de representações manifestadas por terceiros, independentemente de uma maior ponderação sobre as consequências dessa adesão. Esse fato ocorre devido à confiança depositada na outra pessoa ou na própria relação jurídica. O indivíduo que confia, necessariamente, coloca-se numa posição mais frágil e vulnerável dentro de determinada relação jurídica. Assim, para compensar essa vulnerabilidade, cabe ao sistema normativo garantir um mínimo de segurança para o desenvolvimento das atividades do indivíduo. (MARTINS, 2008)

[43] *Trust is a state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster.*

No ordenamento jurídico brasileiro, essa concepção de "confiança" é igualmente valorizada:

> Consagrada no Código Civil de 2002 a teoria da confiança, pode-se afirmar, com renovado vigor, que, na interpretação das diversas cláusulas de um contrato, devem-se considerar vinculantes os deveres que, manifestados pelas partes, suscitam em ambas uma compreensão comum quanto ao conteúdo da declaração. (TEPEDINO, 2005, p. 9)

De acordo com a doutrina pátria[44], com a adequada proteção da confiança, o ordenamento não apenas garante a segurança e a credibilidade nas relações sociais, mas, de maneira reflexa, também acaba por fortalecer a própria confiança no arcabouço jurídico. Portanto, a proteção da confiança legítima assume duplo papel em nosso sistema legal: i) atua como uma proteção das legítimas expectativas; e ii) ao mesmo tempo funciona como justificativa da vinculabilidade das partes à relação jurídica. Nessa dimensão, a confiança permite aos indivíduos prosseguir com suas atividades, protegidos de eventuais condutas levianas ou contraditórias de terceiros, em quem se confiou, garantindo a vinculabilidade aos negócios jurídicos de que participam. (MARTINS, 2008)

Na vida digital não poderia ser diferente. Como já destacado, grande parte das atividades na rede é mediada por relações informacionais, na qual profissionais liberais, instituições privadas, ou o próprio governo detêm informações sobre o indivíduo como forma de contraprestação de um serviço fornecido. Essas relações estão em todo lugar: ao compartilhar informações sensíveis com provedores de serviço de internet, redes sociais, bancos, ferramentas de pesquisa, companhias de cartões de credito etc. Destaca-se, ainda, que, com o surgimento dos *smartphones* e com o desenvolvimento da chamada internet das coisas, a coletivização da informação foi potencializada em grande medida. A inteligência coletiva não é mais produzida apenas por seres humanos, mas, cada vez mais, por sensores. Celulares e câmeras estão se tornando olhos e ouvidos para diversos aplicativos; sensores de movimento e localização indicam onde estamos, para que estamos olhando e quão rápido nos movemos, de forma que os dados são coletados, processados e utilizados em tempo real (O'REILLY e BATTELLE, 2009).

---

[44] Nesse sentido, observe-se os enunciados nºs 362 e 363 da IV JORNADA DE DIREITO CIVIL, realizada pelo Centro de Estudos Judiciários – CEJ – do Conselho da Justiça Federal – CJF, no ano de 2006:
362 – Art. 422. A vedação do comportamento contraditório (venire contra factum proprium) funda-se na proteção da confiança, tal como se extrai dos arts. 187 e 422 do Código Civil.
363 – Art. 422. Os princípios da probidade e da confiança são de ordem pública, estando a parte lesada somente obrigada a demonstrar a existência da violação.

Percebe-se, portanto, que a própria arquitetura da internet depende da habilidade das pessoas confiarem umas nas outras no que diz respeito ao tráfego de comunicações. Para exercer suas liberdades civis digitalmente, os indivíduos precisam poder confiar nos intermediários e destinatários para se envolver politicamente e aumentar os ideais de liberdade de expressão. Nesse cenário, a confiança online significa, principalmente, tornar-se vulnerável para uma pessoa ou organização ao revelar informações pessoais, o que inclui o risco crescente do mau uso dessas informações, vazamento de dados, manipulação e perda da autonomia. Uma vez que a informação é revelada, o indivíduo não detém mais o controle exclusivo sobre o seu uso e disseminação - ele está à mercê daquele que a coletou.

Em março de 2010, às vésperas da revisão das leis de proteção de dados da Europa, o Supervisor de proteção de dados da União Europeia, Peter Hustinx emitiu o seguinte pronunciamento:

> A confiança, ou melhor, a falta dela, tem sido identificada como um assunto central na emergência e emprego bem-sucedido de tecnologias de informação e comunicação. Se as pessoas não confiam nas TICs, essas tecnologias provavelmente falharão. A confiança nas TICs depende de diferentes fatores; garantir que as tecnologias não corroam os direitos fundamentais à privacidade e à proteção de dados dos indivíduos é um dos principais.
>
> A fim de reforçar ainda mais o arcabouço legal de proteção de dados/ privacidade, princípios que permanecem completamente validos na sociedade da informação, a EDPS propõe a comissão incorporar "privacidade por design em diferentes níveis de leis e elaboração de políticas públicas. [45] (HUSTINX, 2010, p. 21)

Assim, para transformar a coleta de dados em um intensificador do relacionamento com o usuário, deve-se abandonar a ideia de que os indivíduos são "pontos isolados" que não reagem aos elementos extrínsecos que restringem ou permitem comportamentos. Na linha do que preconiza Andrew Murray em sua teoria da regulação do ciberespaço, a relação aqui não é unilateral. Nesta troca de valores, os consumidores devem ser tratados como elementos ativos, i.e, parceiros de pleno direito, de forma que entendam com clareza por que seus dados são coletados, como eles serão utilizados, e para qual finalidade. Isso significa transparência e foco em políticas de privacidade claras, inteiramente compreensíveis e fáceis de serem lidas. Assim,

---

[45] *Trust, or rather its absence, has been identified as a core issue in the emergence and successful deployment of information and communications technologies. If people do not trust ICT, these technologies are likely to fail. Trust in ICT depends on different factors; ensuring that such technologies do not erode individuals' fundamental rights to privacy and to the protection of personal data is a key one.*
In order to further strengthen the data protection/privacy legal framework, the principles of which remain completely valid in the information society, the EDPS proposes the Commission to embed Privacy by Design on different levels of law and policy making.

esse direito, incorporado na lei, pode ser visto não como um conceito negativo, mas sim como um trunfo para os processadores de dados ao redor do mundo.

Em termos simples, a privacidade importa porque ela permite a confiança. Leis sobre privacidade que promovam a confiança permitem com que as pessoas revelem de maneira segura informações pessoais em maneiras que beneficiam não só indivíduos, mas as entidades com as quais eles partilham esses dados. Entender como as regras sobre privacidade promovem confiança vai além do princípio do dano. Uma solução mais positiva é projetar e desenvolver as tecnologias de informação e comunicação de forma que respeitem a privacidade e proteção de dados, incorporando esses princípios dentro de todo o ciclo de vida da tecnologia, desde a fase inicial de concepção, até à sua implementação final, utilização e eliminação. Esse processo é normalmente referido como *privacy by design* e será analisado mais abaixo.

2.2.3 Codificando a privacidade – uma aplicação da teoria de Lessig ao conceito de "privacy by design"

Imagine-se a internet como um dispositivo que permite um transeunte – seja ele um agente do governo ou um ente privado - olhar através de paredes aparentemente sólidas de uma casa, observando tudo o que se passa ali dentro. Antes do desenvolvimento desse aparelho, a privacidade do indivíduo era garantida pelas paredes dessa casa - pelo menos uma proteção contra a invasão visual. Contudo, com o surgimento desse dispositivo, o nível de proteção diminuiu. Essa situação pode justificar uma resposta legal, como proibir o uso desse aparelho em determinados contextos ou uma resposta tecnológica, como dar aos moradores aparelhos que bloqueiem a invasão ou incentivar a construção de casas com paredes de materiais diferentes. De qualquer forma, é preciso desenvolver respostas legais, tecnológicas e políticas a fim de assegurar que, mesmo diante dessa nova tecnologia, as pessoas disfrutem da mesma proteção que tinham antes do surgimento desse aparelho (SCHAUER, 1998).

A partir dessa alegoria, percebe-se que existem diversas maneiras pelas quais se pode resguardar a privacidade no mundo real. A lei é uma das maneiras mais tradicionais de fazê-lo, conferindo a esse direito, inclusive, um status constitucional. Todavia, de acordo com a teoria de Lawrence Lessig destacada no capítulo anterior, as leis não são a única maneira de proteger a privacidade individual. As normas sociais, instrumento de coação extralegal, também protegem a privacidade - ao menos em um contexto social, as normas limitam, por exemplo, o tipo de perguntas que se pode fazer para cada pessoa, a depender de diversos fatores como

intimidade, hierarquia, etc. O mercado é um terceiro tipo de restrição efetiva, que pode, por exemplo, atuar como incentivo para produção de produtos com maior nível de proteção da privacidade em troca de preços mais altos.

Entretanto nenhuma barreira é mais efetiva para Lessig do que a arquitetura: muros altos podem tornar casas mais seguras, cadeados sofisticados mantém de fora até os ladrões mais habilidosos; paredes grossas não permite que se ouça através delas e cortinas pesadas não revelam o que está do lado de dentro. Todos estes são exemplos de arquitetura de um determinado lugar, que podem diminuir ou aumentar a privacidade (LESSIG, 2006). Assim, é inevitável perceber que "a discussão jurídica sobre a privacidade de informações que trafegam por meio da Rede é, em boa parte, condicionada pelas características das ferramentas tecnológicas empregadas para sua veiculação. " (LEONARDI, 2011, p. 180).[46]

O ponto em descrever essas múltiplas restrições ao comportamento humano é trazer à tona uma perspectiva muitas vezes deixada de lado em discussões sobre privacidade, em especial a privacidade de dados: são as quatro modalidades operando em sintonia que determinam o nível de privacidade em qualquer contexto em particular. Os quatro juntos podem exacerbar a privacidade ou trabalhar um contra o outro. Assim, deve-se partir da premissa de que o código é avalorativo– ele não é necessariamente invasivo ou protetivo da privacidade. Para que a privacidade seja priorizada pelos programadores do código, é necessário empregar os incentivos adequados, isto é, as outras modalidades devem agir em conjunto.

[46] "Diversos outros exemplos relacionados ao emprego de arquiteturas de controle para proteger ou violar a privacidade podem ser citados: a) empresas monitoram a navegação na Internet e a correspondência eletrônica de seus empregados por meio da arquitetura de seus sistemas, que são projetados para efetuar automaticamente essa vigilância, cabendo ao empregado anuir com esse procedimento se quiser manter o emprego; b) Web sites de empresas de comércio utilizam cookies, pequenos arquivos de texto, para identificar conexões oriundas de um mesmo computador, de forma a "reconhecer" o retorno de um usuário ao Web site; c) cônjuges que suspeitam de traição utilizam programas-espiões, conhecidos como keyloggers, que registram cada botão pressionado no teclado e enviam, por meio da Internet, relatórios periódicos detalhados, de modo a vigiar a conduta online de seus parceiros; d) redes sociais online permitem a seus usuários optar por diversos níveis de privacidade, escolhendo a quem divulgar e de quem esconder certas informações, dependendo do grau de proximidade; e) informações são armazenadas em subdiretórios restritos de um Web site, que somente podem ser acessados utilizando-se um nome de usuário e uma senha previamente fornecidos por seu titular: essa exigência, implementada por meio de mecanismos tecnológicos, restringe o acesso a essas informações, e sua remoção implica a veiculação pública dessas; f) certos Web sites são programados para registrar automaticamente o endereço IP, data e horário da conexão utilizada pelo indivíduo, podendo posteriormente fornecer esses dados caso seja necessária sua identificação; outros Web sites são propositadamente projetados para não registrar esses mesmos dados, ou possibilitam ao usuário decidir se esse registro ocorrerá ou não; g) protocolos específicos, como o Platform for Privacy Preferences (P3P), permitem que Web sites estipulem automaticamente suas intenções de uso sobre as informações coletadas de seus visitantes, permitindo que programas navegadores automaticamente aceitem ou rejeitem a exibição do conteúdo do Web site, de modo a respeitar as preferências pessoais de privacidade previamente estabelecidas pelos usuários." (LEONARDI, 2011, p. 181)

Pelo fato de o código, assim como outras tecnologias, ser uma ferramenta neutra, ele está imbuído com os valores daqueles que o detêm e escrevem – os quais não são necessariamente a mesma pessoa. Nesse sentido, tome-se o exemplo da Microsoft: um grande número de codificadores trabalham para essa empresa, mas os valores imbuídos no código ali produzido certamente não estão conectados com a ética pessoal de cada um deles, e sim com aquilo que traz lucros a Microsoft ou com os ideais de Bill Gates sobre a missão de sua empresa. (EDWARDS, 2009). Nesse mesmo entendimento, observe-se:

> A tecnologia, em si mesma, não é intrinsecamente uma ameaça à privacidade. O ponto central está em como ela é usada. Por exemplo, a tecnologia nos permite proteger a privacidade por meio de métodos como a separação dos identificadores pessoais dos dados ou a criptografia das informações pessoais, de modo que somente possam ser vistas por aqueles que estão autorizados a fazê-lo. Conforme as inovações tecnológicas continuam a apresentar novas ameaças à privacidade, tecnologias intensificadoras de privacidade podem minimizar essas ameaças.[47] (CAVOUKIAN, 2013, p. 3)

Portanto, uma possível solução seria desenhar o código para promover a privacidade como um valor central. A pergunta é: como fazer com que as corporativas que escrevem e instalam esse código considerem a privacidade como um ponto positivo e não uma desvantagem no ciclo de desenvolvimento de seus softwares e hardwares?

Como sustentado ao longo deste capítulo, a arquitetura das tecnologias de informação e comunicação está cada vez mais complexa e apresenta diversos riscos à privacidade e à proteção de dados. Por conseguinte, a demanda por garantias mais efetivas e sofisticadas de proteção às informações pessoais na rede tende a ser cada vez maior. Assim, com usuários mais esclarecidos e interligados, a abordagem que uma entidade pública ou privada oferece à privacidade se mostra, precisamente, como a vantagem competitiva necessária para obter sucesso no mercado. A privacidade, portanto, é essencial para criar um ambiente que promova relações de confiança a longo prazo com os clientes já existentes e, ao mesmo tempo, atrair oportunidades, bem como novos usuários.

Assim, uma boa estratégia para o desenvolvimento de novas tecnologias é incorporar a privacidade e a proteção de dados como elementos intrínsecos, empregando-se uma abordagem

---

[47] *Technology itself is not inherently a threat to privacy. The key lies in how it is used. For example, technology allows us to protect privacy through methods such as severing personal identifiers from data, or by encrypting personal information in a manner such that it can only be viewed by those who are authorized to do so. As technological innovations continue to pose new threats to privacy, Privacy-Enhancing Technologies can minimize these threats.*

caracterizada por medidas proativas e não reativas, que antecipe e previna eventos invasores de privacidade antes que eles aconteçam. Essa abordagem ficou conhecida como a privacidade por design (*privacy by design*).

A privacidade por design visa incorporar mecanismos protetores da privacidade à própria arquitetura dos sistemas e processos desenvolvidos, de modo a garantir, pela infraestrutura do serviço prestado, condições para que o usuário seja capaz de preservar e gerenciar sua privacidade e a coleta e tratamento de seus dados pessoais (ALVES e VAINZOF, 2016). Nessa esteira, Ann Cavoukian (2009), uma das primeiras a cunhar o termo, defendeu que a proteção à privacidade advém da seguinte trilogia: (i) sistemas de tecnologia informação; (ii) práticas negociais responsáveis; e (iii) design físico e infraestrutura de rede.

Outrossim, Cavoukian estipulou sete princípios fundamentais para se atingir esse objetivo, os quais, mais tarde, foram incorporados por diversos policymakers ao redor do mundo. São eles: (i) *Proactive not Reactive; Preventative not Remedial,* pelo qual é adotada postura preventiva, de modo a evitar incidentes de violação à privacidade; (ii) *Privacy as the Default Setting*, pelo qual a configuração padrão de determinado sistema deve preservar a privacidade do usuário; (iii) *Privacy Embedded into Design*, pelo qual a privacidade deve estar incorporada à arquitetura de sistemas e modelos de negócio; (iv) *Full Functionality — Positive-Sum, not Zero-Sum*, pelo qual devem ser acomodados todos os interesses envolvidos, evitando falsas dicotomias que levam à mitigação de direitos; (v) *End-to-End Security — Full Lifecycle Protection*, vez que, na medida em que a segurança de dados é incorporada ao sistema antes da coleta de qualquer informação, esta é estendida para todo o ciclo de vida da informação; (vi) *Visibility and Transparency — Keep it Open*, pelo qual deve ser assegurado a todos os envolvidos que os sistemas e negócio são operacionalizados de acordo com as premissas e objetivos informados; e (vii) *Respect for User Privacy — Keep it User-Centric*, que exige que os operadores dos serviços respeitem os interesses dos usuários, mantendo altos padrões de privacidade. (ALVES e VAINZOF, 2016)

Pelo exposto acima, não resta dúvidas que Lessig estava certo ao prever o papel essencial do código na regulação do ciberespaço. Entretanto, não se deve perder de vista que a lei, embora não seja o único o fator a ser considerado na implementação bem-sucedida da privacidade na rede, tem extrema importância neste mecanismo. É certo que somente a tecnologia não pode defender a sociedade inteiramente do uso indevido dessas novas ferramentas e capacidades. É indispensável um Estado de Direito forte, com estatutos robustos, adequados e proporcionados, que permitam a formação de uma orientação jurisprudencial

consistente, e viabilizem o devido processo e a transparência. É por meio de legislações sólidas e coerentes que se pode exercer influência sobre as demais modalidades e regular um comportamento. Assim, quanto melhores forem as leis na internet, maior autonomia e melhores experiências as pessoas podem ter em suas vidas online.

Confirmando essa necessidade, o General Data Protection Regulation[48], novo Regulamento europeu, aprovado em abril de 2016 e que entrará vigor em 2018, já indica a tendência evolutiva da legislação de incorporar expressamente obrigações decorrentes da *privacy by design*:

> Artigo 25: 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
>
> 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. (...) (REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016)

Verifica-se, portanto, que essa tendência legislativa e de mercado tende a se expandir ao redor do globo, inclusive no Brasil, tornando-se imperativo que os provedores de serviços de internet e demais empresas do mercado digital acompanhem a evolução normativa relacionada à privacidade e proteção de dados pessoais e os potenciais impactos em suas atividades empresariais e modelos de negócio.

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), disponivel em: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

2.3. DADOS PESSOAIS E SUA TUTELA

2.3.1 O paradoxo da proteção de dados

Embora os benefícios proporcionados pelo avanço tecnológico sejam indiscutíveis, a questão envolvendo tecnologias digitais e privacidade ainda é permeada por uma série de paradoxos, cada um deles com sérias implicações para consumidores, empresas e os fornecedores de tecnologia, conforme revela o Índice EMC de Privacidade[49], estudo global realizado pela EMC, fornecedora de soluções de armazenamento e gerenciamento da informação, que avalia as atitudes dos consumidores em relação à privacidade online. O estudo, para o qual foram entrevistadas 15 mil pessoas, revela que os pontos de vista sobre privacidade variam muito conforme a região e o tipo de atividade realizada online.

Entre os paradoxos apontados pelo Índice EMC de Privacidade, à nível global, está o do "queremos tudo": os consumidores querem as conveniências e benefícios da tecnologia digital, embora afirmem não estarem dispostos a negociar sua privacidade para obtê-los. Nesse sentido, segundo o levantamento, 91% dos participantes valorizam o benefício de "acesso mais fácil à informação e ao conhecimento" que a tecnologia digital proporciona, mas apenas 27% dizem estar dispostos a trocar parte da privacidade por maior conveniência e facilidade online. Além disso, 85% dos entrevistados disseram valorizar "o uso da tecnologia digital para proteção contra atividade terrorista ou criminosa". Entretanto, apenas 54% se dizem dispostos a trocar parte de sua privacidade por essa proteção.

Outra contradição está no que a empresa classifica como "não tomar atitude". Embora os riscos à privacidade afetem diretamente muitos consumidores, a maioria diz que não toma praticamente nenhuma atitude especial para proteger sua privacidade — em vez disso, transferem o ônus para os que lidam com suas informações, como o governo e as empresas. Mais da metade dos entrevistados relatou já ter sofrido violação de dados, embora a maioria não tenha realizado as ações necessárias para proteger sua privacidade — 62% não trocam as senhas regularmente; quatro em cada dez pessoas não personalizam as configurações de privacidade nas redes sociais; e 39% não usam proteção por senha nos dispositivos móveis.

---

[49] Pesquisa online com base em uma amostra nacional representativa, tendo sexo e idade ponderados, realizada de 1º de agosto de 2013 a 19 de agosto de 2013, com 1.000 entrevistados por país em 15 países. Para amostras combinadas, tendo a maioria da representação do país ponderadas. Margem de erro para cada país: +3,1%; global: +1%. O teste de significância foi realizado com o nível de 95% de confiança. Os dados foram normalizados colocando os atributos em uma escala de 0 a 100: 100 = estão dispostos a negociar privacidade por conveniência; 0 = não estão dispostos a negociar privacidade para maior conveniência. A pontuação total foi obtida traves de medições quanto à disposição para negociar privacidade para maior conveniência e benefício. Disponível em: http://brazil.emc.com/campaign/privacy-index/brazil.htm. Acessado em 24 de outubro de 2016

Por fim, há o paradoxo do “compartilhamento social”. Os usuários de sites de mídia social afirmam valorizar a privacidade, embora compartilhem livremente grandes volumes de dados pessoais — apesar de manifestarem falta de confiança na proteção que essas instituições dão a suas informações. Há uma convicção entre os consumidores de que as instituições têm pouca habilidade e ética para proteger a privacidade dos dados pessoais em sites de mídia social — apenas 51% declaram ter confiança nas habilidades desses fornecedores para proteger dados pessoais e apenas 39% declaram ter confiança na ética dessas organizações. A grande maioria dos consumidores (84%) afirma não gostar que alguém saiba qualquer coisa a seu respeito ou sobre seus hábitos, a menos que a decisão de compartilhar essas informações seja sua.

No caso do Brasil, que ficou na quinta posição entre os 15 países avaliados, 26% dos entrevistados disseram estar dispostos a negociar a privacidade para maior conveniência online, enquanto 56% declararam que não trocariam a privacidade pela conveniência e desejam mais controle sobre seus dados pessoais. Essa disposição varia de acordo com as posições ou *personae* que assumem quando ficam conectadas: (i) enquanto cidadão interagindo com as agências do governo: 48% (abaixo do nível mundial que é 50%) estão dispostos a trocar privacidade por conveniência; (ii) enquanto paciente interagindo com a equipe médica e seguradoras: 48% (nível mundial é 47%); (iii) enquanto ser financeiro interagindo com bancos e instituições financeiras: 39% (nível mundial 38%); (iv) enquanto empregado interagindo com sistemas relacionados ao trabalho: 34% (nível mundial 33%); (v) enquanto consumidor interagindo com lojas online: 33% (nível mundial 29%); (vi) enquanto ser social interagindo nas redes sociais, uso de email e SMS: 30% (nível mundial 27%)

Assim como nos demais países, no Brasil, os usuários de mídias sociais revelaram ter a menor confiança na ética e nas habilidades das organizações em relação à proteção de sua privacidade. O estudo mostra que 58% declaram ter confiança nas habilidades dos fornecedores para proteger dados pessoais e 53% disseram ter confiança na ética dessas organizações, o que coloca o País entre os menores índices de confiança.

No geral, a confiança na privacidade no país é baixa. Dos entrevistados no Brasil, 71% disseram que sentem ter menos privacidade agora do que há um ano. Além disso, 73% acreditam que a privacidade será mais difícil de manter nos próximos cinco anos. Para 89% dos usuários brasileiros de mídias sociais, devem existir leis que proíbam as empresas de comprar e vender dados pessoais, sem consentimento.

No Brasil, 76% dos entrevistados relataram já ter sofrido violação de dados (conta de e-mail invadida; dispositivo móvel perdido ou roubado; conta de mídia social invadida etc.),

embora muitos deles não tenham tomando medidas para se proteger — 56% não trocam as senhas regularmente; 19% não personalizam as configurações de privacidade nas redes sociais; e 33% não usam proteção por senha nos dispositivos móveis.

Diante desse cenário, resta claro que a proteção de dados é um assunto de extrema importância, mas que está longe de ter um entendimento pacífico e de fácil compreensão, tanto entre a população, como nos setores acadêmicos e legislativos. Ele envolve diversas nuances e definições jurídicas, que serão abordadas ao longo deste trabalho. Nesse sentido, destaca-se o entendimento do celebrado jurista italiano Stefano Rodotà sobre a importância e dificuldade de se proteger os dados pessoais:

> Vivemos num tempo em que as questões relacionadas à proteção de dados pessoais se caracterizam por uma abordagem marcadamente contraditória – de fato, uma verdadeira esquizofrenia social, política e institucional. Tem-se aumentado a consciência da importância da proteção de dados no que se refere não só à proteção das vidas privadas dos indivíduos, mas a sua própria liberdade. Esta abordagem reflete-se em inúmeros documentos nacionais e internacionais, principalmente na Carta de Direitos Fundamentais da Comunidade Européia, na qual a proteção de dados é reconhecida como um direito fundamental autônomo. Ainda assim, é cada vez mais difícil respeitar essa presunção geral, uma vez que exigências de segurança interna e internacional, interesses de mercado e a reorganização da administração pública estão levando à diminuição de salvaguardas importantes, ou ao desaparecimento de garantias essenciais. (RODOTÀ, 2007, p. 13,14)

2.3.2 Informação

Para se falar em “proteção de dados pessoais” nesse cenário marcado pela informatização e digitalização de conteúdos, é imprescindível entender o que, de fato, são esses dados que se busca resguardar, pois a depender da definição adotada, poderá haver uma maior ou menor proteção legal. Para tanto, é preciso dar um passo atrás e compreender um conceito igualmente importante e que não se encontra completamente sistematizado pela doutrina: a informação, definida por Norbert Wiener como:

> (...) o termo que designa o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que o nosso ajustamento seja nele percebido. O processo de receber e utilizar informações é o processo do nosso ajuste às contingencias do meio ambiente e do nosso efetivo viver neste ambiente. (WIENER, 1954)

Em primeiro lugar, destaca-se que, para alguns autores, existe uma diferença conceitual entre os termos "dado" e "informação", muitas vezes usados como sinônimos.[50] Nesse sentido, Danilo Doneda (2006) sustenta que, apesar de ambos representarem um fato, um determinado aspecto da realidade, cada um desses termos carrega um peso particular. Para ele, o dado apresenta uma conotação mais primitiva e fragmentada, podendo ser associado a uma espécie de "pré-informação", que antecede a sua interpretação e elaboração. A informação, por sua vez, vai além da representação contida no dado, chegando ao limiar da cognição; seria uma fase inicial de depuração de seu conteúdo. Não obstante essa diferença técnica, para este estudo usaremos "dados pessoais" e "informações pessoais" como termos intercambiáveis, pois é a regra observada na doutrina e nos textos legais.

Como já reiterado, conforme a utilidade da informação foi ganhando relevo, diversos arcabouços sociais passaram a acolhê-la como um de seus elementos fundamentais. Para o direito, por sua vez, essa crescente importância traduz-se no fato de que, atualmente, uma considerável parcela das liberdades individuais é concretamente exercida por meio de estruturas nas quais a comunicação e a informação têm papel relevante, proporcionando meios para que o homem interprete de forma autônoma o mundo que lhe cerca e dele participe de forma ativa.

Ocorre que, no ordenamento brasileiro, a exemplo de muitos outros, o conceito de informação não é tratado de maneira uniforme – ele é frequentemente abordado em torno de cortes específicos, como, por exemplo, a liberdade de informação, o acesso à informação ou a proteção de informações pessoais (DONEDA, 2010). Assim, diante da dissonância existente na doutrina e na legislação, cumpre tecer algumas considerações sobre o tema.

Pierre Catala, um dos pioneiros a abordar essa sistemática dentro do direito, pretendeu criar uma teoria jurídica da informação. Ele parte do pressuposto de que a informação seria um bem suscetível de apropriação e que, salvo exceções, possuiria um valor patrimonial intrínseco.

---

[50] Essa distinção é oriunda principalmente de campos como a ciência da computação, que define o dado como uma sequência de símbolos quantificados ou quantificáveis. Para a informática, o dado é necessariamente uma entidade matemática e, desta forma, é puramente sintático. Nesse sentido, um texto é um dado, já que as letras são símbolos quantificados e finitos, que podem por si só constituir uma base numérica. Segundo essa definição, também são dados fotos, figuras, sons gravados e animação, pois todos podem ser quantificados a ponto de se ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. A informação, por sua vez seria uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa. Portanto, o que é armazenado em um computador não seria a informação, mas a sua representação em forma de dados. Essa representação pode ser transformada pela máquina, como na formatação de um texto, o que seria uma transformação sintática. A máquina não pode mudar o significado a partir deste, já que ele depende de uma pessoa que possui a informação. (SETZER, 1999)

Para ele, a informação não é um dado da natureza; é, na verdade, produto da atividade humana, cujas condições de apropriação estão ligadas àquelas de sua gênese - o nascimento da informação é gerador de um bem. Esse fato sugere uma afirmação em dois ramos: por um lado, a informação é apropriada desde a sua origem, por outro, ela pertence sempre, em princípio, a seu autor, isto é, àquele que a "põe em forma", tornando-a comunicável, e que detém a posse regular de seus elementos (CATALA, 1998).

Para dar forma à sua teoria, Catala classifica a informação em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios; (ii) as opiniões subjetivas das pessoas; (iii) as obras do espírito; e, finalmente, (iv) as informações que, fora das modalidades anteriores, referem-se a descrições de fenômenos, coisas e eventos. Percebe-se, portanto, que a informação se apresenta como um elemento multifacetado, cujas consequências só podem ser reconduzidas a um denominador comum após um certo esforço (DONEDA, 2006).

A fim de resolver esse problema, alguns teóricos buscaram a solução dentro do direito privado, isto é, "o reconhecimento da qualidade de bem jurídico à informação e, a partir disso, a disponibilização dos instrumentos do direito de propriedade para a sistematização do tema."(DONEDA, 2006. p. 164). Assim, parte da doutrina entende que a criação de um mercado para estes bens seria a resposta para os desafios impostos pela produção e transmissão de informações e que, por meio de mecanismos econômicos de caráter liberal, seria possível otimizar as relações de custo e benefício.

Lessig é um dos defensores dessa corrente que pretende atribuir direitos de propriedade aos dados pessoais. Ele baseia seu argumento no celebrado trabalho de Guido Calabresi e A. Douglas Melamed (1972), que apresentam duas grandes regras do sistema legal norte-americano: as regras de propriedade (*property rules*) e as regras de responsabilidade (*liability rules*).

Nessa teoria, um direito protegido por uma regra de propriedade é aquele que precisa ser adquirido em uma transação voluntária, na qual o valor a ser pago é acordado entre as partes. Portanto, se alguém não quer vender o seu carro por menos de R$ 50.000,00, independentemente de este ser o seu valor real, a lei ainda estará do seu lado. Já um direito protegido por uma regra de responsabilidade envolve uma decisão do Estado – no caso do poder judiciário – relativa ao valor da transação, sem que as partes tenham voz nesse processo; é uma medida *ex post.* Assim, o fato de alguém dirigir seu carro na rua cria um risco para os demais, mas não dá ensejo a nenhuma compensação pecuniária. Caso haja uma batida, comprometendo a propriedade de outra pessoa, aí, e somente nesse momento, a atividade do motorista será

analisada para se determinar a indenização devida, que pode ou não refletir o valor conferido pela pessoa que teve seu carro danificado.

Tendo esses conceitos em mente, Lessig defende que conferir aos dados pessoais direitos de propriedade faria com que o consentimento fosse elemento indispensável para a utilização desse conteúdo. Para ele, as pessoas dão valor de forma diferente à privacidade: para alguns, ter seu número de telefone na rede pode ser um problema grave, para outros, isso pode ser irrelevante. Logo, um instrumento legal que proporciona aos indivíduos a liberdade de dispor de seus dados como faria com seus bens, atribuindo a eles um preço que considera justo, seria o ideal.

Esta ampla gama de interesses econômicos relacionados à informação revela-se em várias ocasiões, como é o caso típico do direito de autor. Neste caso, a informação que preenche determinados requisitos – originalidade, exterioridade, caráter artístico, literário ou científico, autoria, etc. – passa a ser, em geral, uma obra de titularidade de seu criador. Estabelece-se assim uma relação proprietária que possibilita a exploração comercial da obra pelo autor - um dos principais escopos do sistema de direito autoral (DONEDA, 2006).

Contudo, essa abordagem econômica e proprietária não nos parece ser a mais adequada para todas as classificações delineadas por Catala, em especial no que diz respeito à primeira delas – as informações relativas às pessoas e seus patrimônios. Segundo o autor, esse tipo de informação pode ser definido como aquela que se refere a uma pessoa determinada ou determinável, apresentando uma ligação concreta com ela. Tais informações são objetivas, uma vez que a sua formulação não é obra voluntária do sujeito em questão, ela depende da lei (nome, estado civil, domicílio) ou ela se relaciona de pleno direito aos atos do indivíduo (aquisições imobiliárias, contas bancárias, condenações passadas). Assim, mesmo que o indivíduo não seja o autor da informação, no sentido de tê-la concebido voluntariamente, ele é o titular legítimo de seus elementos. Sua ligação com a pessoa é demasiado estreita para que fosse diferente. Quando o objeto dos dados é um sujeito de direitos, a informação é um atributo da personalidade (CATALA, 1998).

Percebe-se, portanto, que existe uma diferença intrínseca entre direitos autorais e as informações pessoais: a política econômica que busca uma solução para cada problema. (LESSIG, 2006). Nos direitos autorais, os interesses ameaçados são poderosos e bem organizados; com as informações pessoais o mesmo não ocorre. Neste caso, os interesses em jogo tendem a ser difusos e desordenados, não se limitando aos vetores patrimoniais. Pelo contrário, os dados pessoais são emanações imediatas da própria personalidade humana e

expressão de dois importantes direitos fundamentais: o direito à identidade e o direito à privacidade. Nessa esteira, Laura Schertel postula:

> A informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por revelar aspectos que lhe dizem respeito. Desse modo, resta claro que tais informações merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade. Fundamental é perceber que tal tutela visa à proteção da pessoa e de sua personalidade e não dos dados *perse*. (MENDES, 2016)

Assim, pode-se afirmar que raiz do problema está além da mera categorização dogmática que considera a informação um bem jurídico. A questão é aqui é possibilitar que ela seja abordada pelo ordenamento jurídico de forma hábil a possibilitar a atuação dos interessados em questão e dos valores a serem ponderados (DONEDA, 2010). Assim, as diversas peculiaridades derivadas de fatores como a natureza dessas informações ou a habilidade de movimentar mecanismos para sua exploração econômica tornaram necessário o desenvolvimento de meios de tutela específicos para esse conteúdo, também conhecidos como "proteção de dados".

2.3.2 Proteção de Dados Pessoais

A disciplina da proteção de dados pessoais emerge no âmbito da sociedade em rede como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos oriundos do tratamento de dados a partir da moderna tecnologia da informação. Nesse sentido, Laura Schertel Mendes explica:

> Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Nessa hipótese, tem-se a violação também da autodeterminação e da liberdade do indivíduo, na medida em que ele deixa de ter controle sobre as suas próprias informações, ficando eventualmente sujeito ao poder de organismos privados ou públicos. (MENDES, 2008, p. 41)

Em um julgamento histórico, o Tribunal Constitucional alemão consolidou o direito à autodeterminação informativa como um direito fundamental dos indivíduos de "decidirem por si próprios, quando e dentro de quais limites os seus dados podem ser utilizados" (PANEBIANCO, 2000 apud DONEDA, 2006. p. 196). Na decisão, a Corte defendeu que a partir das nos tecnologias de processamento da informação, os dados podem ser "combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa

atingida possa controlar suficientemente sua exatidão e seu uso." (MARTINS, 2005, p. 237). Assim, conclui-se, nesse novo contexto de processamento de dados eletrônicos, não há que se falar em dados irrelevantes. Todo dado, pode, a partir de tecnologias de processamento, ser utilizado de maneira comprometedora para o indivíduo.

Dessarte, atualmente, o conceito majoritariamente adotado por diversas legislações ao redor do mundo, é de que os dados pessoais representam algum atributo de uma pessoa identificada ou identificável e mantêm uma ligação intrínseca com seu o titular.[51] Note-se que esta definição abarca um conceito amplo e objetivo de dados pessoais, entendido pela possibilidade de vinculação do dado à pessoa, independente dos dados se referirem a aspectos íntimos e privados ou públicos e notórios. Dessa forma, são considerados dados pessoais tanto os dados relativos à comunicação privada, correspondência, endereço e telefone da pessoa, bem como dados referentes a opiniões políticas, opção religiosa, hábitos, gostos e interesses da pessoa (MENDES, 2008).

É importante destacar que, ao se estabelecer um regime de direitos e obrigações no processamento de dados, o objeto da regulação não é o dado como objeto externo ao indivíduo, mas sim o próprio indivíduo em si. Nesse sentido, Norberto Nuno de Andrade (2010) defende que a proteção de dados é eminentemente procedimental, enquanto privacidade e identidade são os direitos substantivos que se visa proteger. Ele explica que, enquanto direitos substantivos são criados a fim de assegurar a proteção e a promoção de interesses que tanto o indivíduo como a sociedade consideram importantes, direitos procedimentais operam em um nível diferente, estabelecendo as regras, métodos e condições por meio das quais esses direitos substantivos serão efetivamente aplicados e protegidos.

Nuno defende que privacidade e identidade representam interesses específicos da personalidade humana e pressupõem a tomada de escolhas normativas. Ademais, esses direitos frequentemente estão em conflito, fato que requer que eles sejam balanceados e medidos entre si. Assim, para o autor, as regulamentações da proteção de dados pessoais e da livre circulação dessas informações, sobretudo a Diretiva Europeia 95/46/CE, são excelentes exemplos desse exercício procedimental. A fim de conciliar o direito à privacidade, por um lado, e o livre fluxo

[51] Essa definição está expressa na Diretiva Europeia 95/46/CE (DPD), legislação referencial no que diz respeito ao tratamento de dados pessoais e à livre circulação dessas informações que preconiza em seu art. 2º que define dados pessoais como "qualquer informação relativa a uma pessoa singular identificado ou identificável". O dispositivo prescreve, ainda, que "é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

de informações no mercado, esses instrumentos normativos fornecem uma gama de orientações e princípios por meio dos quais se podem obter esse tão desejado equilíbrio (ANDRADE, 2010, p. 97).

O desenvolvimento da proteção de dados pessoais como um setor de política pública autônomo, dotado de instrumentos legais e organismos regulatórios próprios demonstra que, além da sua caracterização como direito fundamental, a liberdade, consubstanciada na garantia de controle do indivíduo sobre as próprias informações, é também uma característica generalizada das diversas legislações nacionais e regionais sobre o tema. Nesse sentido, existe um paradigma bastante difundido na doutrina e em diversos ordenamentos jurídicos, segundo o qual, o exercício da liberdade de controle de dados pessoais estaria ancorado no consentimento do titular, permitindo que este determine o nível de proteção dos dados a ele referentes.

Nessa esteira, Stefano Rodotà (2007), um dos principais teóricos sobre o assunto, adota uma postura de transparência com relação aos dados pessoais. Para o autor italiano, a informação constitui, hoje, a nova concentração de poder ou o fortalecimento de poderes já existentes. Assim, diante da influência da tecnologia dos computadores, faz-se mister a consolidação de um verdadeiro direito ao controle e à "autodeterminação informativa". Em razão das modernas formas de coleta e tratamento das informações, a tradicional visão da privacidade enquanto direito de estar só foi mitigada para dar espaço ao direito de o indivíduo poder escolher aquilo que está disposto e revelar aos outros, concedendo ao privado o direito ao contínuo de controle direto, independentemente da existência de violação.

Assim, com o intuito de possibilitar o controle do titular acerca dos seus dados, foram estabelecidos, na maioria das legislações sobre o tema, direitos subjetivos, tais como os direitos de informação, acesso, retificação e cancelamento, cuja função primordial era a de tornar efetivo o exercício dos princípios previstos nas normas. Embora esses direitos configurem significativo empoderamento do indivíduo, o seu estabelecimento nem sempre é suficiente para garantir a adequada proteção de dados na sociedade da informação.

Como destacado no tópico relacionado à privacidade, apenas o consentimento não pode ser a pedra de toque para legislações que versem sobre proteção de dados. Não há dúvidas de que o exercício do direito de controle do indivíduo sobre as suas informações consiste em uma dimensão importante da disciplina de proteção de dados pessoais. Ocorre que a forma de sua implementação é bastante complexa, num contexto, caracterizado pela sociedade de massas, pelo enorme fluxo de informações e pela predominância de grandes burocracias ávidas por

informação, tanto no setor público, como no setor privado. A evolução das gerações de normas de proteção de dados pessoais reflete a tentativa de se buscar, cada vez mais, um modelo que garantisse efetivamente a autodeterminação do indivíduo, não obstante as diversas dificuldades encontradas para tanto (MENDES, 2008).

Conclui-se, portanto, que uma das finalidades principais da proteção de dados é conferir autonomia e controle ao indivíduo sobre a coleta e a utilização de seus dados pessoais, de modo a preservar a sua capacidade de autodeterminação e o livre desenvolvimento da sua personalidade (MENDES, 2008). Como já destacado, a confiança é um elemento essencial nessa relação simbiótica entre os atores da internet. Para tanto, um elemento essencial em qualquer regulação de dados pessoais é a transparência. A fim de que o processamento seja considerado legítimo, o sujeito dessas informações deve estar ciente de que dados relativos a ele estão sendo processados. Assim, o controlador, responsável por esse processo, deve, no mínimo, fornecer informações claras sobre a sua própria identidade e objetivos, além de oferecer esclarecimentos adicionais sempre que for necessário para garantir o justo processamento, considerando as circunstancias especificas em que o dado é coletado, como por exemplo, a identidade dos destinatários dos dados ou a existência de direito ao acesso e à retificação daqueles (SLOOT e BORGESIUS, 2012).

Desta feita, cabe ao Estado, por meio de legislação, prover os mecanismos necessários para que o cidadão possa exercer o controle do fluxo de informações a seu respeito na sociedade, a partir do consentimento, desde que lhe sejam fornecidas informações claras e precisas. Assim, no capítulo seguinte, será avaliado como a privacidade e a proteção de dados são protegidas no Brasil, analisando-se, em especial, o Marco Civil da Internet e o Decreto nº 8.771, de 11 de maio de 2016.

CAPÍTULO 3 – PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: UMA ANÁLISE DO MARCO CIVIL DA INTERNET

Eternal vigilance is the price of liberty.

Wendell Phillips (1811-1884)

No presente capítulo serão analisados os conceitos de privacidade e proteção de dados, no contexto da Lei nº 12.695/14, o Marco Civil da Internet, que estabelece princípios, garantias,

direitos e deveres para o uso da internet no Brasil. A legislação em comento foi um divisor de águas no que concerne à regulação da internet em âmbito nacional, sobretudo ao que diz respeito à guarda de registros, privacidade dos dados e o conteúdo disponibilizado na Internet. Entretanto, a depeito de todos os aspectos positivos, a lei ainda apresenta alguns pontos de nebulosidade e incompreensão.

Dessa forma, pretende-se analisar o referido instrumento normativo sob dois principais pontos: o da proteção de dados pessoais e registro de conexões e o do sigilo e inviolabilidade das comunicações, sendo que a respeito desse último, será dado especial destaque às recentes decisões que suspenderam o aplicativo de mensagens WhatsApp em todo o território brasileiro, buscando entender os argumentos empregados pelos juízos que determinaram o bloqueio e os argumentos utilizados para rebater esse entendimento.

Por fim, será analisado o Decreto nº 8.771/16, editado para regulamentar o Marco Civil da Internet, a fim de identificar as complementações positivas que foram trazidas ao arcabouço jurídico das relações digitais e os pontos que ainda se apresentam como lacunas e inseguranças jurídicas.

3.1 O MARCO CIVIL DA INTERNET

Muito antes de se pensar em uma legislação específica para a realidade digital contemporânea, os tribunais brasileiros já eram confrontados com o admirável mundo novo da informatização, sendo instados a oferecerem respostas efetivas a situações controvertidas e ainda não reguladas por lei codificada. Naturalmente, os percalços foram variados. Muitos juízes não compreendiam a natureza e as condicionantes dos litígios por absoluto desconhecimento; outros, por falta de sensibilidade às demandas humanas e tecnológicas, adotavam orientações absolutamente desconectadas da realidade contextual em consideração (POLIDO, 2016). Assim, diante de demandas cada vez mais complexas e frequentes, em um cenário de total insegurança jurídica, surgiu a necessidade de se criar um instrumento normativo que oferecesse uma base legal ao Poder Judiciário para melhor responder as questões envolvendo internet e tecnologia da informação (JESUS e MILAGRE, 2014).

Em 2014, após intensa participação social e debate público no processo legislativo, foi editada a Lei nº 12.695/14, mais conhecida como Marco Civil da Internet, que buscou capturar a nova realidade informacional e adequar os institutos jurídicos para melhor responder as demandas sociais nesse contexto. Trata-se da primeira lei criada de forma colaborativa entre sociedade e governo, com a utilização da internet como plataforma de debate – o que não

poderia ser diferente. Como a internet é uma tecnologia essencialmente generativa, nada mais natural que trazer os envolvidos, enquanto criadores e consumidores de conteúdo na rede para o espaço de deliberação legislativa. Como já destacado na teoria dos sistemas sociais e mais tarde incorporado por Murray em sua teoria sobre a regulação do ciberespaço, a comunicação é pressuposto das sociedades e o indivíduo possui papel ativo na regulação do comportamento.

Cumpre ressaltar que o Marco Civil - cuja estrutura está pautada em três pilares: neutralidade, privacidade e liberdade de expressão - não tem a pretensão de ser uma ilha normativa isolada das demais fontes jurídicas. Ele é um dos vários pontos de irradiação que disciplina o comportamento dos indivíduos no mundo virtual. Nesse sentido, a Constituição Federal, como lei fundamental do país, dá as coordenadas principiológicas incontestes do ordenamento jurídico, ao fluxo da qual tramitarão as interpretações que transbordarão do Marco Civil da Internet. Não bastasse, os demais diplomas, como o Código do Consumidor, o Código Civil e outros mais, serão igualmente estimados na regulação dos fatos jurídicos cibernéticos, conforme convite expresso do parágrafo único do art. 3º e o art. 6º da nova lei (OLIVEIRA, 2014).

Como já destacado, o Marco Civil não antecede todos os litígios envolvendo internet e tecnologia existentes no Brasil. Já existem, inclusive, entendimentos solidificados em primeira instância e em Tribunais Superiores sobre tais demandas. Nesse sentido, vale ressaltar o importante papel do Superior Tribunal de Justiça na busca de consensos e orientações sobre temas interseccionando internet, direito público e direito privado, o que proporcionou fundamento para a que discussão técnico-legal sobre as bases legislativas do Marco Civil fosse mais aprofundada. Não por outra razão, esses entendimentos também deverão ser levados em conta na apreciação das demandas sob a égide da lei.

No contexto do Marco Civil, o acesso à internet é mediado por liberdades civis e políticas, bem como garantias individuais, como a liberdade de expressão[52] e a privacidade. Assim, por ter um caráter principiológico, a intenção do instrumento normativo em questão é se manter eficaz, mesmo diante de novas revoluções digitais ou inovações tecnológicas, vez

[52] O legislador fez questão de elencar o fundamento principal no caput do artigo 2º da Lei, qual seja a "liberdade de expressão". Nesse sentido, observe-se: "Tudo que atente a tal direito será uma violação ao Marco Civil Brasileiro. A liberdade de expressão prevalecerá sempre, desde que não viole direitos de terceiros. Pelo texto elimina-se a censura na rede ou remoção de conteúdos da internet com base em mero "dissabor" por parte daqueles que não concordam. Importante destacar que tal garantia era inexistente no Direito brasileiro. Antes do Marco Civil, diante de denúncias "online", muitos conteúdos eram removidos extrajudicialmente, por provedores que se sentiam "inseguros" em mantê-los." (JESUS e MILAGRE, 2014, p. 19)

que está alicerçada em uma base sólida valores indissociáveis do Estado Democrático de Direito. Ademais, a presença desses direitos de ordem constitucional, já indica o compromisso do legislador com os distintos interesses em jogo: de um lado, indivíduos usuários das redes, e, de outro, governos e empresas.

Cumpre destacar, também, que o próprio advento da internet como exemplo representativo do desenvolvimento de ferramentas de comunicações e informação no século XX foi primordial para "o amadurecimento de instituições democráticas, surgimento de estruturas e redes colaborativas, para a governança social, para a construção de entendimentos técnicos nas áreas de políticas públicas, advocacia, governamental, judicial e legislativa." (POLIDO, 2016). Essa maturidade pode ser percebida na inteligência do artigo 4º da Lei[53], que captura a importância da acessibilidade da informação e do conhecimento - há tempos advogada pelo Conselho de Direitos Humanos[54] - e a vincula a um sistema de freios e contrapesos, promovendo um equilíbrio entre direitos e deveres de usuários e provedores.

[53] Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
I - do direito de acesso à internet a todos;
II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

[54] Em junho de 2016, O Conselho de Direitos Humanos das Nações Unidas divulgou resolução que prevê os mesmos direitos que os cidadãos têm offline precisam ser protegidos no ambiente online, dentre eles o acesso à informação:
(...)
1. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;
2. Recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms, including in achieving the Sustainable Development Goals;
3. Calls upon all states to promote and facilitate international cooperation aimed at the development of media and information and communication facilities and technologies in all countries;
4. Affirms that quality education plays a decisive role in development, and therefore calls upon all States to promote digital literacy and to facilitate access to information on the Internet, which can be an important tool in facilitating the promotion of the right to education;
5. Affirms also the importance of applying a human rights-based approach in providing and in expanding access to Internet and requests all States to make efforts to bridge the many forms of digital divides;
6. Calls upon all States to bridge the gender digital divide and enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of all women and girls;
7. Encourages all States to take appropriate measures to promote, with the participation of persons with disabilities, the design, development, production and distribution of information and communications technologies and systems, including assistive and adaptive technologies, that are accessible to persons with disabilities; (HUMAN RIGHTS COUNCIL, 2016)

Diante do turbilhão criativo e inovador proporcionado pelas novas tecnologias de informação e comunicação, é importante que legisladores e tribunais entendam a lógica disruptiva da internet de forma que, ao invés de tentar acompanhar cada mudança tecnológica, alcancem uma consistência interpretativa sobre os consensos já estabelecidos no Direto de Internet. Não seria possível a Lei, a partir de uma racionalidade codificadora, típica de sistemas jurídicos de tradição romano-germânica, pretender a totalidade da regulação dos aspectos das mudanças tecnológicas. Nesse sentido, aplicativos de compartilhamento, produtos e serviços ligados à conectividade entre objetos e pessoas, como, por exemplo, a "internet das coisas" e a inteligência artificial são apenas alguns dos exemplos que desafiam as racionalidades codificadoras e judicantes tradicionais.

É importante destacar que muitos dos conflitos existentes, mais do que questões regulatórias e jurídicas, são, na verdade, produto das variadas percepções sobre as funções da internet. Nesse sentido, Fabrício Bertini Pasquot Polido, fundador e presidente do Instituto de Referência em Internet e Sociedade da Universidade Federal de Minas Gerais, elenca essas diferentes perspectivas dentro da sociedade:

> Para empresas, ela representa segmento lucrativo para fins de exercício da atividade empresarial e da exploração comercial de ativos tangíveis e intangíveis; para governos, como setor potencial de prestação de serviços de utilidade pública, de comunicação com os cidadãos, repertório de informações; para indivíduos, ela materializa verdadeiro ambiente de interação social, de compartilhamento, de participação, autonomia, empoderamento e concretização de liberdades civis e políticas. Para a academia, ela oferece plataforma para produção e disseminação do conhecimento, desafiando premissas, estruturas e condutas específicas na formulação do saber e no exercício da crítica e transformação social, proporcionados pelos ambientes universitários e de pesquisa. (POLIDO, 2016)

Como destacado no capítulo anterior, muitas empresas incorporaram em seus modelos de negócios uma economia baseada na informação. Assim, são os usuários e clientes as principais fontes de capital – social ou informacional - a partir do qual empresas como Facebook, WhatsApp, Google, LinkedIn e outras desenvolvem novos produtos e serviços comercializáveis em larga escala. Diante disso, não restam dúvidas de que para essas empresas que exploram economicamente serviços de comunicação, relacionamento social e aplicações bem como para a sociedade civil, o interesse mais evidente a ser defendido é aquele de um "irrestrito ambiente de liberdade de expressão e de privacidade", mantendo a natureza sistêmica e global da internet como um espaço de construção da circulação de opiniões, ideias, do conhecimento e de participação.

Por essa razão, o ponto chave da legislação reside, justamente, na forma como a equilibra direitos e obrigações em relação à responsabilização de provedores por conteúdo postado, armazenado ou divulgado por terceiros, dentro de um espaço de maior liberdade de circulação das informações e como fez em relação às limitações legais à divulgação de dados pessoais por provedores de acesso, conteúdo e aplicações, salvo em hipóteses muito específicas, consagrando a privacidade não apenas como princípio e direito subjetivo, mas antes como "objetivo sistêmico" a ser alcançado no quadro normativo estabelecido.

Percebe-se, assim, que os modelos brasileiros podem ser mais estratégicos e criativos, construindo experiências legais a partir da enorme contribuição dada pela razão e intelecto humanos, em confronto com as transformações científicas, da engenharia e da dinâmica de novas formas de interação social (POLIDO, 2016). Logo, pode-se dizer que o Marco Civil, é um desses modelos estratégicos e criativos: ele simboliza vanguarda em relação a outras experiências legislativas na área da internet, sempre voltadas para sancionar, criminalizar ou privatizar. Entretanto, como todo instrumento normativo codificado que pretende regular um ambiente marcado por tamanha generatividade, o Marco Civil apresenta algumas incongruências e lacunas que ainda estão por ser solucionadas, consoante será demonstrado mais adiante.

3.2 PRIVACIDADE E PROTEÇÃO DE DADOS NO MARCO CIVIL DA INTERNET

Como destacado ao longo do segundo capítulo, a privacidade e a proteção de dados pessoais na rede passaram a ser duas das maiores preocupações para a sociedade no cenário atual. Diante dos riscos trazidos pela digitalização das informações, esses direitos foram consagrados como fundamentais aos seres humanos e, agora, encontram guarida em diversas legislações mundiais. Da mesma forma, o Brasil passa por um intenso processo de informatização, com o número de usuários da rede mundial de computadores crescendo a cada dia[55]. Dessarte, privacidade e proteção de dados não poderiam ser deixadas de lado no contexto

[55] Em 2014, foi realizada a 10ª edição da pesquisa TIC Domicílios que apontou: "No Brasil, 47% dos brasileiros com 10 anos ou mais usaram Internet pelo aparelho – o que representa, em números absolutos, 81,5 milhões de pessoas. O percentual de brasileiros com 10 anos ou mais que acessou a rede por meio do celular mais do que triplicou nos últimos três anos: em 2011, essa proporção era de 15%, chegando a 47% em 2014. Apesar do rápido crescimento do uso da Internet pelo celular em todas as classes sociais, a TIC Domicílios 2014 também aponta a persistência da desigualdade no acesso à Internet no país, tendo em vista os patamares mais reduzidos verificados nas áreas rurais e nas regiões Norte e Nordeste. A pesquisa investigou, pela primeira vez, os dispositivos utilizados pelos indivíduos para acessar a Internet, constatando a preferência pelo telefone celular (76%) – foi mais citado do que o computador de mesa (54%), notebook (46%) e tablet (22%). Além disso, 84% dos usuários de Internet pelo celular afirmaram acessá-la todos os dias ou quase todos os dias. A pesquisa aponta também para uma

digital pátrio, tendo sido, finalmente, incorporadas no ordenamento jurídico brasileiro como princípios previstos nos art. 3º e 2º da Lei nº 12.695/14, respectivamente.

Como bem estabelecido no caput do art.7º, o acesso à internet é condição essencial para o exercício da cidadania e, como tal, demanda uma série de iniciativas do Poder Público e até mesmo de instituições privadas com esta pauta, de nítida responsabilidade social. Por essa razão, o legislador elencou nos artigos 7º e 8º uma série de direitos e garantias ao usuário na rede:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> **I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;**
>
> **II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;**
>
> **III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;**
>
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
>
> V - manutenção da qualidade contratada da conexão à internet;
>
> **VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;**
>
> **VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;**
>
> **VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:**
>
> **a) justifiquem sua coleta;**
>
> **b) não sejam vedadas pela legislação; e**

---

estabilidade na proporção de domicílios que possuem computador (50%). Já a presença de equipamentos portáteis (laptops e notebooks) apresentou crescimento: 60% das residências com computador possuem notebooks, enquanto os tablets estão presentes em 33% dos domicílios. Pela primeira vez também, a pesquisa mediu a disponibilidade de redes sem fio WiFi nos domicílios e constatou que 66% das moradias com acesso à Internet dispõem desse tipo de rede. Esses dados revelam um cenário de múltiplos dispositivos tecnológicos convivendo no dia a dia do cidadão, o que indica uma tendência à portabilidade e à mobilidade. Essa combinação traz implicações para as atividades e para a frequência de uso da Internet pelo cidadão e, possivelmente, contribui para que os dispositivos sejam cada vez mais utilizados de forma individual. A proporção de domicílios com acesso à Internet em 2014 é de 50%, o que corresponde a 32,3 milhões de domicílios em números absolutos. As desigualdades por classe social e área persistem: na classe A, a proporção de domicílios com acesso à Internet é de 98%; na classe B, 82%; na classe C, 48%; e entre a classe DE, 14%. Nas áreas urbanas, a proporção de domicílios com acesso à Internet é de 54%, enquanto nas áreas rurais é de 22%. Quanto às atividades realizadas pelos indivíduos na Internet, a pesquisa TIC Domicílios 2014 mostra que o percentual de brasileiros de 10 anos ou mais que utilizam a Internet chegou a 55%, o que corresponde a 94,2 milhões de indivíduos. A atividade mais realizada pelos usuários de Internet nos três meses anteriores à pesquisa é o envio de mensagens instantâneas, a exemplo de chat do Facebook, chat do Skype ou WhatsApp (83% dos usuários de Internet). A TIC Domicílios 2014 também aponta que a participação em redes sociais figura entre as ações mais citadas, com 76%." (COMITÊ GESTOR DA INTERNET NO BRASIL, 2015, p. 28)

> **c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;**
>
> **IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;**
>
> **X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;**
>
> **XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;**
>
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
>
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.
>
> Art. 8º **A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.**
>
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:
>
> **I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou**
>
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (grifamos.)

Do destacado acima, percebe-se que especial atenção foi dada ao direito à privacidade, entendido aqui, sob o ponto de vista do direito civil, como o direito de isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa. Embora a proteção à intimidade e à vida privada esteja prevista na Constituição Federal, em seu art. 5º, X, o Marco Civil é a primeira lei infraconstitucional a regulamentar o tema. Nesse ponto, inova o legislador, particularmente por extravasar a própria previsão constitucional nesse domínio, como seria a inadequada comparação entre a "intimidade" do rol dos direitos da personalidade e a privacidade. (POLIDO, 2016)

3.2.1 Proteção de dados – consentimento e transparência

Além de proteger a privacidade em termos gerais, o Marco Civil, em atitude vanguardista na realidade jurídica brasileira, faz referência à proteção dos dados pessoais, *i.e*, as informações biográficas ou comportamentais que podem identificar uma pessoa na rede. Todavia, conquanto a nova legislação aborde a referida temática, não o faz de maneira detalhada e deixa a tarefa a cargo de ulterior lei específica. Nessa esteira, destaca-se que a proteção aos dados pessoais foi regulamentada pelo Decreto nº 8.771/16, que será analisado mais adiante e,

ainda é objeto do Projeto de Lei nº 5.276 de 2016[56], enviado ao Congresso recentemente pelo Poder Executivo, que pretende ser uma nova lei de Proteção de Dados Pessoais no Brasil.

Apesar de não ser uma legislação específica sobre proteção de dados pessoais, o Marco Civil da Internet não poderia ficar alheio a esse tópico, vez que grande parte da utilização da web envolve o uso dessas informações. Assim, o legislador se preocupou em garantir o direito à autodeterminação informativa, consubstanciada no controle das informações pessoais na internet e na autonomia sobre o seu tratamento.

De acordo com o disciplinado no art. 7º, IX, do Marco Civil da Internet, o consentimento livre, expresso e informado é a pedra de toque da utilização dos dados pessoais – incluindo aí registros de conexão e histórico de navegação – e pode ser revogado a qualquer momento pelo próprio usuário. Nesse sentido, os provedores de aplicação[57] devem facultar ao internauta, de modo claro, compreensível e sem emboscadas, o direito de consentir ou não com a transferência de seus dados a terceiros. Deverão, ainda, disponibilizar ao usuário o acesso a canal de comunicação que lhe permita, com facilidade, a revogação do consentimento externado anteriormente.

Infere-se, portanto, que o sistema adotado pelo nosso ordenamento jurídico é o denominado *opt-in*. Neste modelo, o usuário deve consentir de forma expressa e inequívoca, quanto ao tratamento dos seus dados pessoais. Por outro lado, o sistema *opt-out*, que não foi incorporado em nosso sistema, prevê que o usuário deve manifestar de forma expressa o seu interesse em sair, isto porque, o pressuposto é de concordância automática (CELLA e FREITAS, 2016)

Como já suficientemente destacado, a privacidade está assegurada pela Constituição Federal e consiste em um direito irrenunciável, mas cuja a mitigação é possível nos casos autorizados em Lei (artigo 11 do Código Civil[58]). Nesta linha de raciocínio, o sistema *opt-in* adotado pelo Marco Civil da Internet permite que o consumidor licitamente renuncie ao seu direito de privacidade, sendo vedado o consentimento presumido. Por esta razão, para considerar válido o consentimento do usuário é imprescindível que: (i) a informação sobre a

[56] "PL 5276/2016: Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural."

[57] Conforme preleciona o art. 5º, inciso VI c.c/ art. 15 do MCI, os provedores de aplicação têm como atividade principal o fornecimento de serviços de aplicações, ou seja, é aquela que fornece aplicativos por meio da internet (aplicações estas de cujo conceito pode ser expandido a softwares e sistemas web entre outros, a teor da concepção legal acerca deste em seu art. 1º da lei 9.609, de 19 de fevereiro de 1998 – Lei de software).

[58] Art. 11. Com exceção dos casos previstos em lei, os direitos de personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofre limitação voluntária.

coleta dos seus dados ocorra de forma adequada e clara, a permitir a sua inequívoca compreensão; (ii) consentimento prévio e expresso do usuário; (iii) nula de pleno direito a coleta realizada sem a observância dos itens “i” e “ii”.

Ademais, pode-se afirmar que o art. 8º do Marco Civil dialoga com o Código de Defesa do Consumidor, ao considerar nulas de pleno direito todas as cláusulas contratuais que impliquem ofensa ao sigilo das comunicações privadas. Nesse sentido, será possível ler e interpretar os termos de uso e as políticas de privacidade dos sites da mesma forma como os contratos de adesão nas relações de consumo. Isso significa dizer que cláusulas que impliquem danos ao consumidor e à sua privacidade serão eivadas de nulidade.

Por fim, outro direito que nasce para o usuário de internet do Brasil é o direito de exclusão (art. 7º, X). Ao deixar um serviço na internet, não se sabia ao certo o que era feito com os dados fornecidos. Em muitos casos, embora excluídas as contas, os dados permaneciam disponíveis ou armazenados no servidor do provedor do serviço. Agora, com o Marco Civil, o usuário poderá requerer a exclusão definitiva de seus dados pessoais fornecidos a uma aplicação de internet, e o provedor deverá atender, ressalvados, logicamente, os dados que deva guardar por disposição legal (OLIVEIRA, 2014).

Dessa feita, um problema que entrou no escopo da lei em comento foi o uso de *cookies* de internet. Como já destacado no capítulo anterior, muitas vezes informações sobre o usuário são coletadas por meio de arquivos de texto não executáveis capazes de enviar para o servidor onde está registrado o domínio do site informações sobre o comportamento de quem visita a página. Essa prática de monitoração online gera constante discussão, especialmente quando se toca no tema da privacidade e no uso indiscriminado desses dados.

Em tese, a Lei n. 12.965/2014 revela-se como avanço, fixando um marco histórico e jurídico de utilização da web no Brasil. A exemplo da Diretiva nº 95/46, o Marco Civil disciplina o uso dos cookies, determinando que o provedor de aplicações informe, de maneira destacada, ao usuário que seus dados serão coletados e a forma como eles serão utilizados tanto por empresas privadas como por órgãos do governo, além de exigir o consentimento expresso para tanto. No entanto, verifica-se que, mesmo com o advento desta lei, não se conseguiu resolver o problema da proteção dos dados pessoais, uma vez que muito sites brasileiros ainda não seguem essa lógica de esclarecimentos, publicidade e transparência.

Nesse sentido, como muito debatido no capítulo anterior, pautar a utilização de dados pessoais exclusivamente em uma escolha do consumidor pode não ser a melhor alternativa.

Existe uma fragilidade intrínseca na determinação de obrigatoriedade de consentimento expresso e inequívoco para coleta, uso, armazenamento, tratamento e proteção de dados pessoais que, apesar de manifestada no Marco Civil, ainda não assegura a efetiva proteção dos dados pessoais

Para comprovar essa afirmação, destaca-se recente pesquisa realizada pelo InternetLab[59] , cujos resultados não foram muito animadores. Em 2016 a instituição realizou a primeira edição da versão brasileira do "Quem defende seus dados?", baseado no projeto *Who has your back?*, realizado nos Estados Unidos desde 2011 pela Electronic Frontier Foundation – EFF. A pesquisa visa promover a transparência e a adoção de boas práticas em matéria de privacidade e proteção de dados pelas empresas provedoras de acesso à Internet no Brasil, conscientizando usuários de Internet sobre práticas que afetam a proteção de sua privacidade e dados pessoais.

As empresas objeto do estudo foram escolhidas a partir de dados divulgados pela Agência Nacional de Telecomunicações (ANATEL) em outubro de 2015, contanto que possuíssem ao menos 10% do total de acessos à Internet – seja pela infraestrutura de banda larga fixa, seja pela infraestrutura de telefonia móvel. Esse corte garantiu que fossem avaliadas as empresas responsáveis por cerca de 90% dos acessos em ambas as ocasiões. No caso da banda larga fixa, as seguintes empresas se enquadraram nesse recorte: NET, Oi, Vivo e GVT. Em Internet móvel, enquadraram-se Claro, Oi, TIM e Vivo.

Considerando a realidade jurídica e social brasileira, foram elaboradas seis categorias: (i) informações sobre tratamento de dados[60]; (ii) informações sobre condições de entrega de dados a agentes do estado; (iii) defesa da privacidade dos usuários no judiciário; (iv) posicionamento público pró-privacidade; (v) relatório de transparência sobre pedidos de dados; (vi) notificação do usuário, com base em três perspectivas principais: comprometimento público com obediência à lei; adoção de práticas e posturas pró-usuário; e transparência sobre as práticas e políticas.

Para a aplicação da metodologia, foram consultados contratos-modelo disponíveis em websites, salas de imprensa e outras manifestações públicas oficiais por escrito das empresas

[59] O InternetLab é um centro independente de pesquisa interdisciplinar que promove o debate acadêmico e a produção de conhecimento nas áreas de direito e tecnologia, sobretudo no campo da Internet. É uma entidade sem fins lucrativos e atua como ponto de articulação entre acadêmicos e representantes dos setores público, privado e da sociedade civil. (INTERNETLAB, 2016)

[60] O termo "dados" foi utilizado na pesquisa em sentido amplo. Engloba tanto os dados cadastrais, que fornecemos para que o serviço seja prestado (nome, endereço, CPF etc), como os registros de cada conexão à Internet.

avaliadas. Em termos de uso ou em páginas chamadas “Política de Privacidade” não foram encontradas informações relevantes, pois se referem à utilização do próprio website das empresas. Os resultados podem ser observados na tabela abaixo[61]:

Como se percebe, apesar de existir a determinação legal de transparência e notificação ao usuário, as empresas ainda não estão inclinadas a atender essas demandas, deixando o usuário completamente vulnerável. Como destacado no capítulo anterior o mercado da tecnologia tem aspectos parecidos com um “mercado de limões”: independentemente de se tratar de um software de segurança ou da própria segurança de um software com outras finalidades, a maioria dos usuários não consegue distinguir o nível de proteção que é oferecido. Assim, os desenvolvedores não são recompensados pelo esforço de fortalecer o seu código, ficando sem o incentivo necessário para competir entre si no quesito privacidade.

Dessarte, a crença indiscriminada de que regulamentações governamentais podem solucionar o "problema da informação" muitas vezes se mostra equivocada. Inclusive, não é raro que o próprio governo crie tal problema. Um exemplo dessa afirmação aconteceu há alguns anos, em Washington, D.C, quando a câmara municipal promulgou uma lei que proibia os planos de

[61] Imagem extraída do relatório elaborado pelo InternetLab, disponível em http://quemdefendeseusdados.org.br/pt/, acessado em 02 de novembro de 2016.

saúde de discriminar potenciais clientes com base em doenças já adquiridas. Isto é, se um indivíduo já doente quisesse fazer um seguro-saúde para ter menos gastos, ele não poderia ser rejeitado. Com efeito, pela lei, as seguradoras nem sequer poderiam fazer perguntas às pessoas sobre questões relativas à saúde. Algum tempo depois, os vereadores se surpreenderam com as ameaças dos planos de saúde de não mais emitir apólices para absolutamente *nenhum* habitante da cidade (ANDERSON, 2013).

Entretanto, a solução do problema está tampouco na substituição ou erradicação da lei. Pelo contrário, a ação do governo é, de fato, um instrumento positivo que pode operar efetivamente a favor do usuário e mostra-se indispensável nos dias atuais. Ocorre que, diante desse cenário, tornou-se imprescindível entender a lei não como um instrumento de fabricar consentimentos meramente formais, mas sim como um sistema substantivo de regulamentar o processamento de dados pessoais a favor dos interesses de todos. É exatamente por meio da confiança, explorada no segundo capítulo, que se pode proporcionar esse caráter rejuvenescedor à legislação, permitindo com que sejam pensadas regulações positivas, substantivas e inspiradoras, ao invés de pessimistas e procedimentais.

Não é de hoje que as relações de informação possuem papel de destaque na vida em sociedade. As relações tradicionais com médicos, advogados e comerciantes já reconheciam o valor das regras de informação e como estas podiam produzir a confiança necessária para estabelecer relacionamentos sólidos no seio da coletividade como um todo. À medida que embarcamos na criação de novas relações de informação envolvendo novos atores e novas plataformas, é essencial garantir que os elementos essenciais de confiança social sejam incorporados a eles, para que os novos relacionamentos possam ser tão sustentáveis quanto os mais antigos. A confiança é necessária para um futuro digital sustentável, e as regras de privacidade que promovem a confiança podem criar valor individual e social. Assim, quando vista a partir de uma lente da confiança, a confidencialidade, transparência e segurança, transformam-se em honestidade, lealdade e proteção.

3.2.2 Sigilo e inviolabilidade das comunicações

Em consonância com o já previsto na Constituição Federal (art. 5º, XII), as comunicações digitais são igualmente invioláveis e sigilosas, só podendo ser reveladas por ordem judicial. Nesse sentido, a Seção II do Capítulo III do Marco Civil da Internet trata da

proteção aos registros, dados pessoais e às comunicações privadas, preconizando, no art. 10, que

> A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Nos parágrafos do referido artigo, o legislador diferencia as possibilidades que permitem o acesso de autoridades estatais a registros de conexão e a dados cadastrais. Os primeiros, que dizem respeito ao " conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (Lei 12.965/14, art. 4º, VI) somente poderão ser disponibilizados se a entrega for autorizada por ordem judicial (art. 10, §1º). Já os segundos, que se referem à qualificação pessoal, filiação e endereço, podem ser disponibilizados diretamente para autoridades administrativas, sem necessidade de ordem judicial, se e quando possuírem competência legal para a requisição (art. 10, § 3º). Assim, cumpre destacar que, atualmente, autoridades policiais e do Ministério Público possuem legitimidade para requisição de dados cadastrais no âmbito de aplicação da Lei das Organizações Criminosas e da Lei dos Crimes de Lavagem de Dinheiro. Nos demais casos, a ordem judicial ainda é necessária para entrega dos dados.

Embora exista o dever de custódia dos registros de conexão e acesso a aplicações, deve-se destacar que a guarda e o fornecimento desses dados precisam se dar da forma menos invasiva possível ao usuário, respeitando-se, sempre que possível, a sua privacidade.

O artigo 13 do Marco Civil, por sua vez, estipulou que cabe ao prestador de serviço de conexão[62] o dever de manter os registros de conexão dos usuários, sob sigilo, pelo prazo de um ano. Já o artigo 15 da mesma lei dispõe que, para os provedores de aplicações de internet constituídos na forma de pessoa jurídica, que exerçam suas respectivas atividades de forma organizada, existe o dever de manter os registros de acesso às aplicações pelo prazo de 6 meses. Conforme o parágrafo 1° do artigo 10, em ambos os casos, pode haver decisão judicial que obrigue a disponibilização desses registros. Contudo, vale salientar, que a determinação prevista

[62] Conforme predispõe o art. 5º, inciso VI c.c/ art. 13 do MCI, o prestador de serviço de conexão tem como atividade principal o fornecimento de serviços de conexão com a internet, ou seja, é aquela que libera o acesso de conexão ao usuário da rede.

na lei se refere a dados como data, hora e IP do dispositivo que fez o acesso à internet, isto é, informações mínimas para saber que uma máquina se comunicou com outra em um determinado horário.

Chama atenção, contudo, o fato de inexistir tal previsão em relação às comunicações privadas, isto é, o Marco Civil não impõe prazo para que os provedores de aplicações de internet mantenham em sua posse as mensagens trocadas por seus usuários. Assim, o entendimento que mais se coaduna com os princípios previstos na lei é no sentido de que não existe obrigatoriedade para a guarda dessas informações. Em consonância com o princípio da legalidade, se a lei não prevê o dever de coletar e armazenar as comunicações, os provedores não são obrigados a tal. Por conseguinte, também não podem ser compelidos a fornecer o que não possuem ou não custodiam. Não obstante inexista disposição no Marco Civil determinando o armazenamento do conteúdo das comunicações, é possível concluir que ordem judicial poderá obrigar os provedores a assim fazerem, em relação a um usuário específico, mas somente a partir de sua intimação (JESUS e MILAGRE, 2014).

Ao prever que o conteúdo das comunicações privadas somente pode ser disponibilizado mediante ordem judicial, o legislador visa proteger a privacidade e intimidade do usuário, bem como o interesse coletivo. Por isso, no art. 12, estão previstas sanções às empresas que não promovem o adequado gerenciamento, tratamento e manipulação dos dados do usuário, violando o disposto nos art. 10 e 11. Dentre essas penalidades, estão: advertência, com indicação de prazo para adoção de medidas corretivas; multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício; suspensão temporária das atividades; ou proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Nesse sentido, uma questão que vem chamando a atenção das comunidades acadêmica e jurídica brasileiras são as diversas decisões judiciais proferidas ao longo dos dois últimos anos que, com fundamento no art. 12, determinaram a suspensão, por todo o território nacional, do aplicativos de mensagens WhatsApp, que agora é de propriedade da Facebook Inc., em decorrência do descumprimento de ordens judiciais que exigiam a apresentação de determinadas informações.

Cumpre destacar que antes da entrada em vigor do Marco Civil, duas decisões judiciais já haviam suspendido de forma irrestrita, por todo o Brasil, o funcionamento de dois sites: o Youtube, em janeiro de 2007, em decorrência do processo movido pela atriz Daniella

Cicarelli[63], e o Facebook, em agosto de 2012, em virtude da ação ajuizada por Dalmo Deusdedit Meneses[64]. Em ambos os casos, a suspensão dos serviços decorreu da negativa de cumprimento de ordens judiciais de retirada de conteúdo por parte das empresas. No entanto, o fundamento de cada uma delas foi distinto: no primeiro caso se utilizou o art. 461, §1º, do CPC/1973[65] (atual art. 536, §1º do NCPC) para realizar a suspensão; no segundo, a fundamentação da decisão envolveu o art. 57-I da Lei das Eleições (Lei n. 9.504/97)[66] (IBIDEM; LAPIN, 2016).

Após a entrada em vigor do Marco Civil da Internet, em um curto intervalo de tempo, quatro decisões determinaram a suspensão do aplicativo de comunicação instantânea Whatsapp: a primeira foi determinada pela Central de Inquérito da Comarca de Teresina-PI, no processo 0013872-87.2014.8.18.014028; a segunda, proferida pelo juízo da 1ª Vara Criminal de São Bernardo do Campo-SP, no procedimento de Interceptação Telefônica 0017520-08.2015.8.26.056429; a terceira, no processo de nº 201555000783, proveio do juízo da Vara Criminal da Comarca de Lagarto-SE30 e a quarta, proferida pelo juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ, nos autos do IP 062-00164/2016 (IBIDEM; LAPIN, 2016). Será analisada esta última, pelo fato de ter sido a única publicizada em razão do relevante interesse nacional acerca do tema.

Nos autos do IP 062-00164/2016, a MM. Juíza proferiu decisão requerendo que o WhatsApp apresentasse uma solução tecnológica que permitisse o acesso das autoridades às mensagens em tempo real e determinou a suspensão do serviço do aplicativo em todas as operadoras de telefonia, até que a ordem judicial fosse efetivamente cumprida:

> Esta magistrada, no bojo dos autos da investigação criminal em epígrafe, determinou o cumprimento da quebra do sigilo e interceptação telemática das mensagens compartilhadas no aplicativo *Whatsapp* em relação aos terminais-alvos indicados no ofício encaminhado pela d. autoridade policial ao *Facebook* do Brasil, sob pena de aplicação de multa coercitiva diária no valor de R$50.000,00, além de eventual configuração de crime de obstrução à Justiça e suspensão dos serviços até cumprimento da ordem judicial.
>
> (...)
>
> Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma

[63] TJSP, Agravo de Instrumento n. 0113488-16.2012.8.26.0000, Rel. Des. Enio Zuliani, https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=6258764&cdForo=0&vlCaptcha=pwvaz

[64] TRE-SC, Ação Cautelar n. 86-37.2012.6.24.0013, http://www.tresc.jus.br/site/fileadmin/arquivos/noticias/2012/08/decisao_26_de_julho.pdf

[65] CPC/1973, Art. 461. Na ação que tenha por objeto o cumprimento de obrigação de fazer ou não fazer, o juiz concederá a tutela específica da obrigação ou, se procedente o pedido, determinará providências que assegurem o resultado prático equivalente ao do adimplemento

[66] 27 Lei 9.504/97, Art. 57-I. A requerimento de candidato, partido ou coligação, observado o rito previsto no art. 96, a Justiça Eleitoral poderá determinar a suspensão, por vinte e quatro horas, do acesso a todo conteúdo informativo dos sítios da internet que deixarem de cumprir as disposições desta Lei.

> das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia.
>
> (...)
>
> Isso posto, considerando o descumprimento de ordem judicial emanada deste Juízo, passo a decidir:
> 1) Oficie-se à Autoridade Policial, com cópias integrais da presente, a fim de que seja instaurado procedimento contra o senhor representante legal das empresas Facebook Serviços Online do Brasil Ltda, pela suposta prática do crime previsto no artigo 2º, parágrafo 1º, da Lei 12850/2013;
> 2) Determino a imposição de multa diária no valor de R$50.000,00 (cinquenta mil reais) até o efetivo cumprimento da medida de interceptação do fluxo de dados do Whatsapp (na forma da decisão em separado), com fulcro no artigo 139, IV, do Código de Processo Civil c/c artigo 3º, do Código de Processo Penal. Intime-se para pagamento o senhor representante legal da empresa Facebook Serviços Online do Brasil Ltda;
> 3) Oficie-se à EMBRATEL, ANATEL, bem como a todas as operadoras de telefonia celular, a fim de que providenciem, imediatamente, a suspensão do serviço do aplicativo Whatsapp em todas as operadoras de telefonia, até que a ordem judicial seja efetivamente cumprida pela empresa Facebook, sob as penas da Lei;
> 4) As medidas ora cominadas deverão ser cumpridas pela autoridade policial da 62ª DP ou por agentes especialmente designados pela mesma ou pela Chefia da Polícia Civil do Rio de Janeiro;

Em sua defesa, a empresa alega, como alegou todas as outras vezes que foi demandada por um juízo brasileiro, a impossibilidade técnica de cumprir ordens judiciais dessa natureza, sob pena de comprometer a própria segurança do sistema. Seu principal argumento é que, com a implementação da criptografia ponta-a-ponta, a empresa não possuiria uma chave mestra para decifrar o conteúdo das mensagens e entregar as informações buscadas pelas autoridades. Quando os usuários estão em comunicação pelo aplicativo, apenas eles mesmos possuiriam as chaves que decifram suas mensagens, o que serve para proteger sua confidencialidade e garantir que a criptografia seja "forte", isto é, inquebrável (ANTONIALLI, CRUZ, *et al.*, 2016).

A decisão em comento gerou muito debate tanto na sociedade civil como na academia e acabou sendo revertida, no mesmo dia, por determinação do presidente do Supremo Tribunal Federal[67], nos autos da ADPF nº 403, ajuizada pelo Partido Popular Socialista – PPS contra a

[67] STF. ADPF 403. Min.Presidente Ricardo Lewandowski. PARTIDO POPULAR SOCIALISTA – PPS, JUIZ DE DIREITO DA VARA CRIMINAL DA COMARCA DE LAGARTO, INSTITUTO BETA PARA DEMOCRACIA E INTERNET – IBIDEM, FEDERAÇÃO DAS ASSOCIAÇÕES DAS EMPRESAS BRASILEIRAS DE TECNOLOGIA DA INFORMAÇÃO - ASSESPRO NACIONAL, INSTITUTO DE TECNOLOGIA E SOCIEDADE – ITS. 03/05/2016

decisão proferida pelo juízo da vara criminal da comarca de Lagarto (processo nº 201555000783). Nesse sentido, destaca-se trecho da decisão:

> Ora, a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa.
>
> (...)
>
> Sem adentrar no mérito do uso do aplicativo para fins ilícitos, é preciso destacar a importância desse tipo de comunicação até mesmo para intimação de despachos ou decisões judiciais, conforme noticiado pelo sítio eletrônico http://www.conjur.com.br/2016-fev-27/klaus-koplinurgente-intimacao-feita-whatsapp.
>
> Ressalto, de resto, que não se ingressa aqui na discussão sobre a obrigatoriedade de a empresa responsável pelo serviço revelar o conteúdo das mensagens, conforme determinado pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ e supostamente descumprido pelo WhatsApp, eis que isso constitui matéria de alta complexidade técnica, a ser resolvida no julgamento do mérito da própria ação.
>
> Assim, nessa análise perfunctória, própria das medidas cautelares, entendo que não se mostra razoável permitir que o ato impugnado prospere, quando mais não seja por gerar insegurança jurídica entre os usuários do serviço, ao deixar milhões de brasileiros sem comunicação entre si.
>
> (...)
>
> Isso posto, com base no poder geral de cautela, defiro a liminar para suspender a decisão proferida pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ, nos autos do IP 062-00164/2016, restabelecendo imediatamente o serviço de mensagens do aplicativo WhatsApp, sem prejuízo de novo exame da matéria pelo Relator sorteado. (STF. ADPF 403. Min.Presidente Ricardo Lewandowski.)

Para além da discussão sobre a proporcionalidade da medida que afetou milhares de brasileiros, deve-se indagar se a ordem de autoridades judiciais que obriga empresas a desenvolver mecanismos de "desvio" da criptografia utilizada pelo aplicativo teria fundamento legal. Em outras palavras, seria necessário averiguar se há alguma lei no Brasil que proíba a criptografia ponta-a-ponta, ou que exija que empresas como o WhatsApp desenvolvam estruturas que garantam o acesso das mensagens à polícia, o que importaria criar um *backdoor*, isto é, uma "porta dos fundos" que concede acesso privilegiado às mensagens.

Ademais, além das questões jurídicas, existem perguntas de ordem tecnológica, ou seja, é preciso entender como a arquitetura da criptografia funciona, para que serve e quais os argumentos que justificariam sua utilização. Fundamental entender, ainda, quais as

consequências das soluções que visam "driblar" a criptografia de ponta-a-ponta, como pretendeu determinar a magistrada.

Nos últimos anos, diversas entidades governamentais ao redor do mundo vêm demonstrando crescente preocupação sobre uma tendência que está se tornando cada vez mais comum: as comunicações estão se tornando nebulosas. Isto é, grandes companhias da tecnologia – incluindo Apple, Google e Whatsapp[68], estão implementando recursos de segurança em seus produtos e serviços de comunicação, como criptografia de ponta-a-ponta e esquemas de criptografia de disco, que fazem com que o usuário fique fora do alcance investigativo do governo, mesmo em circunstâncias em que, tradicionalmente, a lei permitiria o acesso estatal.

Diante da vasta gama de mudanças arquitetônicas que se desencadearam no contexto atual, foi, sobretudo, a adoção da criptografia ponta-a-ponta nos aplicativos de comunicação que se tornou o ponto focal no debate contemporâneo. Nesse cenário, a informação é codificada nos pontos finais de um canal de comunicação e apenas o remetente original e o destinatário pretendido possuem as chaves necessárias para decodificar a mensagem. Em outras palavras, a informação não é capaz de ser lida por um terceiro, incluindo aí o próprio provedor de serviço intermediário. Da mesma forma, a criptografia de dispositivos – na qual as chaves existem apenas nos dispositivos travados – impede que o conteúdo seja lido por qualquer um que não possua a chave (THE BERKMAN CENTER FOR INTERNET & SOCIETY, 2016).

Dessarte, muitos temem que isso torne mais difícil conduzir investigações, prevenir ataques terroristas e fazer cumprir interesses nacionais relacionados à segurança pública. Uma manifestação do debate pode ser percebida no embate legal ocorrido no início de 2016, em que o FBI pediu que uma corte federal norte americana determinasse à Apple o desbloqueio de um *Iphone* utilizado por um atirador em massa na cidade de San Bernardino, Califórnia. Representada pelo Departamento de Justiça, a polícia federal de investigação pedia que a empresa criasse um novo *software* para contornar o sistema de bloqueio do *iPhone*, onde poderiam estar armazenadas informações relevantes para o caso. A Apple recusou o pedido,

[68] Em setembro de 2014, aproximadamente um ano e meio após as revelações feitas por Edward Snowden, a Apple anunciou a sua decisão de incluir a criptografia *by default* nos conteúdos protegidos por senha de seus dispositivos no sistema de operação iOS8.2. Não muito depois desse anúncio, a Google divulgou que o Lollipop, uma versão do Android OS, também possibilitaria a criptografia do aparelho *by default*. Em seguida, em novembro de 2014, o Whatsapp, popular serviço e mensagens instantâneas para smartphones, que agora é de propriedade do Facebook, anunciou que iria suportar o *TextSecure*, um protocolo de criptografia ponta-a-ponta. Não bastasse, em março de 2015, o Yahoo apresentou um *source code* para uma extensão que criptografa mensagens no Yahoo Mail. (THE BERKMAN CENTER FOR INTERNET & SOCIETY, 2016)

centrando o seu argumento no risco de tal tecnologia cair em mãos hostis – *hackers* ou grupos criminosos e terroristas – ou, ainda, ser solicitada por autoridades judiciais de países não democráticos. [69] (GUERREIRO, 2016)

Não é de hoje que os indivíduos podem se utilizar da tecnologia para cifrar as suas mensagens - o primeiro software de criptografia largamente difundido, Pretty Good Privacy (PGP) se tornou disponível ao público já no início dos anos 1990. Todavia, para o usuário médio, a utilização de softwares de criptografia de e-mails se mostrava extremamente difícil, pois trata-se de um processo complexo, que demanda que tanto o remetente quanto o destinatário entendam seu funcionamento. O grande diferencial é que, agora, essa complexidade foi significativamente reduzida. Quando a criptografia é suportada de origem pelo software de comunicação, i.e., quando ela é harmoniosamente integrada no aplicativo, o usuário não tem que tomar nenhuma ação afirmativa para codificar ou decodificar as mensagens; o processo ocorre de forma automática. (THE BERKMAN CENTER FOR INTERNET & SOCIETY, 2016)

Até o presente momento, oficiais do governo não precisavam se preocupar com o alastramento dessa tecnologia, uma vez que grande parcela dos usuários da internet se comunica por meio de serviços *web-based,* como webmail, mensagens instantâneas e sites de rede social, os quais não são criptografados ponta-a-ponta. Desta feita, tradicionalmente, no curso de uma investigação, as autoridades estatais podem interceptar comunicações e buscar acesso a informações armazenadas por esses intermediários ao obter uma ordem judicial. Entretanto, a natureza padronizada dos novos esquemas de privacidade vem alterando esse cenário. Nos casos em que se utiliza a criptografia ponta-a-ponta, uma empresa como o WhatsApp, sem acesso às chaves, não tem condições de fornecer meios para acessar as comunicações em trânsito ou armazenadas em seus serviços, mesmo diante de uma ordem judicial válida.

O debate traz à tona diversas tensões entre segurança, privacidade, concorrência econômica e acesso estatal à informação. Por se tratarem, quase todas, de empresas norte-americanas, essas operadoras de serviços de comunicação estão, cada vez mais, sob o escrutínio de governos estrangeiros em cujos países fazem negócios. Por essa razão, as corporações

[69] A batalha judicial pelo desbloqueio do iPhone de um dos terroristas de San Bernardino terminou depois de o FBI ter anunciado um método que dispensa a ajuda da Apple. Oficialmente, as autoridades norte-americanas desistem do processo por terem conseguido obter aquilo que, até há poucos dias, era considerado impossível: uma técnica para desbloquear, sem ajuda da Apple, o smartphone. O segredo em torno dessa técnica é um novo motivo de inquietação, intensificando o debate entre privacidade e segurança. (GUERREIRO, 2016)

privadas passam a desempenhar um papel quase-soberano ao enfrentar as decisões de agentes governamentais estrangeiros, como vem ocorrendo no Brasil, que as pressionam para produzir dados sobre cidadãos no exterior.

A exemplo do WhatsApp, muitas empresas se recusam a mudar a arquitetura dos seus serviços para permitir a vigilância estatal, sob o argumento de que configuraria uma patente ameaça à segurança e privacidade dos usuários. Esse também é o entendimento de muitos juristas e estudiosos de temas relacionados à informação e tecnologia. Nesse sentido, destaca-se trecho de memorial apresentado pelos *Amici Curiae*, experts em segurança de Iphones e criptografia aplicada do *Stanford Law School Center For Internet And Society* no processo Apple v. FBI, mencionado acima:

> Por razões práticas, o desvio na segurança da Apple determinado por essa Corte certamente será usado em outros Iphones no futuro. Esse spread aumenta os riscos de que o software forense escape do controle da Apple, seja por roubo, descaminho ou ordem de um outro tribunal, incluindo um governo estrangeiro. Caso isso aconteça, o código personalizado poderia ser usado por criminosos e governos para extrair dados sensíveis pessoais ou relacionados a negócios de Iphones apreendidos, perdidos ou furtados (...) Obrigar a Apple a criar um software forense para o governo também é perigoso em razão de quaisquer falhas que o software possa conter. Além disso, a Corte aqui ameaça estabelecer um precedente legal que órgãos estatais aplicadores da lei utilizarão para forçar companhias a desenvolver outros desvios de segurança para propósitos forenses. Não existe nada no All Writs Act ou na decisão do Tribunal que colocaria fora de limites atualizações nos softwares que ativariam os microfones de uma smart TV para propósitos de espionagem ou ligariam a câmera de um laptop para vigilância de vídeo. Esses outros desvios apresentarão seus próprios (potencialmente ainda piores) riscos para a privacidade, cibersegurança e segurança pessoal do público. (...) Assim, os *amici*, respeitosamente, instam a Corte a reconsiderar a sua decisão.[70] (STANFORD LAW SCHOOL CENTER FOR INTERNET AND SOCIETY, 2016)

Da mesma forma, muitos parceiros geopolíticos dos EUA estão ativamente envolvidos em discussões sobre promoção da cibersegurança e os limites adequados de vigilância através

---

[70] *For practical reasons, the security bypass this Court would order Apple to create almost certainly will be used on other iPhones in the future. This spread increases the risk that the forensic software will escape Apple's control either through theft, embezzlement, or order of another court, including a foreign government. If that happens, the custom code could be used by criminals and governments to extract sensitive personal and business data from seized, lost, or stolen iPhones (...) Compelling Apple to create forensic software for the government is also dangerous due to any bugs the software might contain. Further, the Court here threatens to set a legal precedent that law enforcement will use to force companies to craft other security bypasses for forensic purposes. There is nothing in the All Writs Act or the Court's Order that would put off-limits software "updates" that turn on a smart TV's microphone for eavesdropping purposes, or activate a laptop camera for video surveillance. These other bypasses will pose their own, potentially even worse, privacy, cybersecurity, and personal safety risks to the public. As risky as the Court's Order in this case is, the precedent it would set poses even greater danger. (...)Accordingly, amici respectfully urge the Court to vacate its order.*

das fronteiras. Por exemplo, o porto seguro U.S.-E.U., que proporcionou um arcabouço jurídico desde a virada do século para os fluxos transfronteiriços de dados comerciais, foi recentemente considerado inválido pelo Corte de Justiça da União Europeia devido a preocupações sobre a capacidade de espionagem de agências de inteligência dos EUA.[71] Não bastasse, a Organização das Nações Unidas também se posicionou a favor da privacidade e liberdade de expressão do usuário:

> Criptografia e anonimato, e os conceitos de segurança por trás deles, proporcionam a privacidade e a segurança necessárias para o exercício do direito à liberdade de opinião e expressão na era digital. Essa segurança pode ser essencial para o exercício de outros direitos, incluindo direitos econômicos, privacidade, devido processo legal, liberdade de associação e o direito à vida e integridade física. Em razão de sua importância para os direitos de liberdade de opinião e expressão, restrições à criptografia e anonimato devem ser estritamente limitados em consonância com os princípios da legalidade, necessidade, proporcionalidade e legitimidade no objetivo.[72] (KAYE, 2015, p. 19)

Apesar dessas mudanças nos mecanismos de segurança dos provedores de aplicação na internet, a preocupação de muitos governos de que as comunicações estão se tornando cada vez mais fora de alcance não reflete apropriadamente o estado atual e a trajetória do desenvolvimento tecnológico. De fato, a criptografia torna a vigilância mais difícil em alguns casos, mas o cenário real é muito mais diversificado do que se imagina. Sempre existiram, e sempre vão existir, muitas áreas de sombra e escuridão no processo de comunicação, isto é, canais de diálogo resistentes a vigilância. Isso não significa, contudo, que estamos fadados à escuridão e desordem.

Como já destacado no capítulo anterior, nos últimos anos as empresas da internet passaram a depender, cada vez mais, de anúncios publicitários como principal fonte para o seu modelo de negócios, uma vez que são eles que subsidiam os conteúdos e serviços oferecidos na

---

[71] O Safe Harbor Framework, negociado entre os Estados da UE e das Nações em 2009, foi o principal - e muitas vezes o único - mecanismo segundo o qual mais de 4.400 empresas de todos os tamanhos e em todos os setores, legalmente transferiam os dados da Europa para os Estados Unidos nos últimos 15 anos. Durante esse tempo, a relação comercial transatlântica prosperou, criando novos empregos e novas prosperidade na Europa e nos Estados Unidos.
Em 06 de outubro de 2015, a Corte de Justiça da União Europeia efetivamente invalidou o Safe Harbor Framework sob o fundamento de que a Comissão Europeia não tinha avaliado adequadamente se os Estados Unidos mantêm proteções "essencialmente equivalentes" de dados dos cidadãos da UE. (http://www.itic.org/safeharbor)

[72] *Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective.*

rede gratuitamente. A Google Inc., por exemplo, exibe anúncios de publicidade com base em padrões comportamentais, consultas de pesquisa, e outros sinais recolhidos de seus usuários. Da mesma forma, o Facebook afirma que é capaz de atingir públicos estreitos em campanhas publicitárias com "89% de precisão" com base na localização, demografia, interesses e comportamentos.[73] Percebe-se, portanto, que para abastecer esse mercado lucrativo, as empresas, via de regra, desejam obter livre acesso aos dados do usuário. Portanto, implementar a criptografia ponta-a-ponta para todos, ou mesmo a maioria, dos *streams* de dados iria conflitar com o modelo de publicidade e, provavelmente, reduzir os lucros. As tendências de mercado, até agora, refletem que as empresas têm pouco incentivo para desviar desse modelo de negócios, sendo improvável que a criptografia ponta-a-ponta se torne ubíqua através aplicativos e serviços. Como resultado, muitas empresas da internet, continuarão possuindo a habilidade de responder às ordens do governo e proporcionar acesso às comunicações dos usuários.

Ademais, com o advento da computação em nuvem, os dados e softwares, em vez de estarem sob a guarda direta do usuário, eles são deslocados para locais centralizados operados por empresas. Esta tecnologia, tornada possível pela conectividade onipresente, permite que empresas e indivíduos estendam seus recursos de computação através da Internet em centros de dados remotos, como um serviço utilitário. Nesse sentido, vale destacar a fala de Brad Smith, atual presidente mundial da Microsoft Corporation, em palestra realizada na Universidade de Brasília sobre os principais desafios jurídicos da computação em nuvem

> (...) serviços de nuvem estão avançando rapidamente para um ponto em que quase todo software que anteriormente estava em um servidor está agora se mudando para a nuvem; para um datacenter. Existem, assim, dois grandes tipos de serviços emergindo na nuvem. Um deles é o serviço para os consumidores. Hoje em dia, estamos presenciando não apenas serviços de busca na internet e correspondência eletrônica [email]. Qualquer pessoa que utilizou o Skype, na verdade utilizou uma outra versão de serviço em nuvem. Esse serviço é obviamente um serviço que conecta pessoas ao redor do mundo, ou dentro de um campus universitário, e que faz uso da nuvem. Outro tipo de serviço diz respeito aos serviços para empresas. Pode-se pensar em algo como o Microsoft Office. No Brasil, no próximo mês, nós lançaremos uma versão desse produto baseada em nuvem denominada Office 365, pois estará disponível todos os dias do ano. Ele inclui não apenas os aplicativos que vocês conhecem, como o Powerpoint, o Word e o Excel. Ele também inclui serviços de hospedagem de correspondências eletrônicas, como o Outlook e o Exchange. Ele inclui também o SharePoint, que é um serviço de servidor que nós criamos e que permitem que pessoas compartilhem documentos. Ele inclui uma versão corporativa de um software de colaboração chamado Microsoft Lync, que oferece a possibilidade de uso de vídeo, mas também a possibilidade de pessoas trabalharem em conjunto e compartilharem

[73] Dados retirados da própria página do Facebook, disponível em https://www.facebook.com/business/products/ads//?ref=u2u, acessado em 12 de novembro de 2016

> informação a compartilharem documentos e assim por diante. (SMITH, 2012, p. 200 e 201)

Tais serviços, portanto, oferecem benefícios e conveniência substanciais para os indivíduos e muitas vezes são fornecidas gratuitamente em modelos subsidiados por anúncios publicitários ou arranjos *pay-as-you-go*. Por esse motivo, a criptografia ponta-a-ponta é atualmente impraticável para as empresas que precisam oferecer recursos em serviços de nuvem que requerem acesso a dados de texto puro.

Não há dúvidas de que o debate sobre a criptografia levanta questões difíceis sobre segurança e privacidade. De fato, a realização de certos tipos de vigilância tem, em certa medida, se tornado mais difícil à luz das mudanças tecnológicas. Entretanto, deve-se considerar se fornecer acesso a comunicações criptografadas para ajudar a prevenir o terrorismo e investigar crimes não seria uma forma de aumentar a vulnerabilidade dos cidadãos à espionagem cibernética e outras ameaças, como, por exemplo, aquelas provenientes de nações que não abraçam os princípios de um Estado de Direito.

Embora ainda não exista posicionamento unânime sobre o escopo do problema ou a solução política que atingiria o melhor equilíbrio, uma coisa é certa: sempre existirão canais de comunicação resistentes à vigilância. Isto é especialmente verdade dada a natureza generativa da Internet moderna, em que novos serviços e software podem ser disponibilizados de forma descentralizada. No entanto, a pergunta a ser explorada é a significância desta falta de acesso às comunicações para os legítimos interesses do governo.

A partir do exposto acima, argumenta-se que as comunicações no futuro não serão nem eclipsadas na escuridão, nem iluminadas, sem sombra. As forças do mercado e os interesses comerciais provavelmente limitarão as circunstâncias em que as empresas irão utilizar a criptografia, que esconde os dados do usuário das próprias empresas, e a trajetória do próprio desenvolvimento tecnológico – a exemplo da computação em nuvem - aponta para um futuro abundante em dados não criptografados, que pode, inclusive, preencher as lacunas deixadas pelos canais de comunicação, que estão, supostamente, fora de alcance (THE BERKMAN CENTER FOR INTERNET & SOCIETY, 2016).

Exposto este cenário, percebe-se que a regulação do ciberespaço e as particularidades desta arena pública de interação social têm se mostrado um motivo de estranhamento para algumas autoridades estatais, que veem na arquitetura da rede apenas um meio de obstaculizar

investigações criminais e decisões judicias, ao invés de constituir um sistema de proteção do sigilo de comunicação e dos dados da grande maioria dos usuários (IBIDEM; LAPIN, 2016).

Nessa esteira, observe-se a decisão monocrática que determinou o bloqueio do Whatsapp no Brasil. No *decisum*, a juíza enquadrou o caso como um conflito entre o direito à privacidade e o direito à segurança pública e à segurança nacional, o quais, segundo a magistrada, seriam mais relevantes. Entretanto, conforme destacou Riana Pfefferkorn, pesquisadora na área de criptografia no Center for Internet and Society da Stanford Law School (EUA), em entrevista ao InternetLab, o entendimento da juíza não parece ser o mais correto:

> Criptografia forte promove uma forte segurança, ou seja, isso não ameaça a segurança. O debate sobre a criptografia *versus* aplicação da lei é um debate "segurança *versus* segurança", não um debate "privacidade *versus* segurança". Se a criptografia é quebrada para a aplicação da lei, esse mesmo *backdoor* poderá ser usado por bandidos também. Se o Brasil exige um *backdoor* na criptografia, então todo mundo usando a criptografia está em risco. Isso poderia incluir empresas brasileiras, que precisam se proteger contra a espionagem econômica; os bancos brasileiros que poderiam ser invadidos; e até mesmo o Estado brasileiro, que precisa manter os segredos de Estado seguros em relação a Estados inimigos. Forte criptografia é uma "defesa contra vilões", mesmo que os vilões possam usá-la para esconder suas atividades. Tendo em vista os numerosos outros instrumentos de investigação que descrevi acima disponíveis para a aplicação da lei, enfraquecer a criptografia é um sopesamento negativo. (ANTONIALLI, CRUZ, *et al.*, 2016)

O Marco Civil da Internet, portanto, representa um passo importante na direção da proteção do direito à privacidade e à proteção de dados no Brasil ao consolidar uma série de princípios aplicáveis ao uso da internet. Conclui-se, portanto, que a referida lei deve ser interpretada no sentido de que não há imposição aos provedores de aplicações de internet do dever de manter sob sua guarda as comunicações privadas dos usuários. Deve-se resguardar também a possibilidade de que os provedores utilizem criptografia para proteger ainda mais o sigilo e a segurança online. Apenas na hipótese em que os provedores efetivamente guardem essas comunicações, e que não haja algum meio que impeça o acesso ao conteúdo, pode-se cogitar na aplicação de sanção judicial para a não disponibilização dessas informações. Caso fique demostrado que o provedor não realiza essa guarda, ou que aplica algum meio que impeça o acesso às comunicações passadas dos usuários, a sanção não se coaduna com o Marco Civil da Internet e com a Constituição Federal.

3.3 DECRETO Nº 8.771/16

Não obstante a escolha legislativa tenha sido acertada, verifica-se a insuficiência do Marco Civil para regular a matéria de proteção de dados pessoais, de imensa complexidade. Esse instrumento normativo não dispõe de forma específica sobre temas essenciais ao tratamento de informações, capazes de prever mecanismos efetivos de tutela, tais como previsão de autoridade competente para fiscalizar a atividade de tratamento ou normas específicas que estabeleçam os deveres e responsabilidades das empresas do setor, com vistas a proteger a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua privacidade.

Assim, após intensos debates e diversas consultas públicas, foi editado pelo Governo Federal o Decreto 8.771/16, que regulamentou pontos específicos da Lei nº 12.965 de 2014, quais sejam: (i) Neutralidade da Rede; (ii) Guarda dos registros e Proteção de Dados Pessoais; (iii) Apuração de infrações às disposições do Marco Civil. Interessam para esse trabalho apenas os dois últimos eixos.

Dentre as novidades trazidas pelo decreto está uma definição mais específica de dados pessoais bem como do seu tratamento, que encontra reflexo na icônica Diretiva europeia de proteção de dados e cujos efeitos, na combinação com o artigo 7º, inciso VIII, geram obrigações imediatas aos provedores de aplicação:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
> II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A regulamentação da guarda de registros de conexão e aplicação de internet, por sua vez, se inicia com comando legal de natureza desafiadora: o provedor que não coletar dados cadastrais, como filiação, endereço, nome, prenome, estado civil e profissão, pode alegar tal informação à autoridade que os solicitar que ficará desobrigado a fornecê-los. Todavia, o Decreto não se referiu especificamente aos provedores de aplicação, o que pode gerar uma insegurança jurídica, à medida que se abre margem a algum usuário contratar conexão à internet e não apresentar sequer o nome, dando respaldo para anonimato indiscriminado na rede, que é

vedado pela Constituição Federal (art. 5º, IV) e fere obrigações da própria Anatel com as operadoras: de acesso de banda larga, Resolução nº 614 de 2013, artigo 53[74]; e de telefonia móvel, Resolução nº 477 de 2007, artigo 10º, XXII[75] (SCALZILLI.FMV ADVOGADOS, 2016).

Em contrapartida, a norma do artigo 12 prevê a elaboração de relatórios para requisição de dados cadastrais, contendo: o número de pedidos realizados; a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e o número de usuários afetados por tais solicitações. Em apertada síntese, esses relatórios de transparência são informes emitidos por empresas contendo diversas estatísticas relacionados a pedidos de dados. Eles são um mecanismo cada vez mais adotado ao redor do mundo para informar como e quanto as empresas cooperam com autoridades do Estado, em geral por força de lei, entregando dados para produção de prova em processos cíveis e penais (INTERNETLAB, 2016).

Embora não expressamente previsto na lei brasileira, o princípio da privacidade *by design* está de acordo com a *ratio legis* do Marco Civil da Internet no que concerne à proteção de dados pessoais, ao princípio da finalidade que rege seu tratamento e à necessidade de obtenção de consentimento do usuário para tal finalidade. Nesse sentido, o Decreto nº 8.771/2016 aproxima ainda mais a legislação brasileira desse princípio, ao estabelecer, em seu artigo 13, padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, impondo aos provedores de conexão e de aplicações, obrigações sobre padrões de segurança, tais como acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; utilização de mecanismos de autenticação de acesso aos registros, a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, e o uso de soluções de

[74] Art. 53. A Prestadora deve manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo mínimo de um ano.

[75] Art. 10. Além das outras obrigações decorrentes da regulamentação editada pela Anatel e aplicáveis a serviços de telecomunicações e, especialmente, ao SMP, constituem deveres da prestadora:
(...)
XXII - manter, à disposição da Anatel e demais interessados, os documentos de natureza fiscal, os quais englobam ofs dados das ligações efetuadas e recebidas, data, horário de duração e valor da chamada, bem como os dados cadastrais do assinante, por um prazo mínimo de 5 (cinco) anos, em conformidade com o que prescreve o art. 11 da Lei nº 8.218/1991, de 29/08/1991, c/c art. 19 da Resolução nº 247, de 14/12/2000.

gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Isso reforça a importância da segurança dos dados e o respeito à privacidade dos usuários, por meio da adoção de medidas de tecnologia da informação e de práticas de negócio adequadas, estabelecendo a necessidade da criação de infraestrutura condizente com a preservação da privacidade dos usuários. Nessa toada está a determinação de que devem ser retidas a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, as quais deverão ser excluídos assim que atingidas a finalidade de seu uso; ou encerrado o prazo determinado por obrigação legal.

Destaca-se, ainda, o art. 15 do decreto que se apresentar como um problema para as empresas que utilizam em seus produtos a criptografia ponta-a-ponta:

> Art. 15. Os dados de que trata o art. 11 da Lei nº 12.965, de 2014, deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto.

A inteligência desse artigo cria a obrigação para os provedores tanto de aplicações como de conexão de manter os dados de forma inteligível, principalmente a fim de cumprir decisões judiciais que requisitem informações para a condução de investigações. Corroborando esse entendimento, o Ministério Público Brasileiro e o Conselho Nacional do Procuradores-Gerais divulgaram nota técnica sobre tal obrigação, defendendo as medidas adotadas pela justiça nos últimos meses, que determinaram a suspensão do aplicativo WhatsApp por todo o território brasileiro:

> Já o Decreto nº 8771/16, que regulamenta o MCI, deixou claro que tal obrigação também se refere à transmissão desses dados às autoridades brasileiras sempre que requisitados, devendo ser observada a lei processual brasileira, com comunicação direta às autoridades nacionais, sem a necessidade de pedido de cooperação jurídica internacional (mutual legal assistance request). O argumento de que têm sede no exterior e que, por isto, só devem cumprir decisões judiciais emitidas por autoridades de seus países, tem sido reiteradamente utilizado por empresas como Facebook e WhatsApp.
>
> O artigo 15 do MCI prevê que cabe ao provedor de aplicações de Internet – expressão que inclui aplicativos de mensagens instantâneas online e redes sociais – a obrigação de manter os registros de acesso a tais aplicações, sob sigilo, em ambiente controlado e seguro, pelo prazo de 6 (seis) meses. Contudo, essas empresas ou se negam a guardar os registros de acesso pelo período legal (algumas não armazenam por nenhum período), ou os apagam antes de findo o prazo legal e, por tais motivos, vêm descumprindo sistematicamente ordens judiciais brasileiras, o que dificulta ou mesmo inviabiliza a responsabilização cível e criminal de autores de atos ilícitos na

> Internet. (MINISTÉRIO PÚBLICO BRASILEIRO, CONSELHO NACIONAL DO PROCURADORES-GERAIS, 2016)

Como já debatido, é certo que proibir mecanismos de segurança como criptografia ponta-a-ponta não parece ser a solução mais adequada ou efetiva para os problemas relacionados à segurança nacional. A internet tem profundo apreço pela liberdade de expressão e de opiniões, uma vez que ela potencializa a voz dos indivíduos e multiplica a informação, deixando-a ao alcance de qualquer um que tenha acesso à rede. Em um curto espaço de tempo, a internet se tornou um fórum público e global para o debate, e como tal, deve ser aberta e segura para o concreto usufruto das liberdades de expressão. Todavia, ela está constantemente sob ameaça; é um espaço que, assim como o mundo real, está sujeita a empresas criminosas, repressão de opiniões e coleta de dados em massa. Portanto, é fundamental que os indivíduos encontrem formas de se proteger online, que os governos forneçam tal segurança por meio de leis e políticas públicas e que as empresas desenvolvam e coloquem no mercado produtos e serviços compatíveis com os direitos de privacidade. (HUMAN RIGHTS COUNCIL, 2016)

Criptografia e anonimato, separadamente ou juntos, criam uma zona de privacidade para proteger crenças e opiniões. Eles permitem, por exemplo, que comunicações privadas ocorram e blindam a intimidade do indivíduo do escrutínio público, particularmente em ambientes cuja situação política, social ou religiosa é hostil. Enquanto o Estado impõe uma censura ilegal por meio de sistemas de filtragem de conteúdo e outras tecnologias de espionagem, o uso da criptografia e do anonimato na rede pode empoderar indivíduos para transpor barreiras e acessar informações e ideias sem a invasão das autoridades. A habilidade de pesquisar na web, desenvolver ideias e se comunicar de forma segura pode ser a única forma de explorar aspectos básicos da identidade, como gênero, religião, etnia ou orientação sexual.

Por fim, sobre a fiscalização e a transparência, dispõe que a Anatel atuará na regulação, fiscalização e apuração de infrações relacionadas a telecomunicações, que a Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações relacionadas a direitos do consumidor, e que a apuração de infrações à ordem econômica ficará a cargo do Sistema Brasileiro de Defesa da Concorrência (CADE).

***

Em suma, o balanço geral do Decreto é positivo, pois prevê o reforço na obrigação do tratamento isonômico dos dados, garantindo-se o caráter público e aberto da Internet; o esclarecimento de quais são os requisitos técnicos indispensáveis e o que se consideram de

serviços de emergência para a discriminação ou a degradação de tráfego; o esclarecimento de que as ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa; as definições de "dado pessoal" e de "tratamento de dados pessoais"; o estabelecimento de que o CGI é órgão consultivo para o estabelecimento de diretrizes; e, por fim, a declaração de atuação da Anatel, da Secretaria Nacional do Consumidor e do Sistema Brasileiro de Defesa da Concorrência, como órgãos relatórios e de fiscalização, de acordo com cada área de atuação aplicável ao caso em concreto.

A nova regulamentação, embora muito aguardada pelo setor, trouxe algumas incertezas e um pouco mais de insegurança jurídica para aqueles que ofertam bens e serviços na Internet (i.e., provedores de aplicação) ou operam meios que viabilizam o acesso de usuários à rede mundial (i.e., os prestadores de serviços de telecomunicações, inclusive provedores de conexão). O Governo Federal, a exemplo da redação do Marco Civil, optou por uma linguagem aberta, em alguma forma principiológica, que dá margens a diferentes interpretações pelos diferentes órgãos tidos como competentes para regulação, fiscalização e apuração de infrações à referida lei.

Por certo, o decreto que regulamenta o Marco Civil da Internet, é norma nova e, como tal, estará sujeito à ampla reflexão dos juristas e dos aplicadores do Direito ao longo dos próximos meses e anos. Muitos de seus termos serão definidos na prática, isto é, no exercício da submissão da hipótese legal ao fato. Todavia, é justamente a impossibilidade de se extrair diretamente da norma toda a sua amplitude que traz certa angústia para o mercado. Ao não se prestar a trazer certezas, o decreto reforça a já conhecida possibilidade de que o mundo da Internet seja refém do acaso, de interpretações mirabolantes e de atalhos para ação de "super juízes".

CONCLUSÃO

O presente trabalho procurou entender como se deu o fenômeno da informatização, que alterou os modelos econômico e social, bem como as consequências da transição de um mundo antes pensado em átomos para um mundo em bits. Ademais, pretendeu-se compreender como se dá a regulação do ciberespaço, nesse ambiente novo, desprovido de fronteiras e com soberanias mitigadas. Para tanto, foram analisadas as principais teorias regulatórias do ciberespaço, destacando-se, sobretudo, as teorias de Lessig e Murray. Outrossim, o escopo principal do trabalho foi, a partir dessas teorias, entender a privacidade e a proteção de dados

no contexto da sociedade em rede, pensando em formas de proteger esses dois direitos, considerados fundamentais à personalidade humana. Por fim, a pesquisa analisou as relações digitais na conjuntura brasileira, fazendo um estudo mais profundo da Lei nº 12.695/14, popularmente conhecida como |Marco Civil da Internet, procurando entender como a legislação pátria tratou esses dois temas: privacidade e proteção de dados.

A despeito da natureza generativa da internet e dos princípios de absoluta liberdade sobre os quais a rede mundial de computadores foi erigida, chegou-se à conclusão de que esse ambiente não poderia mais ficar alheio à regulação. Atualmente grande parte das interações sociais acontecem em plataformas digitais; a vida está por demasiado interconectada ao mundo virtual, para que seja deixada à própria sorte, como pretendem os teóricos denominados ciberlibertários. Assim, superado o debate sobre se a internet deve ser regulada ou não, o problema torna-se ainda mais complexo: quem deve ser o regulador e como essa restrição de comportamento deve ser feita de modo a manter a paz social, mas sem eliminar a própria essência criativa e livre da internet.

Nessa esteira, foram apresentados dois grandes nomes da regulação no ciberespaço que muito contribuíram para a discussão de temas envolvendo direito e tecnologia. Lawrence Lessig, proeminente constitucionalista e um dos precursores do ciberpaternalismo, cunhou a famosa frase "o código é a lei", i.e, para este autor, é a arquitetura da internet – software e hardware – que determinará as restrições de comportamentos no ambiente digital. Assim, em última instância, quem detém o código é o regulador e por isso, existe um constante embate entre os códigos da costa leste e oeste, ou seja, entre o governo e as empresas de tecnologia. Ademais, o autor cunha sua famosa teoria das quatro modalidades de regulação, colocando o indivíduo como um "ponto patético", que é objeto da incidência de fatores que viabilizam ou restringem certos comportamentos: lei, normas sociais, mercado e arquitetura. Para ele, no caso do ciberespaço, é a arquitetura a modalidade mais influente.

Andrew Murray, por sua vez, apresenta uma teoria mais fluida e menos pessimista que a de Lessig. Segundo esse autor, os indivíduos são pontos ativos que se envolvem em uma matriz de relações simbióticas com os diversos atores do mundo digital, e são protagonistas no curso de seu destino na rede. Nessa teoria, *accountability* ganha um lugar de destaque, sendo que tanto o governo como as empresas privadas devem estabelecer um diálogo constante com os usuários, sujeitos da regulação.

Explicadas as teorias da regulação do ciberespaço, o ponto central do trabalho foi entender como a privacidade e a proteção de dados pessoais se conformam a essa nova realidade

informacional, em que tudo que se faz na plataforma digital deixa rastros. Cada fragmento de informação na rede pode ser coletado e, a partir de uma série de técnicas e algoritmos, podem sem organizados e moldados para formar um perfil eletrônico do usuário. Essa prática mostrou-se um modelo de negócios extremamente lucrativo para as empresas da tecnologia e uma ferramenta poderosa nas mãos do Estado. Em resumo, a vida ser tornou muito mais monitorável.

Assim como um "mercado de limões" em que as informações são assimétricas e os indivíduos nem sempre tem acesso a todo os elementos necessários para entrar em relações de consumo, a privacidade é um elemento que é fonte de dúvidas e incertezas no ambiente virtual. Uma vez que os indivíduos têm dificuldade em distinguir o nível de proteção da privacidade oferecido por cada provedor de aplicação, sobretudo em razão das longas e complexas políticas de privacidade, o parâmetro de segurança é estabelecido em um nível mais baixo, não proporcionando o incentivo necessário para que as empresas vejam a privacidade como um elemento de competição entre si.

Uma solução para o problema da privacidade é abandonar a abordagem pessimista que muitas vezes esse direito sugere, i.e, em vez que enxergar a privacidade como uma obrigação imposta às empresas, que dificultam a coleta de informações, atual moeda de câmbio, é preciso enxergar a privacidade como um instrumento de confiança. Aqui, pode-se fazer um paralelo com a teoria de Murray, pois para estabelecer a privacidade como um valor positivo e agregador é necessário que os usuários sejam vistos como atores ativos e conscientes nessa relação de troca de dados por serviços.

Outrossim, mais de uma década após ter escrito a sua teoria, a previsão de Lessig ainda se mostra acurada. A arquitetura de fato exerce um papel importantíssimo na regulação das relações digitais. Prova disso, é a forma como princípios de segurança e privacidade têm sido incorporados dentro de todo o ciclo de vida da tecnologia, desde a fase inicial de concepção, até à sua implementação final, utilização e eliminação. Esse novo conceito recebeu o nome de privacidade *by design* e tem sido agregada em diversas legislações ao redor do mundo, como por exemplo a nova diretiva de proteção de dados europeia e no próprio Marco Civil da Internet.

Outra questão que foi trazida à tona com a digitalização das informações é como resguardar as informações biográficas ou comportamentais que estão espalhadas na rede. Foi exatamente nesse contexto que surgiu a disciplina da proteção de dados pessoais como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos oriundos do tratamento de dados a partir da moderna tecnologia da informação. Como constatou-se, o

objetivo dessa proteção não são os dados em si, mas o próprio indivíduo, uma vez que identidade e privacidade são atributos da personalidade humana. Por essa razão, transparência e consentimento são elementos fundamentais para garantir a chamada autodeterminação informativa, elemento importante nessa ceara digital.

No Brasil, como destacado, o acesso à internet cresce exponencialmente, portanto, os problemas e incertezas que vêm com as novas tecnologias não podiam se fazer ausentes. Dessarte, tornou-se imprescindível regular as relações digitais no cenário nacional. Após deliberação foi editada a Lei nº 12.695/14, o Marco Civil da Internet. Concluiu-se que apesar das previsões positivas no que concerne à privacidade e à proteção de dados, a lei ainda está longe de alcançar a sua plena eficácia. Como demonstrado por relatório elaborado pela InternetLab (“Quem defende os seus dados”), apesar das determinações legais de guarda, informação e transparência, os provedores de conexão ainda estão muito aquém das expectativas.

Ademais, a Lei ainda enfrenta diversos desafios no que diz respeito ao sigilo e a inviolabilidade das comunicações em plataformas digitais. Como percebido das recentes decisões judiciais que suspenderam as atividades de aplicativos de comunicação da internet, muitos juízes ainda não estão preparados para lidar com as novas configurações tecnológicas. Não há dúvidas de que o uso de mecanismos de segurança como a criptografia ponta-a-ponta para resguardar a privacidade no ambiente em rede tem causado muita desconfiança em autoridades estatais em todo o mundo, entretanto, como visto, esse não é um problema irremediável. Existem muitos fatores que indicam que as comunicações não ficaram totalmente nebulosas e inatingíveis. Esse é só um passo importante para a internet como plataforma propiciadora da liberdade de expressões e opiniões de forma livre e desimpedida

Assim, a partir deste trabalho é possível indagar: quem estava certo? Lessig, que estabeleceu uma visão determinista e fechada, depositando um alto valor no código e nas tecnologias, e, aparentemente, deixando de lado a própria essência humana que ainda permeia as relações digitais ou Murray que assentou total confiança nos indivíduos como atores conscientes e proativos nas interações em rede, criando uma teoria extremamente fluida, a qual por vezes beira a utopia?

De fato, ambas as teorias trouxeram contribuições valiosas e extremamente aplicáveis ao cenário atual. Como visto, elas se interseccionam em alguns pontos e divergem em outros, muitas vezes se complementando. É inegável que não há modelo fechado que consiga disciplinar completamente o ciberespaço, visto que este é um ambiente de constante mudanças

e desafios. Acrescente-se que nem deve ser esse o objetivo do regulador, já que, como afirmado por Pierre Catala (1998), na busca por acompanhar as transformações tecnológicas, acabaríamos com um emaranhado de normas sem sentido e ineficazes. Uma coisa, porém, é certa: por mais que a tecnologia tenha muda radicalmente o cenário das relações interpessoais, os seres humanos ainda possuem um papel determinante na condução dessas alterações. Como afirmado por Manuel Castells (2005), não é a tecnologia de determina a sociedade, mas a sociedade que conforma a tecnologia de acordo com os valores que deseja proteger.

Assim, não resta dúvidas de que o direito exerce papel importantíssimo na integração das mudanças informacionais e na conformação de novas tecnologias aos direitos individuais e coletivos. A economia em rede, erigida sobre o compartilhamento de dados e digitalização da informação pode ser perfeitamente desenvolvida em harmonia com a proteção de direitos dos usuários, a inovação tecnológica e o oferecimento de produtos e serviços online. A imposição de um discurso maniqueísta, baseado num constante *trade off* entre direitos e inovação, pode levar a percepções frágeis da legislação e dos mecanismos regulatórios, mostrando-se como retrocesso na disciplina e proteção de direitos fundamentais e irrenunciáveis. (SOMBRA, 2016)

REFERÊNCIAS BIBLIOGRÁFICAS

AKERLOF, G. The Market for Lemons: Quality Uncertainty and the Market. **The Quarterly Journal of Economics**, v. 84, n. 3, p. 488-500, 1970.

ALVES, C. S.; VAINZOF, R. Direito Digital: Privacy by Design e Proteção de Dados Pessoais. **Jota**, 6 julho 2016. Disponivel em: <http://jota.info/direito-digital-privacy-design-e-protecao-de-dados-pessoais>. Acesso em: 2016.

ANDERSON, R.; MOORE, T. The Economics of Information Security. **Science**, v. 314, n. 5799, p. 610-613, 2006.

ANDERSON, W. L. "Falhas de mercado" e informações assimétricas. **Mises Brasil**, 2013. Disponivel em: <http://www.mises.org.br/Article.aspx?id=1150>. Acesso em: 04 novembro 2016.

ANDRADE, N. N. G. D. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In: SCHOOL, P. I. S. **Privacy and Identity Management for Life**. Helsingborg: Springer Berlin Heidelberg, v. 352, 2010. p. 90-107.

ANTONIALLI, D. et al. Especial: o que dizem especialistas em criptografia sobre o bloqueio do WhatsApp. **InternetLab**, 2016. Disponivel em: <http://www.internetlab.org.br/pt/opiniao/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/>. Acesso em: 01 novembro 2016.

ANTONIALLI, D.; ABREU, J. Vigilância e privacidade. **InternetLab**, 2016. Disponivel em: <http://www.internetlab.org.br/pt/pesquisa/vigilancia/>. Acesso em: 23 outubro 2016.

BARLOW, J. P. **Declaração de Independência**. Davos. 1996.

BENKLER, Y. **The Wealth of Networks:** How Social Production Transforms Markets and Freedom. New Haven and London : Yale University Press, 2006.

CALABRESI, G.; MELAMED, A. D. Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. **Harvard Law Review**, v. 85, n. 6, p. 1089-1128, April 1972.

CALANDRINO, J. A. et al. “You Might Also Like:” Privacy Risks of Collaborative Filtering, p. 231-246, 2011.e

CASTELLS, M. A Sociedade em Rede: do Conhecimento à Política. In: CASTELLS, M.; CARDOSO, G. **A Sociedade em Rede:** Do Conhecimento à Acção Política. Belém: Imprensa Nacional - Casa da Moeda, 2005. p. 17 - 30.

CATALA, P. Ébauche d'une Théorie Juridique de L'Information. In: CATALA, P. **Le droit à l'épreuve du numérique**. Paris: PUF, 1998. p. 224-244.

CATE, F. H. **Privacy in the Information Age**. [S.l.]: Brookings Institution Press, 1997.

CAVOUKIAN, A. **Privacy by Design: The 7 Foundational Principles**. Information & Privacy Commissioner of Ontario, Canada. Ontario. 2009.

CAVOUKIAN, A. **Privacy by Design**. Information and Privacy Commissioner of Ontario. Ontario. 2013.

CELLA, J. R. G.; FREITAS, C. O. A. Marco Civil da Internet: Limites da Previsão Legal de Consentimento Expresso e Inequívoco como Proteção Jurídica dos Dados Pessoais na Internet. **Revista de Direito, Governança e Novas Tecnologias**, v. 2, n. 1, p. 61-80, 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet, versao 4.0**. CGI.BR. São Paulo. 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. **TIC domicílios 2014: pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiroS**. Comitê Gestor da Internet no Brasil. São Paulo. 2015.

CONSELHO, R. (. 2. D. P. E. E. D., abril 27 2016. Disponivel em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

CORREA, A.-D.; SIMÕES, M. Relatório: Brasil vigia cidadãos sem qualquer escrutínio público. **Publica**, 2016. Disponivel em: <http://apublica.org/2016/10/relatorio-brasil-vigia-cidadaos-sem-qualquer-escrutinio-publico/>. Acesso em: 07 novembro 2016.

CRAVO, V. O Big Data e os desafios da modernidade: uma regulação necessária? **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 8, n. 1, p. 177-192, Maio 2016.

DEBASTIANI, C. A. **Definindo Escopo em Projetos de Software**. São Paulo: Novatec, 2015.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, D. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. [S.l.]. 2010.

EDWARDS, L. Coding Privacy. **Chicago-Kent Law Reviewer**, 84, 2009. 861.

FERREIRA, R. E. **Linux:** guia do administrador do sistema. 2ª. ed. Rio de Janeiro: Novatec, 2013.

FILHO, E. T. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estud. av. [online]**, São Paulo, v. 30, n. 86, p. 269-285, Jan./Apr. 2016.

FTC. **Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers**. Federal Trade Comission. [S.l.]. 2010.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. **Globo.com**, 2013. Disponivel em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 07 novembro 2016.

GUERREIRO, P. Apple vs FBI: não sabemos onde isto vai parar. **Público**, 2016. Disponivel em: <https://www.publico.pt/tecnologia/noticia/apple-vs-fbi-nao-sabemos-onde-isto-vai-parar-1727852?page=3#/follow>. Acesso em: 02 novembro 2016.

HILL, C. A.; O'HARA, E. A. A Cognitive Theory of Trust, 2006.

HIRATA, A. O Facebook e o direito à privacidade. **Revista de informação legislativa**, v. 51, p. 17-27, março 2014.

HUMAN RIGHTS COUNCIL. **A/HRC/32/L.20 - The promotion, protection and enjoyment of human rights on the Internet**. United Nations. [S.l.]. 2016.

HUSTINX, P. **Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy**. European Data Protection Supervisor. Brussels. 2010.

IBIDEM; LAPIN. **Petição de Amicus Curiae na ADI 5527**. Brasília. 2016.

INTERNETLAB. O que é o InternetLab? **InternetLab**, 2016. Disponivel em: <http://www.internetlab.org.br/pt/sobre/>. Acesso em: 13 novembro 2016.

INTERNETLAB. **Quem Defende Seus Dados?** InternetLab. [S.l.]. 2016.

JESUS, D. D.; MILAGRE, J. A. **Marco Civil da Internet:** Comentários à lei n. 12.965/14. São Paulo: Saraiva, 2014.

KAYE, D. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Human Rights Council, United Nations. [S.l.]. 2015.

KERR, O. S. The Problem of Perspective in Internet Law. **Georgetown Law Journal**, Washignton, February 2003.

LATOUR, B. **Reassembling the Social:** an introduction to actor-network-theory. New York: Oxford University Press, 2005.

LEONARDI, M. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2011.

LESSIG, L. The New Chicago School. **The Journal of Legal Studies** , v. 27, n. 52, 1998.

LESSIG, L. **Code and Other Laws of Cyberspace ver.2.0**. New York: Basic Books, 2006.

MACHADO, J. D. M. S. A TUTELA DA PRIVACIDADE NO CONTROLE DE DADOS PESSOAIS NO DIREITO BRASILEIRO. **Revista Juridica Eletrônica da Universidade Federal do Piauí**, v. 2, n. 2, p. 43-65, dezembro 2015.

MARTINS, L. **Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer , 2005.

MARTINS, R. M. O Princípio da Confiança Legítima e o Enunciado N. 362 da IV Jornada de Direito Civil. **Revista CEJ**, Brasília, v. XII, n. 40, p. 11-19, março 2008.

MAYER-SCHÖNBERGER, V.; CUKIER, K. **Big Data:** A Revolution that Will Transform how We Live, Work, and Think. Boston, New York: Houghton Mifflin Harcourt, 2013.

MAZZUCATO, M. **O Estado Empreendedor:** desmascarando o mito do setor público x setor privado. São Paulo: Portfolio-Penguin, 2014.

MELO, L. C. M. A teoria dos sistemas sociais em Niklas Luhmann. **Sociedade e Estado**, Brasília, v. 28, Dezembro 2013.

MENDES, L. S. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. **Dissertação (Mestrado em Direito)- Universidade de Brasília**, Brasília, 2008.

MENDES, L. S. [especial] O que são dados pessoais? **InternetLab**, 2016. Disponivel em: <http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/>. Acesso em: 24 outubro 2016.

MENDONÇA, F. G. **O Direito à Autodeterminação Informativa:** A (Des)Necessidade de Criação de Um Novo Direito Fundamental Para a Proteção de Dados Pessoais no Brasil. Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea. Santa Catarina: [s.n.]. 2014.

MINISTÉRIO PÚBLICO BRASILEIRO, CONSELHO NACIONAL DO PROCURADORES-GERAIS. Nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da internet, 2016. Disponivel em: <http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/>. Acesso em: 08 novembro 2016.

MURRAY, A. Internet Regulation. In: LEVI-FAUR, D. **Handbook on the Politics of Regulation**. Cheltenham: Edward Elgard Publishing, 2011. p. 267-279.

MURRAY, A. **Information Technology Law:** Law and Society. Oxford: Oxford University Press , 2016.

NARAYANAN, A.; SHMATIKOV, V. Robust De-anonymization of Large Sparse Datasets. **IEEE Symposium on Security and Privacy** , p. 111-125, 2008.

NEGROPONTE, N. **A Vida Digital**. São Paulo: Companhia das Letras, 1995.

NEGROPONTE, N. **Being Digital**. New York: Alfred A. Knopf., 1995.

NISSENBAUM, H. **Privacy in context:** technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010.

NISSENBAUM, H. A Contextual Approach to Privacy Online. **Dædalus: Journal of the American Academy of Arts & Sciences**, Fall 2011. 32-48.

O'REILLY, T.; BATTELLE, J. **Web Squared: Web 2.0 Five Years On**. Web 2.0 Summit. [S.l.]. 2009.

O'BRIEN, D. et al. Privacy and Cybersecurity Research Briefing. **Berkman Klein Center Research Publication** , Cambridge, September 2016.

OLIVEIRA, C. E. E. D. Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica. **Núcleo de Estudos e Pesquisas/CONLEG/ Senado**, Brasília, abril 2014.

ONN, Y. et al. Privacy in the Digital Environment. **Haifa Center of Law & Technology, Niva Elkin-Koren, Michael Birnhack**, Haifa, 2005.

PAIVA, T. F. S. A regulamentação do marco civil da internet: um mundo de menos certezas para a web. **Migalhas**, 2016. Disponivel em: <http://www.migalhas.com.br/dePeso/16,MI239397,91041-A+regulamentacao+do+marco+civil+da+internet+um+mundo+de+menos>. Acesso em: 27 outubro 2016.

PANEBIANCO, M. Bundesverfassungsgericht, dignità umana e diritti fondamentali. In: _____ **Diritto e Società**. [S.l.]: [s.n.], 2000.

POLIDO, F. B. P. Levando a sério o Marco Civil da Internet no Brasil: premissas para o repensar das instituições e a justiça na fronteira das tecnologias. **IRIS (Instituto de referência em Internet e Sociedade)**, 2016. Disponivel em: <http://irisbh.com.br/levando-a-serio-o-marco-civil-da-internet-no-brasil-premissas-para-o-repensar-das-instituicoes-e-a-justica-na-fronteira-das-tecnologias/>. Acesso em: 26 outrubro 2016.

PRIMO, A. O aspecto relacional das interações na Web 2.0. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**, Porto Alegre, v. 9, 2007.

RICHARDS, N.; HARTZOG, W. Taking Trust Seriously in Privacy Law. **Stanford Technology Law Review, Forthcoming**, Stanford, September 2015.

RODOTÀ, S. **A Vida na Sociedade da Vigilância**. [S.l.]: Renovar , 2007.

RODRIGUES, L. P.; NEVES, F. M. **Niklas Luhmann:** a sociedade como sistema. Porto Alegre: Edipucrs, 2012.

SANTOS, E. M. D. Aprisionamento tecnológico: novos desafios da gestão das estratégias organizacionais na era da informação, 2001.

SCALZILLI.FMV ADVOGADOS. Marco Civil da Internet: principais efeitos do Decreto 8.771 assinado em 11 de maio de 2016. **Scalzilli.fmv Advogados**, 2016. Disponivel em: <http://www.scalzillifmv.com.br/publicacao/marco-civil-da-internet-principais-efeitos-do-decreto-8-771-assinado-em-11-de-maio-de-2016>. Acesso em: 04 novembro 2016.

SCHAUER, F. Internet Privacy and The Public- Private Distinction. **Jurimetrics**, v. 38, n. 4, p. 555-564, 1998.

SETZER, V. W. Dado, informação, conhecimento e competência. **DataGramaZero Revista de Ciencia da Informação**, v. 0, 1999.

SILVA, B. M. D. **Marco Civil Da Internet:** O Que Muda Com Relação Aos Cookies De Internet? [S.l.]: [s.n.]. 2013.

SLOOT, B. V. D.; BORGESIUS, F. J. Z. Google and Personal Data Protection. In: LOPEZ-TARRUELLA, A. **Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models**. [S.l.]: Asser Press, v. 22 VIII, 2012. Cap. 4, p. 75-111.

SMITH, B. Direito e Regulação na Internet: desafios jurídicos e oportunidades para o crescimento econômico. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 4, n. 1, p. 197-236, 2012.

SOMBRA, T. L. Divulgação de dados pessoais e bloqueio de site. **Observatório do Marco civil da Internet**, 2016. Disponivel em: <http://www.omci.org.br/jurisprudencia/125/divulgacao-de-dados-pessoais-e-bloqueio-a-site/>. Acesso em: 07 novembro 2016.

STANFORD LAW SCHOOL CENTER FOR INTERNET AND SOCIETY. **Brief Of Amici Curiae Iphone Security And Applied Cryptography Experts In Support Of Apple Inc.'S Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search, And Opposition To Government'S Motion To Compel Assistance**. STANFORD LAW SCHOOL CENTER FOR INTERNET AND SOCIETY. [S.l.]. 2016.

TAJRA, M. N.; MACHADO, J. D. M. S. A necessidade de um Código brasileiro de proteção de dados pessoais no Brasil. **Revista de Direito UNINOVAFAPI**, v. 1, n. 1, 2016.

TEPEDINO, G. Novos Princípios Contratuais e Teoria da Confiança: a exegese da cláusula "to the best knowledge of the sellers". **Revista Forense**, Rio de Janeiro, v. 377, 2005.

THE BERKMAN CENTER FOR INTERNET & SOCIETY. **Don't Panick: Making Progress on the "Going Dark" Debate**. The Berkman Center for Internet & Society. [S.l.]. 2016.

TRUDEL, P. Privacy Protection on the Internet: Risk Management and Networked Normativity. In: GUTWIRTH, S., et al. **Reinventing Data Protection**. Springer: [s.n.], 2009. p. 317-334.

USA AIR FORCES. **USAF INTELLIGENCE TARGETING GUIDE**. USA Air Forces. [S.l.], p. 200-218. 1998.

VILA, T.; GREENSTADT, R.; MOLNAR, D. Why we can't be bothered to read privacy policies. In: KLUWER **Economics of Information Security**. [S.l.]: [s.n.], 2004. p. 143-154.

VERLE, L. **Tempo e espaço no cyberspace**, Porto Alegre, 1997. (Não publicado)

WESTIN, A. **Privacy and Freedom**. Nova York: Atheneum, 1970.

WIENER, N. **Cibernética e Sociedade:** O Uso Humano de Seres Humanos. São Paulo: Editora Cultrix, 1954.

WOODS, A.; O'BRIEN, D.; GASSER, U. Privacy and Open Data Research Briefing. **Berkman Klein Center Research Publication**, Cambridge, September 2016. Disponivel em: <Available at SSRN: http://ssrn.com/abstract=2842816>.

ZITTRAIN, J. L. **The Future of the Internet -- And How to Stop it**. New Haven & London: Yale University Press & Penguin UK, 2008.