UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO

CLARISSA MENEZES VAZ MASILI

REGULAÇÃO DO USO DE DADOS PESSOAIS NO BRASIL

Papel do usuário na defesa de um direito à tutela de dados pessoais autônomo

BRASÍLIA
2018

CLARISSA MENEZES VAZ MASILI

REGULAÇÃO DO USO DE DADOS PESSOAIS NO BRASIL

Papel do usuário na defesa de um direito à tutela de dados pessoais autônomo

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre no Programa de Pós-Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa de Transformações da Ordem Social e Econômica e Regulação.

Orientadora: Profa. Dra. Christiana Soares de Freitas

BRASÍLIA 2018

FICHA CATALOGRÁFICA

MASILI, C. M. Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo / Clarissa Menezes Vaz Masili; orientador Christiana Soares de Freitas. - Brasília, 2018. 197 p.

Dissertação (Mestrado - Mestrado em Direito) - Faculdade de Direito - Universidade de Brasília, 2018.

1.direito subjetivo à tutela de dados pessoais. 2.ciberespaço. 3.usuários de internet. 4. consentimento. 5.teorias regulatórias do ciberespaço. I. Soares de Freitas, Christiana, orient. I. FD/UnB. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

MASILI, C. M. (2018). Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo. Dissertação de Mestrado em Direito, Faculdade de Direito, Universidade de Brasília, Brasília, DF, 197 p.

FOLHA DE APROVAÇÃO

Clarissa Menezes Vaz Masili

REGULAÇÃO DO USO DE DADOS PESSOAIS NO BRASIL: PAPEL DO USUÁRIO NA DEFESA DE UM DIREITO À TUTELA DE DADOS PESSOAIS AUTÔNOMO

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre, no Programa de Pós-Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa de Transformações da Ordem Social e Econômica e Regulação.

Aprovada em: 3 de setembro de 2018.

BANCA EXAMINADORA

_____

Profa. Dra. Christiana Soares de Freitas
(Orientadora, Presidente)

_____

Prof. Dr. Sérgio Amadeu da Silveira
(Membro)

_____

Profa. Dr. Alessandra Aparecida Silveira
(Membro)

_____

Prof. Dr. Alexandre Kehrig Veronese Aguiar
(Suplente)

AGRADECIMENTOS

Chegar ao fim de um dos passos de uma trajetória acadêmica, como a apresentação de uma dissertação de conclusão de um curso de mestrado, pode ser uma experiência de bastante reclusão. No entanto, no meu caso, se agora posso realizar esse antigo desejo, devo reconhecer que não estive só e, na verdade, devo essa conquista a outras pessoas que participaram desse processo.

Diante disso, agradeço à minha família, em especial aos meus pais, Celiza e Adão, pelo incentivo e por sempre terem colocado à minha disposição todos os instrumentos necessários para que o estudo fosse vivido como uma prioridade. Agradeço também especialmente ao meu amado marido, Gustavo, por todo o apoio e pelas incontáveis ajudas ao longo desse caminho de estudos, aulas e escrita; você e sua compreensão deixaram esse percurso mais leve. Sou também imensamente grata à minha Giovanna, por ter sido tão boazinha, paciente, calma e motivadora para mim durante esse período tão crucial das nossas vidas, que é sua gestação.

Expresso minha gratidão também à minha orientadora, Professora Christiana Soares de Freitas, primeiramente pela confiança na minha capacidade de desenvolver um trabalho à altura desta Faculdade de Direito. E, de modo especial, por ter norteado a pesquisa com a paciência, a segurança, o sempre alto astral e a perspectiva sociológica que eu precisava como sua orientanda.

Juntamente à Professora Christiana, agradeço ao Professor Alexandre Veronese, pois ambos me apresentaram esse tema de estudo durante as aulas de Direito, Internet e Sociedade neste curso de pós-graduação. Ao Professor sou grata, também, pela oportunidade de ser sua monitora e partilhar a experiência de docência aos alunos da graduação na disciplina de Prática e Atualização e Direito – Direito, Internet e Sociedade, também com a colega Luana Borges.

O amadurecimento da proposta deste trabalho também foi fruto de conversas e ideias trocadas dentro e fora dos corredores desta Faculdade, razão pela qual também menciono meu agradecimento aos meus amigos e colegas com quem tanto pude aprender e em quem pude me espelhar.

Agradeço, também, ao Tribunal de Justiça do Distrito Federal e dos Territórios, onde pude exercer minhas atividades profissionais com a flexibilidade que foi

necessária para conciliá-las com a atividade acadêmica, notadamente durante os meses de afastamento para escrita deste trabalho.

Por fim, agradeço a toda a comunidade acadêmica que desenvolve pesquisas e atua também na construção das políticas ainda tão necessárias para a tutela dos dados pessoais no Brasil, já que o empenho dessas pessoas foi o ponto de partida para a proposta deste estudo. Não posso deixar de mencionar minha gratidão em especial aos doutores Sérgio Amadeu da Silveira, Alessandra Silveira e Alexandre Veronese por aceitarem o convite de composição da banca examinadora que avaliará a qualidade acadêmica deste trabalho e seguramente permitirá o aprimoramento desta pesquisa.

RESUMO

MASILI, Clarissa M. V. Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo/ Clarissa Menezes Vaz Masili; orientadora Christiana Soares de Freitas - Brasília, 2018. 197 p. Dissertação (Mestrado) - Faculdade de Direito, Universidade de Brasília, Brasília, 2018.

Na sociedade em rede, a expansão do desenvolvimento de relações pela rede mundial de computadores potencializou a velocidade, a quantidade e a qualidade na obtenção e no tratamento de dados pessoais. Assim, novas formas de marketing e de produção passaram a moldar uma microeconomia da interceptação de dados, assim como a atuação dos estados também passou a fazer maior uso de tecnologias pautadas na coleta e no tratamento de dados para implementar serviços prestados, executar políticas públicas e realizar vigilância. A variedade de informações coletáveis e de práticas possíveis com esses dados desperta o questionamento sobre a ciência por parte dos usuários acerca de sua condição de fornecedores dessa matéria prima de ações estatais e de mercado. Isso porque, além das situações em que o fornecimento de informações é voluntário, a tecnologia desenvolvida permite a captação de dados também por observação. Nesse contexto, partindo da premissa teórica da autonomia do direito individual à tutela sobre dados pessoais em face da privacidade e da extimidade, propõe-se investigar os valores dos dados pessoais no momento atual do Brasil, a fim de, a partir de teorias regulatórias aplicáveis a esse ciberespaço e empregadas como referencial teórico, identificar qual delas, atualmente, mais bem explica a realidade regulatória brasileira quanto ao direito à tutela dos dados pessoais. Sugere-se e confirma-se que a hipossuficiência de forças do usuário em face do discurso comum de companhias privadas e governos quanto ao seu direito de extrair todo valor desses dados em um modelo normativo pautado no consentimento – que não se mostra efetivo – as teorias regulatórias que pressupõem a capacidade regulatória de usuários em igualdade de forças com o mercado, as leis e a arquitetura da rede não explicam, neste momento da realidade brasileira, o contexto de tutela dos dados pessoais. Há, porém, alguma participação ativa dos usuários nesse contexto regulatório, de modo que a teoria da regulação descentrada, cunhada por Black, pode ser a que mais bem explica esse cenário contemporâneo.

Palavras chave: direito subjetivo à tutela de dados pessoais – ciberespaço - usuários – consentimento – teorias regulatórias.

ABSTRACT

MASILI, Clarissa M. V. *Regulation of personal data in Brazil: role of users in the defense of a of an autonomous personal data protection right*. 2018. 197 p Thesis (Master) - Law Faculty of University of Brasília, Brasília, 2018.

In the network society, the expansion of the development of relationships by the world-wide computer network has increased speed, quantity and quality in obtaining and processing personal data. Thus, new forms of marketing and production began to shape a microeconomy of data interception, as well as the state's performance, which also began to make greater use of technologies based on data collection and processing to implement services, public policies and to carry out surveillance, arising a Virtual State. The variety of collectible information and possible practices with these data raises the question about the knowledge of users about their condition of suppliers of this raw material of state's and market's practices. In fact, in addition to situations in which the information supply is voluntary, the technology now allows the capture of data also by observation. In this context, supported by the theoretical premise of the autonomy of the individual right to protection of personal data regarding privacy and eximity, this dissertation investigates the values of personal data in the current moment of Brazil. The next step proposed consists in identify – based on applicable regulatory theories to this cyberspace and used as a theoretical reference – which one, at present, better explains the Brazilian regulatory reality regarding the right to protection of personal data.

It is suggested and confirmed that there is a users's hyposufficiency besides the common discourse of private companies and governments about their right to extract all of these values of personal data in a normative model based on consent - which is not effective. Thus, the regulatory theories based on the capacity of users on an equal footing with the market, the laws and the architecture of the network do not explain, at this moment of the Brazilian reality, the context of protection of personal data. There is, however, some active participation of users in this regulatory context, so that the theory of decentred regulation, coined by BLACK, may be the one that best explains this contemporary scenario.

Keywords: right to protection of personal data – cyberspace – users – consent - regulatory theories.

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ANATEL – Agência Nacional de Telecomunicações

ARPANET - *Advanced Reserach Projects Agency Network*

ATN - *Actor Network Theory*

ADI - Ação Direta de Inconstitucionalidade

ADPF - Ação de Descumprimento de Preceito Fundamental

CAC- *command and control*

CCP - comunicação por campo de proximidade

CCTV - *Closed Circuit Television*

CGI – Comitê Gestor da Internet

CIA - *Central Intelligence Agency*

CIGI - Centre for International Governance Innovation

COPPA - *Children's Online Privacy Protection Act*

DARPA - *Defense Advanced Research Projects Agency*

DEM – Partido Democratas

DNS – *Domain Name System*

DPDC - Departamento de Proteção de Defesa do Consumidor – Brasil

DPI - *deep packet inspection*

DRM - *Digital Rights Management*

EU – União Europeia

FTC - *Federal Trade Commission*

HIPAA - *Health Insurance Portability and Accountability Act*

IANA - *Internet Assigned Numbers Authority*

ICANN - *Internet Corporation for Assigned Names and Numbers*

ICCPR - Convenção Internacional sobre Direitos Civis e Políticos

IP - *Internet Protocol*

ISO - Organização Internacional de Normalização

ITR - Regulações Internacionais de Telecomunicações

MCI – Marco Civil da Internet

MIT - *Massachusetts Institute of Technology*

NCP - *Network Control Protocol*

NFC - *Near Field Communication*

NPL - *National Physical Laboratory*

NSA - *National Security Agency*

PBD - *privacy by design*

PCPD - *Privacy Commissioner for Personal Data*

PET - *privacy-enhancing Technologies*

P2P - *peer-to-peer*

RE – Recurso Extraordinário

REsp – Recurso Especial

RFID - *Radio-Frequency Identification*

Senacon - Secretaria de Proteção ao Consumidor

SMAC - *social, mobile, analytics, cloud*

SST - *Social Systems Theory*

TCP - *Transmission Control Protocol*

TCP/IP - *Transmission Control Protocol/Internet Protocol*

TIC – Tecnologias da Informação e da Comunicação

TLD - *top-level domain*

UnB – Universidade de Brasília

SUMÁRIO

1. INTRODUÇÃO

Na sociedade em rede, um elemento dessa formatação social se tornou especialmente importante: os dados dos usuários dos produtos e serviços disponibilizados nesse novo modelo de relações. Embora o conhecimento e o domínio sobre a informação já sejam especialmente relevantes desde a passagem da sociedade industrial para a informacional e apesar de as características dos usuários em qualquer modelo de mercado e em qualquer espécie de relação indivíduo-Estado sempre terem tido sua relevância, a expansão do desenvolvimento de relações pela rede mundial de computadores potencializou a velocidade, a quantidade e a qualidade na obtenção e no tratamento dessas informações (MACHLUP, 1962).

No contexto da percepção de que as máquinas focadas na ampliação da força física eram superadas por aquelas com melhor tecnologia, Castells (1999) caracterizou a sociedade da informação como uma sociedade em rede. O sociólogo, ainda em 1997, analisando o capitalismo global informacional e as implicações do desenvolvimento das tecnologias da informação e comunicação, verificou que essas tecnologias emergentes permitiram o surgimento, na segunda metade do século XX, de um novo modo de desenvolvimento em que a produção decorria da criação de tecnologias de geração e uso de conhecimentos.

Assim, qualificou o sistema econômico e tecnológico surgido desde a década de 1980 como capitalismo informacional, em que os meios de produção consistem na informação e no conhecimento. Esse novo modo de produção é, além de informacional, global, pois as atividades produtivas, o consumo e a circulação de capital, trabalho, entre outros, estão organizados em redes de conexões globais.

Uma das principais consequências do contexto social pautado em tecnologias cibernéticas (de comunicação e controle) em vez de analógicas consiste na capacidade de registro das ações. Daí Silveira (2017b) ter comparado fechaduras mecânicas com dispositivos digitais para abertura e fechamento de portas. Naquelas, cada operação de abrir e fechar é realizada com as engrenagens quantas vezes for possível e nada é registrado, ao passo que, nos dispositivos digitais, a porta não apenas é destravada e travada, mas toda ação tem o registro de horário, quantidade de vezes e, em alguns casos, até mesmo da autoria dos movimentos.

Para quantificar um pouco o volume de dados de natureza pessoal presentes na rede, pode-se tomar o exemplo do estudante de direito australiano Max Schrems, o qual, em 2011, pediu ao Facebook para lhe informar todos os dados que a companhia tinha sobre si. À época, a aplicação ainda não disponibilizava a ferramenta de download dos dados e registros do usuário nas próprias configurações do perfil, razão pela qual a demanda judicial foi necessária e o pedido foi respaldado na legislação da União Europeia e, após dois anos de disputa judicial, Facebook enviou ao requerente um CD com 1200 páginas, contendo informações sobre amigos, contatos, informações do *feed*, todas as fotos e páginas em que Max já tinha clicado e toda propaganda que ele já tinha visto naquela rede social (SCHNEIER, 2015).

Além de novas tecnologias permitirem aos agentes econômicos a avaliação mais precisa e detalhada do comportamento de todos que participam do mercado, o modelo de relacionamento da rede ainda moldou-se pela utilização de algoritmos que permitem a automatização tanto de práticas comerciais na Web 2.0, como o marketing diferenciado e segmentado na economia de produção flexível, quanto de ações estatais.

Nesta nova forma de marketing e de produção, notou-se que a produção e a divulgação em massa de produtos e serviços já tinham saturado os mercados industriais (MENDES, 2015). Assim, produtos como carros, televisores, geladeiras e outros eletrodomésticos já estavam presentes na maioria das casas das pessoas com poder para aquisição, o que levou à estagnação dos mercados de massa (PIORRE & SABEL, 1984, *apud* MENDES, 2015). A solução vislumbrada pelo mercado consistiu na criação de produtos e serviços cada vez mais voltados aos públicos especializados, mais competitivos que os massificados.

Nesse sentido, ao passo que a produção em massa serviu para expandir o alcance de vendas de produtos e de prestação de serviços padronizados e a custo baixo, o modelo fundado na especialização destina-se à individualização dos mercados e consumidores, fazendo surgir o que se chama “economia da informação pessoal”, “economia de massa customizada” ou “economia de produção flexível”. Assim, passou-se a ver na customização e na constante inovação a fonte da lucratividade.

Como a exclusividade passou a orientar a criação dos novos produtos e serviços, conhecer os públicos especializados tornou-se imperativo aos agentes econômicos não apenas conhecer muito bem os grupos específicos de consumidores, mas também realizar a divulgação direcionada também de forma especializada. Daí o surgimento do marketing diferenciado e segmentado.

Tanto a criação inovadora especializada quanto o marketing diferenciado e segmentado dependem da obtenção de informações precisas e em grande quantidade dos consumidores pertencentes ao nicho de atuação do fornecedor, o que se tornou possível com o desenvolvimento das novas TICs, as quais viabilizam a coleta e o armazenamento de grande quantidade de dados dos consumidores, bem como seu tratamento para obtenção de aferições (MENDES, 2015).

Por conseguinte, no contexto da sociedade em rede, surgiu a microeconomia da interceptação de dados ou microeconomia da intrusão. Paralelamente à necessidade de obtenção de informações específicas sobre os consumidores, as tecnologias viabilizaram a coleta e o armazenamento de quantidade crescente de dados, a ampliação das redes de comunicação e de troca de informações, o maior uso de dispositivos móveis, a disseminação de sensores em cidade, objetos e pessoas (SILVEIRA, 2017b).

Ao lado disso, novos produtos e serviços passaram a ser disponibilizados com base na internet das coisas, isto é, em redes de conexão entre objetos físicos embutidos com softwares, sensores e conectividades que permitem a coleta e a troca de dados sobre o aparelho e os usuários. Circuitos fechados de televisão (CCTV ou *closed circuit television*) que podem ser instalados em dispositivos espalhados pelos ambientes físicos, por exemplo, permitem a identificação e a coleta de dados para reconhecimento facial e biometria.

A internet das coisas tem também permitido monitorar os indivíduos por meio de dispositivos instalados em telefones celulares, passaportes e cartões de identidade, por exemplo, com base em tecnologias como *near field communication* (NFC) ou comunicação por campo de proximidade (CCP), assim como por identificação por radiofrequência (MURRAY, 2010). Com essa inovação, é possível realizar a comunicação de dispositivos sem contato e sem fio, bastando sua proximidade, tal como já se faz com a abertura de carros pela identificação da proximidade entre chave e porta ou pagamento por meio de cartões magnéticos aproximados de máquinas. Tags de chips de radiofrequência e *near field communication* podem ser adicionados a qualquer equipamento, o que significa que a internet das coisas e a internet dos dados estão começando a se fundir. O crescimento do uso dos celulares para comunicação é um campo em que isso já acontece.

A coleta de dados por companhias efetiva-se especialmente sem o consentimento inequívoco dos usuários, a despeito de o Marco Civil da Internet exigir o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais (art.7º, IX) e vedar a guarda de dados excessivos à finalidade para a qual foram coletados (art. 16, II). A Google Brasil Internet Ltda., por exemplo, foi investigada no Inquérito Civil

Público nº 1.27.000.001406/2015-03 que resultou no ajuizamento da Ação Civil Pública nº 25463-45.2016.4.01.4000 perante a 2ª Vara da Justiça Federal no Piauí, em razão de analisar o conteúdo de e-mails com objetivo comercial de produzir publicidade direcionada.

Embora na sentença prolatada em janeiro de 2018 tenha sido considerado suficiente o consentimento fornecido pelos usuários quando abriam a conta perante a empresa, o que fundamentou o reconhecimento da licitude da conduta impugnada, a Google anunciou em meados de 2017, que deixaria de escanear o conteúdo dos e-mails dos usuários de Gmail. Reconheceu, assim, que adotava essa medida a fim de realizar a segmentação de anúncios (THE GUARDIAN, 2017).

Além de práticas como essas no mercado, a sociedade em rede também tem suas implicações para o estado, já que este também faz uso de tecnologias pautadas na coleta e no tratamento de dados para implementar os serviços prestados e executar políticas públicas. Portais de órgãos públicos tornaram-se vias para obtenção de informações sobre o governo, realização de reclamações a ouvidorias e efetivação de pagamentos devidos ao estado, por exemplo.

Ademais, as atividades que envolvem vigilância também são beneficiadas pelas novas tecnologias da informação e da comunicação, notadamente por meio da coleta e do uso de dados pessoais dos indivíduos e das empresas. Fountain (2015) analisa a formação de um Estado Virtual, no qual a informação cada vez mais flui por meio da internet em vez de canais burocráticos formais tradicionais, gerando mudanças estruturais.

O Decreto nº 8.789/2016, por exemplo, passou a permitir a permuta e o compartilhamento entre órgãos do governo federal de dados dos cidadãos brasileiros como endereço, estado civil e vínculo empregatício, a fim de monitorar políticas públicas tais como a concessão de benefícios, evitando eventuais fraudes e barateando a prestação dos serviços.

Ao lado disso, bancos de dados genéticos já são mantidos pelo estado brasileiro e destinam-se a melhorar as atividades de persecução criminal. O artigo 9º-A da Lei de Execução Penal (Lei nº 7.210/84), introduzido pela Lei nº 12.654/12, a qual passou a prever a obrigação de condenados a crimes dolosos praticados com violência de natureza grave ou por qualquer crime hediondo a submeter-se à identificação de seu perfil genético por meio de extração de seu ácido desoxirribonucleico – DNA, a fim de que tal dado seja armazenado para eventual consulta futura. Essa medida já permitiu a identificação de autoria

de delitos[1], mas teve sua constitucionalidade questionada perante o Supremo Tribunal Federal por meio do Recurso Extraordinário nº 973837, pendente de julgamento, no qual são discutidos os limites dos poderes do Estado e eventual violação ao direito constitucional a não se incriminar (Constituição Federal, art. 1º, III, art. 5º, X, LIV e LXIII).

O uso de dados pessoais pelo estado realiza-se não apenas para a prestação de serviços públicos e para implementação de políticas públicas, mas também na tarefa de vigilância dos cidadãos. Essa realidade foi amplamente divulgada em todo o mundo com as declarações de Edward Snowden, ex-administrador de sistemas da Agência de Inteligência dos Estados Unidos (*Central Intelligence Agency* – CIA) e ex-contratado da Agência de Segurança Nacional do mesmo país (*National Security Agency* – NSA), realizadas por meio dos jornais The Guardian e The Washington Post. As declarações referiam-se a programas do sistema de vigilância da NSA sobre informações e comunicações na internet e em ligações telefônicas. A Agência desenvolveu práticas como usar localizações das pessoas a partir de telefones celulares para associação entre alvos ou para analisar se há perseguição a seus agentes (SCHNEIER, 2016).

O aspecto que gera questionamento não consiste no uso de tecnologias para investigação dos alvos, mas na disseminação da vigilância sobre todo cidadão, investigado ou não. De fato, ao passo que historicamente a vigilância era cara e difícil, a tecnologia e, de forma especial, a internet passou a viabilizar o rastreamento das ações na rede e a coleta e o armazenamento muito mais baratos de dados. Por conseguinte, se o estado, antes, investigava um suspeito específico e, para isso, despendia considerável quantidade de recurso material e humano, agora a vigilância tornou-se mais barata e fácil e, portanto, massificada, camuflada e automática (SCHNEIER, 2016).

Em face dessa realidade, em 2015, o escritório do Comissário de Privacidade dos Dados Pessoais (*Privacy Commissioner for Personal Data* - PCPD) de Hong Kong recebeu recorde de inquéritos referentes às tecnologias de informação e comunicação, em um total de 18.456, e 1971 queixas, dentre as quais 40% referiam-se à utilização de dados pessoais sem o consentimento dos usuários (786 casos), 37% ao propósito e modo de coleta de dados (722 casos), 13% à segurança de dados (252 casos) e 8% aos pedidos de acesso /

[1] A título de exemplo, pode-se mencionar casos de estupro solucionados anos após seu acontecimento com base na coleta de material genético inserido em banco de dados na Polícia Civil do Distrito Federal, na Polícia Técnico-Científica da Secretaria de Segurança Pública e Administração Penitenciária de Goiás e na Polícia Técnico-Científica do Paraná. Casos disponíveis em <https://www.correiobraziliense.com.br/app/noticia/cidades/2017/12/26/interna_cidadesdf,649883/exames-de-dna-auxiliam-a-policia-a-identificar-assassinos-e-estuprador.shtml>; http://www.ssp.go.gov.br/destaques/policia-tecnico-cientifica-desvenda-crime-de-estupro-por-analise-de-dna.html; http://www.policiacientifica.pr.gov.br/modules/noticias/article.php?storyid=115.

correção de dados (156 casos). Um dos comissários do órgão, Stephen Kai-yi Wong apontou o cenário observado a partir do recorde de reclamações:

> "O rápido desenvolvimento das tecnologias de informação e comunicação, o uso de *big data* e da computação em nuvem mudarão ainda mais as maneiras pelas quais os dados pessoais dos indivíduos são coletados, armazenados e usados. Os recentes incidentes de vazamento de dados envolvem grande volume de dados pessoais e são, em grande parte, atribuídos às questões de segurança da Internet (PRIVACY COMMISSIONER FOR PERSONAL DATA, 2016, tradução nossa).

A despeito dessa crescente vulnerabilidade dos usuários, estima-se que, até 2020, trinta e sete milhões de dispositivos estarão conectados à internet (EVANS, 2012).

Diante desse cenário, indicando a formação da economia informacional, em 2011, o Fórum Econômico Mundial descreveu os dados pessoais como uma nova classe de bens no mercado e identificou a existência de uma série de companhias destinadas a coletar, analisar e comercializar informações pessoais, como BlueKai, Rapleaf, Accurint e Avarto (FÓRUM ECONÔMICO MUNDIAL, 2011), o que indica a relevância de tais informações pessoais para os atuais modelos de mercado, incluindo-se aquele que se desenvolve na internet[2].

Foi em face dessa realidade que, no Fórum Econômico Mundial, ao se apontar os dados pessoais como um novo elemento de mercado, tão relevante quanto o capital e o trabalho, destacaram-se categorias de dados com tal potencial, classificando-os em subcategorias dados de identidade digital, comportamentais, financeiros, de saúde, institucionais, entre outros[3].

---

[2] Na ocasião da realização do Fórum Econômico Mundial de 2011, dentre as formas de uso de dados pessoais nos mercados, destacaram-se algumas das utilidades desses elementos para as empresas, tais como a redução de custos na busca por produtos por meio da filtragem personalizada das ofertas, realização de análises de riscos sobre os consumidores, melhora nos resultados dos atos de marketing por meio do direcionamento das divulgações.

3 "•Identidade digital (nomes, endereços de email, números de telefone, endereços físicos, informações demográficas, informações de perfis de redes sociais, por exemplo);
• Relações com outras pessoas e organizações (perfis online e listas de contatos);
• Contexto real e virtual, atividades, interesses e comportamentos (registros de localizações, cliques, pesquisas, históricos de navegação e dados de calendários pessoais);
• Conteúdo de comunicações e logs (emails, SMS, chamadas telefônicas, mensagens em redes sociais);
• Mídia produzida, consumida e compartilhada (em texto, áudio, foto, vídeo e outras formas de mídia);
• Dados financeiros (transações, contas, pontos de crédito, bens físicos e virtuais);
• Dados de saúde (histórico médico, logs de dispositivos médicos, prescrições médicas e cobertura de seguros de saúde);
• Dados institucionais (dados governamentais, acadêmicos e de empregadores) (tradução livre)".
ASCQUISTI, Alessandro; BÖHME, Rainer; HUI, Kai-Lung; SPIEKERMANN, Sarah. "The challenges of personal data markets and privacy". Electron Markets, Institute of Information Management, University of St. Gallen, 2015. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em 14 de maio de 2016.

A diversidade do rol provoca a percepção de que todo participante do mundo digital, em algum momento, é alvo da captação de dados. Apesar disso, na realidade brasileira, muitos dos usuários demonstram não ter ciência de sua vulnerabilidade na rede, sendo memorável, quanto ao tema, o espanto gerado com a divulgação das páginas <http://tudosobretodos.se> e <http://nomesbrasil.com>.

O sítio <http://tudosobretodos.se> foi disponibilizado na rede em 2015, com hospedagem na Suécia, e oferece e vende informações como nome completo, endereço e nomes de vizinhos, sendo que os administradores declaram obter todos os dados de fontes públicas. Embora tenha permanecido desativado em razão da quantidade de denúncias recebidas, voltou à disponibilidade em 2017. Já o <http://nomesbrasil.com> oferecia o número de cadastro de pessoa física – CPF a partir do nome consultado e permanece desativado.

A divulgação da existência desses sítios eletrônicos foi ocasião em que muitos dos brasileiros se depararam ineditamente com sua condição de exposição.

Além disso, a variedade do rol desperta o questionamento sobre a ciência por parte desses usuários acerca de sua condição de fornecedores de seus dados como matérias primas. Isso porque, além das situações em que o fornecimento de informações é voluntário, a tecnologia desenvolvida permite a captação de dados também por observação, mediante, por exemplo, a análise de histórico de localizações do usuário, e por inferência, como o fornecimento de determinado nível de crédito a partir de um histórico financeiro (ASCQUISTI; BÖHME; HUI; SPIEKERMANN, 2015).

A amplitude das categorias de dados apresentadas pelo Fórum Econômico Mundial indica, ainda, a existência de duas possíveis abordagens dessa realidade, isto é, de dois planos de envolvimento dos usuários.

Por um lado, o do modelo de mercado, no qual são utilizadas práticas como o marketing de banco de dados (OECD, 2013) e no qual muitas aplicações são fornecidas como gratuitas enquanto, em verdade, o usuário paga com uma moeda de troca valiosa: seus dados pessoais (DENARDIS, 2014)[4]. E, assim como as mercadorias físicas, esse ativo precisa circular para ter seu valor (ACQUISTI, TAYLOR e WAGMAN, 2016)[5].

4 DENARDIS, Laura. “The global war for Internet governance”, New Haven, CT: Yale University Press, 2014, p.231.

5 Sobre o valor monetário da privacidade e dos dados pessoais: ACQUISTI, Alessando; TAYLOR, Curtis; WAGMAN, Liad. “The Economics of Privacy”, 2016, Journal of Economic Literature, 442. Disponível em < https://pubs.aeaweb.org/doi/pdfplus/10.1257/jel.54.2.442>. Acesso em 16 de março de 2018.

Diante disso, desde o início do desenvolvimento do mercado de dados, suspeitou-se da possibilidade de que os direitos de privacidade pudessem desafiar o desenvolvimento dos dados pessoais como bem de mercado (ACQUISTI e VARIAN *apud* ASCQUISTI *et al*, 2015) e chegou-se a sustentar que a ética inerente ao direito à privacidade tornaria antitética à ideia de um mercado de tal natureza (SAMUELSON apud ASCQUISTI *et al*, 2015).

Os dados, no entanto, efetivamente adquiriram tal relevância para o mercado, no movimento de migração do valor da ideia e do domínio da técnica para os dados (MAYER-SCHNONBERGER, 2013). Se, inicialmente, a relevância para a competitividade pertencia a quem detinha as ideias inovadoras e, posteriormente, a quem dominava as técnicas de gerenciamento de dados, a disseminação do uso de big data melhorou os instrumentos de tratamento dos dados e as ideias de uso dessas informações divulgam-se muito rapidamente. Dessa maneira, pode-se identificar nos próprios dados a fonte de valor no mercado atual, não sendo outra a razão pela qual, já em 2008, a Google, por exemplo, adquiriu a fornecedora de dados da Farecast, a ITA Software, por US$ 700 milhões (MAYER-SCHNONBERGER, 2013).

Apesar disso e de o desenvolvimento de mecanismos como tecnologias de reforço da privacidade (*privacy-enhancing technologies*) ser constante objeto de dedicação para concretizar a proteção dos dados pessoais, o mercado se desenvolve na contramão desse esforço (ZITTRAIN, CRAWFORD e BREM, 2012).

Nesse cenário, observa-se um movimento de integração entre a internet das coisas e a as práticas de coleta e uso de dados pessoais, especialmente no modelo de mercado denominado SMAC (*social, mobile, analytics, cloud*), o qual envolve a coleta de dados dos consumidores a partir de aparelhos como telefones móveis para posterior análise e uso no desenvolvimento de inovações (SMITH, 2015). O crescimento do uso de tais tecnologias e de sua presença na vida dos usuários, dos governos e das companhias torna viável o conhecimento da localização, dos movimentos e dos hábitos de cada pessoa conectada, sem que essa realidade seja de seu conhecimento e possa ser por ela controlada (MURRAY, 2013).

Nessa realidade, a participação dos usuários no universo da internet das coisas[6] costuma ser realizada por meio de seu consentimento no fornecimento e na permissão

6 Sobre a aproximação internet dos dados e das coisas <http://insights.wired.com/profiles/blogs/the-convenience-privacy-trade-off-on-the-internet-of-things#axzz4B2cWRUNs>.

para tratamento e disseminação dos dados, o que se faz por meio da adesão aos "termos de uso", não convidativos à leitura por esses usuários de aplicações e serviços.

De outro lado, há o plano de envolvimento dos dados pessoais dos usuários em face do Estado. A disponibilidade de instrumentos facilitadores da reunião de dados e de acesso às informações particulares é vista também por este agente como mecanismo para a realização de funções estatais, como investigações criminais e para planejamento, execução e avaliação de políticas públicas.

Aliás, a noção de proteção de dados surgiu inicialmente nos Estados Unidos no início dos anos 1960, exatamente como necessidade de proteção da população contra a intervenção estatal na esfera privada, reação que culminou na aprovação do *Privacy Act* em 1974. Vê-se que, assim como se deu historicamente com a construção de uma ideia de direitos fundamentais, a proteção de direitos fundamentais específicos relacionados aos dados pessoais tem como ponto de partida a necessidade de resguardo do indivíduo em face do Estado.

Além desses dois planos de sujeição dos usuários quanto aos seus dados pessoais, há dois campos de relações de tensão entre os participantes desse cenário. Enquanto divergências de interesses na disponibilização e no tratamento dos dados podem existir entre os usuários e os agentes econômicos e estatais, as corporações que utilizam tais dados também têm seus conflitos com os interesses do governo quanto ao nível de liberdade no uso dessa commodity, o que tem representado um problema de regulação.

No mundo virtual, a privacidade se torna, então, motivo de preocupação central para o usuário, quando este tem consciência da realidade vivenciada, e para quem se importa com a regulação dessa área. Este, por sua vez, vê-se em um paradoxo, pois usufruir da internet tem implicado participar desse mercado de dados, ao passo que o prejuízo social e econômico de não participar da rede pode ser ainda maior, como destacado por Lessig (2004).

De fato, um dos tipos de poder da rede consiste, justamente, no de dela participar, o que implica uma relação de inclusão e exclusão apontada por Castells (2015)[7]. Embora Castells identifique o poder de criar redes como o mais sobressalente, não se ignora que o poder de conectar-se em rede tem a imprescindibilidade de permitir o desenvolvimento

7 Ao tratar dos efeitos de comunicação em uma sociedade em rede global, o autor identifica quatro tipos de poder nela caracterizados: poder de conectar-se em rede ("networking power"), poder da rede ("network power"), poder em rede ("networked power") e poder para criar redes ("network-making power"). CASTELLS, Manuel. "O Poder da Comunicação". São Paulo/Rio de Janeiro: Paz e Terra, 2015, p. 72.

de capacidade de criação de redes e de vias de interação por meio dos quais cada ator pode concretizar seus interesses.

Nessa sociedade atual, em que a conexão e as informações podem ser reconhecidas instrumentos de poder, o estado da arte é, também, de constantes tentativas de ajustes legais. No Brasil, por exemplo, ainda se luta por concretizar uma norma específica de proteção de dados, por meio dos Projetos de Lei nº 4060/2012, 181/2014 e 5276/2016[8], embora de forma tímida tenha sido iniciada tal proteção no Marco Civil da Internet e em sua regulamentação no recente Decreto nº 8.771/2016. Ao lado, a União Europeia, por meio de seu Parlamento, adotou recentemente a Diretiva (UE) 2016/680 e o Regulamento Geral Sobre Proteção de Dados (Regulamento 2016/679), já em reforma aos atos normativos existentes (notadamente a Diretiva da União Europeia de Proteção de Dados nº 95/76). O Reino Unido está no seio da discussão da reforma de sua *Investigatory Powers Bill*.

A partir desse contexto, pode-se sustentar que, no atual estágio da sociedade de informação, é relevante compreender como tem sido vivenciada a tutela dos dados pessoais e da privacidade nesse cenário de novos modelos de interações. A riqueza da situação analisada está em que, no contexto configurado na internet, tanto consumidores quanto fornecedores de novos produtos e serviços e o estado usufruem benefícios, além de que esse ambiente não apenas mitiga a privacidade dos cidadãos, mas também pode lhes assegurar maior segurança e melhores serviços[9].

Por outro lado, a despeito de serem mais frequentemente apresentadas, no mundo jurídico, reflexões sobre os prejuízos para os usuários advindos das ações de mercado baseadas em dados pessoais na internet, não se pode ignorar a existência de uma relação simbiótica entre tais usuários e os provedores de serviços "gratuitos" na rede (MURRAY, 2006). Nessa linha, percebe-se que significativo poder da sociedade da informação consiste em tornar seus usuários livres, já que, nela, é possível adquirir bens, usufruir de serviços e acessar conteúdos e informações mais facilmente e de forma personalizada, além de se comunicar mais fácil e livremente.

No entanto, já não se ignora a existência de um preço a ser pago por essas possibilidades de exercício da liberdade: uma vigilância, que, em geral, é velada para o

---

[8] Em seu artigo 20, o Projeto de Lei nº 5276/2016 prevê o direito do titular dos dados de "solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade".

9 David Brin, por exemplo, em "The Transparency Society", apresenta uma visão pessimista do direito à privacidade, reconhecendo ser tarde para prevenir a invasão na esfera privada pelos coletores de dados pessoais, cujos mecanismos não podem ser acompanhados pelos avanços legislativos. BRIN, David. "The Transparency Society". Basic Books, 1999, 384 p.

usuário e pode representar violação aos direitos à privacidade e à tutela de dados pessoais de seu titular. Tal violação, como salientado, sequer costuma ser percebida pelos usuários – que têm seus dados vigiados e coletados – como ameaçadora ou danosa.

Constatadas tais práticas e seu crescimento nas últimas décadas, dentre os vários estudos sobre privacidade dos usuários da rede no controle sobre seus dados pessoais, o relatório O Futuro da Privacidade (ANDERSON e RAINIE, 2014) expõe panorama sobre as perspectivas da privacidade no mundo digital, com foco no compartilhamento de dados pessoais. Em tal estudo, promovido pelo *Pew Research Center*, nos Estados Unidos, a partir de consulta a 2511 especialistas dentre desenvolvedores de tecnologia, pesquisadores, gestores, políticos, comerciantes e analistas, concluiu-se que 55% dos entrevistados não acredita que, até 2025, terá sido criado um regime de privacidade e de infraestrutura asseguradora da privacidade capazes, ao mesmo tempo, de garantir a inovação empresarial.

Ademais, a partir da pesquisa realizada, no jogo de forças na rede, continuará a predominar a capacidade de imposição de regras e comportamentos pelos mercados e pelos governos, cada um em prol de seu interesse, em detrimento do direito à privacidade dos usuários, e não o inverso. A pesquisa, embora realizada apenas por meio de entrevistas a representantes dos *multistakeholders*, ou seja, dos múltiplos setores atuantes na rede, lança questionamentos de interesse de todos que fazem parte da sociedade da informação, especialmente no que diz respeito às perspectivas do direito à privacidade e de sua conciliação com o mercado e o governo.

Diante disso, nos diversos estratos regulatórios existentes, normas e princípios são desenvolvidos com o intuito de obter uma conciliação entre mercado, Estado e sociedade no que diz respeito à utilização de dados e informações pessoais na internet. A despeito disso, no mundo dos fatos, a privacidade precisa ser exercida não apenas sob uma perspectiva jurídica, mas também econômica e tecnológica, o que deve ser especialmente observado, na medida em que as normas jurídicas não têm acompanhado os desenvolvimentos econômicos e, sobretudo, tecnológicos capazes de afetar o exercício desse direito fundamental.

É a partir desse cenário que se pretende investigar os valores dos dados pessoais no momento atual do Brasil, a fim de, a partir de teorias regulatórias aplicáveis a esse ciberespaço e empregadas como referencial teórico, procurar identificar qual delas, atualmente, mais bem explica a realidade regulatória brasileira quanto ao direito à tutela daqueles dados.

As hipóteses sugeridas consistem em que os usuários da internet no Brasil não têm desempenhado a força de estabelecimento de normas como sugerido em teorias regulatórias tais qual o comunitarismo em rede, sendo os desenvolvedores das tecnologias e os agentes econômicos as principais fontes de regulação das práticas com dados pessoais na rede. Isso porque, apesar dos esforços de conciliação entre interesses coletivos (econômicos e do estado) e tutela de dados, a arquitetura da rede mitiga a liberdade dos usuários em participar conscientemente da dinâmica envolvendo seus dados e atrapalha a concretização da autodeterminação informativa.

Para a tarefa sugerida e dentre os objetivos do estudo, propõe-se analisar a existência de valores dos dados pessoais que venham sendo utilizados para justificar a defesa da liberdade em sua captação, tratamento e disseminação por agentes econômicos e por uma parcela de agentes estatais defensora da utilidade pública dos dados pessoais e abordar de que forma tem sido tratada a tensão entre a liberdade e a regulação do uso de dados, com enfoque no exame dos discursos de cada um dos setores atuantes na rede (usuários, agentes privados e estado) e de sua capacidade em participar ativamente da governança na internet. Além dessa análise de posicionamento, também se propõe a analisar a capacidade de cada setor de legitimar seu discurso.

No primeiro capítulo, tendo em vista que as concepções de privacidade e de dados pessoais estão inseridas no contexto mais amplo de diferenciação entre público e privado, serão estudadas mudanças no paradigma da relação público-privado até a pós-modernidade. A premissa dessa análise consiste em que inexiste um espaço que seja público ou privado por natureza, mas que essa delimitação está sujeita a processos de construção social e histórica. A partir disso, serão abordadas as concepções de privacidade e de dados pessoais, pois se trata de conceitos relevantes para o presente estudo.

Posteriormente, serão analisadas as abordagens regulatórias sobre o ciberespaço como forma de apresentação do referencial teórico do estudo, sob o qual será analisada a problemática. Serão abrangidos, então, o ciberlibertarianismo, o movimento cypherpunk, o ciberpaternalismo, o comunitarismo em rede, a regulação responsiva e a regulação descentrada, sob a luz das quais será analisada a realidade brasileira com ênfase no papel do usuário[10].

[10] Vale registrar que, apesar da proposta de abordagem de tais teorias como referencial teórico, a presente pesquisa faz-se no bojo da Linha de Pesquisa Transformações na Ordem Social e Econômica e Regulação, mas dentro da sublinha Regulação Social e Políticas Públicas de Educação, Ciência, Tecnologia e Inovação. Assim, não se tratando da sublinha Regulação e Transformações na Ordem Econômica, o perfil da abordagem será

No quarto capítulo, o objeto de estudo consistirá na discussão sobre o valor dos dados pessoais no ciberespaço, a partir dos discursos dos atores do mercado digital e do estado sobre tal temática. No mesmo capítulo, será analisada, a partir de pesquisas realizadas com usuários, qual a sua percepção acerca das práticas com seus dados na rede e de sua intenção de proteção de sua autodeterminação informacional, visando, assim, delinear qual seu discurso acerca desse direito. Uma vez que essa análise realizar-se-á no mesmo capítulo em que os discursos de cada grupo de interesses nesse cenário regulatório *multistakeholder*[11], será estudado o papel do consentimento como tentativa de expressão do discurso dos indivíduos sobre a realidade estudada.

Examinada a situação dos usuários será avaliado, no quinto capítulo, a partir dos precedentes identificados no Supremo Tribunal Federal e no Superior Tribunal de Justiça relacionados à temática de privacidade e dados pessoais na internet, como os Tribunais do país têm tratado esse tema e sua relação com os novos formatos de relação social viabilizados pelas novas tecnologias contemporâneas. Ainda, o cenário traçado será examinado sob a luz das teorias que compõem o marco teórico, de modo a tentar identificar qual tem melhor poder explicativo da realidade brasileira nessa temática.

interdisciplinar, como proposto na citada Linha, mas voltado principalmente para dilemas contemporâneos referentes a implicações sociais da tecnologia e inovação para usuários.

[11] O termo *stakeholders* foi cunhado por Robert Edward Freeman, na década de 1980, referindo-se a grupos que compõem uma organização social e afetam e podem ser afetados por esse todo. Embora muitas distintas definições de *stakeholder* tenham surgido desde então, todas pressupõem interação entre esses diversos grupos na formação do todo que é a organização e uma dinâmica em que se busca equilibrar interesses de diferentes stakeholders (MASCENA, 2013).

2. PARADIGMAS DA RELAÇÃO PÚBLICO-PRIVADO NA PÓS-MODERNIDADE E DESENVOLVIMENTO DAS NOÇÕES DE PRIVACIDADE E DE TUTELA DE DADOS PESSOAIS

Tendo em vista que as concepções de privacidade e de dados pessoais estão inseridas no contexto mais amplo de diferenciação entre público e privado, neste tópico, serão estudadas mudanças no paradigma da relação público-privado até a pós-modernidade. O propósito consiste em analisar se, no paradigma atual do Estado Democrático de Direito, os usuários da internet têm tido seus direitos à privacidade e à tutela de dados pessoais na internet concretizados.

2.1. Relação público-privado na pós-modernidade

Trazida a noção de paradigma[12] como pressuposto do estudo do direito, é possível reconhecer distintos momentos do constitucionalismo nos quais foram também diferentes as relações entre os Poderes estatais e a participação do Estado na tutela de direitos individuais. Cada paradigma, assim, constitui as premissas que, em cada contexto, orientam o estudo do direito, surgindo como ruptura do paradigma anterior quando encontradas as contradições deste (CARMO, 2010). No tempo, cada paradigma orienta, dentre outros aspectos do direito, a visão da relação entre o público e o privado.

Uma possível delimitação de paradigmas do direito constitucional é aquela adotada por Carvalho Netto (2004) ao questionar como esses parâmetros influenciam a atividade de interpretação constitucional. Nesse propósito, o autor separa dois momentos históricos principais, reunindo a Antiguidade e a Idade Média em um paradigma pré-moderno e os períodos posteriores, da modernidade, nos paradigmas do Estado de Direito, do Estado Social e do Estado Democrático de Direito.

Na forma de organização pré-moderna, o próprio direito confundia-se com religião, moral, tradição e costumes e a justificativa de cada um desses elementos de organização social ultrapassava o que pudesse ser racionalmente identificado e conhecido.

[12] A noção empregada é a apresentada por Thomas Samuel Kuhn em sua filosofia da ciência e, portanto, usa-se o termo paradigma como o conjunto de compromissos conceituais, metodológicos, técnicos e teóricos reconhecidos em um campo científico em determinado lugar no tempo e no espaço como pressupostos de uma comunidade científica. KUHN, Thomas. S. A estrutura das revoluções científicas. São Paulo: Perspectiva, 1991.

Nessa fase, a justificativa da existência do direito era transcendental e não se permitiam questionamentos sobre as formas de organização sociais estabelecidas, mantendo-se também os privilégios e as exclusões inerentes à hierarquia de castas.

Carvalho Netto (2004) aponta a ocorrência da modificação desse parâmetro ao longo de ao menos três séculos, com o abandono de entraves feudais e o desenvolvimento de formas capitalistas de produção. Nesse sentido:

> "As intuições da moral individual racionalista, vistas como verdades matemáticas inquestionáveis, colocam em xeque a tradição, agora reduzida a meros usos e costumes sociais, que, para os homens da época, só pode ser explicada como o resultado da cognição histórica e que, assim, deveria ser alterada pela imposição de normas racionalmente elaboradas pelos homens enquanto sujeitos de sua história, inaugurando ou remodelando um tipo recente de organização política, os Estados nacionais" (CARVALHO NETTO, 2004).

Uma concepção de racionalidade passa a ser exigida e empregada como elemento legitimador da existência das normas jurídicas, de modo que o Direito somente pode ser então entendido como um conjunto de leis racionalmente elaboradas, sem fundamento na religião. De todo modo, o paradigma era o do jusracionalismo, pois as ideias abstratas e de validade universal das quais adviriam as normas jurídicas estavam no Direito Natural.

Além de gerais e abstratas, as normas jurídicas eram essencialmente negativas, estabelecendo os limites do exercício das liberdades individuais, de modo que a privacidade, por exemplo, poderia ser colocada em prática até o limite em que atingisse a privacidade do próximo, o que caracterizou o Estado como mínimo. Entre os Poderes estatais, a prevalência era do Legislativo, na medida em que, desde o jusracionalismo, depositava-se nas leis a legitimidade da atuação do Estado e dos indivíduos.

Com os excessos oriundos da concretização das liberdades sem ingerência estatal, notadamente a liberdade de exploração do homem, a contrapartida foi o surgimento dos movimentos socialistas, comunistas e anarquistas, que passaram a contestar os abusos cometidos sob a luz da legalidade formal. Assim, o positivismo jurídico clássico, no qual não era considerada a justiça como valor, passou a servir de fundamento para ações abusivas. Como apontado por Lunardi:

> "o erro dos positivistas estava na crença de que a introdução de leis gerais e abstratas – isto é, de textos de lei – daria segurança jurídica e poderia, portanto, proteger, satisfatoriamente, os bens jurídicos que devem ser salvaguardados" (LUNARDI, 2012).

A reação, portanto, foi a demanda por direitos coletivos e sociais, inaugurando-se o paradigma do Estado Social, ao qual se atribuiu a obrigação de promover direitos e não mais atuar de maneira mínima. Assim, o Poder do qual mais se esperava a promoção de políticas para concretização dos direitos era o Executivo, mas mesmo este passou a ser alvo de contestações, notadamente em razão das práticas abusivas cometidas nos campos de concentração (CARVALHO NETTO, 2004).

Confrontado aquele Estado Social, não apenas pelos citados abusos, mas também pela evidência da incapacidade da força estatal em promover os direitos sociais na sociedade cada vez mais plural e complexa, inaugurou-se o paradigma do Estado Democrático de Direito. O contexto é o da pós-modernidade, marcado pelo reconhecimento de suas próprias limitações e das limitações da racionalidade. Assim, observando ter sido muito pretensiosa a modernidade quanto à suficiência da racionalidade humana, a pós-modernidade nega o mito da possibilidade de identificação de verdades absolutas e sempre válidas e reconhece-se como um projeto inacabado, como alertado por Carvalho Netto e Scotti (2011).

Isso tem implicações na criação do direito e na forma de atuação do Estado na concretização dos direitos individuais. Se, no Estado de Direito, prevaleceu o Poder Legislativo, criando as leis das quais se retirava a legitimidade de ação, e se no Estado Social o foco estava no Poder Executivo, do qual se esperava a promoção dos direitos sociais, ambos mostraram a possibilidade de serem abusivos. Assim, no Estado Democrático de Direito, a esperança reside no Poder Judiciário.

Reconhecendo que cada um desses paradigmas tem consequências sobre a atividade hermenêutica ou interpretativa do juiz, Carvalho Netto (2004) salienta que, no novo paradigma, exige-se do intérprete do direito que tome decisões trabalhando construtivamente não apenas as regras estabelecidas na dinâmica do tudo ou nada, mas também dos princípios, adequando as decisões a cada caso concreto:

> "podemos ver como se verificou um incremento das exigências relativas à postura do aplicador da lei e do responsável pela tutela jurisdicional que se assenta em uma crescente capacidade de sofisticação da doutrina e da jurisprudência para fazer face aos desafios decorrentes do processo de contínuo aumento da complexidade da sociedade moderna" (CARVALHO NETTO, 2004).

Ao lado disso, isto é, além da necessidade de que o julgador lance mão dos princípios como valores fundamentais na atividade hermenêutica (LUNARDI, 2012), o

próprio estabelecimento dos princípios e das regras vigentes depende da observância de critérios para que essas normas possuam legitimidade.

Para Habermas (2002), o critério legitimador é procedimental, de modo que a teoria do direito e a teoria da democracia guardam relação interna conceitual, ou seja, no Estado Democrático, mostra-se inviável identificar direito sem que haja observância do procedimento democrático em sua criação (HABERMAS, 2002). Nesse sentido, o reconhecimento da norma como direito carece não apenas da possibilidade de coerção estatal para sua implementação, mas de um segundo pressuposto consistente em sua origem no exercício da autonomia e da liberdade dos próprios afetados, o que se garante por meio do procedimento democrático legislativo.

Trata-se, então, de uma questão de legitimidade do direito no paradigma democrático. Tal legitimidade e, portanto, a coercitividade de uma norma jurídica advém de decisões coletivamente vinculativas cuja tomada exige a conciliação entre as autonomias pública e privada (HABERMAS, 2002). Identificando a autonomia pública como a possibilidade de participação do povo soberano no exercício de sua auto-organização e a autonomia privada como os próprios direitos fundamentais de cada sujeito de direitos, Habermas (2002) esclarece que:

> "é a serviço dessa convicção que se põe a idéia de que as pessoas do direito só podem ser autônomas à medida que lhes seja permitido, no exercício de seus direitos civis [autonomia privada], compreender-se como autores dos direitos [autonomia pública] aos quais devem prestar obediência, e justamente deles" (HAMERMAS, 2002).

O instrumento para viabilizar essa conciliação consiste justamente no direito, o qual, ao seu turno, tem como fonte legitimadora o exercício da autonomia pública no procedimento democrático legislativo.

Nos Estados Democráticos atuais, esse procedimento é assegurado por meio da democracia representativa, na qual as escolhas são realizadas com base na manifestação de maiorias nas casas legislativas. Apesar de um dos nortes desses Estados consistir no princípio majoritário nos processos decisórios, é sempre possível que esse mesmo princípio seja utilizado como tentativa de legitimação de escolhas contrárias à concepção material de democracia por meio da sujeição de grupos minoritários à preferência de uma maioria hegemônica.

A via institucional até o momento encontrada nas democracias com divisão tripartite de poderes para contornar essa possibilidade de desvirtuar a democracia representativa consiste na atribuição do poder contramajoritário ao Judiciário. Esse poder pode ser exercido por meio do controle de constitucionalidade das normas criadas pelos representantes no Legislativo ou Executivo e da tutela de interesses de grupos minoritários desprotegidos.

A despeito de a ausência de eleição popular dos membros do Poder Judiciário gerar a chamada dificuldade contramajoritária (BICKEL, 1986), já que podem afastar o poder normativo de criações de representantes eleitos pelo povo, são reconhecidos fundamentos para conferir legitimidade a essa atuação.

Nessa linha, a necessidade de tutela de direitos fundamentais e de proteção das regras do procedimento democrático fundamentam o exercício do poder contramajoritário, tendo em vista a identificação dos direitos humanos com a reserva mínima de justiça e uma perspectiva processualista da jurisdição constitucional (BARROSO, 2016). A concepção de democracia, portanto, não envolve apenas uma perspectiva procedimental, mas também substantiva, nos seguintes termos:

> "A democracia, portanto, para além da dimensão procedimental de ser o governo da maioria, possui igualmente uma dimensão substantiva, que inclui igualdade, liberdade e justiça. (...) Mais do que o direito de participação igualitária, democracia significa que os vencidos no processo político, assim como os segmentos minoritários em geral, não estão desamparados e entregues à própria sorte. Justamente ao contrário, conservam a sua condição de membros igualmente dignos da comunidade política" (BARROSO, 2016).

Dentro do citado paradigma do neoconstitucionalismo, em que há prevalência do Judiciário como instância definitiva de tutela dos direitos, público e Estado já não são identificados como sinônimos. De todo modo, ainda que se atribua ao público (democracia, coletividade) a tarefa de definição dos pilares da vida em sociedade, reconhece-se no Estado um papel relevante na promoção dos direitos. Nesse Estado do neoconstitucionalismo, o Poder Judiciário recebe especial relevância em razão da construção de um ordenamento jurídico composto por normas abertas, conceitos vazios, cláusulas gerais.

De fato, no contexto do neoconstitucionalismo e da substituição do Estado Legislativo de Direito pelo Estado Constitucional de Direito, verificou-se a insuficiência da legalidade formal para a promoção da dignidade da pessoa humana. Perante a percepção de que as mudanças sociais não mais podiam depender, exclusivamente, do Poder Legislativo e

do Executivo, passou-se a outro paradigma do constitucionalismo para permitir que o Judiciário exercitasse a importante função contramajoritária.

Como o nome sugere, o poder contramajoritário consiste na atuação do Poder Judiciário voltada à proteção de minorias contra forças da maioria no Estado Democrático de Direito, já que estas, em geral, refletem nas escolhas legislativas. O próprio Supremo Tribunal Federal passou a fazer referência a um constitucionalismo fraternal, no qual, ao contrabalancear a pura democracia com o pluralismo, há uma preocupação de abrir oportunidades de promoção de direitos fundamentais de segmentos sociais historicamente desfavorecidos.

Em geral, pode-se exemplificar o exercício desse poder por meio das decisões da Suprema Corte em controle de constitucionalidade. Concretamente, há o controle que resulta em ações estatais afirmativas, como a permissão de cotas em universidades públicas e o reconhecimento das uniões estáveis homoafetivas, casos em que a legitimidade da jurisdição constitucional encontra-se na necessidade de conciliação entre o "governo da maioria" e a defesa de direitos fundamentais.

Trata-se, ainda, do poder que permitiu ao Supremo Tribunal Federal, no Brasil, reconhecer a constitucionalidade da ação afirmativa de reserva de vagas em universidades públicas com base no critério étnico-racial como forma de superar e compensar, na sociedade brasileira, um histórico de exclusão e escravidão de afrodescendentes (CARVALHO NETTO e FERREIRA, 2017). A prática desse poder contramajoritário concretizou-se na apreciação, por aquela Corte, da Arguição de Descumprimento de Preceito Fundamental nº 186-2/800, ajuizada pelo Partido Democratas (DEM) com o objetivo de que fosse reconhecida a inconstitucionalidade das cotas na Universidade de Brasília (UnB). Assim:

> "No caso da ADPF nº 186, o papel contramajoritário do Poder Judiciário se reafirma ao assegurar a uma minoria um direito que não passou por uma aprovação de maioria da sociedade, por meio do Poder Legislativo, mas que é componente da identidade constitucional e, por conseguinte, não pode ser desprezado" (CARVALHO NETTO e FERREIRA, 2017).

Vale registrar que, para essa temática, as concepções de maioria e minoria não decorrem do parâmetro exclusivamente numérico, até mesmo porque, a despeito de, por exemplo, as mulheres serem maioria numérica no Brasil, como constatado no último resultado da Pesquisa Nacional por Amostra de Domicílios Contínua do Instituto Brasileiro de Geografia e Estatística (IBGE, 2017), ainda há política afirmativa em seu favor. Trata-se,

por exemplo, da obrigatoriedade de reserva mínima de 10% do tempo de acesso gratuito ao rádio e à televisão à participação feminina (Lei nº 9.696/95, artigo 45, IV).

Portanto, para o exercício do poder contramajoritário, o parâmetro não é simplesmente numérico, mas principalmente histórico, no qual se identifica a trajetória de subjugação de certos grupos aos interesses de outros dominantes por força política, econômica ou jurídica.

Assim, somente por meio da possibilidade de que todos tenham seus direitos e sua dignidade reconhecidos e tutelados pode-se falar em verdadeiro Estado Democrático de Direito. De certa forma, se, durante o procedimento legislativo ordinário, certos grupos não conseguem tutelar seus interesses por meio da criação de normas e políticas públicas, o Poder Judiciário, por meio do contramajoritarismo, mostra-se como via de compensação dessa disparidade. Em outros termos, esse poder contramajoritário pode ser visto como uma das formas dos grupos minoritários de conciliação entre suas autonomias privada (direitos fundamentais) e pública (participação na auto-organização).

Na temática do presente estudo e com retomada de conceitos apresentados alhures, pode-se questionar se, exercendo o poder contramajoritário e a função hermenêutica ampla que lhe é conferida no Estado Democrático de Direito e no neoconstitucionalismo, o Poder Judiciário tem concretizado a tutela da privacidade e dos direitos sobre dados pessoais dos usuários da internet.

Pode-se indagar sobre como tem se dado o exercício desse poder no que tange à tutela da privacidade e da autodeterminação sobre dados pessoais na sociedade da informação. Ainda, considerando que as questões afetas à privacidade e à autodeterminação sobre dados pessoais abrangem a delimitação da relação entre público (estatal e coletivo) e privado, também se pode indagar sobre como tem sido realizada essa delimitação na jurisprudência do Supremo Tribunal Federal, questões que farão parte de parte posterior do trabalho.

2.2. Desenvolvimento da noção de direito à privacidade

Também para subsidiar o exame do papel dos usuários na regulação da privacidade e da tutela de dados pessoais no ciberespaço, pretende-se analisar se houve uma nova configuração da concepção que se tem sobre privacidade, bem como distinguir esse direito daquele à tutela dos dados pessoais.

Na doutrina especializada, aponta-se como menção inédita e expressa da privacidade o texto dos norte-americanos Warren e Brandeis (1980) em uma das publicações da *Harvard Law Review* de 1890.

Muito antes disso, todavia, já havia referências literárias do que hoje se concebe como essência desse direito, ainda que sem menção ao termo. Em verdade, o que contemporaneamente se identifica como traços da privacidade era visto como aspectos da liberdade, sendo possível identificar ainda atualmente a existência de um vínculo entre tais direitos que reforça sua raiz comum e permite buscar no momento pós-Revolução Francesa o marco da concepção da privacidade, já que foi quando a liberdade ganhou proeminência.

De fato, como apontado por Noriji (2005), o princípio da privacidade pode ser buscado em concepções de filósofos como Thomas Hobbes, Robert Price, John Locke e John Stuart Mill, os quais já mencionavam a autonomia dos indivíduos de disposição de sua pessoa e de seus atributos. Dessa sorte, citando Mill, Noriji (2005) aponta que, em meados do século XIX, o filósofo defendia que "os aspectos que só dizem respeito ao indivíduo são absolutamente independentes, resultando ser o indivíduo soberano sobre si, seu corpo e sua mente ('*over himself, over his own body and mind the individual is sovereign*')". As bases da privacidade, então, foram assentadas em noções como liberdade, autonomia e soberania.

O contexto histórico era de pós-Revolução Francesa, com ascensão da burguesia e do iluminismo (CARMO, 2010). A relevância a esta menção está em que, sob o propósito de dar ao indivíduo o valor considerado merecido, notadamente em face dos abusos do absolutismo, passou-se a criar um contexto social favorável ao surgimento de direitos fundamentais conhecidos como de primeira geração, destinados, então, à proteção de cada pessoa em face de arbítrios do Estado e, portanto, com relação direta aos direitos da personalidade (CARMO, 2010).

Para que tais direitos fossem reconhecidos e concretizados, supervalorizaram-se os interesses privados, em detrimento dos regramentos exaustivos das

atividades particulares característicos do período histórico anterior. No Estado Liberal, o estado passou a ser mínimo, gerando a privatização do direito público, com a atração das matérias tipicamente dominadas pelo governo ao âmbito de discussões dominado pelos indivíduos (CARMO, 2010).

Ao lado disso, incrementou-se a separação entre Estado e sociedade, pois o foco consistia em restringir os poderes estatais em favor das liberdades individuais, dentre as quais se situava uma esfera individual intangível (SARMENTO, 2005). Nesse movimento de valorização da autonomia e das liberdades, fortaleceu-se a divisão entre o público e o privado, com prevalência deste (CARMO, 2010). Esse incremento da dicotomia mostrou-se fundamental para o fortalecimento do liberalismo (CORREIA, 2015).

Para a finalidade de identificação de uma privacidade nesse cenário, vale relembrar sua associação à liberdade para destacar que esta pressupunha a criação de um espaço público em que pudesse ser exercida. Assim, exigia-se para a liberdade um local de fácil acesso a todo indivíduo e no qual fosse possível a livre exposição e argumentação sobre os temas de interesse público.

Nos moldes da teoria de Habermas, nos séculos XVII e XVIII, a burguesia passou a usar o espaço público para discutir as práticas arraigadas de monopólio e abusos do Estado absolutista. Daí falar-se em uma esfera pública burguesa, compreendida como o local de reunião do público para que todos, livremente, pudessem exercer o uso público da razão (HABERMAS, 2003).

Habermas associa o início de uma concepção de espaço público na Europa ocidental dos séculos XVII e XVIII, na qual o espaço coletivo passou a ser usado pela burguesia para apresentação de contestações ao monopólio do Estado formal sobre o patrimônio público (HABERMAS, 2003). Passou-se a difundir, assim, o questionamento sobre as arbitrariedades da nobreza, contestação que se realizava sob uma pretensão de racionalidade do discurso de ataque ao poder estatal, premissa que fez parte de sua teoria da ação comunicativa.

A expansão de um espaço público destinado à contestação de práticas do poder estatal e ao exercício da autodeterminação e da liberdade de intervenção nas decisões fundamentais tornou necessário, por outro lado, o reconhecimento de uma esfera privada, na qual jurídica e fisicamente fosse possível a cada indivíduo manter-se livre da ingerência e vigilância dos demais. Assim, a liberdade veio acompanhada da privacidade, compreendida como o exercício da liberdade de ser deixado só. Assim, a privacidade foi associada à intimidade.

Para que o alargamento do espaço público fosse positivo, era necessária ao indivíduo a capacidade de criação de um contexto no qual pudesse ser deixado e conseguisse exercer sua intimidade, o que não era acessível a todos. Nesse sentido, o movimento de incremento de um espaço público tornou imperiosa a cada indivíduo a possibilidade de ter seu próprio espaço para o exercício das atividades cotidianas, pois a nova esfera pública era formada por indivíduos que passaram a considerar um local privado essencial para a constituição de sua individualidade.

Isso, no entanto, somente era acessível a quem tinha condições materiais de ter sua própria habitação e de separar seus locais de moradia e de trabalho. Na prática, essa possibilidade somente existia para a burguesia, razão pela qual se pode sustentar que a privacidade originou-se como um direito tipicamente burguês e associado à intimidade (RODOTÁ, 2008).

Já no final do século XIX, passou-se a atribuir majoritariamente a Warren e Brandeis (1980) a menção à privacidade como direito autônomo. À época, quando uma noção de privacidade ainda não era reconhecida no *common law*, tampouco nos países do *civil law*, uma dificuldade de identificar o direito à privacidade decorria da associação dos direitos a um aspecto físico, tangível, especificamente à proteção da propriedade. De fato, inicialmente, havia um desafio relevante de aceitação de um direito à privacidade não vinculado a alguma proteção à honra ou à propriedade (ZANINI, 2015).

Com relação aos direitos autorais, por exemplo, os autores destacam o fato de que estão relacionados sempre a uma noção de propriedade, de modo que as características da privacidade são similares às dos direitos patrimoniais. Assim, a privacidade era relacionada a um direito de determinar se, a quem e em que medida o indivíduo quer expor seus pensamentos, sentimentos e emoções, mas também era associada a uma proteção das emoções e sensações, superando a vinculação entre a tutela jurídica de um direito e patrimônio físico.

Associava-se o direito à privacidade ao direito de manter certas coisas pessoais “escondidas”, não divulgadas, não mais necessariamente apenas no plano físico. De todo modo, a vinculação com autonomia e liberdade mantinha-se forte.

Além disso, na jurisprudência, geralmente o reconhecimento da violação da privacidade estava sendo relacionado a uma quebra de contrato e de confiança (WARREN e BRANDEIS, 1980). No entanto, o desenvolvimento da sociedade, com novas tecnologias, torna possível que, mesmo sem uma relação prévia de confiança, ocorra uma violação à privacidade. Nos tempos atuais, esse dilema sobre a existência de uma relação contratual

prévia tornou-se desnecessário porque a boa-fé objetiva é cláusula geral de comportamento de todos com todos, independentemente do tipo de vínculo jurídico (obrigacional ou contratual) que une as pessoas.

Ainda no âmbito norte-americano, Rubenfeld (1989) apresentou sua retrospectiva sobre o direito à privacidade desde a concepção de Warren e Brandeis (1980).

Analisando como esse direito foi efetivado na jurisprudência dos Estados Unidos da América, o autor apontou que, por muito tempo, foi relacionado a questões da sexualidade do indivíduo. Nos casos concretos em que os tribunais anularam leis com base no princípio da privacidade, procurou-se evitar que normas prospectivas, que adentravam na seara de escolhas que deveriam ser feitas pelas próprias pessoas, ocasionassem uma padronização dos indivíduos e da sociedade.

De fato, para assegurar a própria personalidade, algumas decisões sobre a vida eram consideradas tão centrais à identidade que não podiam ser impostas pelo Estado, o que permitia reconhecer o direito à privacidade como um direito à autodefinição (RUBENFELD, 1989). Logo, com relação a alguns aspectos da vida (como casamento, direito ao aborto, formas de educação etc.), a imposição de comportamentos padronizados por iniciativa do Estado, na tentativa não de evitar uma conduta proibida, mas de impor uma forma de vida, mostrava-se incompatível com uma noção de privacidade.

Assim, o *right to be let alone* era visto, do ponto de vista de Rubenfeld (1989), como o direito de não ter o curso de uma vida ditada pelo Estado. Por consequência, a promoção da privacidade pelo Estado não carecia apenas da permissão de liberdade para desenvolvimento da privacidade, mas também do impedimento da imposição de comportamentos homogeneizados, de modo que cada indivíduo pudesse fazer suas escolhas sobre vida digna (MARINI apud BAIÃO, 2014).

Sendo assim, já não bastava, ao fim do século XX, o reconhecimento da privacidade como o direito a um espaço reservado, pois ela carecia, ainda, de uma atuação estatal promocional cuja legitimidade, então, exigia a existência de condições para que, democraticamente, os possíveis cursos de vida fossem pensados:

> “o efeito destes desenvolvimentos vinha sendo, no fim do século XX, o de obrigar uma nova articulação - sob a forma de Direito à privacidade - do que é o princípio mais basilar do autogoverno (democracia): que o governo deve existir para o povo, e as pessoas não devem se tornar meros instrumentos do Estado. Este princípio necessita, como tentei mostrar, de um direito de ser deixado sozinho, se por "let alone" nós compreendemos o direito de não ter o curso de uma vida ditada pelo Estado” (tradução livre) (RUBENFELD, 1989).

Esse contexto de demanda pela promoção ativa do direito não foi exclusivo para a privacidade, mas abrangeu todos os direitos oriundos do Estado Social, especialmente aqueles denominados direitos fundamentais de segunda geração (CARMO, 2010). O decesso do Estado Mínimo veio acompanhado da constitucionalização de temas privados em substituição à autorregulação, e da atribuição ao Estado da função de promover o bem-estar.

Destaca-se que, no momento histórico subsequente, já ao final do século XX, a percepção da incapacidade do Estado, incluindo-se o brasileiro, de fazer frente às demandas sociais inaugurou a demanda pelo retorno de um novo momento de prevalência da liberalidade. Nesse novo paradigma liberal, a intervenção direta na ordem econômica e na estatal cedeu lugar a uma atuação indireta do Estado e a uma forma de governar em cooperação (CARMO, 2010).

Pode-se notar, assim, que, em meados do século XIX, a noção de privacidade estava mais associada ao reconhecimento da autonomia dos indivíduos de disposição de sua pessoa e de seus atributos. No fim daquele século, reforçou-se o reconhecimento de um aspecto físico, tangível, e da ocorrência de quebra de contrato e da confiança cuja configuração era considerada necessária para tutela da privacidade.

Aos poucos, a privacidade foi se transmudando para um direito de determinar se, a quem e em que medida o indivíduo queria expor seus pensamentos, sentimentos e emoções. Além disso, era associada a uma proteção das emoções e sensações, superando a vinculação entre a tutela jurídica de um direito e patrimônio físico.

Já no século XX, o reconhecimento da privacidade nos tribunais norte-americanos vinha sendo atrelado ao sentimento da necessidade de evitar que leis padronizassem o comportamento dos indivíduos em prol de demandas governamentais, de modo que o direito de ser deixado só representava o direito à autonomia no comando da própria vida, não ditada pelo Estado.

A privacidade, então, adquiriu feição positiva, ao lado do aspecto negativo já tradicional de não ter seu espaço individual invadido ou devassado, pois também se exigia a promoção de condições de autonomia na condução de uma vida digna.

Percebe-se que os contornos de tal direito vão se moldando e reconfigurando no tempo conforme as demandas sociais que se apresentam. Atualmente, na sociedade da informação e com as práticas de compartilhamento de dados pessoais dos indivíduos como método que contribui para a promoção do desenvolvimento de utilidades governamentais e comerciais, diverge-se entre a identificação de uma modificação de tais

concepções sobre privacidade e o surgimento de novos direitos atrelados a aspectos da individualidade. Para as finalidades do presente trabalho, uma forma útil de abordar tal dissonância conceitual consiste em analisar o surgimento de uma categoria própria de direito à tutela dos dados pessoais.

2.3. Tutela dos dados pessoais como direito autônomo e teorias jurídicas do conceito de dados pessoais

Nesse ambiente de monetização dos dados pessoais e com base em conceitos de direito da personalidade, Bioni (2016) qualifica o direito aos dados pessoais como direito específico desatrelado da privacidade, pois mais se aproximam, em verdade, da identidade que da privacidade da pessoa "datificada". É possível, de fato, que haja ofensa ao direito de autotutela de dados pessoais sem afetar a privacidade do mesmo indivíduo, como quando é necessário retificar dado pessoal perante órgão público ou meramente acessar dado perante instituição governamental ou privada que pode conduzir uma decisão automatizada.

Nos sistemas de *credit scoring*, por exemplo, instituições financeiras avaliam o risco da concessão de crédito e o fazem por meio de modelo estatísticos, resultando na atribuição de uma nota de risco ao consumidor. No Brasil, essa prática é considerada lícita, pois respaldada na Lei nº 12.414/2011 (Lei do Cadastro Positivo), e sequer se exige o consentimento do consumidor avaliado para que sua nota seja calculada. Em razão dessa ausência de concordância, reconhece-se ao menos o direito do consumidor a conhecer as "fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas" (REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014), sob pena de cometimento abuso de direito e responsabilização civil da instituição de crédito.

Bioni (2016) vislumbra não somente a pertinência, mas a utilidade de tal diferenciação entre os direitos, na medida em que ela corrobora direitos que independem da privacidade, tais como o direito à oposição a decisões automatizadas[13].

13 Artigo 21
UE Regulamento Geral sobre a Proteção de Dados
"- Direito de oposição"
O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.o 1, alínea e) ou f), ou no artigo 6.o, n.o 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo

Por conseguinte, o parâmetro de diferenciação entre público e privado não se mostra suficiente para abranger a tutela completa do direito sobre os dados pessoais. De fato, há dados que, embora pessoais, não têm caráter privado, antes possuem uma publicidade natural, como o nome em diversas situações. Desse modo, pensar nos dados pessoais somente sob a perspectiva de proteção do que não é divulgado é insuficiente para tutelar direitos e interesses relacionados a dados que, embora não digam respeito a uma esfera de segredo, estão diretamente vinculados à individualidade (Bioni, 2016).

Contra tal concepção do direito à tutela dos dados pessoais como direito autônomo, poder-se-ia argumentar no sentido de se tratar, em verdade, de desenvolvimento do direito à privacidade, uma vez que esta mesma já não se vincula ao paradigma do segredo, mas ao do controle.

Com efeito, há quem, como Rodotá (2008), trate a tutela dos dados pessoais como novo formato da privacidade, mais adequado ao quadro institucional atual que ao tradicional, em razão de novas dimensões de coleta e tratamento de informações. Nessa linha, afasta-se a qualificação do conceito de privacidade como "direito de ser deixado só" para aderir a uma concepção fundada na autodeterminação sobre as próprias informações em razão de novas questões geradas pela realidade dos sistemas informativos atuais.

A preocupação em redefinir esse direito deriva, justamente, da realidade atual sobre as práticas de governos e organizações privadas com dados pessoais, em especial com uso de novas tecnologias que aprimoram o uso dessas informações e concentram poder. O receio em não reconfigurar a privacidade está em permitir que o usuário seja mero fornecedor de dados, os quais, por sua vez, incrementam o poder de outros atores sociais.

---

tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.

No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.

Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

Esse contexto fático é que conduziu Rodotá (2008) a pensar uma nova normatividade do direito à privacidade que coadune com a impossibilidade de que os usuários sejam tidos por meros fornecedores de dados, mas sem separação conceitual entre direito à privacidade e direito à tutela dos dados pessoais. Para evitar tal subordinação, propôs, então, um fortalecimento do direito individual à privacidade, e não propriamente o reconhecimento de uma nova figura de direito subjetivo autônomo como o direito individual à tutela sobre os dados pessoais.

Nessa linha de pensamento, reconhece-se que, agora, a própria concepção de esfera privada está modificada (RODOTÁ, 2008) e abrange não somente o que se pretende manter sob segredo ("pessoa-informação-sigilo"), mas tudo o que é pessoal sobre o que se pretende manter sob completo controle ("pessoa-informação-circulação-controle"). Assim, as mudanças oriundas do desenvolvimento de tecnologias da informação teriam provocado tanto a redefinição de privacidade para abranger o poder de controle quanto a ampliação da esfera privada.

Ainda, para Rodotá (2008, p. 97), a admissão de um direito fundamental à autodeterminação informativa não contradiz sua proposta de ampliação da privacidade, pois "o reconhecimento de um direito fundamental não exclui que este se manifeste concretamente através da atribuição aos interessados de uma série aberta de poderes". Assumir a identidade entre o direito à proteção dos dados pessoais como parte do direito à privacidade somente pode ser admitido se, de fato, houver a transposição para o paradigma "pessoa-informação-circulação-controle" e se forem admitidas como objetos tuteláveis por meio da privacidade informações que já foram colocadas à disponibilidade de outros sujeitos, como dados fornecidos ao governo, mas que se busca conhecer ou ratificar. A privacidade, para quem a compreende assim, é tida como "direito de escolher o que se está disposto a revelar aos outros".

O autor reconhece, porém, um direito de acesso a informações não como derivação da privacidade, mas da liberdade de informação. Tal direito, sim, é desvinculado por Rodotá (2008) de questões de intimidade ou privacidade, e relacionado apenas ao direito à informação, como forma de ligar tecnologia e democracia. Assim, em vez de separar privacidade e direito sobre os dados pessoais, a separação dá-se entre privacidade e direito à informação. A questão é que, nesse modelo, a tutela de dados pessoais consiste em derivação do direito à privacidade, ao passo que o direito de acesso à informação é visto como direito à parte. Em outros termos, nessa categorização, direito à autotutela de acesso à informação não é identificado com um direito autônomo sobre dados pessoais.

Apesar dessa maneira de identificar a proteção desses dados como "evolução" da concepção de privacidade, a própria dicotomia público-privado em que ampara a identificação do privado não explica a tutela sobre os dados pessoais, pois, como já externado, dados que são pessoais, mas estão em domínio público, também se inserem na esfera de proteção de seu titular.

A taxonomia que mais coaduna com a possibilidade de completa tutela dos dados pessoais sem depender da ofensa a algum aspecto de privacidade, portanto, será adotada neste trabalho e diferencia esses dois direitos subjetivos como direitos autônomos de personalidade. Tal diferenciação permite maior amplitude na tutela do direito sobre os dados pessoais e coaduna com a autonomia de cada um desses direitos como direitos da personalidade.

Isso porque cada um, autonomamente, viabiliza a tutela de aspectos próprios inerentes à dignidade da pessoa humana, princípio que fundamenta a teoria da personalidade em uma sociedade plural, aberta e multifacetada, vinculando todas as regras que fazem parte dessa teoria atualmente (FARIAS e ROSENVALD, 2015).

Essa mesma dignidade constitui, aliás, preceito que deve permear todas as relações jurídicas, não sendo outra a razão pela qual constitui fundamento da República Federativa do Brasil (art. 1º, III, Constituição Federal de 1988), daí que o ordenamento jurídico já não se contenta em assegurar a existência da vida, mas necessariamente de uma vida digna. Se, historicamente, a personalidade jurídica simplesmente assegurava ao seu titular a possibilidade de contrair direitos e obrigações, a concepção atual é mais completa e vai além da atribuição, à pessoa, da qualificação como sujeito de direitos para também atribuir a este sujeito a possibilidade de reclamar proteção jurídica mínima com base nos direitos da personalidade (FARIAS e ROSENVALD, 2015).

Embora a origem dos direitos da personalidade seja razão de dissonância na doutrina, na medida em que, a despeito de prevalecer a concepção jusnaturalista (DINIZ, 2002; JABUR, 2000; BITTAR, 2001), também há a defesa positivista (TEPEDINO, 2009; FARIAS e ROSENVALD, 2015) dessa fonte de direitos, a influência cultural, isto é, não natural, mas constituída em determinado contexto a partir das vivências dos sujeitos de direitos, têm efetivamente moldado o patrimônio jurídico dos detentores de personalidade. Assim é que, apenas no Pós-Guerra, em razão de barbaridades praticadas contra a humanidade, mas com base em autorizações legais de ação, identificou-se a necessidade de tutelar direitos básicos inerentes ao homem e que não podiam depender do ordenamento jurídico positivado em cada país (MORATO, 2011). E, desde então, novas vivências sociais

têm demandado reconhecimento de novos direitos imprescindíveis à concretização da dignidade das pessoas, como direitos de transexuais à mudança física de sexo e ao uso de nome social, direito ao parentesco, direitos trabalhistas em oposição à realidade escravista, direito ao esquecimento e direito à extimidade (direito de usufruir de conteúdos de intimidade em ambientes de sociabilidade sem que isso se torne de conhecimento público[14]).

Observa-se, então, que o conteúdo dos direitos da personalidade é fluido e está em constante modificação para adequar os direitos imprescindíveis ao desenvolvimento da pessoa humana às novas realidades que se apresentam, o que inclui as modificações tecnológicas como as inovações nas tecnologias da informação e da comunicação. Por conta dessa mutabilidade que acompanha o contexto em que a dignidade deve ser exercida, o avanço tecnológico implica a necessidade de tutela de aspectos dessa dignidade que antes não incomodavam ou ao menos não da mesma maneira e intensidade.

Assim, na linha de Bioni (2016), se os dados estão vinculados à esfera de uma pessoa, isto é, se são pessoais, constituem uma das dimensões dessa pessoa e, em razão disso, fazem parte do conjunto de direitos da personalidade. Consideradas as novas demandas de proteção pessoal e de promoção de direitos individuais decorrentes das novas tecnologias, pode-se observar que o atual contexto exige a tutela autônoma do direito sobre os dados pessoais, independente de uma ofensa à privacidade, na medida em que, sendo esses dados informações que projetam a própria personalidade de alguém, devem ser precisos nessa projeção de uma identidade independentemente de violação à privacidade.

Além disso, a independência entre privacidade e tutela de dados pessoais pode ser extraída do ordenamento jurídico brasileiro. De fato, ao regulamentar o Marco Civil da Internet para cuidar de procedimentos de guarda e proteção de dados por provedores, o Decreto nº 8.771/2016 prevê como dado pessoal aquele relacionado à pessoa natural identificada ou ao menos identificável (art. 14). O que o Decreto tutela é, em suma, o controle do acesso aos dados, a autenticidade das informações e a inviolabilidade dos dados, como se pode extrair do respectivo artigo 13. Pode-se notar, então, que nem toda proteção conferida pela norma tem relação com algum aspecto da privacidade do titular dos dados, a exemplo da proteção da autenticidade da informação.

[14] "Por direito à extimidade entende-se: o direito de gozar ativamente da intimidade, através da exposição voluntária de informações da intimidade, as quais se quer não sejam tomadas como públicas, em face de terceiros ou de cenários". BOLESINA, Iuri. "O direito à extimidade no ciberespaço e a transformação do binômio público-privado". 2015, II Mostra de Pesquisa de Direito Civil Constitucionalizado.

No Projeto de Lei nº 4060/2012, ao qual estão apensados os PLs 5276/2016 e 6291/2016, destinado à criação de uma norma específica no Brasil para tutela de dados pessoais, estes são conceituados de forma genérica como "qualquer informação que permita a identificação exata e precisa de uma pessoa determinada".

A despeito de a concepção proposta não ser clara quanto à possibilidade de identificação da pessoa determinada decorrer da combinação de informações pessoais, a teleologia da norma consiste em "garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem". Observa-se, portanto, que o conceito de dado pessoal deve permitir uma tutela individual muito mais abrangente que a proteção da privacidade de seu titular, alcançando outros aspectos inerentes à personalidade, como a honra e a liberdade.

É preciso advertir que, sob o pressuposto da admissão da autonomia dessa tutela como um direito subjetivo, os teóricos divergem quanto aos parâmetros de conceituação dos dados pessoais, permitindo identificar teorias jurídicas realistas e personalistas. A presente exposição adere à vertente personalista e, por expandir a tutela para além de um bem ou um valor econômico, reconhece nos dados pessoais um elemento de expressão de identidade (ROCHFELD, 2018). Como consequência, sua maior implicação no patrimônio jurídico do usuário da internet consiste na possibilidade de autodeterminação informativa.

Não se ignora, porém, a existência do viés realista, para o qual o dado pessoal deve merecer tratamento de bem jurídico, tutelável pelos parâmetros da propriedade ou, pelo menos, por alguma forma de reconhecimento da possibilidade de sua apropriação por uma pessoa (ROCHFELD, 2018). Sob essa premissa é que se admite a coleta e a circulação comercializada dos dados pessoais, ainda que possa haver algumas limitações a essas liberdades.

Mesmo dentre os teóricos realistas, diferentes posições podem ser identificadas quando são analisadas sob alguns parâmetros, como a identificação do proprietário desse bem. Assim, para alguns, o proprietário é o internauta, ao passo que, para outros, a melhor concepção é de que os dados constituem *res nullius*, não pertencendo a ninguém até que sejam captados, momento em que passariam a pertencer a quem conseguiu realizar tal ação. Para outros teóricos, esses bens podem, ainda, ser considerados comuns (propriedade comum ou bem comum), de modo que podem ter uma aplicação coletiva que

atenda a interesses da coletividade, impedindo-se que fiquem limitados ao acesso pelas empresas gigantes da internet (ROCHFELD, 2018).

Ainda que os sistemas normativos atuais, de modo geral, não sejam claros quanto à adoção de uma ou outra vertente, podendo ser encontradas disposições esparsas direcionadas ora a uma, ora a outra corrente teórica, já não se pode negar a necessidade de que a própria pessoa, e não apenas as implicações sobre sua propriedade, sejam tuteladas quando se trata das práticas com dados pessoais.

2.3.1 Dados pessoais, dados sensíveis, dados anônimos e metadados.

O uso de uma tipologia dos dados pode auxiliar na identificação da separação entre o direito à tutela dos dados pessoais e o direito à privacidade. A própria concepção de dado pessoal não é unânime na doutrina e nas legislações existentes, variando sobretudo quanto ao critério da identificabilidade do titular.

Para Doneda, o dado pessoal é vinculado a uma pessoa e refere-se a um aspecto objetivo desse alguém, constituindo "os fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável" (DONEDA, 2006). Assim, imagens obtidas em sistemas de vigilância, registros de IP e de comunicações telefônicas e dados de geolocalização bastam para atrair a proteção do titular dessas informações.

Na mesma direção, no Decreto nº 8.771/2016, artigo 14, conceitua-se o dado pessoal como aquele "relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa", bastando, portanto, a possibilidade de que essa informação permita a identificação de seu titular para que se qualifique como dado pessoal.

A possibilidade de identificação a partir do dado constitui critério de definição de outros ordenamentos jurídicos, como da Colômbia, do México e de Singapura, os quais os definem, em suma, como aqueles dados a partir dos quais os titulares podem ser identificados[15].

15 Para consultar a legislação sobre tutela de dados pessoais ao redor do mundo: DLA Piper's Data Protection Laws of the World Handbook. Disponível em < https://www.dlapiperdataprotection.com/index.html?t=definitions&c=AO>. Acesso em 20 de maio de 2018.

No Regulamento Europeu de Proteção de Dados, que entrou em vigência em 25 de maio de 2018, dado pessoal é toda “informação relativa a uma pessoa singular identificada ou identificável”, sendo considerada identificável a pessoa que “possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”.

Essa linha conceitual é mantida no Projeto de Lei n. 5.276/2016, em trâmite na Câmara dos Deputados, no qual se define o dado pessoal como aquele referente à pessoa natural identificada ou identificável, incluindo-se números identificadores, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa.

Já o Projeto de Lei nº 4.060/2012 traz definição bem mais restritiva de dado pessoal e, portanto, permite uma abrangência de tutela muito menor. Isso porque, para obter a tutela ali sugerida, a informação precisa permitir a “identificação exata e precisa de uma pessoa determinada”. Assim, apenas elementos como nomes não homônimos, dados biométricos e números de Cadastro de Pessoas Físicas receberiam a tutela legal. Se, pelo lado do usuário, essa concepção pode ser considerada deficiente, é apoiada pelos agentes de mercado, pois viabiliza de forma mais ampla o uso dessas informações no fomento das atividades econômicas na economia de dados digitais.

De todo modo, importa perceber que dado pessoal pode ser especificado em dado sensível e diferenciado de dado anônimo, categorias nessa tipologia possível que comportam tratamentos distintos.

Um dado sensível, ao seu turno, não somente tem sua tutela assegurada em tais regramentos jurídicos, mas merece tratamento especial, na medida em que diz respeito a aspectos da pessoa que podem levar à sua discriminação (DONEDA, 2006). Referem-se, por exemplo, a orientação sexual, política ou religiosa, ou a origem racial, dados biométricos, genéticos e de saúde. No já citado Regulamento Europeu, a especificação do dado sensível está pautada na possibilidade de seu tratamento “implicar riscos significativos para os direitos e liberdades fundamentais”.

Os dados anônimos, a princípio, poderiam ser vistos como aqueles que, por não permitirem a identificação que é premissa do conceito de dado pessoal, estariam afastados da tutela jurídica. Para fomentar os debates que antecedem a criação da norma específica de proteção de dados no Brasil, o Ministério da Justiça criou o projeto Pensando o Direito e, no sítio eletrônico respectivo, apresenta como proposta da definição de dados

anônimos aquela que os qualifica como os que "se referem a pessoas que não podem ser identificadas – como dados estatísticos, por exemplo. Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), não permite a identificação de seu titular"[16].

O incremento das tecnologias, no entanto, não permite que se ignore a possibilidade de "desanonimização" dessas informações, notadamente por meio do uso de *big data* e do cruzamento de dados. Diante dessa possibilidade, o Regulamento Europeu de Proteção de Dados não afasta, de imediato, a tutela dos dados anônimos, preferindo especificar como dados passíveis de proteção sob tal regulamento aqueles "pseudonimizados".

Nesse sentido, o Regulamento trata da técnica de "pseudonimização" como o tratamento que não permite associar o dado pessoal a um titular específico a não ser que sejam consultadas informações suplementares. Para isso, essas informações suplementares devem ser mantidas separadas, por meio de medidas técnicas e organizativas suficientes para assegurar essa impossibilidade de associação entre dado e pessoa identificada ou identificável.

Assim, se o uso dessas tecnologias não for assegurado e, a despeito da anonimização, os dados puderem ser associados a informações suplementares, devem ser considerados informações sobre pessoa singular identificável e, portanto, merecerão a tutela jurídica comum dos dados pessoais.

A ideia de dado anônimo precisa ser estudada conjuntamente com a conceituação de metadados, os quais, a rigor, não dão indicação do titular da informação. Embora esse conceito também não seja apresentado, na literatura, de forma unânime, em verdade o que se observa é uma diversidade de pontos de vista sobre esses elementos (LOURENÇO, 2007).

De modo geral, pode-se afirmar que os metadados constituem dados sobre outros dados, e não estão diretamente associados e referidos a uma pessoa (SCHNEIER, 2016). Assim, em geral, os metadados informam algo sobre um dado, constituindo informações que um sistema de computador usa para operar dados que são subprodutos dessa operação (SCHNEIER, 2016), como o horário e a posição geográfica de uma mensagem eletrônica trocada na web, sem descrição do assunto (dado).

O texto de um e-mail, então, pode constituir um dado, ao passo que a rota da mensagem, seu tamanho e seus endereços de emissão e recepção constituem os

16 A plataforma está disponível em <http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/>. Acesso em 20 de maio de 2018.

metadados. O conteúdo de uma fotografia, da mesma maneira, constitui o dado sobre o que está retratado, enquanto a geolocalização de onde foi registrada, o número de série da câmera e o horário, por exemplo, são metadados da informação.

Indicar que a informação constitui meramente metadados, no entanto, não basta para afastá-la da tutela conferida aos dados pessoais, pois a anonimização inicial pode sofrer alteração com o tratamento a que pode vir a ser submetida. Assim, por exemplo, quando houve os primeiros anúncios de Edward Snowden em 2013, incluindo a descrição da coleta de registros de usos de telefones celulares de todos os americanos, a NSA alegou, em defesa do governo norte-americano, que, em verdade, eles coletavam “apenas metadados”, mas não as palavras trocadas na comunicação (SCHNEIER, 2016).

Apesar disso, coletar as linhas usadas para a comunicação, os horários, a data e o tempo de duração das ligações era suficiente para exercer a vigilância. Em estudo da Universidade de Stanford, no qual foram examinados metadados de telefones de 500 voluntários, traçaram-se perfis de pessoas que convivem com esclerose múltipla, tiveram ataque cardíaco, plantam maconha, realizaram aborto etc., mesmo sem conhecer o conteúdo das mensagens (MAYER, MUTCHLER e MITCHELL, 2016).

Nota-se, portanto, que o metadado pode ser qualificado como dado pessoal, a depender do contexto em que é coletado e, principalmente, de como é tratado, não bastando indicá-lo como “dado do dado” para afastar a tutela merecida pelo seu titular.

A despeito das inúmeras possibilidades de diferenciação de dados pessoais, fato é que tal tipologia permite verificar que nem sempre essas concepções associam a tutela jurídica desses dados à proteção de algum aspecto da privacidade. Assim, se a correção, a atualização, e o controle sobre o dado pessoal mostram-se suficientes para afetar a integridade da personalidade do sujeito de direito, independentemente de isso afetar algum aspecto de sua privacidade, a possibilidade de tutela de dados pessoais, anonimizados ou não, na forma de metadados ou não, sensíveis ou ordinários, reforça a autonomia do direito à tutela sobre dados pessoais em face do direito à privacidade. Isso constitui premissa do presente trabalho.

2.3.2. Autonomia dos direitos à privacidade, à tutela dos dados pessoais e à extimidade.

Apesar dessa possibilidade de distinção analítica entre os direitos à privacidade e à tutela sobre os dados pessoais, ambos têm essa origem comum na individualidade como aspecto da personalidade do indivíduo. Além disso, também se aproximam ao dizerem respeito à faculdade do sujeito de direitos de ter controle sobre como quer viver dignamente, o que afeta escolhas tanto sobre seus dados quanto sobre sua vida privada. Ainda, em especial no ciberespaço, há quem sustente que a dicotomia público-privado foi modificada com a internet porque este ambiente virtual não mais permite as associações "visível/público" e "não-visível/privado" (BOLESINA, 2015).

Nesse cenário da individualidade, diferenciam-se três direitos inerentes à personalidade e autônomos, a saber a privacidade, a tutela de dados pessoais e a extimidade.

Após as mudanças sofridas desde quando passou a ser tratada como direito – especificamente como direito de estar só –, a privacidade hoje pode ser reconhecida como o direito de não ser invadido em sua esfera íntima nem exposto no que não se pretende expor. Implica, assim, o "legítimo interesse de salvaguardar do conhecimento alheio (e da curiosidade indevida) tudo o que diz respeito à esfera íntima de uma pessoa" o que, para Rosenvald e Farias (2015), abrange duas facetas, a saber: o direito à intimidade e o direito ao segredo. Por força da intimidade, o titular da privacidade tem o direito de resguardar informações a seu respeito, ao passo que o segredo abrange o direito de não dar publicidade a fatos relacionados à vida de alguém.

Embora haja quem aponte a mudança do paradigma do segredo para o do controle no âmbito da própria privacidade, essa modificação só se faz realmente necessária se não for identificada, como direito autônomo, a tutela sobre dados pessoais (RODOTÁ, 2008). De fato, reconhecida a autonomia desse direito subjetivo da personalidade, como já sustentado, é em seu âmbito que se encontra a perspectiva positiva de promover ao titular mecanismos de controlar quem, como e para que finalidades tem acesso aos dados pessoais, direito presente independentemente do caráter íntimo da informação. Assim, para exercício de tais faculdades, basta que a informação diga respeito à pessoa.

Nessa perspectiva de separação entre a privacidade e a tutela dos dados pessoais, a manutenção, por exemplo, do sítio eletrônico http://tudosobretodos.se viola o direito subjetivo de tutela dos dados pessoais, na medida em que as informações são ali

compiladas e vendidas sem anuência do titular das informações. Ainda que os mantenedores do sítio aleguem que as informações têm publicidade e foram extraídas da internet, de publicações em diários oficiais e em decisões judiciais publicadas, por exemplo, a reunião de tantos dados afetos a uma mesma pessoa, sobretudo para finalidade econômica de venda, afronta o direito subjetivo individual por falta da possibilidade de controle da exploração das informações.

A nova realidade social e tecnológica demandou, ainda, uma terceira categoria de direito, o direito à extimidade, como uma dimensão da intimidade. Essa nova categoria mostrou-se necessária sobretudo com a expansão do uso de redes sociais na internet, nas quais os usuários expõem aspectos de sua vida íntima, devendo ter a possibilidade de eleger quem tem acesso a tais informações.

Tendo em vista que essa exposição não inclui tal informação ou dado no domínio público e constitui simplesmente o exercício de uma faculdade do titular da informação baseada no princípio da exclusividade, o que foi voluntariamente partilhado somente pode ser mostrado ou ocultado com base na discricionariedade do próprio sujeito (ARENDT, 1959).

Falar-se em extimidade adquirida pela informação mostra-se coerente com o termo lançado por Lacan na área da psicanálise para indicar “algo do sujeito que lhe é mais íntimo, mais singular, mas que está fora, no exterior. Trata-se de uma formulação paradoxal: aquilo que é mais interior, mais próximo, mais íntimo, está no exterior” (CHATELARD e SEGANFREDO, 2014). Assim, a intimidade que passou a ser êxtima não deixou de ser íntima, mas apenas foi exteriorizada voluntariamente (BOLESINA, 2015).

Tal direito expressa-se, por exemplo, quando a divulgação de uma imagem em rede social não autoriza os demais a reproduzir essa mesma imagem indiscriminadamente sem autorização do titular, ainda que este a tenha divulgado, inicialmente, de forma voluntária.

Nessa direção, ao passo que a privacidade confere ao seu titular a faculdade de impedir a invasão à esfera íntima e a exposição de aspectos da intimidade não publicizados e a extimidade implica a faculdade de controlar o limite de divulgação de aspectos da intimidade voluntariamente divulgados pelo sujeito de direito, o direito à tutela sobre dados pessoais atrai as faculdades de controlar a coleta, o uso, a divulgação e a disseminação de dados relacionados ao indivíduo, podendo ser ligados a alguma intimidade ou não.

Dessa divisão entre os três tipos de direito (privacidade, tutela de dados pessoais e extimidade) pode-se notar que, embora sejam autônomos e cada um seja suficiente para tutelar direitos e interesses do sujeito de direito, há um cerne comum não apenas na dignidade da pessoa humana, mas no espaço privado do sujeito de direitos. Todos esses direitos têm relação com a manutenção de um espaço privado, temática que tem sido trazida à tona especialmente no contexto atual, de incremento das tecnologias de informação e comunicação na internet.

Daí que, embora autônomos, são relacionados e, apesar de a ofensa a um não implicar necessariamente a ofensa ao outro, é muito comum que isso ocorra, razão pela qual, na doutrina e na jurisprudência, frequentemente a violação ao direito de tutela sobre os dados pessoais é tratada como afronta à privacidade.

Apesar do reconhecimento desta proximidade, neste trabalho, a tutela dos dados pessoais será tratada como direito autônomo que, embora possa ser relacionado à privacidade e à extimidade, merece proteção independente.

Para compreender como essa tutela ocorre no Brasil e analisar de que maneira as teorias regulatórias abordadas neste trabalho explicam, ou não, essa realidade, os modelos serão tratados no capítulo seguinte a fim de subsidiar esse exame ao final. Antes, porém, para subsidiar a compreensão da forma como esse tema já é, atualmente, abordado no ordenamento jurídico nacional, será apresentado um breve panorama normativo.

2.3.3. O panorama normativo atual e iminente no Brasil

Além de a privacidade modificar-se no tempo, novas configurações sociais podem passar a exigir o reconhecimento também de direitos inéditos, como se pode notar na atual sociedade em rede. Nessa linha e no contexto dessa sociedade em rede, há constantes tentativas de ajustes legais com pretensão de acompanhar as novas demandas e desafios surgidos na realidade, tanto nas relações entre usuários e governos, quanto nas relações entre usuários e empresas e governos e empresas. Essas tentativas de regulação formal decorrem não apenas da necessidade de proteger direitos, como privacidade e tutela de dados nesse contexto em que praticamente toda ação humana (e não humana) é registrada, mas também da premência de fomentar um ambiente jurídico seguro.

No contexto internacional, pode-se notar que as duas principais vertentes normativas podem ser identificadas nos Estados Unidos e na União Europeia. Com efeito, mesmo com a convergência de democracias sobre as normas basilares de tutela de dados – como a própria existência de um direito à autodeterminação sobre os dados pessoais -, há diferenças nos extratos regulatórios que permitem diferenciá-los entre liberal ou social protetivo (REIDENBERG, 2000). Assim, enquanto os Estados Unidos inspiram ordenamentos com proteção mais liberal, baseados na governança pelo mercado e na perspectiva do usuário como consumidor, a normatividade europeia é mais fundada em direitos, buscando considerar todos os aspectos da individualidade e da cidadania dos usuários.

Logo, os Estados Unidos possuem conjunto normativo menos intervencionista e no qual predomina o tratamento jurídico da questão, quando existente, pela perspectiva do mercado, sendo o usuário visto como consumidor. Nessa abordagem de implementação, com uma intervenção estatal mais tímida e menos garantista, a legislação é setorial, dirigindo apenas alguns setores, o que resulta em disposições como o Ato de Proteção de Privacidade em Vídeo*, o Children's Online Privacy Protection Act* – COPPA, que regula a coleta de dados pessoais de crianças, o *Health Insurance Portability and Accountability Act* – HIPAA, referente aos dados de saúde de pacientes, a *Gramm-Leach-Bliley Act*, referente à tutela sobre dados bancários, financeiros e de seguro social.

Ao lado disso, a ausência de uma normativa uniformizada e geral sobre esse tema não tem impedido a fiscalização no cumprimento das normas esparsas já existentes, o que se deve, em considerável parte, à atuação da Comissão Federal de Comércio (*Federal Trade Commission* – FTC) daquele país, a qual tem competência fiscalizatória e executiva, judicializando demandas destinadas a forçar o cumprimento das normas existentes.

A atuação da Comissão tem levado grandes companhias como Google e Facebook ao enfrentamento de ações referentes à tutela dos dados dos usuários, muitas das quais envolvendo a aplicação de vultosas multas, como se nota a partir da quantidade de ações destinadas a investigar práticas consistentes em "*unfair and deceptive acts"* relacionados à privacidade (MACHADO; PACÍFICO, 2016). Em face disso, mesmo à míngua de uma norma geral sobre essa temática, tais empresas têm demonstrado alguma preocupação no cumprimento das leis e de regras de boas condutas sugeridas pela FTC.

A União Europeia, ao seu turno, já vivencia a reforma de seu quadro normativo, substituindo a Diretiva da União Europeia de Proteção de Dados nº 95/76 por seu

Regulamento Geral Sobre Proteção de Dados (Regulamento 2016/679), o qual, diferentemente da norma anterior, não apenas fixa objetivos gerais de todos os componentes da União, mas verdadeiramente vincula cada país.

O novo regramento é fruto de anos de debate entre entidades governamentais, parlamentares, acadêmicos, sociedade civil e empresas e têm como foco restituir aos usuários o exercício da tutela sobre seus dados pessoais. Mesmo com a criação da Diretiva, em 1995, a União Europeia não deixou de vivenciar o fortalecimento das práticas de empresas e governos na coleta, no armazenamento, no processamento e na interpretação dos dados pessoais dos cidadãos, gerando cada vez mais impactos no mercado, na concorrência, na vigilância estatal e nas possibilidades de construção de uma cidadania que, agora, é inevitavelmente plasmada também no ambiente digital.

No plano nacional, no que diz respeito às convenções internacionais, o Brasil é signatário de diferentes tratados internacionais relacionados à proteção da privacidade, dentre os quais a Convenção Internacional sobre Direitos Civis e Políticos (ICCPR) e o Pacto de San José da Costa Rica. Em relação ao ICCPR[17], os países participantes possuem a obrigação de adotar medidas que garantam a efetividade da proibição contra interferências e contra ataques, bem como que garantam a própria proteção à privacidade. Em relação ao Pacto de San José, no entanto, apesar de ser signatário desde 25 de setembro de 1992 até a presente data, o Brasil não aceitou a jurisdição compulsória da Corte Interamericana de Direitos Humanos. Adicionalmente, o Brasil esteve envolvido, junto às Nações Unidas, com a discussão da proteção à privacidade, tendo participado ativamente da elaboração da Resolução 68/167 sobre privacidade na era digital.

Ao se refletir sobre a questão da vigilância à comunicação, as revelações de Edward Snowden tiveram forte impacto para a construção de mecanismos efetivos de proteção dos cidadãos contra vigilância excessiva ou ilegal, com a atuação do governo brasileiro no sentido de estimular a proteção à privacidade, levantando a questão em diferentes fóruns internacionais, como Unesco e Nações Unidas. Uma das repercussões foi a elaboração de uma proposta de lei que regulasse a transferência de dados de cidadãos brasileiros para organizações internacionais. Posteriormente, o conteúdo da proposta foi

[17] "O artigo 17 estabelece que 'ninguém será sujeito a interferências arbitrárias ou ilegais em sua privacidade, família, domicílio ou correspondência, assim como a ataques ilegais à sua honra e reputação'. O Comitê de Direitos Humanos observou que os estados participantes do ICCPR possuem a obrigação positiva de 'adotar medidas legislativas, entre outras, para dar efeito à proibição contra tais interferências e ataques, bem como à proteção desse direito (privacidade)'". Tradução livre (PRIVACY INTERNATIONAL, 2016).

incorporado ao Marco civil da Internet, que passou a conter diversas previsões sobre a proteção à privacidade.

O relatório da *Privacy International* chama atenção para o fato de que, apesar da forte militância internacional do Brasil pela proteção dos dados pessoais, não se verifica a mesma preocupação em medidas adotadas pelo governo, que surpreendeu ao

> "implementar a retenção obrigatória de dados, bem como ao não aprovar a lei de proteção de dados (...), tendo expandido gradualmente seu enquadramento legal quanto às capacidades institucionais de vigilância, e tendo adquirido novas tecnologias de vigilância, um processo que foi acelerado enquanto o Brasil se preparava para sediar diversos eventos internacionais de larga escala, tais como o Rio+20, a Copa do Mundo e os jogos Olímpicos" (PRIVACY INTERNATIONAL, 2016).

O panorama normativo hoje existente internamente no país aponta as condições para a proteção dos dados pessoais e como vem sendo – ou não – preservado o direito à privacidade. Nesse relatório produzido pela *Privacy International* sobre o estado da privacidade no Brasil, verifica-se que o tratamento da matéria é feito com base em princípios gerais e normas contidas na Constituição, no Código Civil e em leis e regulamentos associados a situações específicas, como a proteção de comunicações telefônicas.

No Brasil, em termos gerais, as previsões legais sobre a matéria da proteção à privacidade estão na Constituição Federal de 1988. Nela são tratadas questões como o sigilo de correspondência, o sigilo bancário, as comunicações telegráficas, telefônicas e a comunicação de dados de forma geral. Observa-se, ainda, a existência de um mecanismo específico para solicitação de acesso a dados que se encontrem em bases de dados governamentais: o *Habeas Data*, regulado pela Lei Nº 9.507 de 1997.

Assim, o primeiro fundamento de um direito não à tutela sobre dados pessoais, mas à informação, pode ser identificado na Constituição Federal, a qual, ao implantar o Estado Democrático de Direito, previu o direito de acesso a informações públicas e até mesmo privadas quando presente um interesse maior, como se pode extrair dos artigos 5º, XXXIII, e 37. Também do texto constitucional se extraem o direito de certidão e a garantia do *habeas data*, respectivamente nos incisos XXXIV e LXIX do artigo 5º.

Posteriormente, a Lei da Transparência (Lei Complementar nº 131/2009), complementou a Lei de Responsabilidade Fiscal, passando a exigir que sejam disponíveis, em tempo real, informações precisas sobre a execução orçamentária e financeira dos Municípios, da União, dos Estados e do Distrito Federal.

Em uma mesma linha de proposta de transparência na gestão pública, a Lei de Acesso à Informação (Lei nº 12.527/2011 veio regulamentar o exercício do citado direito de acessar as informações públicas referentes aos atos governamentais (CF, art. 5º, XXXIII). Essa norma estabelece o relevante conceito de informação pessoal como o dado relacionado a uma pessoa natural identificada ou identificável (artigo 4º, IV). Com o propósito de balancear o interesse particular na manutenção do sigilo sobre esses dados e o interesse público e coletivo no uso das informações pessoais, a Lei passou a permitir que informações pessoais referentes à intimidade, à vida privada, à honra e à imagem sejam disponibilizadas, independentemente de consentimento prévio, quando houve utilidade médica a pessoa física ou legalmente incapaz, para cumprimento de ordem judicial, bem como defesa de direitos humanos e de interesse público.

Maior polêmica surge da autorização de divulgação dessas informações para elaboração de estatísticas e pesquisas científicas de evidente interesse público ou geral. Isso porque, a despeito de a própria norma prever que esse uso científico deva assegurar o anonimato das pessoas às quais se referem as informações, não se ignora que o tratamento de *big data* permite, mediante cruzamento de dados, a "desanonimização" dos indivíduos. Assim, pesquisas em saúde com uso de *big data*, por exemplo, podem acarretar a possibilidade de relacionar indivíduos identificados a certos dados clínicos e hábitos sem que tenha havido prévio consentimento do titular das informações. Por outro lado, o crescente desenvolvimento de novas tecnologias permite utilizar cada vez mais o potencial da informação para atividades de interesse público, o que exige permanente esforço de equilíbrio entre os interesses envolvidos.

Essas normas, no entanto, dadas suas especificidades, não abrangem a proteção da privacidade dos usuários na rede quando não se trata de comunicações, tampouco tutelam o direito à autodeterminação sobre a coleta, o armazenamento, o tratamento e o uso de dados pessoais em larga escala, como acontece em contextos de *big data*.

Em termos específicos de proteção ao consumidor, a Constituição também apresenta artigos que tratam especificamente da matéria, estabelecendo sua proteção como princípio da ordem econômica[18]. Ainda, o artigo 48 determina a elaboração do Código de Defesa do Consumidor. Em relação a isso, a *Privacy International* destacou a atuação da Secretaria de Proteção ao Consumidor (Senacon) como a principal entidade pública a fiscalizar as medidas de proteção à privacidade, uma vez ausente legislação compreensiva

[18] São exemplos o artigo 5, XXXII e o artigo 170, V.

sobre a matéria. A despeito da possibilidade de identificação da configuração de relação de consumo entre os usuários e os provedores na internet, independentemente de contraprestação financeira[19], a normatividade de tutela dos consumidores também se mostra, ainda, insuficiente. Em verdade, a ausência de controle sobre as práticas de agentes econômicos e estatais na coleta e no uso de dados pessoais impede, até mesmo, que os usuários as evidencie e demande sua proteção, seja judicial ou extrajudicialmente.

Ainda ao analisar a legislação sobre proteção de dados no Brasil, observa-se que, de maneira geral, há previsões sobre a proteção dos dados contidas no texto do Código Civil. No entanto, considerando o espectro de aplicação do código apenas às relações entre indivíduos e deles para com entidades legais, o Código Civil aplica-se nas situações de dados pessoais. Os regulamentos específicos, por sua vez, são aplicados em casos determinados aos quais se referem à internet, telecomunicações, entre outros. Também se verifica a aplicação das disposições do Código de Defesa do Consumidor, com a especificidade de sua incidência se dar quando caracterizada relação de consumo com o indivíduo.

As previsões do Marco Civil da Internet sobre a matéria determinam a incidência das normas do direito brasileiro aos provedores de conexão à internet e aos provedores de aplicação nos seguintes casos:

> "coleta, armazenamento e tratamento de dados pessoais no Brasil, se pelo menos um dos terminais envolvidos na comunicação estiver localizado no Brasil; ou se os provedores oferecerem serviços a brasileiros ou se tiverem, direta ou por meio de companhia pertencente ao mesmo grupo, um estabelecimento no Brasil. (...) O ato estabelece que qualquer tratamento de dados pessoais que seja processado no Brasil, ainda que parcialmente ou que os dados sejam meramente coletados por meio de um terminal localizado dentro do território, deve obrigatoriamente se submeter à legislação brasileira[20].

Além disso, o artigo 7° do Marco Civil da Internet prevê direitos e garantias dos usuários da internet, como a inviolabilidade da intimidade e da vida privada,

---

[19] Resp 1193764/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 14/12/2010, DJe 08/08/2011.

[20] O artigo 11 se aplica aos dados coletados em território nacional e ao conteúdo das comunicações nas quais pelo menos um dos terminais esteja localizado no Brasil. O artigo se aplica mesmo se as atividades forem desenvolvidas por uma entidade legal localizada fora do país, caso ela ofereça serviços ao público brasileiro, ou caso haja pelo menos um membro do mesmo grupo econômico estabelecido no Brasil. Companhias estrangeiras estão sujeitas a essa regra sempre que prestarem serviços a cidadãos brasileiros. Isso significa que mesmo que uma companhia não foque ou aborde usuários brasileiros, mas os admita como consumidores, as previsões do Marco Civil devem incidir sobre elas. O mesmo se aplica caso a companhia tenha subsidiárias no Brasil. (tradução nossa) (PRIVACY INTERNATIONAL, 2016).

sua proteção e indenização pelo dano material ou moral decorrente de sua violação; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet (salvo por ordem judicial, na forma da lei) e a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial[21]. Ainda no artigo 7º, especificamente no inciso IX do Marco Civil da Internet, prevê-se a necessidade do consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais. Na mesma linha, os incisos VII e X estipulam os direitos do usuário ao não fornecimento de suas informações pessoais a terceiros a não ser mediante consentimento livre, expresso e informado, e de obter a exclusão definitiva de seus dados mediante requerimento quando extinta sua relação contratual com o fornecedor.

Destaca-se que o Decreto nº 8.789/2016 trata do compartilhamento de bases de dados entre órgãos da administração pública federal, com exceção de informações sobre sigilo fiscal. A norma surgiu, no entanto, mais para legalizar a troca de tais informações do que para instrumentalizar a autodeterminação dos indivíduos sobre seus dados pessoais. Com efeito, passou a ser legalmente admitido o compartilhamento, entre os órgãos e as entidades da administração pública federal e independentemente da anuência do titular, dos dados cadastrais, estes qualificados como as informações referentes ao número de Cadastro de Pessoas Físicas ou Jurídica, Número de Identificação Social, do Programa Integração Social - PIS, do Programa de Formação do Patrimônio do Servidor Público - Pasep, título de eleitor, dados de pessoas jurídicas, nome civil e social de pessoas naturais, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e informações sobre vínculos empregatícios. Assim, ainda que tenha sido dado um passo na regulamentação do tema, a nova normatividade veio a avalizar as práticas de disseminação dos dados pessoais entre as entidades e os órgãos da Administração Federal que, não raro, estabelecem parcerias para uso desses dados.

A respeito das práticas e mecanismos de vigilância, o Brasil apresenta diferentes previsões legais, a começar pela Lei 9.296/96, que regula as interceptações

[21] "O artigo 7° assegura ao cidadão, ainda, o direito de não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; de manutenção da qualidade contratada da conexão à internet; de obter 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; de 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; de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta; não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet".

telefônicas e as dos sistemas informativos. A Lei estabelece parâmetros para a instrução de procedimentos criminais ou investigações, estabelecendo que o pedido de interceptação deva ser fundado em suspeita razoável de que a pessoa de quem se solicitou a interceptação tenha cometido crime, não havendo ainda outro meio possível de obtenção das evidências de cometimento do crime[22]. Merece atenção o panorama da retenção de dados no Brasil, com destaque para as Resoluções 426/05, 477/07 e 614/13 da Agência Nacional de Telecomunicações - Anatel, requerendo aos provedores de serviço, em linhas gerais, a retenção dos metadados pertencentes às linhas fixas e aos serviços de telefonia móvel[23].

No que se refere ao acesso aos dados armazenados, as autoridades policiais, bem como a Advocacia Geral da União, nos casos de lavagem de dinheiro (Lei 9.613/98) e de crime organizado (Lei 12.850/13), podem solicitar acesso diretamente aos provedores de serviço, não sendo necessária a apresentação de ordem judicial. Da mesma forma, a ANATEL também pode solicitar as informações necessárias diretamente aos provedores de serviço[24]. Podem acessar também informações como nome, afiliação e endereço às autoridades administrativas, segundo previsão legal do parágrafo 3, do artigo 10 da Lei que estabelece o Marco Civil da Internet (Lei 12.965/14).

A despeito de essas normas destinarem-se especificamente à proteção dos dados pessoais dos usuários, o fato de terem como pilar da autodeterminação informacional o consentimento dos usuários as torna insuficientes para impedir o uso indiscriminado dos dados pessoais, especialmente daqueles armazenados como *big data*. Isso porque tal anuência tem sido dada, em geral, por meio dos termos de uso, cuja leitura não é comum pelos

---

[22] O relatório da *Privacy International* continua, destacando as preocupações que persistem mesmo diante da proteção legal: "Apesar das garantias apresentadas na lei, existem preocupações em relação a sua implementação. Por exemplo, o artigo 5 da lei observa que o período não pode exceder 15 dias, mas pode ser renovado por igual período, uma vez provada a indispensabilidade da evidência. Portanto, essa legislação deixa margem para interpretação relacionada ao limite temporal, uma razão pela qual já houve tantos casos de abuso" (Tradução nossa; PRIVACY INTERNATIONAL, 2016).

23 Para tanto: "Artigo 22 da Resolução No. 426/05 requer que os provedores de serviço para telefonia fixa retenham os dados por pelo menos 5 anos, e não inclui detalhes no tipo de dado, limitações de uso ou especificações sobre o propósito. O artigo 10, XX, da Resolução No. 477/07, dispõe que os provedores de serviço para telefonia móvel devem reter as informações sobre a conta e documentos de cobrança contendo dados sobre ligações recebidas ou efetuadas, datas, horário, duração e preço, por um mínimo de 5 anos. Artigo 53 da Resolução No. 614/13 requer que os provedores de conexão de internet retenham os dados por, pelo menos, 1 ano. Artigo 17 da Lei No. 12.850/13, sobre crime organizado, requer que as companhias de telefonia fixa e móvel retenham 'os logs de identificação dos números de origem e de destino de um terminal de conexão' por 5 anos. Lei 12.965/14, também conhecida como o Marco Civil, requer que os provedores de conexão de internet retenhas os logs de conexão por 1 ano, de acordo com o artigo 13. Provedores de serviços de aplicação com fins lucrativos são requeridos para que armazenem logs de acesso a aplicativos por um período de 6 meses, segundo o artigo 15. O parágrafo 2 de ambos os artigos possibilita a extensão dos períodos de retenção em determinadas circunstâncias, mas não há um limite máximo de tempo para a extensão – que pode ser teoricamente ilimitada" (Tradução livre) (PRIVACY INTERNATIONAL, 2016).

24 Segundo o artigo 38 da Resolução No. 596/12.

usuários. Diante disso, a ausência de efetividade do consentimento tem representado a permissão de utilização irrestrita dos dados, também por meio do uso secundário, tornando-se ineficaz esse mecanismo de validação de coleta e de uso dessas informações.

Na prática, mesmo essas tais normas setoriais ainda não têm assegurado a tutela da autodeterminação dos usuários da internet sobre seus dados pessoais e ainda permitem a manutenção de um cenário em que a insuficiência da regulamentação das práticas com tais dados naturaliza a existência e o uso de *big data*, tornando ilimitada a geração de valor desses instrumentos.

Ao lado disso, não são disponibilizadas de forma clara e facilmente acessível alternativas à simples adesão aos termos de uso e às políticas de privacidade padronizadas. Nesse contexto, diante dos prejuízos sociais e econômicos decorrentes da exclusão da participação da rede, os usuários optam por aderir aos termos padrões ainda que sem plena consciência das implicações disso para a proteção de seus dados pessoais (LESSIG, 2005).

Assim, o cenário ainda é de luta por concretizar uma norma específica de proteção de dados, por meio dos Projetos de Lei nº 4060/2012 (no qual se encontram incorporados os PLs 5276/2016 e 6291/2016), 181/2014 e 330/2013. De forma tímida, a busca por essa proteção foi iniciada com o Marco Civil da Internet e em sua regulamentação no recente Decreto nº 8.771/2016, além do Decreto nº 8.789/2016.

Vale registrar que o primeiro Projeto de Lei destinado a tratar do acesso a informação pessoal foi elaborado em 1908 – PL nº 2.796, Deputada Cristina Tavares, visando a tratar da garantia dos cidadãos de acesso às informações sobre sua pessoa presente em bancos de dados. Apesar disso, a motivação da proposta foi perdida e, de todo modo, essa proposição não estava ligada à dinâmica atual da internet.

Percebe-se que, embora o caráter ainda setorial da legislação nacional sobre esse tema seja muito visível, há, ao mesmo tempo, uma preocupação do legislador que não é nova e começou a ser delineada no artigo 7º do Marco Civil da Internet.

Recentemente, em 29 de maio de 2018, a Câmara dos Deputados aprovou, em unanimidade, o PL 4.060/2012, que prevê a criação da Lei Geral de Proteção de Dados Pessoais. O início da vigência do GDPR trouxe uma pressão maior sobre o Brasil, pois considerável parte de agentes do setor comercial que atua no país tem base em estados da União Europeia e precisa submeter-se ao novo Regulamento, o qual possui aplicabilidade extraterritorial (SEMINÁRIO INTERNACIONAL, 2018).

Na proposta aprovada e enviada ao Senado Federal, temas decorrentes da temática da tutela de dados que são, hoje, essenciais para a formação de uma nova cidadania foram tratados e ainda serão objeto de debates dos Poderes Legislativo e Executivo antes da efetiva edição de uma norma geral. Destaca-se, por exemplo, o fato de que o consentimento está inserido no texto como apenas uma das hipóteses de legitimação da coleta e do tratamento de dados pessoais, as quais ainda abrange, exemplificativamente, o atendimento a finalidades históricas, estatísticas ou de pesquisas científicas, a execução de obrigações legais ou contratuais e o atendimento ao legítimo interesse dos titulares.

Em 10/7/2018, em regime de urgência, o Senado Federal aprovou por unanimidade o PL 53/2018, mantendo os termos em que houve a aprovação pela Câmara dos Deputados. O projeto, agora, segue para sanção presidencial, a qual deverá ocorrer em meados de agosto do corrente ano.

Esses esforços normativos surgiram em um contexto de criação e expansão da internet como uma ferramenta não prevista para o exercício de vigilância estatal sobre os cidadãos ou para o desenvolvimento de práticas de mercado. Em verdade, o anseio dos criadores nos Estados Unidos consistia na elaboração de um mecanismo de comunicação eficiente, abrangente e que viabilizasse inovação de maneira fácil e amplamente acessível.

Em face disso, propõe-se que, no capítulo seguinte, seja possível perceber em que contexto e sob quais demandas a tutela sobre dados pessoais tornou-se necessária como um direito autônomo, apontando-se a peculiaridade de que o surgimento dessa tecnologia que, posteriormente, veio a constituir um novo ambiente de construção de relações sociais, políticas e econômicas deu-se de forma horizontal e globalizada, o que implica desafios regulatórios próprios desse contexto.

Dentre essas inquietações, pode-se notar que algumas teorias regulatórias dão maior ênfase à importância e, até mesmo, à necessidade de leis formais estatais para a regulação desse ambiente, ao passo que outras focam mais na atuação de agentes que não o estado ou na ingerência estatal por mecanismos não necessariamente legislativos.

A busca por um arranjo regulatório que se mostre adequado para salvaguardar os direitos que passam a demandar proteção no ambiente da internet - tais qual o direito à autodeterminação sobre os dados pessoais - apresenta-se, em verdade, como uma procura por uma forma de conciliar os diversos poderes exercidos nesse contexto do ciberespaço não apenas pelo estado, em suas formas tradicionais, mas também pelos usuários, pela sociedade civil, por agentes econômicos e por desenvolvedores de tecnologia. A premência é de conciliação não apenas desses poderes, mas também de criação de um

cenário de vivência com alguma segurança jurídica e, ao mesmo tempo, viabilidade de desenvolvimento tecnológico e de livre iniciativa de forma compatível com uma nova cidadania que já é vivenciada no ciberespaço.

Daí a relevância de analisar algumas das teorias regulatórias de possível emprego nesse contexto, embora não exista a pretensão de abrangência de todos os modelos possíveis. Nessa linha, a fim de analisar como a valorização normativa está configurada em algumas teorias e como a tutela dos dados pessoais tem efetivamente ocorrido no Brasil, com o contexto normativo já existente, e seguir no objetivo de analisar como cada teoria regulatória estudada neste trabalho tem, ou não, capacidade explicativa da realidade brasileira na tutela de dados pessoais, os modelos sugeridos serão tratados no capítulo seguinte.

3 MODELOS REGULATÓRIOS SOBRE A GOVERNANÇA DA INTERNET

A forma de surgimento da rede mundial de computadores explica por que o desafio regulatório nessa seara é especialmente provocante. De um histórico desse movimento de criação e expansão desacompanhado de leis formais destinadas à regulação dessa tecnologia e do ambiente de relacionamento que ela posteriormente viabilizou, observa-se que o ponto de partida consistia na efetiva instituição de um ótimo instrumento de comunicação destinado a subsidiar ações norte-americanas contra a União Soviética, sem que houvesse uma pretensão inicial econômica ou de gestão estatal.

Isso porque se tratou de tecnologia cujas regras de funcionamento surgiram na medida da necessidade, sobretudo em virtude do imperativo de viabilizar o caráter global da rede, e, assim, não foram impostas horizontalmente pelo estado, mas criadas pela ação dos próprios usuários e, principalmente, pelos desenvolvedores com habilidades técnicas de influenciar na formação dessa tecnologia. A partir da compreensão desse processo de criação é possível notar que a origem e a expansão da internet tornaram-na um ambiente multissetorial e que acarretou grandes desafios regulatórios.

Menciona-se que o primeiro registro de ideia de uma rede formada por meio de computadores encontra-se em escritos de Licklider, do Instituto de Tecnologia de Massachusetts (*Massachusetts Institute of Technology* - MIT), em 1962, nos quais era idealizada uma interconexão global de computadores, a Rede Galáctica, em que seria possível acessar rapidamente dados e programas de qualquer local do planeta. Também dentro do Instituto, ainda na década de 1960, foi publicado estudo de Leonard Kleinrock sobre a viabilidade da comunicação, nessa rede, por meio de pacotes em vez de circuitos, o que foi apresentado em sua teoria das filas (MURRAY, 2013).

Posteriormente, a primeira comunicação entre máquinas ocorreu entre computadores de Massachusetts e da Califórnia, em 1965, e a noção de rede de computadores foi mais bem elaborada na Agência de Projetos de Pesquisa Avançada de Defesa Norte-americana (DARPA - *Defense Advanced Research Projects Agency*), criada por militares e pesquisadores sob a supervisão do governo dos Estados Unidos[25], na qual se inventou a ARPANET (*Advanced Reserach Projects Agency Network*). Até o final da década, o MIT, a Corporação RAND, originada de um projeto destinado a conectar militares e pesquisadores

25 Sobre esse histórico: <https://www.darpa.mil/>.

norte-americanos e o laboratório londrino *National Physical Laboratory* – NPL, de maneira independente, realizaram pesquisas que viabilizaram a comunicação global por pacotes hoje existente na internet. Até 1969, havia 4 pontos comunicados à rede, em 4 instituições de ensino e pesquisa dos Estados Unidos (ISOC, 1997).

Mais computadores passaram a se conectar na rede e, entre 1971 e 1972, tinha sido implementado protocolo *Network Control Protocol* – NCP, o que tornou possível o desenvolvimento de aplicações pelos usuários finais dessa rede, na medida em que as máquinas e os programadores sabiam se comunicar na mesma linguagem. De fato, uma das ideias chave preconizada por tais pesquisadores desde o início da ARPANET consistiu na arquitetura aberta, a qual permite que toda pessoa capaz de realizar programações consiga inserir uma aplicação na rede e torná-la disponível mundialmente a todos os usuários conectados.

A ARPANET, porém, ainda era uma rede fechada e outras redes similares também foram criadas (ALOHANET e SATNET), mas cada uma contava com linguagens, isto é, protocolos de comunicação próprios. Para melhorar a interação, criou-se o protocolo TCP ou *Transmission Control Protocol*, que funciona por meio do "encaixotamento" dos pacotes a serem transmitidos na rede, criando um cabeçalho que permite às máquinas lerem os endereços de origem e de destino do conteúdo e, assim, direcioná-lo ao local adequado. Esse protocolo foi aperfeiçoado ao longo do tempo e, em 1978 John Postel desenvolveu um protocolo duplo, o *Transmission Control Protocol/Internet Protocol* ou TCP/IP (MURRAY, 2013), utilizado até hoje.

Para que seu uso seja possível e, assim, todas as máquinas conectadas à rede possam funcionar e interagir, cada uma deve possuir um número de identificação único, que será utilizado como "endereço" na identificação dos pacotes a serem trocados com uso do TCP/IP. Tal identificação consiste no protocolo IP, atribuído a cada dispositivo que se conecta à rede mundial. Com base nesse número de IP e no cabeçalho gerado em cada pacote que transitará pela estrutura física da rede (cabos de fibra ótica, por exemplo), é possível a transmissão das informações por meio da leitura das informações de remetente e destinatário inseridas em tais cabeçalhos.

Desse breve histórico, pode-se notar que a internet surgiu, inicialmente, por uma necessidade do governo e da academia norte-americana de desenvolvimento de tecnologias com destinação militar, já que a implementação da DARPA visou, inicialmente, a evitar surpresas às forças militares dos Estados Unidos tais como ocorreu com o lançamento do satélite Sputnik I pela União Soviética. A pretensão, então, era de criação de um

instrumento de comunicação eficiente e muito abrangente, por meio de tecnologia com a última camada da arquitetura com fácil acesso para criação de inovações. Não havia, à época, propósitos comerciais diretos e ostensivos na ideia de desenvolvimento desta rede originada praticamente como uma criação norte-americana.

Aos poucos, porém, os atores econômicos passaram a notar o potencial dessa via de comunicação e a abertura da arquitetura da rede permitiu inovações destinadas à criação de novos produtos e serviços, bem como a utilização da internet como ambiente de exercício de atividades econômicas. Ao mesmo tempo, outros estados além do norte-americano identificaram as utilidades dessa tecnologia de comunicação e informação para incremento das atividades estatais, notadamente para a vigilância, na medida em que, cada vez mais, as ações dos indivíduos governados passaram a ocorrer nessa rede, em que tudo é registrado e deixa rastros.

Assim, a expansão desse cenário virtual para além de finalidades acadêmicas e militares foi desacompanhada da apresentação de normas formais pelo estado. Em vez disso, a rede desenvolveu-se com alguns propósitos, foi aproveitada para outros e a regulação foi desenvolvida na medida da necessidade pelos próprios agentes atuantes nesse ambiente.

A imprescindibilidade, por exemplo, do uso de uma linguagem única que permitisse à rede ser mundial conduziu ao estabelecimento de padrões técnicos acolhidos por todos esses agentes, tais qual o protocolo TCP/IP, o que independeu da imposição por normas formais estatais. Na mesma linha, a comercialização nos pontos de troca de tráfego foi surgindo para sustentar os desenvolvedores das tecnologias físicas e de software necessárias para o funcionamento da rede e isso se deu sem a utilização de parâmetros regulatórios governamentais.

Ocorre que, como em outros ambientes de atuação humana (e, na situação da internet, também não humana), a disparidade de forças entre os participantes da rede e as consequências sociais, políticas e econômicas das interações nesse contexto cibernético tornou necessária, para alguns, a intervenção do estado na fixação de normas vigentes nesse contexto.

De todo modo, mesmo nas situações em que essa atuação estatal ocorreu e vem ocorrendo, isso se dá dentro da dinâmica da multissetorialidade e da governança participativa. Não se vivencia, então, um movimento de intervenção estatal vertical e definido no tempo, mas intervenções pontuais no processo de governança da internet.

Assim, por exemplo, intervenção estatal na gestão de recursos críticos da internet como nomes de domínio e números IP deu-se sobre a Corporação da Internet para Atribuição de Nomes e Números *(Internet Corporation for Assigned Names and Numbers* - ICANN), por meio de sua associação ao Departamento de Comércio norte-americano, mediante acordo que visava a fazer uma transição para o gerenciamento do DNS do setor privado (MEMORANDUM, 1998). As preocupações principais consistiam em criar um:

> "organismo independente de interesses comerciais ou governamentais, no qual todas as categorias de agentes da Internet seriam representadas, todas as partes do mundo seriam ativas e suficientemente legítimas para estabelecer regras de jogo aceitas por todos para que decisões críticas pudessem ser tomadas sem provocar uma contestação demasiada, e sobretudo capaz de impedir outros agentes de estabelecer um sistema de gestão de nomes de domínio alternativo" (MOUNIER, 2006).

Embora a transição da administração da Autoridade para Atribuição de Números da Internet (*Internet Assigned Numbers Authority* – IANA) somente tenha acontecido em 2016, desde o início havia a pretensão de sua abertura para uma governança mais participativa e multissetorial. Assim, os processos de tomada de decisões deveriam decorrer da concordância de todos os representantes de setores da internet, como representantes institucionais, comerciais, industriais etc (MOUNIER, 2006). Mesmo assim, sempre se tratou de uma instituição de natureza privada, criada e regida sob a luz da legislação da Califórnia – o que dava ao governo dos Estados Unidos a segurança de que não se tornaria uma agência internacional como a União Internacional de Telecomunicações -, mas que tem ingerência sobre recursos que dizem respeito ao funcionamento da internet em todo o planeta, pretendendo incorporar interesses multissetoriais e globais (MOUNIER, 2006).

Algumas especificidades da internet, portanto, acarretam grandes desafios no estabelecimento de políticas regulatórias em razão de fatores como: i) a significativa influência da tecnologia para seu desenvolvimento - o que gera assimetria informacional entre os diferentes *stakeholders* -; ii) o caráter globalizado da rede, de sua estrutura física, do fluxo de dados e das interações pessoais, econômicas e políticas nela estabelecidas.

Em face disso, no contexto dessa interação entre forças de diversificados atores e arquitetura da rede, questiona-se, na literatura, qual mecanismo regulatório mostra-se adequado para assegurar a privacidade e a tutela de dados pessoais sem prejuízo do emprego dos dados pessoais na geração de valor, isto é, que seja capaz de conciliar os interesses e os direitos dos usuários, do Estado e dos mercados. Tal questionamento perpassa a análise sobre

a efetiva capacidade dos usuários, fonte da matéria prima desse modelo de mercado e de governança - os dados pessoais-, de exercer papel ativo na criação de normas e, portanto, de comportamentos, para exercer sua autonomia e sua privacidade na sociedade da informação contemporânea, especificamente no que concerne aos seus dados pessoais.

Muitas teorias regulatórias são, com esse foco, desenvolvidas, passando-se do ciberlibertarianismo, pelo ciberpaternalismo e pela corregulação, até teorias como a regulação descentrada, sem prejuízo da existência de outras formas de pensar não qualificadas entre essas. O propósito deste exame consiste em indagar se, nos moldes das teorias a serem abordadas, os usuários têm efetivamente desempenhado um papel ativo e significante na formatação da governança da internet tal como sustentado no comunitarismo em rede, mais preponderante do que o das normas jurídicas ou se, nos moldes do ciberpaternalismo de Lessig, representa apenas um agente inerte alvo das forças regulatórias ao seu redor.

A fim de viabilizar essa análise até o final do presente trabalho, objetiva-se, neste capítulo, apresentar teorias regulatórias aplicáveis ao contexto da internet.

3.1 Cipherpunk

A virtualidade das interações e práticas que ocorrem na internet trouxe questionamento sobre a viabilidade de o estado, como em outras áreas da vida, intervir e impor o cumprimento de normas. O questionamento inicial, portanto, sequer disse respeito ao modo como a regulamentação formal poderia ser realizada, mas à própria possibilidade dessa ingerência.

Dentre as correntes mais libertárias de regulação da rede e do comportamento na rede, os cypherpunks ou criptopunks, encabeçados por Timothy C. May, John Gilmore e Eric Hughes, apresentaram como alerta a todos os indivíduos, desde a década de 1990, o ideário de que, por meio da criptografia, os usuários fizessem a necessária modificação social e política na rede (SILVEIRA, 2015). Em 1994, MAY (1994) redigiu o *The Cyphernomicon: Cypherpunks FAQ and More, Version* 0.666, no qual, embora alertando para a ausência de disposições oficiais sobre a doutrina *cypherpunk*, listou como pontos centrais dessa teoria então emergente:

> "- Que o governo não deve poder espionar as atividades das pessoas;

> - Que a proteção de conversas e negociações das pessoas seja um direito básico;
> - Que esses direitos possam ser assegurados pela tecnologia em vez das leis;
> - Que o poder da tecnologia muitas vezes crie novas realidades políticas (daí o mantra: 'Cypherpunks escrevem códigos')".

Nota-se, portanto, que a lei não é reconhecida como mecanismo regulatório eficaz na rede mundial de computadores, mas sim os próprios usuários - diretamente ou por meio da tecnologia e de artefatos tecnológicos. Estes usuários, ao seu turno, teriam como instrumento a criptografia forte para assegurar seus direitos na internet e, assim, ter força nesse universo de mecanismos regulatórios.

A lógica da *bitcoin*, por exemplo, acompanha esse modo de pensar, pois se trata de unidade monetária que não é emitida nem regulada pelo governo, mas emitida e transacionada diretamente pelos próprios usuários. As operações com essa moeda são realizadas sem a necessidade de intermediação pelo governo ou instituição financeira, pois a tecnologia usada para a transferência é *peer-to-peer* (P2P). Embora seja possível a intermediação das operações por um terceiro, como uma instituição, esta é dispensável e não está vinculada a entidades governamentais. Dessa maneira, os usuários são os próprios gestores das transações quando emitem o numerário ou quando confirmam seu recebimento (ROMA, 2016).

Além de a autonomia dos usuários nesse processo coadunar com a teoria dos cypherpunks, o uso da tecnologia da criptografia também acompanha a proposta, na medida em que a segurança das trocas de *bitcoin* é buscada por meio do uso da criptografia por chaves públicas, numa estrutura de registros e conferência de chaves denominada *blockchain*.

Até mesmo as conferências das chaves são feitas por usuários, e não por entidades governamentais, pois se executam por cálculos matemáticos operados por computadores espalhados pelo mundo e disponibilizados também por usuários (*miners*). Por conseguinte, a emissão da moeda é totalmente descentralizada e inexiste influência de política monetária estatal (ROMA, 2016) - ao menos por enquanto -, concretizando a autonomia total pregada pelos cypherpunks.

Já em 2012, por meio da obra de Julian Assange (2013), os cypherpunks lançaram um alerta para o que chamam de caminho a uma "nova distopia transnacional" da vigilância pós-moderna, indicando que a internet, tal como está formatada, conduz a um caminho sigiloso rumo ao totalitarismo, em ameaça à civilização. A premissa do pensamento reside na identificação do Estado como ator nesse cenário, especialmente a partir da

manipulação sobre a estrutura física em que se formou a internet e por meio da interceptação do fluxo das informações na rede. O contexto condutor dessa crença é assim descrito:

> "O Estado se agarraria como uma sanguessuga às veias e artérias das nossas novas sociedades, engolindo sofregamente todo relacionamento expresso ou comunicado, toda página lida na internet, todo e-mail enviado e todo pensamento buscado no Google, armazenando esse conhecimento, bilhões de interceptações por dia, um poder inimaginável, para sempre, em enormes depósitos ultrassecretos. E passaria a minerar incontáveis vezes esse tesouro, o produto intelectual privado coletivo da humanidade, com algoritmos de busca de padrões cada vez mais sofisticados, enriquecendo o tesouro e maximizando o desequilíbrio de poder entre os interceptores e um mundo inteiro de interceptados. E, então, o Estado ainda refletiria o que aprendeu de volta ao mundo físico, para iniciar guerras, programar *drones* manipular comitês das Nações Unidas e acordos comerciais e realizar favores à sua ampla rede de indústrias, *insiders* e capangas conectados (ASSANGE, 2013).

Assim, o ponto de partida dos adeptos de tal doutrina consiste na percepção de que a internet, enquanto passou a viabilizar maior comunicação entre todos, também passou a ser instrumento totalizador. Os usuários divulgam suas ideias, seus planos e suas relações, o que permite uma vigilância antes impossível, de sorte que, em vez de aumentar as liberdades e as possibilidades de livre manifestação, a rede passa a constituir instrumento de impedimento do exercício de direitos civis.

O ideário libertário preconiza que a reação necessária para assegurar os direitos individuais na rede advenha dos próprios usuários, e não do Estado ou do mercado: "não podemos esperar que os governos, as empresas ou outras grandes organizações sem rosto nos conceda a privacidade" (HUGUES, 1993[26]). A crença, portanto, é de que a tecnologia tem poder político de modificar a realidade social e alterar o jogo de poder nesse ambiente (SILVEIRA, 2015).

3.2. Ciberlibertarianismo

Na linha da descrença sobre a possibilidade de regulamentação formal do ciberespaço, em meados da década de 1990, John Barlow passou a asseverar em sua

[26] Referência direta sem indicação de página em razão de se tratar de documento virtual, disponível em <http://www.activism.net/cypherpunk/manifesto.html>. Acesso em 9 de março de 2018.

Declaration of Independence of Cyberspace, que o ambiente virtual constituía um mundo distinto do físico. Segundo o autor, os "Governos do Mundo Industrial" não têm soberania no ciberespaço, já que não teriam sido eleitos para atuação nesse ambiente e não possuem instrumentos de execução de suas normas (BARLOW, 1996).

Em suma, o fato de o ciberespaço não se encontrar dentro das fronteiras físicas dos estados constituiria impeditivo para atuação estatal, de modo que, na medida do surgimento dos problemas e conflitos, deveria ser moldado um contrato social pelos próprios usuários da rede. Em face disso, para a escola ciberlibertarianista, os legisladores tradicionais apenas têm legitimidade para exigir o cumprimento das normas no interior do espaço físico geográfico do país onde foram eleitos.

Nessa mesma direção, Johnson e Post, em 1996, defenderam em seu trabalho *Law and borders: the rise of Law in cyberspace* a impossibilidade de a regulação tradicional funcionar nesse novo ambiente. Assim, sustentaram que os indivíduos, na rede, movem-se entre zonas de jurisdições distintas de acordo com sua preferência quanto ao regime regulatório aplicável, o que geraria uma arbitragem regulatória (JOHNSON e POST *apud* MURRAY, 2013).

No entanto, os fundamentos dessa teoria falham quando se observa, primeiramente, que a despeito de as interações na internet ocorrerem em ambiente virtual, a rede em si é caracterizada por uma estrutura física que se mostra imprescindível nos países em que a internet é acessível.

Além disso, ainda que as questões relacionadas à coercibilidade de ordens e leis de gestão da internet por agentes públicos nacionais ainda gerem controvérsias e desafios, a alegação da ausência de coercibilidade por falta de territorialidade não se sustenta quando se percebe que essa questão é mais de soberania do que de geografia. Diante disso, o ciberlibertarianismo passou a sofrer críticas por supor que, para atuar no ciberespaço, os indivíduos são transpostos para um mundo à parte, onde seria impossível reconhecer o cometimento de condutas ilícitas e a elas reagir, chamando-se tal suposição de "falácia do ciberespaço" (REED, 2004).

Ademais, a sustentação de que, na medida em que os erros e as dificuldades surgem no mundo digital, os próprios usuários os identificam e resolvem por seus próprios meios tem se mostrado insuficiente quando se nota a vulnerabilidade dos atores em determinadas matérias, como do estado em face dos desenvolvedores das tecnologias ou dos usuários em face dos governos e dos agentes econômicos atuantes na rede.

Assim, a crença de que “da ética, do autointeresse esclarecido e do bem comum” (BARLOW, 1996) surgirá a governança da internet, a partir de escolhas da maioria dos usuários, não pressupõe a disparidade de forças dos diversos agentes participantes desse contexto tampouco é apresentada com a explicação sobre o critério para identificação daquela maioria.

Além disso, também não há explicação sobre quem compõe o grupo de atores atuantes na internet e que poderá ou conseguirá participar da governança pregada. Atualmente, a ausência de uma definição quanto a esse aspecto, isto é, sobre quem compõe a comunidade de usuários da internet, e quem está autorizado a falar por eles, associada à ausência de regulação estatal em alguns aspectos da rede, tem conduzido à percepção de que os interesses econômicos dos provedores e dos responsáveis pela criação e manutenção da arquitetura física da rede têm predominado como fonte regulatória desse ambiente (DENARDIS, 2014; SCHEWICK, 2010), ou seja, não têm sido todos os participantes da rede os moldadores da regulação nesse espaço.

3.3 Ciberpaternalismo

A partir da contraposição aos fundamentos dos ciberlibertarianistas, nova corrente de pensamento baseou-se na necessidade e na viabilidade de regulação do ciberespaço, inaugurando o ciberpaternalismo. Embora dividido em diferentes vertentes, o ciberpaternalismo assume a possibilidade de criação de normas específicas para regulação desse espaço, de modo que as especificidades desse novo ambiente exigem adaptações regulatórias, mas não impedem a ingerência regulatória estatal.

O propulsor anunciado desse pensamento, Reidenberg, partiu da derrubada do argumento dos ciberlibertarianistas do impedimento territorial, apontando a existência de uma arquitetura física da rede, a partir da qual seria viável o reconhecimento de uma nova geografia, criada pelo homem. Sugeriu, então, seguir os padrões da arquitetura física da rede para moldar a arquitetura regulatória. Considerando a influência dos contratos celebrados entre os provedores de serviço e a arquitetura de camadas da rede, Reidenberg propôs uma regulação a partir das normas “impostas” aos usuários pelas tecnologias e sistemas, o que denominou *Lex Informatica* (REIDENBERG, 1996).

Nesse sentido, para obter êxito na regulação, não caberia ao estado impor normas que desconsiderassem a influência das estruturas físicas e técnicas inerentes à

existência da internet, mas levar em conta, no estabelecimento de sua metodologia regulatória, o fato de que as ingerências precisam ser feitas sobre a arquitetura da rede. Assim, as normas estatais são reconhecidas como apenas um dos múltiplos fatores que compõem o conjunto de fontes capazes de regular o ciberespaço.

Assim, enquanto os ciberlibertarianistas acreditam que a falta de uma identificação do espaço físico em que atua o usuário da rede e a inexistência de irrestrita legitimidade das autoridades por todo o globo impedem uma regulação por um centro oficial de poder, os ciberpaternalistas creem que, dada a natureza do ciberespaço, as normas devem focar nos desenvolvedores de tecnologia e na arquitetura da rede. Para estes, então, a regulação é possível, mas apenas não se faz por um centro oficial, e sim de forma descentralizada.

Um dos expoentes dessa linha, Lessig identifica 4 instrumentos que podem ser utilizados para a regulação da rede, juntamente ou não e direta ou indiretamente, a saber: o direito, que regula por ameaças de punição; as normas sociais, das quais decorre a possibilidade de aplicação de sanções sociais; o mercado, que constrange pelos preços; e a arquitetura da rede, a qual impõe constrições físicas.

O que distingue a teoria de Lessig de outros ciberpaternalistas é o papel do usuário nesse contexto, ou melhor, a ausência de um papel ativo desse ator. Embora reconheça a força regulatória de leis formais mesmo no ciberespaço, superando, assim, a visão dos ciberlibertarianistas, na modalidade regulatória sustentada por Lessig não há postura ativa dos usuários na criação das normas regulatórias, já que estes situam-se, em verdade, como *pathetic dots*. Nessa senda, apenas o mercado, a arquitetura da rede, as leis estatais e as normas sociais conseguem ter força regulatória, podendo variar a intensidade e as forças de cada um desses elementos em cada momento ou contexto.

A distinção da teoria consiste em reconhecer nos aspectos técnicos da rede de computadores a força regulatória, de modo que o novo "código", que atribui nome à sua obra (LESSIG, 2006), é a conjunção dos softwares e hardwares que moldam o ciberespaço. A capacidade regulatória desse código decorre do fato de que, por meio das características técnicas e do design moldados pelos técnicos de grandes companhias privadas, estes são capazes de escolher que ações são tecnicamente possíveis ou não na rede.

Nessa direção, além de indicar a capacidade de regulação do ciberespaço pelas leis criadas pelos governos, por meios tradicionais como coerção penal ou poder de polícia, também identifica a regulabilidade pelo código (arquitetura), de sorte que, na

intenção de impor comportamentos em determinada direção, cabe ao estado, ao mercado e às normas sociais atuar por meio da imposição de regras também a esta arquitetura.

Com o intuito de mais bem desenvolver a teoria ciberpaternalista já lançada, sobretudo no que diz respeito ao papel do usuário como elemento ativo ou inativo nesse conjunto de forças regulatórias, Murray apresentou sua teoria do comunitarismo em rede, tratada no tópico seguinte.

3.4 Comunitarismo em rede

Contrapondo-se a Lessig, Murray (2013) apresentou sua ideia de regulação simbiótica e seu comunitarismo em rede como uma das correntes de corregulação. Na pretensão de tratar a relação entre o mundo virtual e o mundo físico de maneira mais fluida que as escolas anteriores, Murray baseia-se no modelo de apresentação de Lessig, o qual havia situado os usuários como atores humanos sem poder de ação (*pathetic dot*), no meio de um sistema de forças regulatórias compostas pelo mercado, pela arquitetura, pelas normais sociais e pelas leis.

Uma representatividade da dinâmica proposta por Lessig pode ser realizada pela seguinte figura:

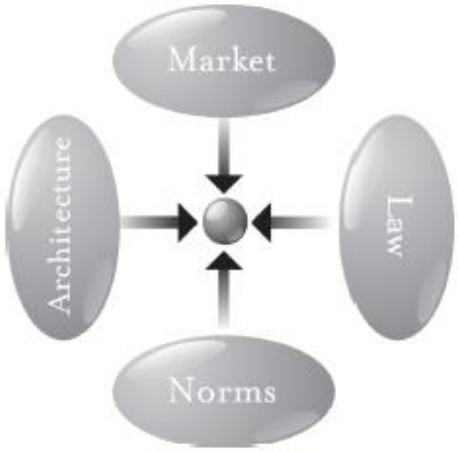

Figura 1 – Fontes de regulação para LESSIG
Fonte: LESSIG, 2006, p. 123.

No entanto, Murray reposiciona aqueles atores para que, saindo do centro desse sistema, isto é, deixando de ser apenas destinatários dessas forças, o próprio ponto (usuário) passe a, ativamente, fazer parte de uma rede de atores, uma matriz da qual o direito,

as normas sociais e o mercado retiram sua legitimidade a partir de um diálogo entre si e com o usuário.

O autor destaca sua percepção de que o código ou regulamento por design da arquitetura constitui uma segunda ordem de regulação, mas que não substitui as forças de primeira ordem de imposição de regras, isto é, leis, normas sociais e mercados. Com base nisso, o autor baseou sua concepção regulatória na Teoria do Ator Rede (*Actor Network Theory* – ATN) e na Teoria dos Sistemas Sociais (*Social Systems Theory* – SST).

No desenvolvimento da ATN, Latour (2012) resgata os conceitos de "social" e "explicações sociais", indicando a necessidade de sua reformulação. Criticando a banalização do termo social, no qual tudo tem sido encaixado na sociologia, defende que social deve constituir apenas ligações, associações feitas por meio de determinados canais, as quais precisam passar a ser consideradas pelos sociólogos. A identificação de novas associações depende do reconhecimento de que há mais espécies de seres no mundo social em interação do que a sociologia tem reconhecido.

De fato, a limitação da sociologia tradicional (sociologia do social) faz com que não se consiga explicar certas situações originadas de inovações e nas quais há inéditas formas de associações de atores. Assim, Latour modifica o foco do social para as associações, lançando sua sociologia das associações. Para a finalidade de contribuição na formação do comunitarismo em rede, a sociologia das associações tem a contribuição de identificar o social como uma rede composta de nós, sendo estes todos os pontos de associações e conexões, podendo ser humanos ou não-humanos (artefatos tecnológicos como uma máquina ou um software). Assim, seres humanos e não-humanos são considerados igualmente potenciais actantes (*actant*) e exercem essa capacidade quando conseguem efetivamente desempenhar algo.

Outro ponto central de contribuição consiste na aceitação, pela ANT, de que há transações sociais feitas com atores não-humanos em toda situação vivida. O local onde uma experiência ocorre, por exemplo, afeta o resultado dessa vivência, pois os elementos não-humanos compõem o ambiente e interferem nas sensações, interações e resultados percebidos. Os atores não-humanos, então, fazem parte do próprio contexto, afetando e transformando esses ambientes de interação com os atores humanos.

Para Murray, isso tem grandes efeitos quando se trata da internet, pois esta rede é rica em interações e experiências entre pessoas e permite transações sociais entre indivíduos com localizações geograficamente remotas e sem um passado comum. Assim, uma das capacidades da internet está em viabilizar a formação e dissolução de novas redes,

deixando de ser considerada apenas um meio de comunicação e passando a ser vista como um instrumento social (MURRAY, 2013).

Ao lado disso, a Teoria dos Sistemas (SST) de Luhman contribuiu na composição do comunitarismo em rede por meio do tratamento das noções de comunicação e de interação social. Na SST, a compreensão de sistema consiste em um composto isolado e fechado do seu entorno, ainda que vários tipos de sistema (jurídico e econômico, por exemplo) possam conviver. A despeito desse fechamento, os sistemas são comunicativos, sendo que a comunicação é necessariamente social, pois depende de interação entre os sistemas, ou seja, inexiste comunicação individual (RODRIGUES, 2012).

Outro aspecto central na teoria em tela consiste na complexidade, reduzida no interior de cada sistema, mas alta nos processos comunicacionais, isto é, de interação entre os sistemas. Assim, Luhman procura explicar como os processos de comunicação afetam as transações sociais.

Analisando essas noções juntamente com a ANT, Murray identifica o *pathetic dot* não como um ator sem ação no sistema regulatório, mas um ponto material nos termos da Teoria do Ator Rede e uma parte do sistema nos moldes da Teoria dos Sistemas. Assim, não se trata de um elemento isolado, mas uma parte de uma matriz de outros pontos. Significa dizer que não é separado das forças regulatórias identificadas por Lessig (mercado, direito, normas sociais e arquitetura da rede), mas um componente do sistema em que todos estão inseridos e atuantes. Por conseguinte, o indivíduo não é mero alvo do processo regulatório da internet, mas elemento que compõe essa dinâmica e interage com os demais.

Esse processo de interação é figurado da seguinte maneira:

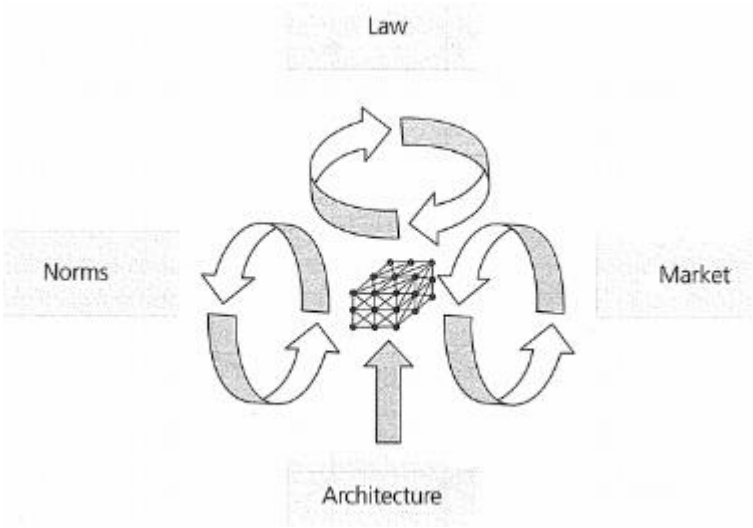

Figura 2 – Fontes de regulação no comunitarismo em rede

Fonte: MURRAY, 2013, p. 69.

O autor apenas não identifica tal interação com a arquitetura. De fato, quanto às normas sociais, aponta que elas mesmas são resultado de escolhas de representantes eleitos pela própria comunidade, ao passo que os mercados constituem reflexo de valores e demandas humanas e as normas sociais codificam os valores de uma comunidade, composta pelos indivíduos. Por outro lado, quanto à arquitetura da rede como uma das fontes regulatórias, não há efetivo diálogo e participação por parte dos usuários na teoria desenvolvida por Murray.

Neste ponto, é válido destacar que essa ausência de interação entre arquitetura e usuários como fonte regulatória trata de uma construção própria do comunitarismo, que nem sempre é acompanhada por outros modos de pensar. No movimento software livre, por exemplo, cuja criação é atribuída a Richard Stallman em meados da década de 1985 nos Estados Unidos, tem-se como um dos propósitos centrais o controle, pelos usuários, da tecnologia presente em suas vidas (STALLMAN, 2002)[27]. Como isso pressupõe a abertura do código dos softwares para que os usuários tenham liberdade para executar o programa, conhecer e/ou mudar seu código-fonte, redistribuir cópias e repassar versões modificadas no software, os defensores do movimento creem na viabilidade de que, por meio desses princípios éticos (as 4 liberdades), as pessoas não sejam reféns do controle pelos proprietários de programas.

Esse movimento, portanto, tem como premissa o reconhecimento de que, por meio das liberdades exercíveis sobre os códigos dos softwares, os usuários não apenas participam, mas também definem a arquitetura e, assim, conseguem atuar no ambiente regulado também por meio dessa interação, não reconhecida no comunitarismo em rede.

Feita essa ressalva, nota-se que, a partir das premissas apresentadas e por meio da análise de diversos casos concretos, Murray chega a uma concepção de matriz regulatória dentro da qual as escolhas dos usuários possuem um papel de proeminência quanto ao alcance dos objetivos, de sorte que um adequado formato de regulação deva ser uma "regulação simbiótica" entre os participantes dessa rede.

De fato, Murray trata não apenas de comunitarismo em rede, mas também de um modelo de regulação simbiótica que leva em consideração a existência de um papel ativo da comunidade em responder e influenciar ações regulatórias (MURRAY, 2007).

[27] Para mais informações sobre a Fundação Software Livre: https://www.fsf.org/.

Ademais, sugere que, por meio do mapeamento dos vínculos entre os diversos atores, uma regulação adequada resultará da amarração entre tais relações. Entendendo que o papel que a comunidade pode desenvolver é essencial para o processo de regulação na internet, o modelo de regulação simbiótica explicaria aquela função e sugeriria um caminho efetivo para a abordagem regulatória.

Assim, em vez de ser algo imposto, a regulação decorreria de um diálogo entre indivíduo e sociedade. Em algumas situações, a sociedade, por meio de seu comportamento ou da expressão de opinião, refutará a aplicação das leis formais e, em outras, o conjunto regulatório formal é que será capaz de modificar o comportamento dos componentes da sociedade. A título de exemplo, o autor menciona a superveniência da perda de aplicação da Lei das Publicações Obscenas de 1959 (*Obscene Publications Act* 1959), que condenava o acesso particular a material com conteúdo obsceno. A sociedade do Reino Unido, de fato, coletivamente decidiu, por meio do comportamento de seus indivíduos, que ver pornografia por conexão pela internet não é, por si só, conduta moralmente passível de objeção (MURRAY, 2011).

Ocorre que, na temática específica deste trabalho, dada a assimetria informacional acerca da coleta e do uso dos dados pessoais, mostra-se de difícil concretização esse modelo regulatório no qual a força do usuário é realmente reconhecida como uma das fontes regulatórias sendo, assim, mais valorizada. No contexto analisado, em verdade, ao menos por enquanto, são os desenvolvedores de tecnologia e os agentes de mercado as principais fontes de regulação das práticas na rede.

Merece registro o fato de que, embora o domínio sobre a tecnologia dê a esses programadores especial poder nesta sociedade da informação (CASTELLS, 2015), boa parte dos benefícios advindos desse domínio são econômicos e são aferidos com base em acordos dessa natureza. Tais agentes de mercado, assim, acabam por controlar a própria arquitetura da rede, notadamente nas camadas de infraestrutura e na camada lógica por meio de práticas que viabilizam, por exemplo, a violação da neutralidade da rede, como quando são oferecidos pacotes de dados por empresas de telefonia com acesso ilimitado a apenas algumas aplicações, como Whatsapp. Por meio desses negócios jurídicos de viés econômico, os agentes de mercado, juntamente com os desenvolvedores de tecnologia, modulam comportamentos, ideias e valores.

Brown e Marsden já apontavam, em seu *Regulating Code: Good Governance and Better Regulation in the Information Age*, como mesmo o mais trabalhado

conjunto regulatório sobre a internet pode sucumbir quando os aspectos da arquitetura da rede se sobrepõem às teses jurídicas subjacentes ao texto normativo.

Em sua concepção, a noção de corregulação decorreu do trânsito de uma abordagem neoliberal para uma autorregulatória, tendo-se alcançado a corregulação como modelo no qual se asseguraria maior transparência, democracia e respeito aos direitos fundamentais (MARSDEN, 2011). Na participação nesse processo de intercâmbio de forças, no entanto, os focos têm sido os estados e os agentes econômicos. O domínio sobre a técnica subjacente à formatação física da internet mune os agentes econômicos da força necessária para influenciar quais e em que medida os direitos dos usuários serão observados, incluindo-se aqueles afetos aos seus dados pessoais. Ao lado disso, embora possa ter variações quanto à forma de exercício do seu papel, os governos têm instrumentos para interferir, nem que seja pela via da sanção, nas práticas de violação ou garantia de tais direitos.

Na ideia central da perspectiva da corregulação, os múltiplos atores do cenário da internet, incluindo-se os consumidores, constituem parte do processo de construção do modelo regulatório e tal possibilidade de participação mostra-se como pressuposto da legitimidade da regulação (MARSDEN, 2011), o que se compatibiliza com as noções do comunitarismo em rede de MURRAY.

3.5 Regulação responsiva

Na busca de um meio termo entre as teorias libertárias e as mais intervencionistas, Ayres e Braithwaite (2011) apresentaram sua teoria da regulação responsiva, a qual pode ser reconhecida como uma modalidade de regulação descentrada, já que também se constrói sob a premissa de um meio termo entre comando e controle e desregulação (PINHEIRO, 2017). A proposta foi exposta ao final do século passado e tem como pilar a noção de pirâmide regulatória, idealizada inicialmente não para o ciberespaço, mas para mercados econômicos e posteriormente ampliada para outros contextos.

Os autores partem da premissa de que inexiste um modelo único de boa regulação, sendo que o formato adequado variará conforme a estrutura de cada mercado e das razões que levam os atores a agir de uma ou outra maneira.

No modelo da pirâmide regulatória, a base da pirâmide é o ponto de partida do regulador e nela predomina, em verdade, a autorregulação. A partir da observação do

comportamento dos atores do mercado autorregulando-se, cabe ao gestor analisar em que aspectos são praticados abusos ou ilicitudes, demandando sua ingerência. Para agir ativamente, a ele caberá eleger entre mecanismos de persuasão e dissuasão, com preferência àqueles por serem menos invasivos na dinâmica natural do mercado regulado.

Assim, aplicando-se, primeira e preferencialmente, medidas de persuasão e partindo-se para as dissuasórias, mais incisivas e voltadas à punição, somente quando as primeiras não acarretarem uma resposta positiva do agente regulado, pretende-se criar um modelo de colaboração. A estratégia do regulador consiste em deixar clara a possibilidade de uso de instrumentos de dissuasão, mas mostrar ao agente econômico que, com sua colaboração, técnicas não punitivas serão empregadas preferencialmente.

Para que esse método de preferência entre as técnicas de *enforcement* funcione, disponibilizam-se ao gestor muitas opções de persuasão, ao passo que, quanto mais se aproxima da técnica de dissuasão mais grave e raramente usada, a exclusão do agente do mercado, reduzem-se as possibilidades de medidas à disposição do regulador. Por isso, fala-se em pirâmide.

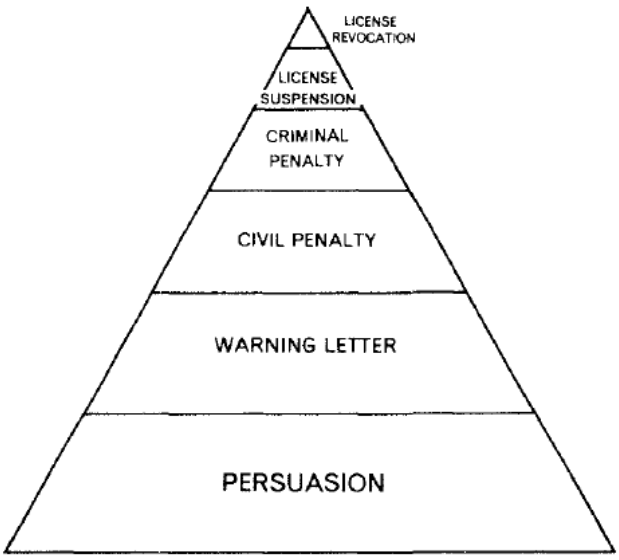

Figure 2.1. Example of an enforcement pyramid. The proportion of space at each layer represents the proportion of enforcement activity at that level.

Figura 3 – Pirâmide de *enforcement* na regulação responsiva

Fonte: AYRES; BRAITHWAITE,1992, p. 35.

Assim, partindo-se do comportamento natural dos agentes em determinado campo de regulação, aplicam-se medidas de persuasão quando necessária a intervenção do

regulador, as quais são mais voltadas para cooperação e prevenção. A depender da resposta desse agente – daí falar-se em teoria responsiva -, parte-se para alguma medida um pouco menos persuasiva e mais dissuasiva, em gradação, de forma que os mecanismos mais acusatórios e punitivos são usados de forma subsidiária aos cooperativos.

Para ser responsivo nos moldes da teoria proposta, o regulador precisa conseguir observar como os demais participantes desse cenário regulatório (empresas e indivíduos) reagem à intervenção estatal e como têm se autorregulado.

A teoria sofreu críticas e reconstruções desde sua apresentação e o próprio Braithwaite expôs, em 2011, seu refinamento da proposta, apresentando seus 9 princípios da teoria de regulação responsiva.

O primeiro deles preconiza que não se pode partir de uma teoria preconcebida, sendo necessário estudar o contexto a fim de identificar que metodologia pode ser a mais adequada. No segundo princípio, o que recomenda que se ouça ativamente os atores do campo de regulação, indica a necessidade de que se dê aos atores a possibilidade de participação e se permita identificar suas motivações. Isso conferirá o caráter colaborativo da regulação, já que, a partir do diálogo, o maior número possível de envolvidos na regulação vão perceber que suas motivações e interesses são relevantes, além de que poderão participar da criação das regras (BRAITHWAITE, 2011).

Pelo terceiro princípio dessa reformulação, visa-se a obter o engajamento dos atores que resistem a colaborar, o que deve ser feito a partir do aproveitamento dessa situação, por parte do regulador, como oportunidade para melhorar o sistema. No quarto preceito, estimula-se a inovação e o aprimoramento, por meio da valorização dos que melhoram sua atuação dentro do contexto regulado. Cabe ao gestor, ainda, deixar claro a todos os envolvidos a preferência pelo emprego dos métodos colaborativos, os quais, porém, dependem da reação positiva do regulado. Esse quinto princípio complementa-se com o sexto, pelo qual deve ficar evidente aos regulados a existência de mecanismos de sanção, incluindo-se o mais grave, consistente na proibição de atuação.

Já pelo sétimo princípio, apregoa-se a criação de uma escalada da pirâmide em rede. Em outros termos, a cada degrau que o regulador sobe em direção à sanção mais gravosa e mais onerosa ao sistema, deve engajar mais participantes que apoiam essa subida.

O oitavo pilar da teoria reformulada recomenda ao regulador estimular a responsabilidade ativa dos atores, a qual é atingida quando eles obtêm desempenhos cada vez melhores dentro do sistema regulado. Apenas subsidiariamente vale-se da responsabilização passiva, pela qual se atribui ao agente a responsabilidade por um ato pretérito.

Por fim, deve o regulador sempre avaliar as escolhas realizadas e os impactos que elas causaram no contexto regulado. Essa prática vai ao encontro da premissa do modelo teórico de que inexiste um formato ideal previamente estabelecido para a melhor regulação, a qual, em verdade, é contextual e depende de adaptações ao campo regulado.

Especificamente para setores em que ocorrem grandes mudanças tecnológicas, os autores propõem a ingerência estatal mais focada na persuasão que na dissuasão, sob pena de esta, de toda forma, não ser efetiva em razão de sua rápida desatualização em face das inovações.

3.6 Regulação descentrada

Compondo as propostas teóricas atuais sobre regulação e no propósito de alcançar o conceito do que é regulação e de quem a executa, Black apresentou sua nova concepção sobre o tema na forma da regulação descentrada, contrapondo-a à regulação tradicional baseada na fórmula de "comando e controle" (CAC- *command and control*).

A autora aponta que, cada vez mais, a ideia de regulação tem sido formada de maneira descentralizada, isto é, fora do Estado e até mesmo dos fóruns tradicionais de regulação (BLACK, 2002). De forma geral, percebe que descentralização é um termo sempre usado para expressar situações em que o governo não tem ou não deve ter o monopólio na regulação; a retirada da situação de hierarquia estado-sociedade.

Isso tem permitido aos estudiosos reconhecer, como parte da regulação, entidades e atores sociais antes marginalizados, o que conduz, também, à identificação de novas configurações da relação entre estado, comunidade, mercado e outros participantes de determinada rede. Nesse ponto de vista, não existe apenas o estado regulador, mas também a sociedade reguladora, de modo que a atividade de regulação é descentralizada.

No regime tradicional, de comando e controle, a ideia base da regulação consiste em impor normas a um setor destinadas a coibir comportamentos em desacordo com a orientação visada pelo estado. Para isso, o estado se assume como ator dotado – e exclusivamente dotado – da capacidade de controlar e comandar. Em outros termos, impõem-se comandos a fim de controlar comportamento, sendo que a apresentação de comandos prévios destina-se a conferir segurança e previsibilidade quanto aos parâmetros de controle (O'SULLIVAN; FLANNERY, 2011).

Na regulação descentrada, uma de suas premissas impede a lógica do comando e controle. De fato, a teoria presume que a autorregulação é um fato que os agentes políticos precisam aceitar; não se trata de uma escolha regulatória, sendo que o desafio do regulador consiste em regular a autorregulação. Assim, se a atuação do estado já presume o início do processo regulatório provocado pelos próprios regulados, a apresentação de comandos para controle não se sustentará se não considerar a dinâmica já estabelecida.

Nessa direção, Black apresenta os pilares da regulação descentrada a partir das falhas do formato tradicional de comando e controle. Dentre tais pilares, situa-se a percepção da complexidade das interações entre os atores da sociedade (ou entre os sistemas, na teoria dos sistemas), das quais resultam os problemas sociais.

Ao lado disso, a fragmentação do conhecimento também é uma das bases teóricas, pois se assume que cada ator participante do processo regulatório tem conhecimentos e instrumentos para solucionar problemas. Embora os conhecimentos de cada ator sejam limitados, e não absolutos, essa possibilidade de utilizá-los no ambiente regulado não é uma exclusividade de um ou outro grupo. Igualmente é fragmentado o exercício do poder e do controle, os quais não cabem exclusivamente ao estado, antes são divididos entre diversos atores sociais.

Cada um desses atores, ademais, é dotado de autonomia, não no sentido de liberdade em relação à interferência governamental, mas no de que, ainda que esta intervenção exista, cada um guarda seu próprio jeito de agir. A regulação, então, não consegue sempre modificar o comportamento dos regulados. Por conseguinte, nenhum ator social consegue dominar o processo regulatório unilateralmente, pois os resultados de suas ações não serão necessariamente aqueles por eles esperados, não somente em razão da limitação de seu conhecimento, mas também em virtude da autonomia dos demais.

Outro pilar apresentado pela autora consiste na existência e complexidade de interações e interdependência entre os atores sociais. Logo, a regulação é um processo de várias vias, existentes entre todos os reguladores e regulados, isto é, a regulação é coproduzida. Assim, para uma regulação eficiente, não é possível tratar o cenário regulatório como uma situação em que a população tem questões e o governo tem soluções. Em verdade, todos têm necessidades e capacidades e são mutuamente dependentes.

Uma das bases da regulação descentrada decorre das demais anteriormente citadas. Em razão da complexidade das relações, da fragmentação do conhecimento e do exercício de poder e controle, do reconhecimento da autonomia dos atores sociais e da complexidade das interações entre os atores sociais, o papel do estado precisa ser repensado

para que sua regulação surta os efeitos desejados. Daí a autora assumir o colapso da distinção público-privado em termos sócio-políticos. Isso leva a repensar o papel da autoridade formal na governança e na regulação, pois, na visão descentrada da regulação, esta ocorre na ausência de sanções formais, pois é o produto das interações, e não de ações do governo.

Por fim, Black diferencia as sociedades entre sistemas autorreferenciais cognitivamente fechados e abertos. A ideia é que a regulação deve ser indireta, focada nas interações entre os sistemas e atores, o que deve ser considerado não apenas pelos governos, mas por todos que atuam na regulação.

Por identificar a autonomia de todos os participantes do processo regulatório, uma das preocupações da autora consiste em definir o papel da autorregulação em sua teoria. Nesse intuito, verifica que a autorregulação pode caracterizar-se de diversas maneiras, mas, em todas as concepções, a iniciativa regulatória ocorre de forma separada do governo, o que implica reconhecer que há sistemas de organização da sociedade existentes separadamente do aparato estatal. Logo, por definição, a autorregulação não pode abranger uma forma híbrida, isto é, alguma forma de participação do estado.

Há um perigo de que a autorregulação seja configurada apenas como uma nova forma de regulação por comando e controle. O sucesso de uma autorregulação depende da relação entre seus membros. Além disso, há uma feição implícita à autorregulação que deriva do seu nome. Implícita no termo está a suposição de que o alvo e o agente da regulação são o mesmo. Supõe-se que esse eu seja autônomo, na medida em que constroi as razões de suas ações e o que está em questão é sua capacidade de influenciar a criação das normas.

Na regulação descentrada, uma das ideias consiste em que “um governo nunca deveria regular uma área em que não há autorregulação”. Um aspecto normativo dessa regulação descentrada consiste em que a intervenção na autorregulação dos atores deve ser indireta. Os governos podem usar seu poder regulatório para ajustar, balancear, facilitar, negociar, mas nunca para diretamente controlar.

Black trata de como essa capacidade autorregulatória é aproveitada. Os instrumentos do governo são os mesmos (financeiro – financiamentos, empréstimos, subsídios -, legal e informacional), mas o modo de uso é diferente na sua proposta.

Uma sugestão de estratégia indireta consiste na criação de um cenário de colaboração nos sistemas autorregulados, a partir da constante oposição entre estados alternativos de forças. O governo atua estabelecendo procedimentos de tomadas de decisão dos demais atores de modo que a política pública desejada seja alcançada. Assim, alternando estados de maior ou menor rigor de algumas forças, o criador da política pública atua numa

dinâmica que já existe, por exemplo, no sistema de pesos e contrapesos, nas políticas de educação dos consumidores, no uso de subsídios em favor ou desfavor de certos agentes no mercado etc.

A atuação estatal, portanto, será sempre uma via pós-regulatória. Em que consiste, então, essa pós-regulação? Basta a criação de normas acompanhadas de mecanismos de fiscalização e coerção? Pode-se definir como as formas de intervenção do estado na economia? Ou é todo instrumento de controle social ou de influência em comportamentos?

Uma definição que não seja tão genérica limita a regulação às atividades intencionais de tentativa de controle, ordenação ou influência sobre o comportamento dos outros. Embora não tão aberta quanto as definições que incluem todas as ações na noção de regulação, esta permite identificar ação regulatória em outros atores que não apenas o governo, o que significa descentralizar a regulação.

Ainda que essa concepção não seja tão genérica ao ponto de abranger toda conduta no contexto da regulação e que permita identificar ação regulatória fora do estado, Black ainda busca uma definição mais precisa. Nisso, define regulação como um processo que envolve a tentativa sustentada e focalizada de alterar o comportamento dos outros de acordo com padrões ou propósitos definidos a fim de produzir resultados definidos.

A fim de analisar como tais propostas teóricas podem, ou não, explicar a realidade brasileira quanto ao contexto regulatório das ações que envolvem os dados pessoais de usuários da internet, serão expostos, no próximo capítulo, os valores que essas informações possuem para três conjuntos de atores regulatórios. Assim, o valor dos dados pessoais no ciberespaço para o mercado, para o estado e para os usuários será abordado, acompanhado dos discursos de cada um desses atores quanto ao direito à autotutela dos dados e à viabilidade e necessidade de regulação estatal nesta seara.

4 VALOR DOS DADOS PESSOAIS NO CIBERESPAÇO E OS DISCURSOS DOS AGENTES ECONÔMICOS, DO ESTADO E DOS USUÁRIOS

A fase atual do direito, como um todo, é marcada pela "abertura do sistema judiciário impregnado de valores humanistas, solidaristas e despatrimonializantes de uma sociedade democrática, igualitária e pós-moderna" (GAMA, 2007). Nesse contexto, nos direitos subjetivos podem ser identificados vetores axiológicos decorrentes do princípio da solidariedade constitucional.

Essa noção de solidariedade trouxe transformações no modo de conceituar institutos jurídicos, inaugurando a ideia, por exemplo, da função econômico-individual de estruturas jurídicas como posse, propriedade e contrato. Dessa forma, identificam-se o contrato, a propriedade e a posse, por exemplo, como instrumentos de tutela não somente dos interesses e direitos dos negociantes, proprietários e possuidores, mas igualmente da coletividade que pode ser afetada pelo exercício de tais direitos (TEPEDINO, 2018).

Pode-se notar, assim, que o sistema jurídico, principalmente na segunda metade do século XIX, passou por um movimento social e intelectual que visou a superar o individualismo egoísta formado no Estado liberal, voltando-se para a solidariedade nos planos econômico, social, político e jurídico. O objetivo da renovação era obter a harmonia social, para o que não tinha se mostrado suficiente a previsão de liberdades formais.

Nessa época, a luta contra o formalismo estava geralmente associada à oposição ao individualismo, já que, na nova compreensão do direito, buscava-se assegurar harmonia social por meio da aplicação de princípios de justiça ou de técnicas que permitissem a convivência entre interesses conflitantes. Apenas com a ruptura do formalismo do Estado Liberal, apegado à legalidade estrita, tornou-se possível falar em teorias como a da função social, a qual pressupõe que o direito não se limita à previsão legal (LOPES, 2006).

De fato, o momento histórico e jurídico era o de decadência do modelo liberal do século XIX no contexto posterior à Revolução Francesa, quando se consagrava, também, o direito à liberdade. Nesse contexto, passou-se a identificar a necessidade de que, em um Estado de Direito, o Poder Público assegurasse que a liberdade fosse exercida de forma compatível com os interesses coletivos (GAMA, 2007). Tal necessidade de superação do individualismo e do formalismo foi acompanhada da consolidação do pensamento filosófico e jurídico da solidariedade social, no fim do século XIX.

Nesse movimento, os direitos subjetivos deixaram de ser absolutos e passou a se reafirmar de forma enfática a necessidade de sua convivência com o bem comum e com os interesses maiores da sociedade. A própria concepção de direito subjetivo precisou remodelar-se, a fim de que sua titularidade fosse compatível com o bem comum e com os interesses da sociedade. A premência dessa ideia já tinha sido apontada por Jhering, ao defender a necessidade de que os direitos, para serem juridicamente protegidos, atendessem ao propósito para o qual foram criados (JHERING apud LOPES, 2006).

Além da compatibilidade com o bem comum e com os interesses da sociedade, o novo conceito de direito subjetivo tinha também como critério não a extirpação da autonomia de seu titular, mas a "eliminação dos privilégios que seriam incompatíveis com o igual direito de todos os membros da sociedade de exercerem efetivamente os seus direitos e liberdades" (LOPES, 2006).

A mudança da perspectiva individualista para a solidarista pode auxiliar na leitura do valor adquirido pelos dados pessoais desde o surgimento e o início da ampliação da internet, mas nunca afastando a imprescindibilidade de que a existência desses valores seja conciliada com o direito à autodeterminação dos titulares dos dados. Vale realizar tal ponderação porque, no que concerne, por exemplo, ao valor econômico dessas informações ou ao valor político, agentes econômicos e estado costumam dar grande ênfase às utilidades dos dados, aproveitando-se do fato de que os riscos oriundos da disseminação dessas informações são de difícil percepção pelos usuários e, em geral, não são tão imediatos quanto o retorno nos produtos, serviços e políticas públicas.

No exame da própria história do desenvolvimento das relações sociais, percebe-se que a concepção de privacidade, por exemplo, vem se moldando e remodelando. Ao analisar as modificações sobre essa figura ao longo dos 100 anos de seu reconhecimento jurídico, Gormlay (1992) já apontava, no fim do século passado, que, sendo a privacidade uma criação da história, é impossível prever uma mutação precisa desse direito, na medida em que os acontecimentos históricos são imprevisíveis, daí a razão pela qual os autores terem preferido mencionar uma concepção de privacidade do que o conceito absoluto. Assim, não se nega que a mais distinta característica da privacidade consiste em sua sensibilidade às mudanças históricas, de modo que cada tipo de privacidade reconhecido ao longo do tempo está intimamente relacionado às transformações na vida dos cidadãos e nas tecnologias, "as quais tem criado um ambiente social poderoso o suficiente para gerar um direito novo e legalmente protegido" (GORMLAY, 1992).

Com a expansão das técnicas de coleta, tratamento e disseminação de dados, os interesses do mercado e dos estados passaram a alinhar-se e a suportarem-se no que tange à alegada ausência de riscos aos usuários quanto à proteção de seus dados e de sua privacidade na rede (SCHNEIER, 2016).

Tal realidade já tinha sido notada desde as revelações feitas por Edward Snowden, na medida em que os sistemas de vigilância utilizados pela Agência Nacional norte-americana, como o PRISM, não foram por ela desenvolvidos, mas criados por empresas para obter dados coletados por companhias como Microsoft, Google e Yahoo. A empresa Vodafone, por exemplo, fornece acesso livre ao tráfego de suas informações a aproximadamente 29 países. Em algumas situações, as companhias desenvolvedoras das tecnologias trabalhavam conjuntamente com a Agência, ao passo que, em outros casos, era compelida judicialmente a fornecer os dados ou tinham sua infraestrutura invadida pela agência. Além disso, mais de 160 companhias (BONIFAZ; DELGADO-RON, 2018), como Hacking Team e Finfisher, fornecem programa de monitoramento em computador e telefone celular, tendo como consumidores governos como Azerbaijão, Colômbia, Egito, Coréia, Marrocos e Arábia Saudita (SCHNEIER, 2016).

A relação entre empresas e governos também foi alvo de polêmicas quando, em março de 2018, a companhia Facebook perdeu quase US$ 50 bilhões em valor de mercado em apenas dois dias (FINANCIAL POST, 2018) em virtude de suposto vazamento de dados de aproximadamente 50 milhões de seus usuários causado pela consultoria britânica *Cambridge Analytica* a fim de fazer predições e influenciar eleitores em favor de Donald Trump na campanha de 2016 (THE NEW YORK TIMES, 2018a).

O caminho inverso, de provimento de dados pelo estado às empresas, também constitui uma realidade. Os governos de estados norte-americanos como Illinois, Ohio, Texas e Florida, a título de exemplo, vendem dados de licenças concedidas a motoristas para empresas privadas (SCHNEIER, 2016).

Por conseguinte, os discursos desses *stakeholders* nas discussões sobre regulação do ciberespaço também têm se aproximado e é essa realidade que se pretende delinear nos próximos tópicos, reforçando a dificuldade dela oriunda para a criação de um cenário de efetiva tutela dos dados pessoais.

Além disso, o caráter multissetorial da internet, decorrente até mesmo da história de formação e expansão dessa rede, faz com que diversos grupos queiram participar de sua governança, mas com interesses diferentes que, por sua vez, moldam seus discursos. Assim, companhias privadas pretendem assegurar seus investimentos e evitar o

protecionismo dos estados, ao passo que os estados buscam exercer seu controle e soberania nas questões afetas à internet e a sociedade civil objetiva proteger direitos individuais e coletivos (SARTI. 2017).

Dado o modo como a internet foi criada, inicialmente como sistema para interação entre grupos acadêmicos e com o propósito de ser democrática em seu uso e nas inovações que possibilita – com a última camada da rede modificável por todos que consigam dominar a técnica e, por exemplo, lançar aplicações -, as questões afetas à governança da rede estão vinculadas à própria estrutura da internet. Por conseguinte, a gestão da rede abrange questões como administração da arquitetura técnica, assim como questões de políticas públicas afetadas pelos aspectos técnicos.

Uma das consequências dessa realidade consiste em que, sendo as companhias privadas as principais desenvolvedoras e mantenedoras da estrutura física da arquitetura, a gestão da rede deve considerar seus interesses de mercado, sob pena de apenas a atuação estatal ser insuficiente para a expansão e a própria manutenção da internet.

Assim, disputas entre estados e empresas privadas sempre marcaram o cenário da governança da rede, sendo marcos dessa disputa, por exemplo, a defesa da ideologia de que a internet deve ser ambiente de total liberdade de expressão; a disputa entre POSTEL e governo norte-americano pelo controle dos servidores raiz e a Declaração de Independência do Ciberespaço, de Barlow (SARTI, 2017). Em razão dessas disputas, estabeleceu-se o modelo multissetorial de regulação e governança da rede, com a pretensão de que, mediante participação de todos os envolvidos nas deliberações que envolvem a internet, houvesse equilíbrio na distribuição de poder e a rede fosse realmente democrática.

Esse desafio de governança com conciliação de interesses existe em toda área da vida que precisa ser regulada. No caso da internet, porém, é ainda potencializado em razão de seu caráter transfronteiriço (CANABARRO, 2014), já que isso exige a conciliação de jurisdições nacionais soberanas (que nem sempre coincidem com a geografia da rede) e envolve conflitos de privacidade, liberdade de expressão, segurança, propriedade intelectual etc.

Tal configuração acarreta divergências entre duas lógicas de desenvolvimento do setor, sendo uma com foco nas dinâmicas do mercado e outra, na soberania nacional (SARTI, 2017). Historicamente, a ênfase no mercado é defendida por quem ainda detém a hegemonia nesse setor, isto é, os Estados Unidos, a maior parte dos países do ocidente e suas empresas, ao passo que a defesa contra-hegemônica centrada na soberania é feita pelos países que não estão naquela mesma posição.

A percepção dessa dinâmica foi descrita por Sarti (2017) na análise dos efeitos das discussões sobre a governança da internet na Conferência Mundial de Telecomunicações Internacionais ocorrida em 2012 em Dubai. O autor apontou que a proposta inicial do encontro, de atualizar as Regulações Internacionais de Telecomunicações (ITRs), fracassou em razão da inserção da temática da governança da internet nos debates.

Quando um grupo de países liderado pela China e pela Rússia propôs que os estados tivessem maior capacidade de influenciar nos modelos de fluxos de informações pela internet, por meio de regulação pautada em acordos multilaterais entre países, os Estados Unidos e países do ocidente recusaram-se a assinar o *Final Acts* da Conferência. Isso porque tal inovação na gestão implicaria conferir a cada país mais poder, em detrimento do modelo decisório multissetorial já instalado (SARTI, 2017). A discordância derivou da premissa do modelo multissetorial de que a internet constitui bem da coletividade – e não de estado -, de sorte que toda deliberação relevante sobre ela deve permitir a participação de todos os setores interessados.

Essa multiplicidade de participantes implica também diversidade dos discursos de cada grupo, o que será abordado nos tópicos seguintes deste capítulo. Traçando o contexto do mercado pautado nos dados disponibilizados na internet, será estudado o discurso dos agentes econômicos privados. Em seguida, a perspectiva estatal constituirá o objeto do estudo e o respectivo discurso será apresentado juntamente com a indicação de inúmeras utilidades dos dados pessoais para as atividades do estado. Finalmente, a abordagem do discurso dos usuários será realizada a partir de pesquisas realizadas com esses indivíduos acerca de seu conhecimento, sua percepção e suas preferências sobre as práticas com seus dados pessoais.

4.1 Mercado de dados e o discurso dos agentes econômicos

Ao longo do tempo, a sociedade moldou-se em diversas formas de organização social, podendo ter suas fases diferenciadas de acordo com os atributos mais marcantes em cada momento. Utilizando esse parâmetro, Bell (1974) destacou-se em razão da influência de suas ideias no pensamento sociológico contemporâneo, tendo dividido etapas de modificação social em agrária ou pré-industrial, industrial e pós-industrial. Assim,

o modo de estruturação da sociedade foi o que diferenciou e estabeleceu seus marcos históricos para o autor.

Na sociedade agrária, o poder associava-se aos proprietários de terra, pois desse bem é que provinham as riquezas e o motor econômico. Com a criação das máquinas a vapor e a invenção da eletricidade, o poder passou a pertencer aos detentores e produtores de bens industriais, marcando-se a sociedade industrial. Já na sociedade pós-industrial, inaugurada após a Segunda Guerra Mundial, a fonte de poder econômico passou a decorrer dos serviços. Para destacar-se nessa nova formação social e, assim, adquirir poder, tornou-se necessário ser dotado de conhecimento e informação (BELL, 1974), os novos recursos econômicos.

Embora o referencial empírico de Bell tenha sido a sociedade norte-americana, a expansão da internet contribuiu para que esse modelo também alcançasse outros grupos sociais, já que, com essa evolução tecnológica, o processamento e a transmissão das informações passou a ser viável em velocidade e quantidade antes não imaginadas. Além disso, empresas como as gigantes da internet puderam expandir sua atuação mundialmente, alcançando países como o Brasil.

A relevância da informação na sociedade pós-industrial ocasionou a especial importância dos dados pessoais para a prestação de novos serviços e o fornecimento de novos produtos pela rede mundial de computadores. Essa realidade iniciou-se, como analisado anteriormente, com o marketing especializado na economia de especialização flexível (SCHERTEL, 2015), mas expandiu-se para além dessa funcionalidade dos dados, permitindo a formação de uma microeconomia de dados (SILVEIRA, 2017b).

Assim, os dados pessoais de cada usuário que navega pela rede têm grande valor para as atividades de marketing, não mais sustentadas pela propaganda em massa. Em face disso, tais informações são objeto de captação e leilão na rede (ADFOR US, 2014), práticas que ocorrem muito rapidamente e sem percepção por parte do titular do dado.

Além disso, não apenas para o marketing os dados dos usuários ganham valor. Em verdade, por meio de algoritmos e de mecanismos de inteligência artificial, esses dados transformam-se em todo tipo de informação e, a partir delas, muitas decisões são tomadas, de modo que os algoritmos e outros mecanismos de inteligência artificial transformam-se em oráculos dessa sociedade tecnológica.

Isso possui desdobramentos nos direitos da personalidade, na medida em que, embora haja um apelo à objetividade das tecnologias, há vieses dos criadores das tecnologias. Essa inevitável interferência da subjetividade dos criadores impacta os direitos

dos destinatários na medida em que, atualmente, os algoritmos são chamados também à tomada de decisões de caráter subjetivo e que envolvem juízos de valor, como escolhas sobre quem deve ser contratado em uma empresa, quanto um consumidor pode e deve pagar de prêmio por um seguro, por exemplo.

Em junho de 2018, por exemplo, dentro desse modelo de economia da segmentação e da predição, a companhia Decolar.com, agência online de turismo que comercializa, dentre outros itens, passagens aéreas e hospedagem, foi multada em R$ 7,5 milhões pelo Departamento de Proteção de Defesa do Consumidor (DPDC) brasileiro por diferenciar preços de acomodações e, em alguns casos, recusar venda. A avaliação da empresa para adotar uma ou outra forma de discriminação dos consumidores consistia no *geopricing*, com base na identificação da localização geográfica do consumidor, o qual realizava suas buscas por meio da internet, o que causava, por exemplo, discriminação de consumidores brasileiros em favor de argentinos (DPDC, 2018).

Esse cenário resulta no grande valor econômico e social que tais informações assumiram no mercado desenvolvido na rede, o que tem refletido na circulação monetária nessa economia informacional. Para mensurar o valor econômico dos dados pessoais, a Organização para a Cooperação e Desenvolvimento Econômico desenvolveu, em 2013, o estudo *Exploring the economics of personal data: a survey of methodologies for measuring monetary value* (OECD, 2013), no qual foram apresentados métodos para permitir tal medição.

Os critérios sugeridos consistiam no lucro advindo do registro de dados, no valor de comercialização das informações, nos custos de violação de dados e os preços dos dados nos mercados ilícitos. Além disso, para refletir o ponto de vista dos usuários, foram sugeridas ainda outras duas possibilidades de medição, consistentes na propensão em pagar pela proteção dos dados e em experiências econômicas pretéritas. Embora reconheça que a proposta ainda é rudimentar, a Organização apontou a utilidade do estudo para o início de uma compreensão do papel do dado pessoal na economia.

Assim, por exemplo, com base no valor de mercado do Facebook, a Organização concluiu que, em 2012, o valor dos registros de cada usuário da rede social correspondia a U$ 111,00, o que representou queda considerável desde 2007, quando esse valor era de U$ 300,00. Apesar disso, a renda total atribuída a esses dados cresceu entre 2007 e 2012, passando de 2 bilhões para 100 bilhões de dólares.

Uma avaliação do valor de cada espécie de dado ao longo do tempo também foi realizada, baseando-se nos preços exigidos por empresas que desempenham suas

atividades com uso de dados coletados por terceiros. Assim, à época do estudo, um endereço valia U$ 0,50; uma data de nascimento, U$ 2,00; e um número de carteira de motorista, U$ 3,00. Ao mesmo tempo, um conjunto de informações sobre determinada pessoa, como endereço, data de nascimento, número de segurança social, registro de crédito e militares, era estimado em U$ 55,00.

As utilidades dos dados pessoais para as atividades de mercado vão além do marketing e sequer podem ser declinadas em rol exaustivo, sobretudo porque, com as tecnologias de *big data*, o único limitador de criação de inovações de mercado a partir de dados pessoais consiste na criatividade.

Apesar disso, a indicação de alguns dos empregos dos dados mostra-se necessária para criar uma noção do cenário em que se pretende reconhecer o valor econômico dessas informações.

A cada acesso a um sítio eletrônico, por exemplo, as informações desse usuário são apresentadas em um servidor de anúncios a empresas corretoras de dados (*databrokers*) como DoubleClick, Adzrerk e Adgear e inicia-se um processo de troca da informação entre diversas companhias. Realiza-se, então, um leilão da possibilidade de envio de marketing para aquele usuário e o espaço na tela é vendido para a companhia que fornecer o maior lance, pelo segundo preço mais alto oferecido naquela concorrência. Para o consumidor, então, aparece o banner na página em que navega, e todo esse processo leva menos de ¼ de segundo (ADFOR US, 2014).

A viabilidade dessas tecnologias originou-se na criação dos *cookies*, inventados para facilitar a navegação, especialmente em sites de compras. Nestes, os clientes selecionavam os itens para o carro de compras e, se precisassem modificar a página para navegar em outra, encontravam seu carro de compras vazio, pois o sítio não tinha capacidade de armazenar as informações quando o usuário deixava aquela página de compra. Para melhorar essa navegação, um desenvolvedor da Netscape criou um pequeno código que poderia ser instalado no computador do visitante a fim de se lembrar de itens como nome de login, senhas, endereço e preferências de compras (ZITTRAIN; CRAWFORD; BREM, 2012). Este mecanismo era o *cookie*.

Na medida em que as tecnologias se tornavam mais sofisticadas, novos tipos de *cookie* foram criados e o perfil de cada usuário passou a ser empregado para, por exemplo, receber recomendações de produtos que com ele combinassem. Também passou a existir uma variedade de tipos de *cookies*, como os *session cookies*, que atuam enquanto o

usuário está navegando no site, e os *persistent cookies*, criados para permanecerem no computador por determinado período de tempo.

Essa diversidade chegou não apenas nas diferentes naturezas de *cookies*, mas também nos seus utilizadores. Alguns sites visivelmente utilizam dados coletados por eles mesmos, a fim de incrementar a experiência de consumo de seus próprios clientes (*first party cookies*). No entanto, sites não são os únicos capazes de coletar informações dos usuários. Empresas passaram a se especializar na instalação de *cookies* em sites de outros provedores a fim de traçar o comportamento dos usuários, dando origem aos chamados *third-party cookies*.

Assim, surgiram algumas empresas especializadas em coletar *cookies* em sítios dos outros, isto é, na atividade de *tracking*, como a DoubleClick, Rubicon Project, AdSonar, Quantcast, Pulse 260, Undertone, Traffic Marketplace, e as propagandas começaram a seguir os usuários na rede (SCHNEIER, 2016). Um repórter instalou programa de detecção de *cookies* em seu computador e identificou 105 diferentes empresas o perseguindo na internet durante um período de 36 horas.

Outros mecanismos de rastreio consistem nos *web beacons*, *web-bugs* ou *pixel tags*, que permitem registrar quem acessou uma página ou email, quando isso ocorreu e até mesmo constatar se uma mensagem de email foi reencaminhada.

Uma das técnicas mais invasivas empregadas para analisar o comportamento dos usuários na rede consiste na inspeção profunda de pacotes (*deep packet inspection*), por meio da qual o provedor analisa o conteúdo dos pacotes de dados trocados entre seus usuários, o que permite completo controle das ações dos indivíduos na rede (SILVEIRA, 2017b).

O nível de sofisticação dessas tecnologias permitiu a criação de *beacons*, capazes de gravar as teclas digitadas e transferir tais informações para uma empresa de tratamento de dados, a qual analisa o comportamento do usuário na rede, suas conexões e características pessoais (THE WALL STREET JOURNAL, 2010).

Nessa mesma linha, a plataforma Buzzfeed, por exemplo, pede aos usuários para que respondam a vários testes atrativos e, assim, coletam informações íntimas, como dados de hábitos financeiros, de estabilidade em emprego e de saúde mental.

Ainda dentre as aplicaçoes no âmbito do mercado digital, Schneier (2016) menciona o mecanismo de *license plate scanner*, o qual tem serventia de reconhecer placas de carros. Originado no Reino Unido, especificamente pela Polícia Britânica na década de 1970, os algoritmos do programa foram aprimorados para permitir um uso maior. Em suma,

o *license plate scanner* captura imagens fotográficas ou e vídeo de placas de veículos e transforma essa informação em códigos alfanuméricos. Com base nessa tecnologia, empresas mantêm dados dos veículos com base em autorizações-padrão dadas pelos motoristas nos contratos de empréstimos de seus carros. Câmeras observadoras são instaladas em carros e caminhões de reboque que continuamente digitalizam placas e enviam às empresas na busca por acidentes, utilizando *license plate scanners*. Muito dinheiro circula no negócio de recuperação, então muitos interessados participam conjuntamente dessa vigilância. Além de lucrar no negócio de veículos propriamente, tais empresas vendem essas infomrações a advogados de família e investigadores pessoais, ou repassam à polícia em tempo real (SCHNEIER, 2016).

É conhecida, também, a declaração do executivo senior da Ford Motor Company em 2014 de que "nós sabemos de todo mundo que viola as leis de trânsito, nós sabemos quando voces estão fazendo isso. Nós temos gps em seus carros, então sabemos o que estão fazendo". A surpresa é que os donos dos veículos não sabiam da existencia de tais aparelhos instalados nos carros (SCHNEIER, 2016).

Existem, ainda, tecnologias baseadas em algoritmos capazes de fazer reconhecimento de face, de iris e de andar. Ademais, algumas manipulações de dados são quase inimagináveis, como a possibilidade de câmeras de "ouvir" conversas telefonicas a partir do foco em objetos ao redor do falante, como um saco de batatas chips, e medir sua vibração (SCHNEIER, 2016).

Com base nesse modelo de mercado, grandes grupos atuantes na internet, como Facebook e Google, deixam de exigir contrapartida financeira de seus usuários pelos serviços fornecidos e auferem sua renda com publicidade segmentada, já que possuem volume e variedade de dados dos consumidores que poucas empresas conseguiriam reunir.

Pode-se observar que as atividades comerciais que envolvem os dados pessoais obtidos na internet abrangem camadas que podem ser divididas em coleta e armazenamento, processamento e mineração, análise e formação de amostras e modulação (SILVEIRA, 2017b).

Para coleta e armazenamento, as companhias utilizam redes sociais, sites, mecanismos de busca, registros de tempo de permanência em sítios eletronicos, formulários, pesquisas com usuários e rastreadores de localização de aparelhos telefônicos, por exemplo. Na segunda camada, ocorre o processamento e a mineração dos dados, isto é, o tratamento do que foi reunido e o eventual cruzamento com outros dados para obter o traço mais preciso do perfil do usuário ou para obter conclusões a partir de *big data*. Na análise e formação de

amostras, atuam departamentos de marketing e plataformas de venda de dados, como aquelas que trabalham com os *third-party cookies*. E, na modulação, são efetivamente oferecidos produtos e serviços ao público direcionado.

Na camada de modulação, destacam-se as aplicações e os mecanismos capazes de, sutilmente, apresentando-se como facilitadores do cotidiano, construir situações sociais e interações, atuando sobre a subjetividade dos usuários (SILVEIRA, 2017b). Em vez de disciplinar os alvos por mecanismos de medo e punição, a modulação cria um contexto de aparência de liberdade e conforto, levando a certos comportamentos desejados pelos moduladores.

Essa forma de moldar comportamentos por meio das aplicações reduz a capacidade de influência ativa e consciente no ambiente regulatório por parte dos usuários. Estes, em razão das funcionalidades presentes nos produtos e serviços, são levados não apenas a aceitar o estado de coisas, mas também a desejá-lo em razão do aparente conforto e liberdade dele oriundos, como poderá ser constatado nas análises do item "Percepção dos usuários sobre as práticas com seus dados pessoais" (4.iii).

Fala-se, então, em um "poder de captologia" por "computadores persuasivos" (FOGG, 1998), termo cunhado pelo psicólogo Fogg há 20 anos, na Universidade de Stanford, no intuito de esclarecer como uma tecnologia de interação pode modificar as condutas de uma pessoa. Trata-se, então, de tecologias computacionais que visam à persuasão. Com a popularização da internet e, portanto, da quantidade de registros das ações dos usuários, o conhecimento sobre seus hábitos e suas escolhas confere a quem tem acesso a tais registros a possibilidade de, conhecendo muito bem tais usuários e utilizando algoritmos, conduzi-los a um processo de pensamento (consciente ou não) que os conduz a determinadas escolhas.

Em face dessa realidade, o comunitarismo em rede perde sua capacidade explicativa porque o usuário, dada sua falta de consciência, não pode ser efetivamente identificado como um ator que efetivamente consegue desempenhar um papel ativo nos processos de construção dos mecanismos regulatórios. De fato, para a concretização do comunitarismo, tem-se como premissa a atuação do usuário com ciência da capacidade de ser um dos nós na matriz de relações de forças regulatórias, o que não se verifica quando tal usuário é, na verdade, alvo da modulação de comportamentos.

A regulação responsiva poderia ser uma boa resposta a esse cenário de desequilíbrio de forças, mas desde que focada em reverter essa condição de hipossuficiência dos usuários. Uma vez que ela parte do pressuposto de que todo ambiente a ser regulado pelo

estado já tem sua autorregulação - como se dá, de fato, no ciberespaço -, poderia ser empregada para estimular a responsabilidade dos agentes econômicos, dos detentores do conhecimento técnico e até mesmo dos governos de agir em colaboração com os usuários e assegurando sua consciência sobre as práticas que envolvem seus dados pessoais. De fato, esse caráter colaborativo que faz parte da regulação responsiva depende de se conferir aos usuários a efetiva possibilidade de conhecer suas motivações e participar do ambiente regulatório, o que depende de uma transparência sobre os atos de coleta, uso, tratamento e disseminação de dados pessoais ainda não existente no contexto estudado.

Essa análise sobre a regulação responsiva também pode ser feita em relação à regulação descentrada. Embora os usuários tenham potencial de participar ativamente do ambiente de regulação das práticas que envolvem os dados pessoais, já que constituem uma peça central para que a economia baseada em dados e as políticas estatais fundadas nessas informações aconteçam, esse pontencial não tem sido aproveitado por todos os fatores elencados acima.

Nesse sentido, embora a regulação descentrada possa ser reconhecida como aquela das teorias regulatórias expostas que mais bem explica a realidade brasileira nessa temática, não fica a salvo de que se questione a ainda reduzida influência consciente dos usuários na regulação e na tutela de seus dados pessoais. De fato, o cenário regulatório estudado não se amolda completamente a nenhuma solução regulatória apresentada porque seria questionável uma teoria regulatória – sobretudo no âmbito pretensamente democrático da internet - que se admitisse excludente em relação ao usuário.

Isso pode ser melhorado, começando-se por uma maior transparência acerca dessa realidade sobre as práticas de governos e mercados com essas informações.

A expansão da atividade de vigilância tornou-a não apenas diluída dentre diversos autores, mas também muito menos ostensiva, graças ao desenvolvimento de tecnologias, sobretudo de informação e comunicação, que permitem vigiar de maneira velada e sem indicativo de ameaça a qualquer direito individual. Com o aumento do uso de tecnologias baseadas no registro de informações, tais qual a internet, a ação e interação de grande parte das pessoas passou a deixar rastros caracterizadores de um fenômeno por alguns nomeado “digitização da informação” (MURRAY, 2010).

Com a mudança de um foco dos átomos para os bits na sociedade da informação, a necessidade de adequação do mercado e dos governos a essa realidade impulsionou o desenvolvimento de tecnologias que levaram à redução dos custos de armanezamento de dados e de transmissão de informações (MURRAY, 2010). Informações

que antes eram guardadas em fichas escritas em repartições públicas, por exemplo, hoje são mantidas em arquivos digitais, apenas para citar um exemplo bastante simples. Por conseguinte, com a disseminação das tecnologias, mais baratas, acessíveis e espalhadas, a geração de informações também se torna mais fácil.

Os resultados da redução dos custos de vigilância com as novas tecnologias não afetam apenas o valor dessa atividade, mas também sua extensão. Uma vigilância mais barata, especialmente neste cenário de reconhecimento de valor das informações, acaba por ser, também, uma vigilância em massa. Essa mudança de uma vigilância antes focada em determinado grupo de consumidores ou determinado suspeito de prática de conduta investigada pelo estado implicou um movimento de mudança da perseguição de pessoas para a perseguição de todas as pessoas, já que, com as novas tecnologias, todos tornaram-se alvos potenciais de governos e agentes econômicos (SCHNEIER, 2016).

O movimento seguinte da troca da vigilância pontual para uma vigilância em massa pode ser identificado na vigilância camuflada e automática. O mero uso de aparelhos eletrônicos que já fazem parte da vida da maioria das pessoas, a criação de uma conta de email, a utilização de um mecanismo de busca, e pesquisa de preços de determinado produto, ações corriqueiras para a maior parte dos indivíduos tornam possível um nível de vigilância eletrônica que provavelmente não seria admitido no mundo físico.

Em face dessa realidade é que Schnoenberger e Cukier (2013) falam em dataficação da rotina dos indivíduos, na medida em que estes “permitem” o vasto registro de suas ações, criando uma sombra de dados que eles mesmos não conseguem moldar, controlar ou deletar. E isso ocorre porque nossas condutas são dataficadas, isto é, são constantemente registradas, permitindo-se uma forma de vigiar que se tornou camuflada, criando-se o cenário de “dataficação da sociedade”.

A assimetria de conhecimento sobre quando e como ocorrem esses processos nao apenas contribui para que eles se disseminem, mas também dificulta aos próprios fornecedores da informação que interfiram no estabelecimento de padrões para essas liberdades de registrar, coletar, tratar e disseminar dados em que se identificam estados e agentes do mercado. De fato, a ignorância quanto a essa realidade impede que os próprios usuários coloquem limites que considerem devidos e legítimos para essas práticas.

Assim, como aponta Murray (2010), o problema do modelo da atual indústria informacional reside na assimetria informacional entre os consumidores e quem manuseia tais tecnologias. Em face disso é que tornar mais ostensivas ou ao menos

conhecidas e informadas tais práticas constitui premissa para que as teorias de regulação descentrada encontrem aplicação nesse contexto de vigilância fundada em dados pessoais.

Na polêmica que envolve Facebook e Cambridge Analytica, a título de exemplo, esta empresa valeu-se de dados de mais de 80 milhões de usuários daquela rede social a fim de instrumentalizar sua atividade de consultoria política na campanha eleitoral de Donald Trump em 2016 e na saída do Reino Unido do Brexit. Para isso, utilizou, em tese, dados obtidos em teste psicológico veiculado no Facebook, mas, em verdade, *Cambridge Analytica* teve acesso e usou dados também de usuários não participantes desses testes, o que trouxe à tona o questionamento sobre o modelo de negócios da plataforma, baseado nos dados pessoais dos usuários.

O CEO da companhia Facebook, Mark Zuckerberg, informou em seu perfil na rede social (ZUCKERBERG, 2018) que o acesso aos dados de pessoas não participantes dos testes foi possível em razão da política de privacidade vigente à época do teste de personalidade, modificada em 2014. Nessa política, era possível ao desenvolvedor da aplicação acessar dados de amigos dos participantes, e não apenas destes, de modo que, claramente, os titulares dos dados não tinham conhecimento do que acontecia com seus dados pessoais e, principalmente, não tinham mecanismos para evitar o uso indevido ou de modo diverso à sua própria vontade.

O teste de personalidade sequer tinha sido desenvolvido pela *Cambridge Analytica*, mas pelo pesquisador Aleksandr Kogan em nome da empresa *Qualtrics*, além de que, inicialmente, os usuários somente teriam sido informados da possibilidade de uso de suas informações para fins acadêmicos, e não comerciais. Ocorre que, uma vez dotada das informações dos indivíduos, *Qualtrics* celebrou negócio com a Cambridge Analytica e a ela transferiu todos esses dados.

Nada obstante o Facebook tenha declarado que essa prática comercial contraria sua política de privacidade, não possuía mecanismos para auditar os desenvolvedores de aplicações que coletam dados na sua plataforma, deixando para a boa vontade dessas companhias a atribuição de resguardar os dados e não buscar lucro com sua venda. Apenas com o escândalo a companhia declarou que passará a exigir auditoria das empresas como condição para que atuem por meio da rede social e utilizem as informações dos usuários.

Fato é que, por meio de modulação de comportamento de usuários eleitores, a companhia declarou ter obtido efeitos no processo eleitoral norte-americano. Embora ainda não tenham sido apresentadas evidências da eficiência do mecanismo da

empresa, esse resultado teria advindo do uso dos dados para criar algoritmos que auxiliavam a identificar personalidades dos eleitores e a influenciar seu comportamento por técnicas de modelagem psicográfica (THE NEW YORK TIMES, 2018b).

A técnica estaria baseada em pesquisa desenvolvida pelo *Psychometrics Center* da Universidade de Cambridge e publicada em artigo de 2015 sob o nome *Computer-based personality judgments are more accurate than those made by humans* (KOSINSKI, STILLWELL; YOUYOU, 2015). Com base nisso, teria sido realizada segmentação psicológica com algoritmo alimentado com curtidas do Facebook, dados que, segundo os pesquisadores, permitem medir 5 grandes traços de personalidade, a saber: abertura, conscienciosidade, extroversão, amabilidade e neuroticismo.

Embora segmentação de grupos constitua prática já tradicional em pesquisas com eleitores, os quais são separados por idade, região de domicílio, escolaridade, renda etc., a nova funcionalidade permite a análise não apenas dessas características objetivas dos eleitores, mas de seu comportamento. Por conseguinte, segmentando as pessoas por personalidade por meio da modelagem psicográfica, torna possível convencer cada usuário em determinada direção política com uso de formas de publicidade convincentes para o seu perfil.

Ao lado disso, o jornalista Jamie Bartlett, em seu livro *The People Vs Tec* (BARTLETT, 2018), noticiou ter sido declarado por Theresa Hong, membro da campanha eleitoral de Donald Trump, que tal campanha investiu considerável montante de seu orçamento em publicidade no Facebook, o qual teria sido a razão do sucesso eleitoral .

Assim, na seara cibernética, por exemplo, criam-se aplicações capazes de controlar as rotas das pessoas, solucionar problemas, modular comportamentos, melhorar experiências no dia-a-dia e em viagens, gerando sensações de controle, conforto, facilidade e aumento de produtividade. Tais aplicações têm capacidade de modular o que passará a ser considerado imprescindível ou útil para os grupos sociais, o que é possível graças a tecnologias de controle dos perfis dos usuários e de instrumentos como *big data*, com os quais se pode fazer predições sobre as tendências e demandas dos grupos de consumidores.

Trata-se do que acontece, por exemplo, com o aplicativo Whatsapp, cuja suspensão no Brasil em razão de decisões judiciais provocou reações negativas de usuários em razão da dependência do instrumento para comunicações pessoais e para o exercício de atividades profissionais.

As sensações dos usuários, portanto, não são necessariamente associadas à vigilância, disponibilização de informações sensíveis e vulnerabilidade, pois as facilidades

oriundas dos novos serviços são imediatas, ao passo que as consequências da captura de dados e das negociações de seus perfis e informações não são claras, tampouco imediatamente percebidas. Isso coaduna com o discurso das companhias de que apenas disponibilizam aos usuários serviços gratuitos e inofensivos, sem os quais a vida seria mais difícil e muito menos interessante.

Nesse sentido, a prática discursiva das companhias funda-se na extinção da privacidade no mundo atual como decorrência de escolha dos próprios indivíduos, e não das estratégias comerciais das empresas, uma vez que os novos produtos e serviços baseados nos dados pessoais somente seriam acolhidos no mercado por opção de adesão pelos próprios usuários.

"As pessoas que instalam o app fazem uma escolha de ceder seus dados" foi a declaração de Monika Bickert (FOLHA DE S. PAULO, 2018a), vice-presidente global de políticas públicas do Facebook quando a empresa foi alvo de notícias de vazamento de dados de 50 milhões de usuários da rede de relacionamento, em março de 2018. Em 2010, Mark Zuckerberg, criador do Facebook, já declarava que a privacidade não mais consistia uma norma social – mas adquiriu as 4 casas adjacentes à sua em Palo Alto a fim de assegurar sua privacidade (SCHNEIER , 2016).

Deixar de ter a privacidade como preocupação passou a ser sustentado pelos agentes econômicos não apenas como algo necessário para dar o próximo passo do desenvolvimento na sociedade informacional, mas também como uma mudança positiva. Afinal, isso permite, por exemplo, que o comerciante filtre as propagandas e faça chegar a cada pessoa apenas aquela que realmente é de seu interesse, ou viabiliza a vigilância sobre pessoas que representam risco à sociedade, o que não deveria ser visto como um problema por quem não tem algo a esconder.

Apesar diso, essa perspectiva limita a visão do indivíduo na sua condição de consumidor, como se seu exclusivo interesse consistisse em adquirir mais produtos e serviços. A tutela dos dados pessoais e da privacidade não se restringe a esse ângulo, pois abrange as consequências da divulgação de informações pessoais nas esferas familiar, profissional, moral, íntima etc. Assim, o discurso dos agentes econômicos apenas pode encontrar algum sentido em seu próprio universo e para a específica finalidade de disponibilização de mais serviços e produtos, o que constitui somente uma das facetas de vivência dos indivíduos.

Ao lado disso, a incoerência do discurso dos agentes de mercado pode ser reconhecida, por exemplo, na defesa dos segredos industriais, o que não se compatibiliza

com a abertura sustentada pelas próprias companhias. Na prática, isto é, nos fatos reais da sociedade da informação, tem se consolidado a compreensão de que não é razoável exigir privacidade para os cidadãos, mas também não se pode demandar transparência nas ações de empresas e estados. Assim, “estamos vivenciando a construção da opacidade legítima para o Estado e para as empresas enquanto se aceita a transparência completa da vida das pessoas. São as razões do mercado” (SILVEIRA, 2017b, cap. 3).

A diversidade de utilidade dos dados pessoais não se limita às atividades empresariais, alcançando também as políticas públicas e outros serviços do estado, o que será analisado no tópico seguinte, em que será possível perceber a proximidade entre os discursos dos governos e de agentes econômicos.

4.2 Vigilância, políticas públicas e o discurso do estado

Se o estado promulgasse uma norma com exigência de que as pessoas utilizassem dispositivos capazes de indicar sua localização e que informasse sempre que uma nova relação social fosse estabelecida, muito provavelmente, nos estados democráticos de direito, tal norma seria considerada inconstitucional. Apesar disso, é o que se faz diariamente quando cada indivíduo carrega consigo dispositivos móveis conectados à iternet, como celulares, e usa aplicações de redes sociais (SCHNEIER, 2016). Com isso, proveem não somente as empresas com os dados pessoais, mas também os governos, que já reconhecem o valor dessas informações para o incremento das atividades estatais.

Não apenas as companhias se valem dessas novas tecnologias, mas também os responsáveis pelas políticas públicas e pela prestação de serviços públicos. Assim, utilizando como exemplo algumas práticas das autoridades norte-americanas, Schneier (2016) traça um cenário ilustrativo de como os dados dos cidadãos podem ter grande utilidade aos governos. A Agência Nacional de Segurança dos Estados Unidos, por exemplo, tem capacidade de coletar e analisar dados referentes a ligações telefônicas, por meio dos quais identifica os locais por onde as pessoas costumam ir e os demais indivíduos com quem se relacionam. Pelos geolocalizadores de aparelhos de telefonia, a Agência também consegue identificar se algum de seus agentes está sendo perseguido e por intermédio da identificação de linhas telefônicas utilizadas apenas uma ou pouquíssimas vezes, alcança pessoas que pretendem se esconder das autoridades. A tecnologia ainda permite que a Agência acione

remotamente o microfone de aparelhos celulares para realizar escuta ambiental de determinados alvos.

A utilização de dados de ordem pessoal pelas autoridades norte-americanas também se faz por meio do *Isolation Control and Tracking*, usado pelo serviço postal norte-americano para fotografar o exterior de toda mensagem postada no serviço postal nos Estados Unidos, o que representa cerca de 160 bilhões de produtos fotografados por ano.

A utilidade dos dados dos usuários da rede para vigilância se expande para os circuitos fechados de televisão (*closed-circuit television* - CCTV*)*, os quais podem ser capazes de estabelecer padrões de reconhecimento de indivíduos a partir de algoritmos, e para os chips de radiofrequência para identificação (*Radio-Frequency Identification* - RFID), que viabilizam a coleta e o armazenamento de dados remotamente a partir de dispositivos que compõem a internet das coisas.

Ainda nas atividades de persecução criminal, governos de mais de 35 países contratam empresas como a italiana Hacking Team (http://www.hackingteam.it/index.html) para adquirir mecanismos de vigilância como software espião e, assim, controlar o que os cidadãos fazem em suas aplicações em computadores e aparelhos de celular. O uso do software PRISM pelo governo norte-americano, por exemplo, foi divulgado em 2013 por meio do jornal britânico *The Guardian*, permitindo que fossem acessados emails, conversas online, e chamadas de voz.

Não somente os Estados Unidos são protagonistas dessas práticas. O grupo APT1 é associado ao governo chinês no desenvolvimento de atividades de hacker desde 2006 (MANDIANT, 2013). A agência de inteligência e a polícia alemãs já reconheceram seu envolvimento em atividades de hacking[28].

Na América Latina, com o desenvolvimento de um mercado de softwares de vigilância, esses instrumentos chegaram a países menos desenvolvidos. Em 2015, com a violação de informações da empresa Hacking Team, soube-se que softwares de espionagem por ela comercializados foram vendidos em países como Brasil, Chile, Colômbia, Equador, Honduras, México e Panamá, nos quais o uso desse tipo de tecnologia por governos depende de autorização judicial e da suspeita da prática de delito (BONIFAZ, Rafael; DELGADO-RON, 2015). No México, no Equador e no Panamá, tornou-se pública a utilização do software Galileu, vendido por aquela companhia, para espionagem política, tendo sido até

28 Sobre o reconhecimento: <http://securityaffairs.co/> e <wordpress/166/cyber-crime/trojan-co-the-new-frontiers-of-espionage.html>.

mesmo expedida ordem de prisão contra o presidente do Panamá em razão de ordenar a espionagem de cerca de 150 pessoas, dentre as quais opositores políticos. Além disso, também sem autorização judicial, o software da Hacking Team foi empregado para espionar juízes, o Conselho Nacional Eleitoral, o movimento político Pachakutik, dentre outros.

Com envolvimento brasileiro, verificou-se, em 2015, o uso de softwares como CyberGate e AlienSpy, os quais, usando códigos maliciosos, infectam computadores e celulares para viabilizar a vigilância remota do que é feito em tais aparelhos. Soube-se que tal espionagem envolvia Brasil, Argentina, Equador e Venezuela, com uso de uma estrutura comum e foram identificados alvos como opositores políticos dos governos em vigência e jornalistas (BONIFAZ, Rafael; DELGADO-RON, 2015).

Assim, por meio de parceria com empresas ou pelo desenvolvimento de tecnologias próprias, os estados têm tentado acompanhar as habilidades dos criminosos atuantes na internet.

Na legislação brasileira, o valor identificado nos dados pessoais pode ser verificado, por exemplo, no Decreto nº 8.789/2016, instituidor da metodologia de compartilhamento de bases de dados na administração pública federal. Em tal legislação, permite-se o compartilhamento de dados, por exemplo, dos órgãos federais promotores da saúde com instituições de ensino federais com a finalidade de desenvolvimento de pesquisas nessa área, ainda que os titulares dos dados sobre saúde não estejam cientes dessa troca. Isso está em concordância com uma das finalidades da Política de Dados Abertos do Poder Executivo Federal, consistente em fomentar a pesquisa científica, tal como previsto no artigo 1º, I, do Decreto nº 8.777/2016.

Verifica-se que, sob o argumento da utilidade da informação para a realização de pesquisas científicas, a autodeterminação dos usuários da rede pública de saúde sobre dados sensíveis é ignorada. De fato, os únicos parâmetros estabelecidos no Decreto nº 8.789/2016 são a observância do sigilo fiscal e o pertencimento dos órgãos e entidades participantes da troca à administração pública federal direta ou indireta ou ser entidade controlada direta ou indiretamente pela União detentora ou responsável pela gestão de bases de dados oficiais.

As finalidades das trocas, na mesma linha, são delineadas na norma de maneira muito abrangente, permitindo que toda política pública ou serviço público, tais qual a segurança, seja incluído no rol do artigo 2º.

Não se ignora que o cruzamento de dados pode ter grande valor para incrementar as atividades estatais, quando permite que se evite, por exemplo, o pagamento

duplicado ou indevido de benefícios sociais. No desempenho de políticas públicas, essas informações constituem instrumentos relevantes para que o Estado desenvolva mudanças. São usadas, por exemplo, plataformas destinadas a incrementar a participação democrática dos cidadãos na elaboração de normas e de orçamento público, como e-Democracia (https://edemocracia.camara.leg.br/) e Participa Maranhão (https://participa.ma.gov.br/). Também já há interação entre governo e governados por meio de uma diversidade de aplicações, como os aplicativos do Bolsa Família, da Carteira Nacional de Habilitação Digital, da Caixa Econômica Federal, da ANATEL - consumidor e da declaração anual de Imposto de Renda.

A despeito disso, a realidade normativa avaliza a transação de dados pessoais dos usuários dos serviços públicos de forma muito abrangente, viabilizando que, por exemplo, atividades de pesquisa sejam realizadas sem observância mínima da privacidade dos usuários cujos dados pessoais serão usados. A despeito de o argumento da anonimização dos dados ser utilizado com frequência para justificar essas práticas, já se sabe que a desanonimização é viável em razão dos resultados dos cruzamentos de dados.

É ínsita ao próprio conceito de *big data*, por exemplo, a extração de informações implícitas previamente desconhecidas e apenas com potencial utilidade (RUBINSTEIN, 2013). Assim, é por meio das técnicas de mineração desses dados que se chega às inferências a partir de correlações. Essas tecnologias, então, desafiam todas as leis de privacidade ao permitir a reidentificação de dados por meio do uso de dados não pessoais.

Diante disso, danos individuais podem advir dessas técnicas de agregação de dados. Assim, a reidentificação incrementa os danos associados à agregação, permitindo que os controladores de dados conectem mais informações ao perfil de um usuário além daquelas por ele mesmo fornecidas, levando ao que se chama de "banco de dados de ruína" (RUBINSTEIN, 2013).

No Brasil, por exemplo, divulgou-se que o governo federal utiliza serviços da companhia Isobar Brasil não somente para melhoramento de serviços públicos, mas também para monitorar focos de manifestações e influenciadores na rede sobre os principais temas de interesse estatal (FOLHA DE S. PAULO, 2017).

Também no Brasil, embora tenha sido anunciado que a Polícia Federal pretendia utilizar virus em telefones de suspeitos para copiar informações como mensagens enviadas por meio de aplicativos, emails, comentários em redes sociais e comunicações por vídeo (FOLHA DE S. PAULO, 2015), não houve confirmação do desenvolvimento dessa tecnologia pelo estado ou da aquisição desse produto. Fato é que, a rigor, toda atuação estatal

nesse sentido, ainda que para a persecução criminal, deve ser submetida às normas constitucionais de liberdade de expressão, intimidade e sigilo de comunicações (Constituição Federal, artigo 5º, IX, X e XII), bem como às Leis nº 9.472/97, 9.296/96 e 12.965/14, isto é, as leis sobre serviços de telecomunicações e interceptação de comunicações telefônicas e o Marco Civil da Internet.

Nesse cenário, a tecnologia permite um alcance das atividades de vigilância até então não experimentado, até mesmo porque o volume de interações vivenciadas na rede expande-se com o aumento da diversidade de aplicações disponíveis, o que torna disponíveis ainda mais informações e dados pessoais. Ao lado disso, a mudança da natureza da vigilância implica reconhecer que não se trata de perseguir as pessoas, mas de vigiar todas as pessoas, suspeitas ou não, realidade diversa daquela vivenciada quando a vigilância era mais cara e não era feita em massa.

A fim de justificar o uso dos dados dos cidadãos e de apontar a legalidade dessas práticas, os estados sustentam, desde as declarações de Edward Snowden, que usam apenas metadados, o que asseguraria a privacidade de quem não é suspeito. A alegação dos Estados Unidos, por exemplo, acerca do uso de dados de ligações telefônicas dos americanos era de que a NSA não coletava as palavras ditas nas comunicações, mas apenas o número dos interlocutores, o horário da ligação e o tempo de duração.

A questão é que isso já revela muito sobre as pessoas. De fato, quando se tem uma única pessoa como foco de vigilância, saber o conteúdo das informações pode ser muito importante. No entanto, quando se trata de vigiar uma população inteira, metadados podem ser muito mais significantes, importantes e usáveis, pois permitem realizar correlações e, assim, obter conclusões concretas em maior escala. Como informou o ex-conselheiro geral da NSA, Stewart Baker, “metadata diz absolutamente tudo sobre a vida de uma pessoa. Se há metadados suficientes, não é necessário saber o conteúdo de nenhuma informação”. Na mesma linha, em 2014, o antigo componente da NSA e ex-diretor da CIA Michael Hayden asseverou: “nós matamos pessoas com base em metadados” (SCHNEIER, 2016).

Essa realidade reforça a necessidade de que, independentemente da existência de uma violação direta à privacidade, a tutela dos dados pessoais seja realizada, incluindo-se os dados na forma de metadados. Nas situações descritas como exemplos, de fato, especialmente quando utilizados metadados, não haveria fundamento para contestar as práticas estatais com amparo na alegação de ofensa à privacidade, já que inexistia indicação de afronta à esfera privada dos titulares de dados. A despeito disso, a possibilidade de uso

indevido das informações anonimizadas, embora pessoais, desvelou a efetiva potencialidade de afronta à esfera jurídica individual do titular dos dados, com alcance de conclusões a seu respeito não aferíveis diretamente dos metadados, mas alcançáveis após seu tratamento.

Em tecnologias de uso de *big data*, os dados trabalhados podem não ser explicitamente pessoais, mas sua análise ou combinação com outros grupos de dados podem indicar a titularidade da informação. Em 2006, por exemplo, o provedor AOL liberou 3 meses de pesquisa de dados sobre 657.000 de seus usuários, o que representava 20 milhões de buscas no total. A ideia era que essas informações poderiam ser úteis para pesquisadores e, para proteger a identidade dos usuários, os nomes foram substituídos por números. Ocorre que repórteres do *New York Times* conseguiram, a partir dos históricos de buscas, identificar nomes de usuários, foram às suas residências e os mostraram.

Ao lado disso, a adoção do consentimento como elemento legitimador das práticas estatais com dados pessoais não tem se mostrado eficiente. Embora o Marco Civil da internet e importantes legislações destinadas à tutela de dados pessoais ao redor do mundo, a exemplo do Regulamento Europeu, sejam fundados na escolha informada dos usuários, esse modelo pressupõe uma escolha informada entre consentir ou não com a coleta e o compartilhamento de dados.

Esse formato baseado no consentimento pode tornar impossível o fornecimento de uma notificação adequada ao usuário especialmente porque não se sabe, de antemão, quais usos secundários podem ser feitos com aquela informação e que dados elas podem gerar. Além disso, como apontado por Rubinstein (2013), outras duas dificuldades podem ser identificadas. Uma consiste na inviabilidade de consentir quando inexiste conhecimento sobre possíveis técnicas de correlação por meio de mineração ou análise de *big data*. A outra está na indefinição de diversos ordenamentos jurídicos quanto à concepção de dados pessoais, já que a normatização, em regra, aplica-se somente a eles, e não aos dados anonimizados.

A possibilidade de desanonimização e a deficiência do atual modelo de consentimento, portanto, mitigam a força da argumentação estatal quanto ao caráter inofensivo das práticas de uso e tratamento de dados pessoais, notadamente quando realizadas sem o conhecimento dos cidadãos governados.

A postura estatal acerca da temática pode ser analisada a partir das manifestações de órgãos durante a tramitação do projeto de lei que resultou no Marco Civil da Internet. Sob essa perspectiva, Maia, Pinheiro e Mira (2016) examinaram as disputas

ocorridas na temática sobre guarda de dados, especificamente quanto à tendência de situar o usuário na condição de suspeito e de institucionalizar um modelo de vigilância.

De um lado, figurou um grupo de parlamentares, apoiados por órgãos estatais como a Polícia Federal, em favor de aumentar o tempo de guarda obrigatória de dados para facilitar ações policiais, especialmente na persecução contra cometimento de crimes de pedofilia e pornografia. Um dos grandes pontos de debate disse respeito à obrigatoriedade dos provedores de aplicação em guardar os dados de acesso, sobretudo porque se sustentou que, para pequenos provedores, o cumprimento dessa obrigação acarretaria gastos muito altos. Diante disso, grupos defensores da privacidade pleitearam a proibição dessa guarda, pois vislumbravam o risco de que o armazenamento das informações ocorresse sem consentimento dos usuários. Ao fim, prevaleceu proposta do relator, Deputado Alessandro Molon, no meio termo entre os defensores da guarda por no mínimo 12 meses e os proponentes da vedação de guarda, estabelecendo-se a obrigação pelos provedores de aplicação pelo período de 6 meses.

O discurso estatal também pode ser analisado a partir das normas formais aprovadas na temática de tutela dos dados pessoais na rede. No Marco Civil da Internet, por exemplo, não se olvidou a previsão principiológica dos direitos à privacidade e à proteção dos dados pessoais (art. 3ºª, II e III), bem como os direitos à inviolabilidade da intimidade, da vida privada, do sigilo do fluxo das comunicações e do não fornecimento de dados pessoais a terceiros sem consentimento (art. 7º, I, II, III e VII). Também ficou vedada a guarda dos registros de acesso a aplicações pelos provedores de conexão (art. 14).

Apesar do avanço reconhecido em relação a tais previsões normativas, que vieram reduzir a carência de um cenário até então de completa omissão regulatória, inexiste, até o momento, entidade ou órgão administrativo competente para fiscalizar o cumprimento da obrigação dos provedores de observar tais direitos dos usuários.

Com efeito, embora a Lei esteja vigente há quase quatro anos, não houve criação de órgão competente para tal fiscalização, tampouco essa competência foi atribuída a algum órgão existente, omissão que dificulta grandemente a defesa dos direitos dos usuários. Assim, apesar de a criação da previsão normativa ter atendido, inicialmente, à demanda dos usuários e de quem demandava a tutela de seus direitos, o Estado ainda é omisso na disponibilização de órgão ou entidade que instrumentalize a execução dessas normas regulatórias.

As normas estatais também excetuaram a necessidade de prévia autorização judicial para o acesso, por autoridades administrativas competentes, a dados cadastrais

(filiação, qualificação pessoal e endereço) mantidos pelos provedores. Não houve, porém, especificação da natureza da competência necessária para a identificação dessa autoridade administrativa, tampouco fixação de parâmetros para o exercício dessa faculdade pelo estado. Nem mesmo no Decreto nº 8.771/16 o estado aproveitou a oportunidade para fixar os limites desse acesso, como o modo de identificação da competência necessária para a requisição ou as situações em que tal disponibilização de dados justifica-se.

Na mesma linha, o Decreto nº 8.789/2016 oficializou, de forma genérica, o compartilhamento automático de dados pessoais entre órgãos e entidades da Administração Pública Federal, independentemente de ter havido prévio e expresso consentimento do indivíduo a esse uso secundário de tais informações, legalizando a perda da autodeterminação informacional em face do estado.

A postura estatal diante da diversidade de interesses envolvidos na regulação das práticas que envolvem dados pessoais dos usuários da internet tem permitido a tutela dos direitos individuais apenas de forma principiológica, sem disponibilização de instrumentos ou autoridade específica por meio dos quais seja possível exigir a fiscalização do cumprimento das normas protetivas. Ao mesmo tempo, a possibilidade já mencionada de identificação de usuários mesmo em bancos de metadados e a possibilidade de uso dessas informações além da utilidade inicial para a qual os dados foram coletados reforça o discurso estatal mais concordante com os interesses das companhias privadas que dos usuários.

Permite-se notar, assim, que embora empresas e governos tenham objetivos diferentes quanto aos dados pessoais dos usuários, utilizam metodologias parecidas para alcançar tais objetivos, valem-se de parcerias para satisfazer seus interesses (SCHNEIER , 2016) e, na prática, têm discursos aproximados quanto à abertura dessas informações.

Pode-se observar, por exemplo, que a Agência Central de Inteligência dos Estados Unidos usa tecnologias desenvolvidas pela própria Agência ou obtidas perante outros órgãos governamentais ou por contratos com companhias privadas de tecnologia, como Baitshop. Por meio desses mecanismos desenvolvidos por governo e empresas, que geram falhas para dispositivos com sistema operacional Android e iOS, a Agência consegue hackear computadores, aparelhos de televisão e dispositivos móveis, como desvelado pelo Wikileaks no vazamento de informações intitulado, pelo próprio grupo, como Vault 7 (WIKILEAKS, 2017).

Antes de observar qual o discurso dos indivíduos nesta temática, no tópico seguinte, será analisado como a utilização das tecnologias de *big data* e de algoritmos reforça

essa proximidade dos interesses de empresas e estados, situando o usuário em posição de sujeição ao poder desses demais *stakeholders*.

4.2.1 *Big data*, anonimização, desanonimização e proximidade dos discursos das empresas e dos estados

Nesse universo em que os valores dos dados pessoais para o estado e para o mercado dão o tom da postura desses personagens acerca do direito à tutela dessas informações, seus discursos aproximam-se na exaltação dos benefícios que tais dados podem proporcionar no oferecimento de novos serviços e produtos e na elaboração e execução de políticas públicas e na prestação dos serviços públicos, bem na alegação da ausência de prejuízo aos titulares dos dados individualmente considerados. Isso porque, com o uso de *big data* e metadados, seria, ao menos em tese, assegurado o anonimato dos usuários cujos dados foram usados para alimentar esse enorme banco de dados.

Não se nega que a expansão das práticas de coleta e de uso de dados pessoais reforça-se com as inúmeras funcionalidades dos *big data*. A ideia subjacente a essa tecnologia está no reprocessamento de dados, o que permite a utilização das informações muito além da utilidade inicial para a qual foram coletadas. De fato, embora o valor imediato dos dados seja claro para quem os coleta, como quando a Amazon registra os produtos comprados pelo usuário e as páginas por ele visitadas, pode haver um uso secundário dessas informações. Nessa senda, a capacidade tecnológica de processar e reprocessar grandes volumes de dados por meio de algoritmos é multiplicadora do próprio valor dos dados, especialmente porque eles não se perdem ou gastam pelo uso.

Assim, embora as técnicas tradicionais tenham sido desenvolvidas para obter dados escassos, estáticos, limpos e pouco relacionais, com adesão a suposições rígidas destinadas a um uso específico que o coletor tem em mente, o desafio do *big data* consiste em lidar com dados em enorme quantidade, exaustividade, variedade, dinamismo e alta relacionalidade, além de que grande parte das informações inicialmente geradas não têm um propósito prévio ou é até mesmo subproduto de outra atividade.

Nessa capacidade de processamento como multiplicadora do valor dos dados, ainda há a possibilidade de os dados serem recombinantes, de sorte que a utilidade advém não da detenção de tais informações, mas da combinação de bases de dados. Mayer-

Schonberger e Cukier mencionam, por exemplo, conclusões em estudo da Sociedade Dinamarquesa para o Estudo do Câncer que procurava a relação entre o uso de aparelhos celulares e aquela doença. Como a quantidade de dados que os pesquisadores geralmente conseguiam coletar era pequena e o tempo de coleta também não era significante, desta vez usaram dados de clientes de companhias telefônicas do período entre 1987 e 1995, num total considerável de 385.403 pessoas. Essas informações foram combinadas com o banco de dados nacional de pacientes com câncer no sistema nervoso central entre 1990 e 2007, bem como com o registro nacional de educação e renda dos dinamarqueses. Somente com a recombinação desses dados é que foi possível concluir pela ausência de relação entre o uso dos aparelhos e a incidência de câncer no sistema nervoso central (MAYER-SCHNONBERGER, 2013).

Em um estudo como esse e nas diversas atividades desempenhadas por governos e empresas com utilização de *big data*, alega-se inexistir perigo à privacidade dos titulares dos dados, aos argumentos de que somente são utilizados metadados e de que há a anonimização das identidades. Já é sabido, no entanto, que a tese da garantia da privacidade e da proteção dos dados pessoais por meio da anonimização já não se sustenta nem mesmo com o uso das técnicas mais elaboradas de anonimização em databases (BROEDERS, Dennis; SCHRIJVERS, Erik; SLOOT, 2016).

Em uma database, pode-se diferenciar as tipologias de dados em, por exemplo, identificadores, atributos-chave e atributos confidenciais (DOMINGO-FERRER, J; TORRA, 2008). Aqueles são os dados que inequivocamente permitem identificar seu titular, como nome, número de passaporte, número de identidade, e, em regra, precisam ser suprimidos nos *big data* para garantir a não identificação. Os atributos-chave, por sua vez, consistem nas principais características do indivíduo e que, combinadas, permitem facilmente a reidentificação, como profissão, endereço, idade e sexo. Por fim, atributos confidenciais consistem em informações sensíveis do titular, como remuneração, religião, afiliação política e estado de saúde.

Um *big data* mais seguro seria aquele em que, para cada grupo de registros de indivíduos com atributos em comum, haja variações de atributos confidenciais. No entanto, ainda assim, se a variação de atributos confidenciais for muito baixa, ainda será possível “desanonimizar” os titulares dos dados (DOMINGO-FERRER, J; TORRA, 2008). Assim, técnicos podem recuperar as identidades supostamente desvinculadas a uma pessoa ou identificar informações adicionais sobre elas, como ocorreu na disponibilização de dados “anônimos” pela AOL em 2006, mencionada no tópico anterior.

Além disso, nem mesmo a concepção de privacidade empregada pelos desenvolvedores das tecnologias é sempre a mesma, de sorte que a forma com que se busca, pela técnica, assegurar tal direito individual também não é uniforme. Assim, há quem tome a privacidade, e o direito sobre dados pessoais, como direitos de ter suas informações não reveladas (privacidade como confidencialidade), ao passo que outros os veem como direitos que conduzem à faculdade de controle sobre as informações.

Para quem identifica o exercício da privacidade e da tutela de dados com a confidencialidade de tais informações, importam as capacidades dos demais de violar a confidencialidade das comunicações, assim como dos tráfegos de dados. Em razão disso, aqueles direitos precisam ser tutelados por meio de tecnologias de criptografia ou de *privacy-enhancing technologies* (PETs), nas quais se busca coletar o mínimo possível de informações e se busca assegurar a privacidade por meio do design (*privacy by design* – PBD) de dispositivos e aplicativos.

Para quem identifica os direitos à privacidade e à tutela dos dados pessoais com a possibilidade de controle sobre as informações pessoais na rede, o foco está na criação de mecanismos que concedam controle, pelos usuários, sobre os fluxos de dados, pois já se pressupõe que, em um mundo cada vez mais conectado, as informações pessoais terão de circular. Assim, os indivíduos devem ter poderes para tomar decisões informadas sobre o uso de serviços, o que pode ser buscado por meio de maior transparência e maior controle sobre os fluxos de informações pessoais (BROEDERS; SCHRIJVERS; SLOOT , 2016).

Essa perspectiva coaduna com a diferenciação entre os direitos à privacidade e à tutela sobre os dados pessoais. Com efeito, nas alegações de governos e companhias privadas no sentido de que a anonimização dos dados afasta a afronta a direitos individuais porque, em razão de não ser possível - em tese – reidentificar os titulares, inexiste afronta à privacidade, está subjacente a falácia de que a totalidade dos direitos individuais está garantida.

Em verdade, vislumbrada a tutela sobre dados pessoais como direito subjetivo autônomo, o fato de não ser identificado o titular do dado continua a ofender tal direito individual se o sujeito de direito não possui possibilidade de controle sobre suas informações. De fato, como visto no tópico 2.ii, na tutela dos dados está abrangido não apenas o direito à não identificação e à não exposição, mas também a faculdade de controle sobre a disseminação das informações pessoais.

Então, *big data* e algoritmos sempre violariam a tutela sobre os dados pessoais? Em verdade, não, mas a observância desse direito subjetivo, pautado na faculdade

de controle, carece da possibilidade de concessão de adequado consentimento. O cerne da situação, portanto, parece estar não propriamente nas práticas com os dados, mas na insuficiência dos modelos de consentimento até hoje empregados por governos e empresas desenvolvedoras de tecnologias. Basta notar, por exemplo, o escândalo em que se envolveu o Facebook em março de 2018, quando o uso de dados pessoais de seus usuários afetou a credibilidade e o valor de mercado da empresa em razão de a política de privacidade vigente até 2014 e de a tecnologia por trás da plataforma ter permitido que terceiros usassem aquelas informações pessoais para finalidades não autorizadas pelos usuários.

Nestes pontos, então, nota-se que tanto a alegação de anonimização dos dados em *big data* quanto a atribuição aos algoritmos da execução das funcionalidades dessas tecnologias constituem tentativas de objetivar os processos de exploração dos dados pessoais e legitimar ameaças à privacidade e à tutela sobre os dados pessoais. Nesse discurso comum, companhias privadas e governos aproximam-se e a análise desse contexto conduz à percepção de que isso somente tem sido viável em razão de a força do discurso dos usuários ser negativamente desproporcional em face do domínio das tecnologias pelos demais atores no ciberespaço. Essa hipossuficiência de forças poderá ser notada no próximo item, em que será estudado o discurso dos usuários nesse contexto.

4.2.2 Influência da governança algorítmica e da arquitetura da rede para reforçar a assimetria informacional

O funcionamento de uma rede mundial de comunicação e troca de informações como a internet depende de uma linguagem e de padrões técnicos que sejam globalmente uniformes e aceitos. Por conseguinte, essa funcionalidade exige a modelagem, a criação de políticas e a gestão de tecnologias imprescindíveis para a parte operacional da rede.

No Capítulo 3, para compreender o contexto das teorias regulatórias aplicáveis a esse ambiente, foi possível observar como a criação e a implantação da internet a partir de iniciativa conjunta da academia e do governo norte-americanos originou um jogo de disputas sobre o controle desses fatores operacionais da rede.

A operacionalidade da rede mundial envolve recursos não apenas técnicos, mas também escassos, os denominados recursos críticos, como nomes de domínio e os números de endereço IP. A relevância deste tema reside não somente na manutenção da viabilidade de

funcionamento da rede com interoperabilidade e sem fragmentação, mas na influência sobre o exercício de direitos, já que decisões de governança da internet afetam crescentemente o exercício de liberdades políticas e econômicas, além de outros direitos subjetivos.

Essa gestão envolve, então, o desenvolvimento e a aplicação de normas e procedimentos que abrangem tomadas de decisão, o que tem sido feito por governos, bem como por entidades do setor privado e da sociedade civil. Embora essa governança seja, então, multissetorial, pode-se observar a predominância dos setores governamental e de mercado sobre a sociedade civil (DENARDIS, 2010). Para compreender esse fenômeno, é preciso algum entendimento sobre o que é, de fato, gerido, objeto que envolve pelo menos a arquitetura da rede e os principais recursos críticos.

A arquitetura da rede, isto é, a infraestrutura física por meio da qual os pacotes de informações transitam foi criada de modo a permitir a ampliação do acesso e da inovação. Assim, essa estrutura física é dividida em camadas de funcionalidade técnicas, sendo cada uma delas formada por um conjunto de hardware e software responsável por um grupo de tarefas que serão necessárias para o conjunto de tarefas da camada superior. Cada camada superior está em um nível decrescente de abstração e de distância do usuário final.

Dessa maneira, a camada mais basilar pode ser designada camada de ligação/conexão/rede (*link layer*), na qual protocolos padronizados são utilizados para transmissão de dados, sendo nesta camada escolhida a melhor rota a ser seguida pelo pacote para se deslocar do nó emissor para o nó receptor. Nela, então, ocorre o roteamento do conjunto de dados entre a origem e o destino, sendo realizado o controle de congestionamento nos diversos caminhos possíveis para essa transmissão, a fim de viabilizar a melhor operação das comunicações. Posteriormente, as camadas de internet e transporte usam protocolos para a comunicação direta entre dois nós da rede (*end-to-end*), fazem a comunicação entre a estrutura física da rede e o nível de aplicação e a divisão dos pacotes de dados em datagramas para percorrerem os caminhos disponíveis. Ao fim, na camada de aplicação, a mais próxima do usuário final, faz-se a comunicação entre a aplicação usada e a camada de transporte, usando portas que são reconhecidas pelo protocolo de transporte (SCHEWICK , 2010).

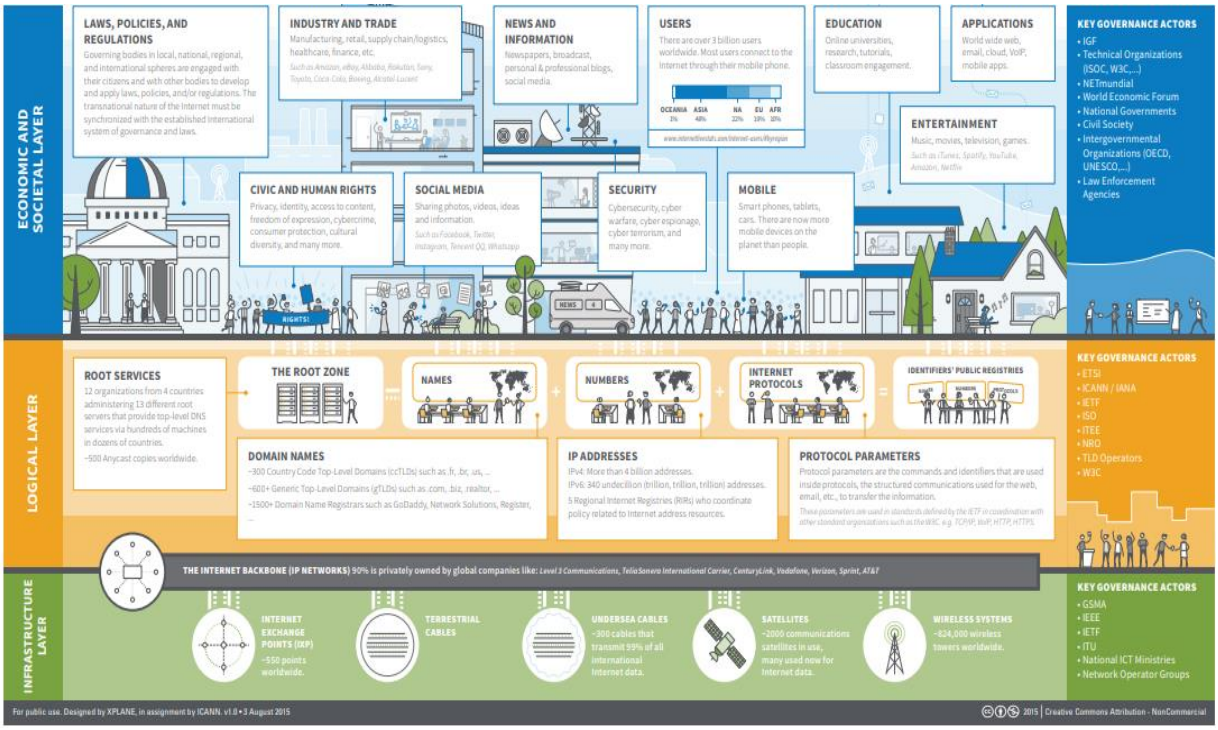

Figura 4 – Infográfico das camadas de governança digital
Fonte: ICANN, *Three Layers of Digital Governance Infographic*, 2015. Disponível em https://www.icann.org/news/multimedia/1563. Acesso em 19 de junho de 2018.

Um dos preceitos que orientaram e orientam essa estruturação da rede consiste no princípio *end-to-end*, destinado a viabilizar que a internet seja uma plataforma de inovação, liberdade de expressão e crescimento econômico. Por tal princípio, é necessário haver uma liberdade tal que o controle sobre o que é trocado na internet (conteúdo dos pacotes) somente deve ser feito pelos próprios usuários que fazem as trocas. Além disso, todo conteúdo que transita na rede deve ser tratado igualmente e distribuído sem discriminação (SCHEWICK , 2010). Já pelo princípio da estratificação, o sistema deve ser organizado em camadas, ficando as aplicações no topo e as funcionalidades mais básicas e estruturais nas camadas inferiores.

Esses princípios, conjuntamente, auxiliam o exercício de liberdades na rede e o desenvolvimento de inovações, já que, para a criação de uma nova aplicação, por exemplo, basta dominar a programação na camada de aplicação. Logo, pelo modo como a arquitetura foi implementada, basta realizar modificações na última camada para instituir uma inovação, o que amplifica o acesso à criação de inovações e reduz até mesmo os custos das criações.

Por outro lado, as camadas de base da rede ficaram sob ingerência dos desenvolvedores da tecnologia dessa estrutura basilar. Estes, em contexto livre de regulação

governamental, foram responsáveis pela formatação de toda essa estrutura operacional, situação que tem consequências econômicas e políticas. Embora a neutralidade no tratamento das informações e a ampliação do acesso e da possibilidade de inovação tenham orientado a formatação da rede, interesses dos agentes privados passaram a interferir em decisões sobre questões técnicas imprescindíveis às comunicações e ao exercício de direitos na rede, como liberdades e privacidade.

Assim, por exemplo, no estabelecimento do protocolo a ser empregado na rede, essa linguagem pode ser usada para as mais variadas intenções econômicas e políticas. Escolhas políticas sobre uma maior ou menor liberdade a ser concedida na rede são concretizadas mediante interferências nos padrões técnicos da internet, invisíveis aos usuários e manipuláveis pela indústria privada, detentora da tecnologia, do que pelas legislações ou pelos governos.

Não somente os agentes econômicos e a arquitetura da rede, mas também governos e, principalmente, governos repressivos desvelam a possibilidade não apenas de regular, mas também de abusar de seu poder por meio da influência sobre o fluxo de informações mediante manipulação da infraestrutura da internet. O apagão prolongado na rede da Síria em 2012, a título exemplificativo, reduziu a capacidade de coordenação de reação política por parte dos cidadãos, ordenação que estava respaldada no exercício de uma liberdade de disseminação de informações e da divulgação de abusos governamentais pela rede (DENARDIS, 2013).

Logo, estabelecer os padrões técnicos passa a ser o mesmo que estabelecer as normas que valem nesse ambiente, isto é, o código normativo, o qual compõe o que DENARDIS denomina arquitetura legal, formada na tecnologia e capaz de modificar comportamentos, estabelecer políticas públicas, aumentar ou reduzir o exercício da liberdade etc. (DENARDIS, 2009).

Também na gestão do recurso crítico de nomes de domínio, a discussão sobre a definição do número e da variedade de domínios de nível superior (.com, .edu, .org etc.) tornou-se polêmica quando a indústria de entretenimento adulto sugeriu a criação do .xxx. Nessa ocasião, além da resistência daqueles que se opunham a conferir maior visibilidade à indústria adulta, muitas empresas não relacionadas a esse mesmo ramo de mercado temiam a despesa adicional de ter que registrar URLs no novo domínio para proteger suas transações comerciais.

Ainda acerca desse recurso crítico, o exercício das funções da Autoridade para Atribuição de Números da Internet (*Internet Assigned Numbers Authority* – IANA) de

atribuição e controle de nomes de domínio e de números de IP não submete-se mais ao controle direto do governo dos Estados Unidos, em razão do fim do pacto que para isso existia entre o Departamento de Comércio daquele país e a Corporação da Internet para Atribuição de Nomes e Números (*Internet Corporation for Assigned Names and Numbers* - ICANN) em outubro de 2016. A gestão passou a ser feita por um grupo multissetorial ligado à ICANN, composto de técnicos, acadêmicos, empresários e representantes de governos e de organizações não-governamentais.

Apesar disso, quando surge uma disputa sobre registros de nomes de domínio, a postura dos fornecedores de serviços de registro acreditados pela ICANN é de aguardar a solução da controvérsia em ação judicial[29]. Significa dizer que o caráter de multissetorialidade não está tão presente diante de eventuais decisões que precisem ser tomadas nessa temática, já que essa ação é transferida exclusivamente para os estados, por meio de seus Poderes Judiciários.

Mesmo em situações não referentes a conflitos na distribuição desses nomes, governos autoritários abusam de seu poder para, manipulando DNSs, impedir acesso a sítios com conteúdos que não lhes beneficiam, realizando tão somente o redirecionamento dos nomes de domínio, como feito pelo *Great Firewall* da China (BRADSHAW, Samantha; DENARDIS, 2016).

Também na gestão da estrutura física da rede não se observa a concretização da multissetorialidade que viabilizaria, em tese, a efetiva participação da sociedade civil. De fato, como o funcionamento das camadas mais inferiores que compõem a espinha dorsal da rede (*backbone*) depende da interação entre diversos sistemas autônomos e pontas de trocas de tráfego (*internet exchange* – IX) e esses são mantidos por agentes privados, são os acordos comerciais entre os intervenientes que têm orientado efetivamente a transferência dos pacotes de dados (DENARDIS, 2014).

Esse poder de controle sobre a transferência dos pacotes representa a capacidade de determinar quais informações são trocadas na rede e por quem, o que significa a capacidade de orientar processos regulatórios nessa sociedade da informação, com prevalência de poder sobre governos e usuários. A partir disso, nota-se que o domínio da arquitetura da rede representa, por si só, um mecanismo de regulação, aproximando o cenário estudado da regulação descentrada.

29 Sobre o procedimento: <https://www.icann.org/resources/pages/faqs-2014-01-22-pt>.

De fato, manter a sistemática tradicional do “comando e controle”, simplesmente com uso de normas legais e de sanções administrativas e penais, neste ambiente, não constituiria estratégia eficiente se o próprio governo está em posição de inferioridade quanto ao domínio dos mecanismos que controlam a transferência de informações. Aliás, não apenas para esse ambiente, mas para todo local regulado, Black (2001) salienta que o formato de “comando e controle” constitui mais uma ideia no plano abstrato do que um sistema regulatório efetivamente experimentado, já que o início do processo regulatório por alguma forma de autorregulação, antes mesmo da chegada do estado, é praticamente inevitável.

Assim, se a dinâmica do “comando e controle” cada vez mais é empregada como exemplo de péssimas características regulatórias, como rigidez excessiva e falta de equilíbrio entre as propostas e os resultados, essa incapacidade não apenas explicativa, mas também preditiva dessa forma de regulação é potencializada na internet. A sobreposição dos técnicos e dos agentes econômicos sobre estados e usuários no domínio da capacidade de influenciar como e o que é trocado na rede afasta a possibilidade de que o estado seja o exclusivo controlador e comandante desse ambiente.

Uma regulação descentrada mostra-se mais adequada para explicar esse cenário do ciberespaço também porque tem como premissa a complexidade das interações no ambiente regulado. Especificamente na temática da tutela dos dados pessoais, essa complexidade faz-se presente não apenas porque há essa superioridade dos técnicos e agentes econômicos sobre o próprio estado no que tange à possibilidade de controle do fluxo informacional, mas também porque o usuário, hipossuficiente nessa relação de controle, é a própria fonte dos dados pessoais.

Nos pontos de troca de tráfego, os sistemas autônomos trocam pacotes de informações por meio de acordos de *peering* ou de troca de tráfego, um contrato comercial, mas de caráter colaborativo. No entanto, com cunho econômico e não colaborativo, há os contratos de troca de trânsito (compra de trânsito), nos quais inexiste uma relação de parceria e igualdade de forças entre provedores. Nessas avenças, em verdade, provedores menores não têm o mesmo conteúdo a fornecer aos provedores maiores, daí que estes exigem compensação financeira para viabilizar o trânsito dos pacotes por sua estrutura (GETSCHKO; MOREIRAS, 2008).

É fato que trocas econômicas, como as realizadas nos contratos de troca de tráfego, não são, em si, uma novidade na vivência humana. Tampouco a regulação de relações comerciais é um assunto inédito. A peculiaridade da situação analisada referente à

arquitetura da internet decorre do fato de que esses contratos de interconexão são inovadores, sobretudo quanto aos seus efeitos econômicos e políticos, na medida em que não é simples identificar a que normas estão submetidos, envolvem agentes atuantes sob diferentes jurisdições espalhadas pelo mundo, faltam órgãos encarregados do controle dessas transações e não há transparência[30] sobre o conteúdo da comercialização (DENARDIS, 2014).

Essa falta de transparência afeta, também, pilares da criação da internet graças à hegemonia dos agentes econômicos privados no controle do funcionamento da rede. Assim, por exemplo, a neutralidade da rede fica prejudicada quando provedores usam tecnologias como inspeção profunda de pacotes (*deep packet inspection* - DPI) para, conhecendo o conteúdo da informação trocada, fazer uso distorcido dessa tecnologia, a qual poderia ser mais bem empregada para evitar pornografia infantil ou para questões de segurança.

Desvirtua-se, assim, o emprego de uma tecnologia como DPI para diferenciar a qualidade ou o preço das transações de conteúdo. Em outros casos, mesmo sem essa distorção tecnológica com uso de DPI, companhias privadas simplesmente manipulam o controle sobre a tecnologia e, ignorando vedações legais como a contida no artigo 9° do Marco Civil da Internet[31], dão prioridade a provedores de conteúdo como Whatsapp ou Facebook em pacotes de dados em prática de *zero rating*. Como explanado por Lefèvre (2017), quando as companhias telefônicas brasileiras que comercializam pacotes de dados oferecem acesso exclusivo a certas aplicações quando o volume inicialmente vendido de

30 No Brasil, a Agência Nacional de Telecomunicações realizou consulta pública em 2017 no intento de modificar seu regulamento de interconexão, a fim de atuar sobre empresas que trocam tráfego de telecomunicações na rede, como Facebook e Google. O intento consistia em ter a possibilidade de fiscalizar os contratos de interconexão para troca de tráfego, alegando a viabilidade dessa ingerência com suporte no artigo 61, "caput" e §2º, da Lei Geral de Telecomunicações ("Art. 61, Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações. §2º. É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações".)

31 Art. 9o O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
§ 1o A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
II - priorização de serviços de emergência.
§ 2o Na hipótese de discriminação ou degradação do tráfego prevista no § 1o, o responsável mencionado no caput deve:
(...)
IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais".

dados é completamente usado, são realizadas duas condutas vedadas, de bloqueio e de discriminação, afrontando também o artigo 9º do Decreto 8.771/2016[32].

Assim, novamente interesses econômicos de quem domina a tecnologia têm moldado a própria arquitetura da rede e viabilizado a afronta de noções basilares da criação da internet como estímulo à inovação, acesso à informação e neutralidade. Esta é violada quando, ignorando as vedações impostas pelo governo, provedores priorizam certos conteúdos e não sofrem consequências incisivas de órgãos fiscalizadores.

A inovação é ignorada quando a associação entre provedores dominantes no mercado (companhias que comercializam acesso à rede) com grandes companhias desenvolvedoras de aplicações como Facebook, WhatsApp e Twitter acarretam a manutenção de uma hegemonia de mercado superior a 70% (LEFÈVRE, 2017). Desse modo, a rede passa a controlar as inovações e o sucesso de uma aplicação passa a depender não de uma escolha dos usuários, mas dos provedores. A ofensa ao acesso à informação, ao seu turno, dá-se quando poucos provedores dominam o conteúdo mais fácil e popularmente acessado, limitando a utilidade da internet como promotora de liberdade, de criação de espaço para participação democrática, o que significa limitar seu papel social, político e cultural (SCHEWICK, 2010).

A respeito de tal afronta à informação pela própria tecnologia criada para democratizá-la, pode-se observar, por exemplo, que, em 2015, mais de 40% das notícias veiculadas na internet eram acessadas por meio do Facebook. Para isto, este provedor se valia de contratos com empresas jornalísticas para fazer essa intermediação do conteúdo e, dessa forma, em 2017, por possuir mais de 1 bilhão de usuários em suas plataformas, essa rede social influenciava (e influencia) o próprio exercício do direito à informação, notadamente nas regiões de pobreza e em desenvolvimento, nas quais o acesso à internet confunde-se com o próprio acesso ao Facebook (LEFÈVRE, 2017).

A tutela sobre os dados pessoais dos usuários fica igualmente à mercê dos interesses econômicos das companhias que atuam nesse ambiente, sobretudo das que desenvolvem as tecnologias, já que a inexistência de transparência sobre as práticas comerciais que envolvem tais dados e a ausência de um órgão gestor desse mercado impedem a fiscalização do cumprimento das normas de proteção de dados já existentes.

---

32 “Art. 9º Ficam vedadas condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que: I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País; II - priorizem pacotes de dados em razão de arranjos comerciais; ou III - privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico”.

Atualmente, a instituição que mais se aproxima de uma figura como essa é o Comitê Gestor da Internet, o qual estipula diretrizes estratégicas e de administração da internet no Brasil, de padrões como nomes de domínio (com uso do .br) e endereços IP, promove estudos e programas de pesquisa sobre internet no país, nos termos do Decreto nº 4.829/2003. Apesar disso, sua atuação é concretizada em recomendações de normas, procedimentos e padrões técnicos, não possuindo, todavia, caráter de órgão fiscalizador e com competência para aplicação de sanções. Em razão disso, embora haja fiscalização e denúncias por violação das normas recomendadas e até mesmo de leis já aplicáveis ao ciberespaço, como o Marco Civil da Internet, frequentemente as empresas não modificam suas práticas em razão da ausência de sanções aplicáveis e de um órgão com competência administrativa para isso.

O escândalo em que foi envolvido o Facebook em março de 2018 reforça a falta de transparência e de auditorias nas atividades empresariais capazes de afetar o direito individual dos usuários à tutela sobre seus dados. Ao lado disso, a reiteração dessa mesma empresa em atuar abusivamente em detrimento da privacidade e do direito de dados de seus usuários mesmo após, por exemplo, a aplicação de penalidades da Comissão Federal de Comércio dos Estados Unidos (ZITTRAIN; CRAWFORD; BREM, 2012) reforça o fato de que os interesses econômicos dos agentes privados ainda são a força mais relevante no estabelecimento do comportamento na rede.

Ao lado disso, os algoritmos são o mecanismo que viabiliza o uso de *big data* com dados pessoais, pois é por meio deles que o imenso volume de informações pode ser tratado e gerar conclusões. São eles que fazem nossas rotas no Waze e organizam os resultados de buscas no Google, por exemplo (SILVEIRA, 2017b). Dessa maneira, sem que haja clareza quanto ao seu funcionamento, os algoritmos delimitam as ações dos usuários e aquilo a que terão acesso, daí falar-se em governança algorítmica.

Tal governança, na prática, é exercida pelos criadores dos algoritmos, isto é, empresas privadas e entidades governamentais. Para a maioria dos usuários leigos, no entanto, inexiste clareza quanto à submissão a essa ingerência de agentes econômicos e estatais, já que o funcionamento dessa tecnologia não é anunciado aos destinatários dos algoritmos e os desenvolvedores de tais tecnologias ainda vindicam a privacidade sobre sua criação por uma questão de mercado ou de segurança.

Com isso, porém, não apenas o direito à tutela sobre dados pessoais fica prejudicado, mas a autonomia na escolha de comportamentos livres na rede, já que a

modulação da ação dos usuários os conduz a determinados caminhos cuja adesão nem sempre é escolhida livremente, mas induzida pelos algoritmos.

Estes, de fato, são invisíveis ao usuário final e, ainda que fossem apresentados, sua linguagem matemática poderia ser entendida por pouquíssimas pessoas, o que incrementa a assimetria informacional dos usuários na medida em que tal linguagem deveria ser traduzida ao leigo para que suas tomadas de decisão fossem conscientes pelo menos na adesão, ou não, dos serviços e produtos baseados em algoritmos. Tal invisibilidade pode ser e é usada não apenas para proteger segredos de mercado, mas também para cometimento de abusos baseados na hegemonia no controle sobre a tecnologia. Assim, a título de exemplo, a Volkswagen foi pega, em 2015, no cometimento de fraude na emissão de poluentes em cerca de 11 milhões de automóveis, sendo a fraude caracterizada pelo reconhecimento por algoritmo de software instalado nos veículos da submissão dos carros a testes (BASTOS, 2016).

Pode-se observar, então, a capacidade de sistemas técnicos de desestruturar um sistema normativo pretendido com a criação de normas governamentais. Isso se percebeu, por exemplo, com a tutela dos direitos autorais quando, com a internet, quase todas as pessoas passaram a ter condições de reproduzir um conteúdo protegido sob aqueles direitos com baixo custo e com a viabilidade de fiscalização muito reduzida, sobretudo inicialmente. Na mesma linha, no âmbito da temática deste trabalho, a ausência de transparência sobre as práticas técnicas com dados pessoais pelas empresas que lucram com essas commodities na internet e sobre os contratos que orientam essa atividade econômica tem inviabilizado a concretização de legislações destinadas a tutelar dados pessoais em todo o mundo.

Também no âmbito governamental, pode-se observar a sujeição dos usuários à atuação dos algoritmos no setor público, em auditorias fiscais, na gestão da sinalização de trânsito, na identificação de fraudes em pagamentos de agentes públicos, por exemplo. Em primeiro lugar, os próprios órgãos governamentais que adquirem tais tecnologias são conduzidos a uma percepção de que o produto desenvolvido pelas empresas vendedoras como uma tecnologia neutra e não-política (SILVEIRA, 2017a).

Questiona-se, então, como os algoritmos podem ser tornados claros para os gestores, já que, a despeito de sua dimensão técnica, essas tecnologias podem ser políticas sem conhecimento do seu destinatário (neste caso, órgãos governamentais). Tal questionamento é ainda mais relevante em face da realidade do *machine learning* ou aprendizagem de máquina, casos em que as próprias máquinas adquirem capacidade de

aprender na medida de seu funcionamento. Nesses casos, nem sempre o resultado da utilização do algoritmo é previsível.

Em face dessa ausência de transparência também para o próprio governo e, sobretudo, para os governados, Silveira (2017a) sugere a abertura dos códigos-fonte dos algoritmos. Essa opção, porém, afastaria a maior parte dos desenvolvedores de tecnologia, por uma questão de mercado, daí que uma opção viável poderia consistir no controle por mecanismos como auditoria (O'NEIL, 2016). Isso depende, porém, da existência de uma entidade competente para essa fiscalização, o que ainda não há no Brasil. Vale reiterar que, embora o CGI tenha atribuição de fixar diretrizes e recomendar normas, padrões técnicos e procedimentos para a internet no Brasil, não constitui um órgão do Governo e não tem competência para impor normas e muito menos sanções.

Dessas considerações observa-se que a ausência de transparência nas práticas de empresas e governos e de uma contrapartida à sociedade sobre a fiscalização das atividades na internet, capazes de violar direitos individuais dos usuários, como a privacidade e a tutela de dados pessoais, têm formalizado a governança pelos agentes de mercado e pelos governos em detrimento da sociedade civil sob o véu dos supostos benefícios do multistakeholderismo (DENARDIS, 2013).

A esse quadro, em que governos e indústrias se unem em defesa mútua na fixação de padrões técnicos, econômico, político e cultural para mineração e análise de dados, o sociólogo Philip Howard chamou *Pax Tecnica*. O autor ponderou que esse arranjo contribui para o fortalecimento das empresas e somente pode ser confrontado com a análise crítica dessas tecnologias (HOWARD apud SILVEIRA, 2017a), o que, no caso dos algoritmos, depende de maior transparência e fiscalização.

Além disso, é preciso relembrar que, de modo geral no que diz respeito à arquitetura da rede, o estabelecimento dos padrões técnicos imprescindíveis ao funcionamento dessa tecnologia foi e vem sendo realizado por instituições privadas. Não se ignora que a governança na internet não é realizada por um único grupo de atores, mas por uma multiplicidade de comunidades, instituições, especialistas e governos, em níveis local, regional e global. Há, no entanto, ingerência de cada um desses grupos em diferentes camadas da rede (ver item 4.2.2), sendo que, em uma divisão possível entre camadas de infraestrutura, lógica e econômica e social, a fixação de padrões técnicos dá-se na camada lógica.

Nesta, estabelecem-se as regras para servidores, zonas de raiz, nomes de domínio, protocolos de internet, números de IP, registradores etc. Na camada de

infraestrutura, é a fixação de padrões para a parte física da transmissão de dados, sistema de transmissão wireless, pontos de troca de internet que se mostra imprescindível. Nesses dois planos, dada a tecnicidade dos temas envolvidos, a governança é realizada essencialmente por instituições privadas, como ICANN, IANA, Organização Internacional de Normalização (ISO), W3C, operadoras de domínio (*top-level domain* ou TLD) etc. O que se observa, portanto, é a muito reduzida capacidade de influência, nessas camadas determinantes quanto ao funcionamento da rede por parte da sociedade civil, representada naquelas instituições de forma muito tímida ou inexistente.

A relevância de poder atuar sobre a camada lógica, por exemplo, decorre do fato de que é nela que se determinam os padrões necessários para que haja uma rede mundial de comunicação com identificadores e protocolos exclusivos (números, protocolos e nomes), o que é realizado essencialmente por comunidades técnicas detentoras do domínio tecnológico (ICANN, IANA, ISSO, W3C, provedores etc.).

Já é notável, porém, que conseguir atuar nessas camadas lógica e de infraestrutura vai muito além de estabelecer padrões técnicos. Em verdade, a existência dessas organizações vinculadas a poucos grupos corporativos tem implicações na dinâmica de exercício de poder. Ao examinar por que, por quem e como relações de poder são moldadas na sociedade em rede, Castells aponta que, embora uma sociedade em rede pressuponha uma dinâmica de fontes de poder que se complementam, é possível identificar "expressões concentradas de relações de poder em certas formas sociais, que condicionam e forjam a prática do poder na sociedade como um todo ao reforçar a dominação" (2015, p. 61).

Em outros termos, nessa análise sociológica referente à sociedade em rede, embora o poder esteja difundido em diversas esferas sociais (de poder), há pontos de dominação. Assim, se, na sociedade em rede, as redes constituem estruturas comunicativas, os atores sociais capazes de formatar essas tecnologias de comunicação e informação são os detentores da forma mais relevante de poder. Esse poder pode ser visto como "o processo mais fundamental na sociedade, já que a sociedade é definida em torno de valores e instituições e o que é valorizado e institucionalizado é definido pelas relações de poder" (CASTELLS, 2015, p. 57). Logo, se, nesta sociedade contemporânea, valoriza-se a comunicação e a troca de informação, dominar a técnica e os mecanismos estruturais da tecnologia necessária para essas ações representa exercer um poder mais forte que aqueles, como a sociedade civil de forma geral, a quem resta submeter-se aos padrões estabelecidos, com reduzida capacidade de realizar sua própria vontade.

Interferir, por exemplo, na dinâmica envolvida nos pontos de troca de tráfego mostra-se como uma competência limitada a poucos provedores, instituições privadas e com pretensões de lucro (ver item 3), de modo que algumas poucas organizações, por meio de acordos comerciais, tornam-se canais concentrados de relações de poder e, portanto, de dominação (CASTELLS, 2015; DENARDIS, 2014). Essa realidade sequer é percebida pelo usuário final na rede, o qual desconhece essa dinâmica comercial e técnica por trás de suas ações na internet, tampouco, especificamente no que concerne ao objeto deste estudo, as práticas com seus dados pessoais.

Em razão disso, aumentar a transparência sobre o funcionamento das práticas que podem violar direitos individuais (como tutela sobre dados pessoais e privacidade) é necessário para criar instrumentos de equilíbrio entre forças dos múltiplos atores que podem participar da governança desse ambiente.

4.3 Percepção dos usuários sobre as práticas com seus dados pessoais

Com enfoque específico na tutela dos dados pessoais dos usuários da internet, busca-se identificar, a partir da capacidade de participação desses usuários no cenário regulado, qual modelo regulatório tem capacidade de explicar, no presente momento, as práticas de governança da internet no Brasil.

Para isso, vale apresentar resultados de pesquisas realizadas com usuários destinadas a aferir seu grau de conhecimento sobre o uso de seus dados pessoais na rede. De fato, sem conhecimento sobre a realidade regulada, mostra-se inviável participar conscientemente do estabelecimento das normas desse contexto.

O Centro Internacional para Inovação em Governança (Centre for International Governance Innovation - CIGI) (2017), por exemplo, tem realizado pesquisas desde 2014, em 24 países, dentre os quais o Brasil, e abrangeu, no último ano, 24.225 usuários.

No Brasil, constatou-se que 83% dos usuários preocupam-se com sua privacidade na rede, percentual que aumentou em relação aos 72% do ano anterior. Além disso, 36% estão muito mais preocupados que no ano 2016. Entre os usuários da América Latina participantes, 70% apontam governos estrangeiros como causa para o aumento de sua preocupação acerca da privacidade online. Dentre todos os pesquisados, os principais alvos de preocupação consistem em crimes praticados na rede e nas companhias atuantes na internet. Em terceiro lugar, encontram-se os demais usuários e, em quarto, o governo.

No que concerne às compras online e à segurança nessas operações, 94% de todos os participantes consideram necessária proteção sobre seus dados pessoais, sendo que 5% pensam que tal proteção é relevante, mas não muito. Especificamente no Brasil, 92% declararam ser importante a proteção dos dados pessoais do consumidor online.

Ainda foi questionado aos participantes se acreditavam não serem monitorados na rede. Apenas 30% dos entrevistados brasileiros responderam afirmativamente. 46%, porém, tem confiança na internet no geral.

Dentre os que não confiam na segurança da rede, 86% procuram usar alguma medida para minimizar os riscos para sua segurança e privacidade, como não disponibilizar informações pessoais, usar a rede mais seletivamente, usar criptografia etc. Especificamente no que tange ao uso voluntário de criptografia, apenas 17% dos brasileiros participantes afirmaram ser muito provável que utilize esse mecanismo no ano seguinte. Para

os que responderam não pretenderem usar essa tecnologia protetiva, 36% justificaram não saberem como usá-la e 30% alegaram não confiar nesse método.

Ademais, da completude do grupo de pesquisa, dentre os que não confiam nos provedores de serviço, para 63% a justificativa para tal desconfiança consiste na crença de que tais provedores monitoram as ações na rede ou não protegem a privacidade.

Para solucionar as inseguranças, desconfianças e demais prejuízos advindos do desenvolvimento de tais tecnologias, os entrevistados foram questionados sobre métodos como fornecimento, pelos governos, de treinamento para quem foi colocado para fora do mercado do trabalho em razão de novas tecnologias, ou a realização de medidas de regulação das atividades a fim de frear o crescimento do desenvolvimento tecnológico. Como primeira solução mais eleita pelos entrevistados, situou-se a necessidade de as empresas considerarem as consequências sociais e econômicas no momento do desenvolvimento das tecnologias.

Outro estudo internacional foi realizado pela empresa de tecnologia da informação Unisys Security em abril de 2017, em 13 países, dentre os quais o Brasil, o que resultou na pesquisa Unisys Security Index (UNISYS, 2017). Em cada país, foram entrevistados mais de 1000 usuários e as conclusões são baseadas nos seguintes parâmetros: segurança financeira (fraudes bancárias), segurança da internet (vírus e problemas em transações online); segurança pessoal (roubo de identidade) e segurança nacional (desastres e epidemias).

Um dos resultados mais destacados na pesquisa consistiu no percentual de 72% dos brasileiros que apontaram sua preocupação com a possibilidade de roubo de identidade, qualificando-a como “extremamente” [preocupados] ou “muito preocupados”. Tal porcentagem ainda refletiu o receio de uso indevido das informações pessoais. Com relação às fraudes bancárias, a mesma porcentagem de participantes manifestou-se extremamente ou muito preocupados.

Já a plataforma de pesquisa Opinion Box realizou pesquisa em 2016, com 1.884 internautas brasileiros distribuídos representativamente por sexo, idade, classe social e região do país. Um dos resultados alcançados foi o percentual de 30% de brasileiros que acreditam não ter sua privacidade respeitada na internet em nenhum grau. Quando questionados sobre a informação de seus dados pessoais para realização de compras na internet, 40% declararam discordar em entregá-los. Na mesma linha, apenas 28% dos participantes sentem-se à vontade em fornecer dados cadastrais quando vão aderir a uma nova rede social (OPINION BOX, 2016).

Dessas descrições, pode-se notar que as pesquisas tiveram a serventia de indicar que a preocupação dos usuários com sua privacidade e com a tutela sobre seus dados pessoais na rede tem crescido. Apesar disso, a grande maioria permanece conectada e utiliza as aplicações mesmo com a crença de que suas ações são monitoradas e de que sua privacidade não é resguardada. Não se pode concluir, porém, que tal permanência deriva do consentimento dos usuários em serem monitorados ou, por qualquer forma, terem sua autodeterminação sobre os dados pessoais desconsiderada por provedores ou governos.

De fato, os participantes não foram questionados acerca de seu efetivo conhecimento sobre práticas concretas de coleta, uso e disseminação de seus dados pessoais, o que impede analisar os resultados a partir da premissa de que os participantes deram suas respostas cientes do que realmente acontece com tais informações.

Embora tais pesquisas não reflitam o grau de ciência, por parte dos usuários sobre as práticas de empresas e governos com base em seus dados, indicam que, também a despeito de a quantidade de pessoas conectadas aumentar a cada ano[33], há considerável inquietação dos indivíduos sobre sua privacidade e segurança na rede. Em outros termos, não se pode concluir que a expansão das conexões e de uso dos serviços fornecidos na internet resulte de sua conivência com a indiscriminada coleta, tratamento e disseminação de seus dados pessoais.

Questionamentos mais especificamente destinados a medir o grau de informação direcionada aos usuários sobre as práticas comerciais pautadas em seus dados pessoais foram realizados pelo centro de pesquisa Internetlab. Desenvolvendo o projeto Quem Defende Seus Dados? (INTERNETLAB, 2016) em parceria com a Electronic Frontier Foundation, o grupo analisou as práticas em termos de privacidade e proteção de dados adotadas por provedores de acesso no Brasil entre outubro de 2015 e março de 2016.

A análise tinha por escopo central alcançar a resposta para o questionamento: "O provedor de Internet fornece informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados?". A pesquisa foi realizada perante companhias fornecedoras de acesso à internet no Brasil, por estrutura de banda larga fixa ou de telefonia móvel, tendo como exigência que cada empresa correspondesse a pelo menos

33 Eram 64,7% dos brasileiros com mais de 10 anos de idade no 4º trimestre de 2016, representando acréscimo em relação aos 49,4% da pesquisa de 2013. Instituto Brasileiro de Geografia e Estatística. "Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD. Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal". 2018. Disponível em < ftp://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_continua/Anual/Acesso_Internet_Televisao_e_Posse_Telefone_Movel_2016/Analise_dos_Resultados.pdf>. Acesso em 5 de março de 2018.

10% do total de acesso no Brasil para ser participante. Assim, com base em informações divulgadas em outubro de 2016 pela Agência Nacional de Telecomunicações, foram eleitas companhias representantes de aproximadamente 90% do acesso à internet no país.

No intuito de verificar o nível de observância ao artigo 7º, VI e VIII, do Marco Civil da Internet[34] - nos quais são previstos os direitos dos usuários a informações claras e completas, nos contratos de prestação de serviços, acerca da proteção dos registros de conexão e acesso e a informações sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais -, foram analisados os contratos dos provedores de internet, concluindo-se que nem mesmo as informações aos usuários sobre a utilização e a coleta de seus dados são satisfatórias.

Dentre outros aspectos da pesquisa[35], no quesito referente ao oferecimento de informação sobre o tratamento de dados pelas empresas, 5 dos 8 contratos analisados não atenderam a nenhum dos parâmetros consistentes em fornecimento de informações ou referências legais acerca da coleta de dados, do uso e/ou tratamento de dados, do armazenamento de dados e sua exclusão, da proteção dos dados e práticas de segurança e da utilização dos dados por terceiros e referentes, ainda, à facilidade de acesso a tais informações no sítio eletrônico da companhia. Além das 5empresas que não atenderam a nenhum desses quesitos (Oi, Vivo e GVT no fornecimento de banda larga fixa, e Oi, TIM e Vivo no fornecimento de internet móvel), as outras 3 companhias (Claro móvel, TIM móvel e Net banda larga fixa) observaram apenas dois dos seis parâmetros de avaliação.

No relatório realizado em 2017, houve melhora nesse quesito, agora com 2 companhias atendendo à totalidade dos quesitos, 2 atendendo a três dos quesitos e outras 2

34 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

35 Os parâmetros de avaliação consistiram em:

"(I) A empresa fornece informações ou referências legais claras sobre coleta de dados, incluindo quais dados são coletados e em que situações a coleta ocorre;

(II) A empresa fornece informações ou referências legais claras sobre uso e/ou tratamento de dados, incluindo os fins para os quais são utilizados e como se dá a utilização;

(III) A empresa fornece informações ou referências legais claras sobre armazenamento de dados, incluindo por quanto tempo são armazenados, onde são armazenados e quando/se são apagados;

(IV) A empresa fornece informações ou referências legais claras sobre proteção de dados, incluindo quais práticas de segurança observa na guarda de dados, se há política de anonimização de dados e quem teria acesso aos dados, observando também o disposto no art. 16 do Decreto no 8.771/2016;

(V) A empresa fornece informações ou referências legais claras sobre utilização de dados por terceiros, incluindo informações sobre as circunstâncias em que isso aconteceria ou/e a necessidade de autorização do cliente para tal;

(VI) Há facilidade de acesso a essas informações a partir do site da empresa".

atendendo a dois deles. De todo modo, ainda era uma minoria de empresas que efetivamente atendia aos comandos previstos no Marco Civil da Internet em sua completude.

Posteriormente, no relatório divulgado em 2018, após revisões realizadas em novembro de 2017 a março de 2018, não houve uma melhora proporcional, já que foram incluídas novas empresas na análise, mas 9 das 11 companhias inseridas na pesquisa ainda não atendiam, a contento, aos quesitos de informação:

Relatório de 2017:

Figura 5 – Relatório Quem Defende Seus Dados 2017

Fonte: http://quemdefendeseusdados.org.br/pt//

Relatório de 2018:

Figura 6 – Relatório Quem Defende Seus Dados 2018

Fonte: http://quemdefendeseusdados.org.br/pt/

Ao lado desse parâmetro referente à informação aos consumidores sobre o tratamento de seus dados pessoais, as companhias também foram analisadas sobre a postura de comunicar o consumidor individualmente quando há concreta situação de requisição de seus dados ou registros de conexão. Considerando que essas ocasiões foram consideradas oportunidades relevantes para o exercício de direitos de defesa contra abusos e irregularidades, foi apresentado, então, esse parâmetro para investigação, a qual foi limitada aos contextos em que não há sigilo no procedimento que justificou o pedido.

Verificou-se que nenhuma das empresas tem a prática de notificar o usuário previamente à entrega de dados cadastrais e registros de conexão, mesmo quando não há sigilo cominado por lei ou ordem de autoridade, e ainda que se trate apenas de procedimento administrativo. A relevância desse critério de análise está em que a regulação capaz de tutelar efetivamente os dados pessoais, nos moldes até mesmo dos princípios já previstos na legislação brasileira, precisa abranger a obrigatoriedade de transparência por parte das empresas que, de alguma maneira, contribuem para a coleta, o armazenamento e a disseminação dos dados.

O relatório, então, apenas reforçou a razão de ser da preocupação dos usuários brasileiros sobre as ofensas aos direitos de tutela dos dados pessoais na rede, na medida em que obrigações básicas previstas no Marco Civil da Internet não estão sendo suficientemente cumpridas pelos provedores analisados.

A partir desses estudos, nota-se não apenas que a autodeterminação sobre os dados pessoais não é adequadamente exercida pelos usuários brasileiros, mas também que a maioria deles (70%) acredita ser monitorado na rede e uma parte dos usuários (30%) é completamente descrente quanto à possibilidade de manutenção de sua privacidade nesse ambiente. E, apesar de estarem crescentemente inseridos no universo da internet, os indivíduos têm aumentado sua preocupação sobre privacidade na rede e possuem receio do uso indevido de suas informações e, no Brasil, 92% considera importante a proteção de dados pessoais do consumidor.

Tais posicionamentos dos usuários - de preocupação crescente quanto às práticas comerciais e governamentais que envolvem seus dados - sequer partem da premissa da ciência de tais indivíduos quanto ao que efetivamente é realizado com seus dados. De fato, as pesquisas analisadas também permitiram constatar que a maioria das empresas fornecedoras dos serviços de conexão sequer cumpre adequadamente as obrigações de informar o consumidor sobre o tratamento de dados realizado, além de que nenhuma os comunica da entrega de dados quando requerido em procedimento desprovido de sigilo imposto por lei ou autoridade.

A própria falta de transparência por parte das fornecedoras de serviços, além de violar o direito básico do consumidor à adequada informação (artigo 6º, III, e artigo 31, do Código de Defesa do Consumidor), impede ou dificulta muito que, nos moldes das teorias corregulatórias, o usuário participe ativamente da modulação dos comportamentos na rede que envolvem seus dados pessoais e, principalmente, da criação de normas formais regulatórias em que haja prevalência da tutela de seus direitos na rede.

De fato, considerando que o fluxo das informações é extenso e envolve diversos atores e práticas com os dados, o efetivo posicionamento dos usuários em relação a essa realidade e, portanto, o real exercício de sua autodeterminação informacional e da influência na governança sobre essa realidade dependem de seu conhecimento acerca desse contexto.

A ausência da adequada informação aos usuários não pode ser desconsiderada quando se pensa no Paradoxo da Privacidade (BRIAN, 2010; STONE, 2008), expressão cunhada para designar o cenário percebido nas pesquisas mencionadas, no qual os

indivíduos prezam sua privacidade e a proteção de seus dados, mas, ainda assim, cada vez mais os disponibilizam aos fornecedores de serviços e produtos.

Diante disso, destaca-se a investigação realizada por Hsing (2016), a qual, na tentativa de obter alguns esclarecimentos sobre o fenômeno do paradoxo da privacidade e de, até mesmo, compreender se ele existe, investigou como a coleta de dados pessoais afeta a escolha de aplicativos móveis. A pesquisadora considerou riscos e benefícios da divulgação de informações sensíveis de usuários desses serviços, considerando dados sensíveis as permissões solicitadas pelas aplicações a dados do indivíduo ou de seu dispositivo. A partir disso, investigou a relação entre as preocupações dos usuários com sua privacidade (intenção de uso) e o efetivo uso do aplicativo (comportamento real).

O estudo foi dividido em três etapas, sendo que, na primeira, realizou-se análise documental de comentários e descrições das aplicações em loja de aplicativos móveis na loja do sistema operacional Android, bem como de artigos e livros sobre o tema. A intenção da pesquisadora consistia em analisar se os dados coletados eram compatíveis com a funcionalidade da aplicação, se a empresa informava sobre o uso de dados dos usuários e comunicava as fontes de receita do negócio, tudo analisado a partir da descrição do produto na loja virtual, dos comentários de outros usuários, da política de privacidade e do sítio eletrônico da companhia.

Na segunda fase, a análise foi quantitativa com base em aplicações de fotografia e de segurança, visando-se a obter elementos para compor a pesquisa realizada na etapa três. Nesta, foi aplicado questionário a um grupo de pesquisa, composto por alunos de graduação de administração e tecnologia de instituições de Ensino no Estado de São Paulo, a partir do que se realizou análise estatística.

Assim, na etapa de aplicação do questionário aos usuários, eram descritas 4 aplicações avaliadas como populares (Whatsapp, Instagram, Antivírus Acelerador & Limpeza da PSafe, GuiaBolso Controle Financeiro da empresa GuiaBolso e mCent). Dentre perguntas sobre a instalação dos aplicativos e a frequência de uso, foram apresentadas aos usuários questões sobre sua percepção acerca da coleta de dados (”acho que ele coleta POUCOS dados pessoais”; “acho que ele coleta minha localização”; “acho que ele lê meu histórico na web”).

Nos resultados sobre a influência da coleta de dados sensíveis sobre a opinião dos usuários, tanto em relação às aplicações de fotografia quanto de segurança, a autora pode concluir que, em geral, a coleta de dados sensíveis não afasta os usuários da adesão ao aplicativo quando analisado o comportamento real das pessoas. Em verdade, foi possível concluir que, quanto mais popular a aplicação, maior é a disponibilidade dos usuários

em permitir o acesso a dados pessoais: “os resultados desta etapa indicam que há possibilidade de encontrar na *survey* usuários despreocupados com a coleta de dados, desde que o produto tenha boa reputação e funcionalidades adequadas” (HSING, 2016, p. 108).

Analisando os aplicativos de fotografia, identificados os 40 mais populares e os 40 menos populares no site oficial Google Play, verificou-se, por método estatístico, que o grupo de aplicações mais populares coleta mais dados pessoais dos usuários (HSING, 2016). Além disso, as permissões de acesso a dados fornecidas pelos usuários também foram proporcionais ao sucesso da aplicação no mercado, percepções que indicam a manifestação do paradoxo da privacidade. Concluiu-se que as permissões excessivas não levavam à rejeição da aplicação pelo consumidor, mas o estudo não abrangeu a explicação dos motivos dessa preferência pelos serviços mais demandantes de dados pessoais.

O estudo também incluiu 78 aplicativos de proteção, como antivírus, limpadores de arquivos, mecanismos antifurto, localizador de celular e anti-spam, os quais eventualmente acessam dados sensíveis para que seja possível seu funcionamento. Identificou-se forte associação entre as funcionalidades das aplicações e o total de permissões dadas pelos usuários, ou seja, quanto mais mecanismos eram oferecidos pela aplicação, mas permissões totais e sensíveis foram concedidas. Por outro lado, não houve tamanha associação entre a reputação do fornecedor do serviço e a quantidade de permissões, o que indica que a disponibilidade dos usuários em fornecer acesso a seus dados decorre mais da necessidade de utilizar os serviços e produtos, do que na confiança no desenvolvedor do produto e na qualidade do próprio produto.

Assim, tanto em relação às aplicações de fotografia quanto de segurança, a autora pode concluir que, em geral, a coleta de dados sensíveis não afasta os usuários da adesão ao aplicativo quando analisado o comportamento real das pessoas.

Em verdade, foi possível perceber que quanto mais popular a aplicação e mais funcionalidades são oferecidas, maior é a disponibilidade dos usuários em permitir o acesso a dados pessoais independentemente do volume de dados a ser oferecido: “os resultados desta etapa indicam que há possibilidade de encontrar na *survey* usuários despreocupados com a coleta de dados, desde que o produto tenha boa reputação e funcionalidades adequadas” (HSING, 2016, p. 108).

A intenção de confirmar essa assertiva foi buscada na etapa seguinte da pesquisa, na qual foram analisados 363 questionários respondidos por alunos de cursos de graduação do estado de São Paulo, dentre os quais a maior parte tinha menos de 25 anos, que usavam regularmente smartphones com o sistema Android.

Dentre o total de participantes, 35% declarou-se fundamentalista (excessivamente preocupados) em relação à privacidade, 58% pragmático e 7% despreocupado.

Ao lado disso, quando houve o questionamento sobre a expectativa de coleta de permissões mais sensíveis e a prática das fornecedoras das aplicações, a maioria dos participantes errou na estimativa. Quanto ao Whatsapp, 58% cometeram algum erro. Quanto ao antivírus, por exemplo, o erro foi de 82%.

Após serem apresentadas as reais práticas de coleta de dados dos indivíduos, estes foram novamente questionados sobre a intenção de uso da aplicação. As médias totais dos que tinham baixa intenção de uso das aplicações foi de 10% para o Whatsapp, 45% para o Instagram, 74% para o Antivírus e para o GuiaBolso, isto é, apesar de tudo, a maioria dos usuários ainda tinha intenção considerável de uso do Whatsapp e a minoria ainda pretendia utilizar as aplicações Antivírus e GuiaBolso. Apesar disso, as variâncias de tais medidas eram bastante grandes, chegando a 90%, por exemplo, no caso do Whatsapp.

Nessa pesquisa com os usuários, confirmou-se proposta apresentada ao final da etapa anterior no sentido de que contingente significativo de consumidores não leva em consideração as práticas de coleta de dados pelos fornecedores no momento de escolher um aplicativo.

Na tentativa de compreender a razão desse fenômeno de comportamento contraditório indicador do paradoxo da privacidade, passou-se a investigar se os usuários que dão mais valor aos dados pessoais têm comportamento real compatível com essa filosofia, ou seja, usam aplicações que coletam menos dados. Para isso, Chen cruzou o comportamento real aferido com as respostas dadas no questionário quanto ao critério geral da importância dos dados pessoais e quanto à percepção específica sobre a coleta em cada aplicativo, o que foi realizado por meio da aplicação de testes estatísticos.

Uma das justificativas que se pode alcançar para aquele comportamento contraditório consistiu no fato de que, apesar da grande coleta de dados, superior à esperada pelos usuários, há adesão às aplicações em virtude dos benefícios advindos das funcionalidades.

Além disso, ao analisar se usuários que mais valorizam os dados pessoais efetivamente usam aplicações que coletam menos informações pessoais, percebeu-se que a associação entre esses dois fatores era fraca (Whatsapp), inexistente (Instagram e Antivírus) ou inconclusiva (GuiaBolso).

Assim, nas conclusões gerais, a autora notou que a funcionalidade da aplicação e sua reputação no mercado são os fatores que realmente afetam o uso e a intenção de uso dos usuários. Por outro lado, a efetiva coleta de dados e a percepção dos usuários sobre isso gerou resultados contraditórios, pois aparentemente influenciam o uso e a intenção de uso apenas para alguns usuários, ainda que grande parte do universo de indivíduos tenha se declarado preocupada com a violação de sua privacidade. Na mesma linha dessa ressalva, provavelmente a diferença entre a expectativa de coleta e a coleta real de dados pelo aplicativo não inibe o uso ou a intenção de uso para a maioria das pessoas.

Em razão disso, ao fim do estudo, não foi confirmada a proposição de que "o usuário usa mais aplicativos que solicitam menos permissões sensíveis" (HSING, 2016, p. 156). Ainda dentre as conclusões, uma das explicações prováveis para o paradoxo da privacidade consistiu na valorização superior das funcionalidades do que nas práticas dos fornecedores relacionadas aos dados pessoais.

Estudos complementares, embora não realizados no Brasil, têm a utilidade de indicar que, em verdade, as pessoas estão resignadas com a realidade da economia baseada em seus dados, mais do que estão de acordo com as práticas envolvidas. A crescente adesão às aplicações, apesar da grande preocupação, em geral, com a autotutela sobre dados pessoais, não decorre da sensação dos usuários de que seus interesses estão sendo acolhidos no cenário regulado, mas de que já não vislumbram possibilidade de melhora nesse sentido, sucumbindo, então, à prevalência dos demais (sobretudo das companhias desenvolvedoras dessas tecnologias). Essa resignação, portanto, não se confunde com aceitar a realidade tal como vivenciada hoje, mas com a descrença em um cenário mais favorável à privacidade e à tutela dos dados pessoais.

Essa percepção vai ao encontro de conclusões obtidas em pesquisas realizadas também com usuários de outros países.

Em estudo executado com americanos na Faculdade de Comunicação da Universidade de Annembergh (TUROW; HENESSY; DRAPER, 2015) [36], por exemplo, no qual se procurou evidenciar a falácia do *tradeoff* existente na economia de dados pessoais, constatou-se que as pessoas estão lenientes com esse modelo de economia, ainda que apenas 21% dos participantes realmente tenham manifestado concordância com a troca dos produtos e serviços por seus dados pessoais.

36 TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. "The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation", 2015. Disponível em: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>. Acesso em 5 de março de 2018.

Uma das utilidades da pesquisa consistiu em evidenciar que, quanto maior o nível de conhecimento[37] da população acerca do que se faz com seus dados pessoais, maior é o percentual de resignação com essa realidade (TUROW; HENESSY; DRAPER, 2015). Não é maior, portanto, a mudança de postura em face das aplicações, mas apenas a leniência com uma realidade que tais usuários não se sentem capazes de mudar. Ou seja, ao invés de o incremento na consciência sobre as práticas melhorar a tomada de decisões dos usuários para proteger seus dados e sua privacidade, apenas torna tais usuários ainda mais conscientemente resilientes a essa realidade, ainda que eles não concordem com ela.

Os estudos mencionados permitem identificar o discurso dos usuários sobre a temática de sua privacidade e da autotutela sobre dados na rede. Em suma, são preocupados com essas questões e gostariam que seus interesses fossem considerados. No entanto, veem-se em posição de sujeição à sistemática de mercado estabelecida pelos desenvolvedores das aplicações, na medida em que suas únicas alternativas são utilizar as funcionalidades oferecidas, abrindo mão de seus dados pessoais, ou ficar excluídos da rede de indivíduos que usam tais aplicações.

Essa alternativa da exclusão, no entanto, não representa apenas limitar as vivências ao mundo físico. Como apontado por Castells (2015), como as redes são os instrumentos da economia capitalista baseada na inovação, a reorganização do poder dá-se dentro dela. Em face disso, há uma necessidade de estar em rede para não sucumbir na dinâmica de poder que se estabelece nesse formato de sociedade (*networking power*), de modo que a perda do poder de conectar-se em rede como uma das alternativas aos usuários (ao lado apenas da alternativa de abrir mão da tutela sobre seus dados pessoais) indica a situação de ausência de opções que assegurem a permanência na rede com a plena tutela dos direitos subjetivos.

---

37 A medição foi realizada por meio do cálculo do percentual de acertos para as 13 perguntas a seguir: a) o facebook é capaz de relacionar o que as pessoas fazem quando acessam a internet por meio de um computador com o que fazem ao acessarem seus aplicativos em celulares ou tablets?; b) é legalmente permitido que uma loja cobre preços diferentes a depender da localização dos consumidores?; c) quando permito que um aplicativo móvel conheça minha localização, esse aplicativo está legalmente autorizado a compartilhar esse local com outra empresa?; d) uma empresa pode saber que abri email por ela enviado ainda que eu não responda?; e) por lei, as lojas que fornecem internet sem fio gratuita precisam assegurar que ninguém saiba o que os clientes estão fazendo online?; f) por lei, um supermercado deve obter minha permissão antes de vender informações sobre minhas compras a outras empresas?; g) os bancos enviam emails a seus clientes com links que devem ser acessados para confirmação de dados das contas bancárias?; h) por lei, sites de viagens como Expedia e Orbitz, que comparam preços em diferentes companhias aéreas, devem sempre incluir os preços mais baixos?; i) é lícito que uma loja online cobre preços diferentes a depender do horário do dia?; j) é legal que uma loja offline ou física cobre diferentes preços a depender do cliente, em uma mesma hora do dia?; k) quando um site tem uma política de privacidade, significa que o site não compartilhará minhas informações com outros sites ou empresas sem minha permissão?; l) se eu quiser ter certeza de não ser rastreado no meu celular, devo limpar os cookies do telefone?; m) por lei, as farmácias devem obter minha permissão antes de vender a outras empresas informações sobre os medicamentos de compra livre que adquiro?

Pode-se verificar que os usuários não têm conhecimento suficiente acerca das tecnologias que fazem parte do fluxo de informações na internet para tomarem suas decisões acerca das práticas com seus dados pessoais, isto é, para exercer sua autodeterminação sobre os dados. A ausência dessa competência coloca em questionamento a capacidade de tais indivíduos, no contexto de governança da internet, de efetivamente participarem como um dos atores com capacidade de influenciar comportamentos e regular esse ambiente.

4.3.1 A interpretação da concessão do consentimento como expressão do discurso dos usuários

Governos e companhias privadas têm utilizado como fator legitimador de suas práticas com dados pessoais de usuários da internet a emissão de consentimento por parte dos usuários quando aderem a uma aplicação ou passam a navegar em determinado sítio eletrônico, por exemplo. De fato, no ordenamento jurídico brasileiro, a manifestação de vontade constitui premissa para a prática de atos e negócios jurídicos. Ao lado disso, essa vontade deve ser exteriorizada para que tais fatos tenham relevância jurídica, especialmente com a consagração da tutela da confiança desde o Código Civil de 2002.

Assim, tutelada a confiança, e não apenas a vontade, as condutas dos demais participantes do contexto em que a vontade é expressa baseiam-se na manifestação efetivamente exteriorizada. Daí que, por exemplo, permanece válida e surte seus efeitos a manifestação de vontade exteriorizada independentemente de eventual reserva mental feita pelo emitente, tal como previsto no artigo 110 do Código Civil, o que é imprescindível para a segurança das relações jurídicas e para a tutela da boa-fé objetiva.

A partir disso, para quem é conveniente, defende-se que a concordância dos usuários ao aderirem a aplicações por meio da aceitação da política de privacidade e dos termos de uso (acordos de *browsewrap*) ou aos avisos de coleta de cookies em sítios eletrônicos bastam para validar e legitimar todas as práticas de coleta, tratamento e disseminação de seus dados pessoais (ROHRMANN; SILVA, 2017).

Esse princípio do consentimento constitui um dos preceitos basilares de diferenciação entre os estados totalitários e os democráticos na temática de proteção de dados pessoais e de privacidade, dentre aqueles *First Principles* assim nomeados por Reidenberg

(2000), destinados a assegurar padrões de qualidade dos dados, transparência e abertura do modo de processamento, tratamento de dados sensíveis (dados médicos, sexuais, religiosos, relacionados à raça, mecanismos de coerção). Ainda que haja diferenças na interpretação e na concretização desses princípios, há uma convergência entre as democracias sobre seus elementos centrais, podendo-se notar uma coincidência do seguinte conteúdo: coletores de dados devem informar especificadamente o propósito da coleta dos dados; necessidade de consentimento dos usuários quanto ao tratamento dos dados; transparência sobre as práticas com os dados, incluindo alerta sobre a coleta e a possibilidade de acesso aos dados guardados; especial proteção para dados sensíveis; necessidade de criação de remédios e mecanismos de coerção.

Segundo Reidenberg (2000), ao menos as democracias convergem em um conjunto central de princípios para proteção de dados ou privacidade de dados, os quais o autor denomina “First Principles”, cuja aceitação separa as nações democráticas dos regimes totalitários. Dentro dessa temática, Reidenberg se propõe a demonstrar que, mesmo com a convergência das democracias acerca desses princípios, as diferenças em sua interpretação e concretização decorrem de uma escolha central de cada país sobre duas formatações dos papeis do estado, do mercado e dos indivíduos: liberal, baseado na governança pelo mercado; ou social-protetivo, baseado em direitos.

Nesse contexto, os Estados Unidos possuem conjunto normativo menos intervencionista e no qual predomina o tratamento jurídico da questão, quando existente, pela perspectiva do mercado, sendo o usuário visto como consumidor. Nessa abordagem de implementação, o papel do Estado é mais reduzido e menos garantista e a legislação é direcionada a apenas alguns setores de proteção, como o Ato de Proteção de Privacidade em Vídeo. Nesse modelo, predomina a autorregulação, isto é, códigos de conduta, normas da indústria e contratos, em vez da ingerência do Estado por meio de leis. A proteção de dados torna-se, então, uma questão de mercado mais do que de política pública e as pessoas são tratadas mais como consumidoras do que como cidadãs.

Em contraste, a União Europeia tem modelo de proteção mais fundado em normas e direitos e trata o usuário como cidadão, não se limitando ao ponto de vista da relação de consumo. Trata-se de uma “lei de proteção de dados compreensiva”. Nesse modelo, a legislação se destina a criar um rol completo de direitos e responsabilidades relacionados ao uso de dados pessoais no âmbito público e no privado. Os Primeiros Princípios originam direitos subjetivos de natureza fundamental e normas cogentes, e agências são criadas especificamente para controlar a obediência a tais normas. Nessa linha é

que o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia contém previsão expressa não apenas de princípios, mas de direitos concretos e fundamentais dos titulares dos dados pessoais, tais como o direito de acesso (artigo 15), o direito à retificação (artigo 16) e o direito ao apagamento dos dados (artigo 17).

A existência desses dois formatos políticos torna necessária a cooperação internacional para efetivar a proteção de dados pessoais no ciberespaço, notadamente porque essas diferenças podem levar à obstrução do fluxo de dados, como destacado por Reidenberg. O Regulamento da União Europeia e leis de alguns dos estados membros, a título de exemplo, contêm previsão de vedação do fluxo de dados para países sem uma proteção da privacidade que se mostre suficiente, o que poderia afetar toda a atividade de trânsito de informações pela rede.

O terceiro modelo de implementação dos Primeiros Princípios é técnico. Especificações técnicas embasam leis de proteção de dados. Esse modelo, então, é híbrido. Ele contém normas formais, mas não é regulado por escolhas políticas do Estado, nem pelo mercado, mas por normas técnicas.

No Brasil, quando sequer havia previsão normativa sobre esse tema no MCI, admitia-se até mesmo que o consentimento fosse dado por meio do silêncio, com base na regra de que "o silêncio importa anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa" (artigo 111 do Código Civil). Com a sobrevinda da legislação específica, passou-se a exigir que o fornecimento dos dados pessoais a terceiros tenha como premissa o consentimento livre, expresso e informado (MCI, art. 7º, VII) e também para coleta, uso, armazenamento e tratamento é imprescindível o consentimento expresso (MCI, art. 7º, IX).

Ocorre que, em verdade, a grande relevância do poder de estar em rede (CASTELLS, 2015) não deixa aos usuários alternativa a não ser aderir às condições dos provedores para que usem as aplicações ou naveguem pelo conteúdo disponibilizado. Ainda que o consentimento possa ser expresso, baseado em cláusulas destacadas nos termos de uso e na política de privacidade das aplicações, a vontade expressada não pode ser considerada livre se inexiste alternativa ao usuário.

Além disso, com as tecnologias de *big data* e, principalmente, com a possibilidade de uso secundário dos dados, a exigência do consentimento como critério de legitimação e validade das práticas com dados pessoais, ao lado da ausência atual de mecanismos de fiscalização do cumprimento das normas já existentes, torna esse critério obsoleto. Veja-se que mesmo as companhias que adotam alguma política de proteção de

dados não conseguem assegurar um controle do cumprimento de sua própria política, o que ocorreu, por exemplo, com o uso secundário de dados de pesquisa comportamental para fins eleitorais pela *Cambridge Analytica*, contrariando a política do Facebook, plataforma em que houve a coleta dos dados[38].

A deficiência desse critério não tem diminuído sua relevância nem mesmo nos ordenamentos jurídicos que já vêm se aprimorando nessa temática. Em verdade, é possível reconhecer, em gerações de leis de proteção de dados pessoais[39], que ainda se busca incrementar os requisitos para a validade do consentimento, em vez de modificar esse critério legitimador, já que os ordenamentos estão pautados na manifestação de vontade. O que se fez foi adjetivar o consentimento, exigindo-se que seja livre, informado, inequívoco, explícito e específico, mas sempre sendo mantido como vetor central do conjunto regulatório (BIONI, 2016).

A manutenção do formato do consentimento prévio ainda é apontada, por alguns, como impasse para os avanços tecnológicos possíveis (GOMES, 2017) e como verdadeira carga que dificulta inovações pelas empresas, como já divulgado em relatório da Comissão Europeia (2017), especialmente porque, no momento inicial de coleta, é inviável antever todas as viabilidades de uso da informação.

Assim, interpreta-se a concessão do consentimento como expressão do discurso dos usuários, sem que se considere, no entanto, a deficiência dessa manifestação de vontade em um contexto de uso secundário dos dados. Além dessa viabilidade de usos não antevistos, vivencia-se a ausência de mecanismos de controle do cumprimento das normas já destinadas a tutelar o titular dos dados, em especial do princípio da finalidade, segundo o qual a coleta dos dados deve ser pertinente com sua posterior utilização, seu uso não deve ser abusivo e os dados devem ser descartados quando não mais necessários para a destinação à qual foram coletados[40].

---

38 Esta foi, pelo menos, uma das alegações de Mark Zuckerberg, chefe executivo do Facebook, ao Congresso Americano quando submetido a sabatina: "quando a Cambridge Analytic nos disse que não estavam usando os dados e que os excluíram, nós consideramos um caso encerrado. Nós não deveríamos ter acreditado em sua palavra". Disponível em https://canaltech.com.br/redes-sociais/cambridge-analytica-os-principais-momentos-do-depoimento-de-mark-zuckerberg-111626/. Acesso em 24 de maio de 2018.

39 Apontando gerações de leis de proteção de dados pessoais, identificadas desde a formação do Estado Moderno: SCHÖNBEGER, Viktor Mayer. "Generational development of data protection in Europe". Technology and privacy. MIT Press Cambridge, MA, USA ©1997. pp. 219-241.

40 DONEDA, Danilo. "Da privacidade à proteção dos dados pessoais". Rio de Janeiro: Renovar, 2006, p. 378: "De acordo com o princípio da finalidade, o motivo da coleta ou fornecimento de um dado deve ser compatível com o objetivo final do tratamento aos qual este dado será submetido (...) Cria-se, desta forma, uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, o modo que esta deverá ser levada em consideração em qualquer tratamento ulterior(...) No caso específico, através do princípio da finalidade, é

Além do mais, a falta da adequada transparência e a hipossuficiência informacional dos usuários conduzem à conclusão de que tais consentimentos não constituem verdadeira expressão de sua vontade livre e consciente, isto é, não podem ser tomados como manifestação de seu discurso. Essas falhas impedem a existência de real acordo de vontade ou *meeting of minds*.

Ao analisar a forma de oferecimento do consentimento em 13 aplicações do governo paulista e federal, pode-se notar que, além de apenas 7 possuírem uma política de privacidade, nenhuma delas obtém consentimento expresso sobre tratamento de dados pessoais[41]. Assim, nenhuma delas questiona o usuário se concorda com os termos e políticas da aplicação.

Partindo-se da premissa de que a lei exige o consentimento como fator de legitimação da coleta e do tratamento dos dados, mas não estabelece o modo de sua obtenção pelo coletor e fornecimento pelo usuário, pode-se concluir que o consentimento é dado somente de forma implícita, com a adesão à aplicação, contrariamente ao que já se exige no Marco Civil da Internet.

Para tratamento dessas questões, Kerber (2016) sugere três abordagens: da lei de concorrência, das leis de defesa do consumidor e das normas de proteção à privacidade. Do ponto de vista do direito do consumidor, o fornecimento de insuficientemente clara e inteligível informação sobre a coleta e o uso de dados pode ser visto como uma prática comercial desleal, violadora de direitos do consumidor como propaganda desleal, pois o serviço ou produto é anunciado como gratuito. Nessa senda, deveria ser obrigatória a disponibilidade de mais de uma opção de privacidade e a opção de pagamento em dinheiro para que os dados não fossem coletados. Outra solução seria a disponibilização de mais aplicações com padrão *opt-in* em vez de *opt-out*.

Apesar disso, as pesquisas já analisadas indicaram a insuficiência da opção de pagamento como alternativa à coleta dos dados pessoais, dada a ausência de disposição da

---

possível estabelecer um mecanismo que evite a chamada utilização secundária da informação pessoa à revelia de seu titular. Este princípio é tanto mais importante ao se levar em conta que, quebrando-se o vínculo entre o consentimento de uso dos dados pessoais para um fim específico, estar-se-ia abrindo a possibilidade para qualquer uso secundário da informação pessoal e, por consequência, tornando inócuos outros meios secundários de proteção e controle desta informação por parte de seu titular".

[41] O estudo foi conduzido pelo centro de pesquisa Internetlab em 2018, para analisar como o consentimento sobre tratamento de dados pessoais ocorre em aplicações disponibilizadas pelo governo, especificamente os aplicativos do Bolsa Família, da Caixa Econômica Federal, da Carteira Nacional de Habilitação Digital, da Anatel – Consumidor, da CPTM Oficial, da EMTU, do FGTS, do Metro SP, do Meu Imposto de Renda, do Meu INSS, da Nota Fiscal Paulista, da SNE DENATRAN e do SP Serviços. Disponível em < http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 19 de junho de 2018.

maioria dos usuários para isso. Ademais, ainda que houvesse aceitação dessa alternativa, ainda não há mecanismos de controle da não coleta ou do descarte dos dados pelos agentes econômicos e governos.

Em face disso, já se propõe a modificação do enfoque legitimador e validante das práticas com os dados pessoais, retirando-o do consentimento e transpondo para a igualdade, especificamente na igualdade do indivíduo dentro de um contexto específico de organização social, política e econômica (RODOTÀ, 2008). De fato, somente em um contexto de igualdade de instrumentos e conhecimento pode-se falar que efetivamente a tutela da privacidade e dos dados pessoais está compatível com o paradigma “pessoa-informação-circulação-controle”.

5 PARTICIPAÇÃO DOS USUÁRIOS NO CONTEXTO REGULATÓRIO E ANÁLISE DA CAPACIDADE EXPLICATIVA DAS TEORIAS REGULATÓRIAS

Analisados os discursos do estado, dos agentes econômicos e dos usuários, isto é, dos autores e alvos das práticas que envolvem a coleta, o uso e a disseminação dos dados pessoais, passa-se a analisar precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça na tentativa de compreender de que forma os Tribunais do país têm tratado a temática da privacidade e da tutela dos dados pessoais e de sua relação com os novos formatos de relação social viabilizados pelas novas tecnologias contemporâneas e, especialmente, pela internet. Busca-se, assim, verificar como aqueles discursos estão sendo acolhidos ou rejeitados nestas Cortes.

Posteriormente, as conclusões a serem alcançadas serão examinadas conjuntamente com as percepções obtidas na análise dos discursos dos atores a fim de buscar identificar qual das teorias regulatórias expostas na revisão bibliográfica mais bem explica a realidade brasileira na temática da tutela dos dados pessoais.

5.1 Concepções de privacidade e dos dados pessoais contempladas na uniformização da jurisprudência nacional e a formatação dos discursos no Supremo Tribunal Federal e no Superior Tribunal de Justiça

Embora novas demandas referentes aos desafios de compatibilização entre privacidade, sociedade da informação e internet tenham sido apresentadas cada vez mais frequentemente perante os demais tribunais do país, elegeram-se apenas aquelas Cortes Superiores em virtude da limitação do presente trabalho e do foco na jurisprudência forjada nos tribunais competentes pela uniformização da hermenêutica constitucional e infraconstitucional.

Para isso, foram empregados os termos de busca “privacidade e internet”, “internet e dados”, “dados pessoais”, “honra e internet”, “esquecimento e internet”, “dados e direito e informação e privacidade”, “autonomia e informação e privacidade”, “autodeterminação informacional” e “autodeterminação sobre dados”. Dentre os precedentes localizados, foram filtrados aqueles que, de fato, têm relação imediata com a temática da

privacidade sobre dados pessoais e, de modo mais abrangente, da relação entre privacidade e o público e o privado, os quais foram abaixo analisados, excluídos aqueles repetidos e os que, a despeito de identificados nas buscas, não se referiam à presente discussão. Deve-se registrar que a privacidade foi tratada por aquela Corte sob outras perspectivas, como a da possibilidade de limitação das uniões matrimoniais entre pessoas do mesmo sexo, mas tais situações foram excluídas da presente análise em razão da limitação desta pesquisa ao âmbito da internet.

Deve ser ponderado que a análise é qualitativa e voltou-se não apenas para as implicações da privacidade no âmbito da internet e da sociedade da informação como um todo, mas para o exame, em geral, da relação entre informações pessoais e a suposta dicotomia público-privado.

Nessa senda, com intenção descritiva, analisaram-se os julgados a fim de identificar se, na solução adotada em cada um, houve preponderância da proteção da privacidade, isto é, do plano privado do indivíduo, ou da publicidade da informação pessoal, sendo esta publicidade considerada para a satisfação de um interesse coletivo na atividade do Estado ou para a utilidade do dado no desempenho de uma atividade econômica.

Nessa pesquisa, foram identificados 11 julgados relevantes (que realmente trataram da temática e não eram repetições de julgados pretéritos) no âmbito do Supremo Tribunal Federal e 19 no Superior Tribunal de Justiça e, dentre esses, a pesquisa iniciou-se com a identificação do interesse prevalecente, elegendo-se entre a prevalência do interesse individual, do interesse do Estado ou do interesse do agente econômico eventualmente envolvido.

No plano do Supremo Tribunal Federal, em apenas um dos julgados houve evidente preponderância da proteção ao interesse individual do titular da privacidade, isto é, do indivíduo, especificamente no Inquérito nº 2245/MG. Neste julgamento, reconheceu-se a necessidade de autorização judicial prévia à utilização de informações pessoais financeiras pelo Ministério Público e por Comissões Parlamentares de Inquérito. No Inquérito, um dos investigados pela Comissão Parlamentar Mista de Inquérito dos Correios alegava que referida Comissão quebrou seu sigilo bancário com base exclusivamente em matérias jornalísticas, além de que o banco BMG teria prestado informações ao Ministério Público Federal diretamente, sem ordem judicial. Na apreciação do mérito de tal alegação, a Corte identificou a necessidade de decisão judicial prévia autorizadora do afastamento do sigilo, como forma de tutela da privacidade da pessoa investigada.

No Recurso Extraordinário nº 673707, embora não tenha havido uma escolha sobre prevalência de direito individual ou coletivo acerca da tutela de dados pessoais ou de privacidade, afirmou-se que cada indivíduo contribuinte fiscal tem direito ao acesso de seus próprios dados fiscais, como decorrência de sua autodeterminação sobre dados. Posteriormente, porém, como será relatado adiante, no Recurso Extraordinário nº 601314, superando entendimento anterior, a Corte reconheceu a possibilidade de que a autoridade fiscal, independentemente de autorização judicial, acesse e analise registros de instituições financeiras a fim de utilizá-los para investigação de delitos fiscais.

Por outro lado, em 5 dos julgados, em detrimento da privacidade individual, preponderou o interesse coletivo sobre a informação pessoal para atendimento de necessidades das atividades estatais ou para uso em atividades econômicas e, portanto, de repercussão social.

No viés da utilidade pública da informação privada, pronunciou-se, em análise de pedido cautelar de suspensão dos artigos 5º, 6º e 10, da Medida Provisória nº 1638/98, formulado na Ação Direta de Inconstitucionalidade nº 1790, a compatibilidade da veiculação diária dos processos tirados e cancelamentos efetuados às entidades representativas da indústria ou do comércio e aos serviços de proteção do crédito. Nada obstante a autora, Associação Nacional dos Notários e Registradores do Brasil – ANOREG, tenha sustentado, dentre outras teses, que a formação e a veiculação de listas com os nomes de cidadãos que tiveram títulos protestados, ou mesmo apenas apontados ou prenotados - chamadas listas negras - sem consentimento de tais pessoas violava o direito constitucional à intimidade (artigo 5º, X, da Constituição Federal) e o princípio da defesa do consumidor na ordem econômica (artigos 5º, XXXII, e 170, V, da Constituição Federal), sobressaiu a apreciação do Ministro Relator Sepúlveda Pertence. Este analisou a alteração da legislação sobre a viabilidade de divulgação de listas (certidões coletivas) dos nomes consultados pelas entidades de classe do comércio, da indústria e das instituições financeiras para a permissão de expedição de certidões diárias de todos os protestos tirados e cancelados, independentemente da prévia indicação dos nomes a serem consultados. O Relator ponderou que a economia da sociedade de massas exige a convivência entre a privacidade e os arquivos de consumo mantidos pelos fornecedores, de modo que a vedação de divulgação de tais informações, assegurada no Código de Defesa do Consumidor, não se aplica entre a entidade responsável pelo banco de dados e os cartórios de protesto, os quais alimentam aqueles bancos com informações das anotações. O voto foi seguido por maioria e, apesar da divergência do Ministro Marco Aurélio, este apenas deferia o pedido cautelar de suspensão

dos dispositivos por questão formal de ausência de urgência e relevância necessárias para regulamentação do tema por medida provisória. Registra-se que o mérito da ação não foi apreciado antes da extinção do processo, pois esta se deu pela perda do objeto em razão de a última reedição da Medida Provisória, de nº 1894-20, não ter reproduzido os artigos então impugnados.

Também com reconhecimento da prevalência do interesse coletivo sobre informações e dados de caráter privado, foi emblemático o julgamento da Ação de Descumprimento de Preceito Fundamental nº 130, referente à Lei de Imprensa (Lei nº 5.250/1967). Na ocasião, o Supremo Tribunal Federal pode assentar a tese de que os direitos constitucionais de liberdade de pensamento, criação, expressão e informação, previstos especialmente no artigo 220 da Constituição Federal, não podem estar submetidos a censura prévia em nenhuma de suas formas física ou tecnológica de expressão, na medida em que constituem sobredireitos. Considerada a realidade tecnológica atual, foi ponderado expressamente que "silenciando a Constituição quanto ao regime da internet (rede mundial de computadores), não há como se lhe recusar a qualificação de território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique plenitude de comunicação".

Posteriormente a tal julgamento, a Corte Suprema enfrentou a questão trazida na Reclamação nº 9428, com temática similar. Originariamente, a ação tinha natureza inibitória e foi ajuizada em face de S.A. O Estado de São Paulo, a fim de obter proibição de divulgação de dados sigilosos sobre o autor presentes em investigação policial em andamento. O fundamento do reclamante consistia na violação da decisão prolatada na citada ADPF nº130, na qual foi declarada a não recepção da Lei de Imprensa. Em seu voto condutor da maioria dos pares, o Relator ponderou que o conflito envolvia não apenas os direitos à privacidade e à liberdade de imprensa, mas também a inviolabilidade do sigilo das comunicações telefônicas. Apesar disso, não identificou afronta ao dispositivo ou aos motivos determinantes da citada Ação Constitucional, pois, na causa de pedir do autor da ação na origem, não foi invocada a Lei de Imprensa e porque, do julgamento da ADPF nº 130, não seria possível concluir que os direitos da personalidade, tais como a privacidade, nunca poderiam ser tutelados em face do direito de imprensa. Diante disso, a Reclamação acabou por ser extinta sem apreciação de seu mérito, mas, no voto minoritário, ainda assim, a Corte manifestou-se novamente pela precedência da liberdade de imprensa sobre os direitos individuais como intimidade, honra, imagem e vida privada.

Depois disso, na Reclamação nº 19548, ainda na temática da liberdade de imprensa, foi levada a julgamento a questão afeta à crítica jornalística realizada na internet, como decorrência da liberdade de expressão. O autor tinha obtido, em face de S.A. A Gazeta, ordem inibitória de vinculação de seu nome a prisão sofrida na Operação Pixote no contexto das eleições ao cargo de Defensor-Geral do Estado do Espírito Santo. O Tribunal corroborou a orientação de que nenhum ato de poder, nem mesmo lei ou ato judicial, pode restringir a liberdade de expressão ou de imprensa, independentemente do meio de comunicação de seu exercício. Nesse contexto, a crítica jornalística, ainda que seja dura, deve ser reconhecida como exercício da liberdade de expressão, tendo em vista o interesse coletivo sobre ela, pois "o interesse social, que legitima o direito de criticar, sobrepõe-se a eventuais suscetibilidades que possam revelar as figuras públicas independentemente de ostentarem qualquer grau de autoridade". Com base nisso, concluiu-se ser legítima a divulgação de opinião jornalística, ainda que no ambiente digital, com caráter mordaz, irônico, ou com crítica severa quando não há o ânimo de injuriar ou difamar.

Já na Ação Direta de Inconstitucionalidade nº 1945, discutia-se a compatibilidade entre a Lei matogrossense nº 7.098/98, artigo 2º, §1º, VI, dentre outros, trazendo à tona questionamento sobre a incidência do Imposto Sobre Operações de Circulação de Mercadorias e Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicações (ICMS) sobre operações com programa de computador (software) por transferência de dados (via download). O cerne do julgamento, considerada a posição majoritária, residiu na identificação da troca de dados como verdadeira transferência de mercadoria, ainda que se trate de mera transferência de uma linguagem matemática binária. Identificou-se, assim, a possibilidade de tributação do licenciamento ou cessão de direito de uso de software ainda que a circulação do produto ocorra virtualmente, sendo esta uma necessidade da realidade atual do mercado digital.

A conclusão aponta a possibilidade de que também a troca de dados pessoais dos usuários seja reconhecida como atividade lucrativa e, portanto, que a transferência de dados na internet como um todo, não apenas de dados de licenciamento ou cessão de direito de uso de software, seja reconhecida como mercadoria virtual e tenha sua função social reconhecida.

Nos julgamentos do Recurso Extraordinário nº 766390, da Suspensão de Segurança nº 3902 e da Ação Direta de Inconstitucionalidade nº 4815, deu-se prevalência à utilidade pública ou coletiva de informações de natureza pessoal, permitindo sua divulgação independentemente da anuência do titular do dado. Nos dois primeiros julgados, a função

social dos dados mostrava-se mais evidente, por tratar-se das informações sobre remunerações de agentes públicos, em relação aos quais se excluiu a tutela da privacidade, da intimidade e da segurança em prol dos princípios da transparência e da publicidade da Administração Pública.

Já na Ação Direta de Inconstitucionalidade nº 4815, julgou-se a constitucionalidade de biografias não autorizadas, o que foi analisado com situação de conflito entre as normas dos artigos 5º, V, VI, IX, X e XIV, da Constituição e do artigo 20 do Código Civil *versus* artigo 220 da Constituição, isto é entre os direitos individuais à privacidade e intimidade e a liberdade de expressão. O julgado mostra-se especialmente relevante no estudo das modificações da dicotomia público-privado porque nele foi expressamente anunciada a necessidade de que, na sociedade democrática, limitações ao exercício dos direitos fundamentais, tais qual o direito à liberdade de expressão, somente ocorram se o prejuízo advindo dessa restrição for menor que o prejuízo da limitação do interesse público sobre a informação, em razão da dimensão social das liberdades de expressão e informação.

Nessa linha, à liberdade de expressão foi conferida uma *preferred position*, como referido no voto do Ministro Luís Roberto Barroso, sob o fundamento de que, a despeito de não ser possível hierarquizar direitos fundamentais, o sistema constitucional permite posições privilegiadas de alguns valores, tais como reconhecido em relação à liberdade de expressão.

Ao listar os motivos para o posicionamento de tal liberdade como sobredireito, mencionou-se a necessidade de preservação da cultura, da história e da memória da sociedade, sendo a liberdade comunicativa uma premissa para a preservação do patrimônio cultural da nação. Assim, "a narrativa biográfica, que busca escrever a história de uma vida, acaba por se confundir com a própria escrita da História".

A Corte asseverou, ainda, que o direito à privacidade não alcança matérias de interesse público, sopesando os interesses privado e público da seguinte maneira:

> "havendo – vou repetir – conflito entre o interesse individual e o coletivo, a solução, sopesando-se valores, está em dar-se primazia, em dar-se predominância, ao interesse coletivo, e este – pelo menos falo, porque, repito, leio apenas as biografias não autorizadas – é o dos cidadãos em geral".

A leitura de tal fundamentação pode sugerir o absolutismo do direito à liberdade de expressão, sempre se sobrepondo à privacidade em razão de seu caráter de

sobredireito e de sua utilidade para a cultura, a história e a memória social. Apesar disso, sob pena de, a partir do precedente analisado, justificarem-se abusos ao interesse individual, é preciso ler restritivamente a conclusão da Corte para a prevalência do interesse coletivo na situação das biografias não autorizadas e como resultado de ponderação de valores.

Novamente em favor do interesse coletivo e público sobre a informação pessoal, a Corte Constitucional reconheceu a constitucionalidade do artigo 6º da Lei Complementar nº 105/01, que autoriza o exame, por autoridades fiscais, de registros de instituições financeiras independentemente de autorização judicial e do titular da informação. Julgando o Recurso Extraordinário nº 601314, admitiu-se o acesso a tais dados ainda que, futuramente, sejam utilizados em persecução criminal por delitos fiscais e ainda que a norma autorizadora seja aplicada retroativamente. Para os julgadores, o fundamento encontra-se na necessidade de não situar os interesses da sociedade civil em contraposição aos do Estado, já que existe um interesse coletivo na tributação. Assim, sob uma perspectiva de solidariedade, concluiu-se que a repartição de direitos e danos é necessária para que a transparência seja mecanismo de redução dos problemas da Sociedade de Risco.

Vale ponderar que o julgamento do RE nº 601314 representou o abandono da orientação anteriormente firmada no Recurso Extraordinário nº 389808, em que se identificava a privacidade como regra quanto aos dados financeiros, pois se exigia o crivo judicial para violação de tal sigilo ainda que se tratasse de prática da Receita, parte na relação jurídico-tributária, de acesso a tais informações.

Assim como os julgamentos acima descritos favoráveis aos interesses do Estado e da coletividade, em detrimento da autodeterminação sobre informações pessoais, A nova orientação indica que, na sociedade da informação, a relevância atribuída à informação pessoal tem tornado o conjunto de dados que compõem a esfera privada social, econômica e politicamente relevante. O alcance dessa relevância tem sido avalizado na jurisprudência do Supremo Tribunal Federal, permitindo-se reconhecer que, embora a privacidade tenha status de direito fundamental, a função social e a utilidade pública sobre as informações pessoais têm conduzido à prevalência da sua publicidade em detrimento da autodeterminação sobre esses dados. É o que se deu, por exemplo, com dados que compõem biografias, informações sobre remunerações de agentes públicos ou dados fiscais.

Neste ponto, essa utilidade coletiva da informação e do dado pessoal não pode deixar de ser limitada ao direito à extimidade. Este, embora ainda não reconhecido expressamente na jurisprudência destas Cortes Superiores, demanda que informações e dados que chegaram ao conhecimento de outras pessoas além de seu titular ainda possam ser objeto

de autodeterminação informacional. Em outros termos, ainda é preciso aguardar como será sopesado, na jurisprudência, o reconhecimento da relevância do dado pessoal com o direito à extimidade de seu titular.

No contexto do Superior Tribunal de Justiça, pode-se observar de forma direta o movimento de reconhecimento do potencial lesivo das práticas na internet no que tange à privacidade dos usuários e à tutela de seus dados, notadamente quando se vislumbra a ocorrência de lesão à honra. Assim, dos 19 julgados identificados, em 7 houve prevalência dos interesses do usuário que alegava a ocorrência de afronta à sua privacidade ou à tutela de seus dados pessoais na rede. Nos demais julgamentos, predominou a utilidade da publicidade da informação pessoal, seja para as atividades estatais ou econômicas, ambas, de todo modo, de proveito para a coletividade.

Nos retornos da pesquisa, o primeiro julgado em que a ofensa à privacidade do usuário foi identificada pelo Tribunal é datado de 2007 (Recurso Especial nº 320.958/RN) e abarcou o reconhecimento da necessidade de tratamento específico do direito à retratação quando a ofensa violadora da honra da pessoa ofendida foi praticada na rede mundial de computadores. A demanda era criminal e não se referia diretamente à privacidade, mas teve a utilidade de reconhecer a internet como ambiente em que as ofensas à honra são potencializadas em virtude de seu alcance. Na ocasião, foi reconhecida a prática de delito de calúnia na internet, o que demandou o exercício do direito à a retratação também na rede, para que tenha o mesmo alcance da ofensa.

Especificamente na tutela de dados pessoais e privacidade, o Recurso Especial nº 1.168.547 refere-se à controvérsia no estabelecimento de competência para apreciação de pleito de retirada de sítio espanhol de conteúdo referente à autora, uma pessoa física. No passado, a autora tinha celebrado contrato com empresa espanhola para realização de shows típicos brasileiros na Europa e na África. Depois do fim do contrato, a demandante verificou que sua imagem era recortada e utilizada indevidamente no endereço eletrônico da contratante, sem autorização prévia, razão pela qual a autora requeria a exclusão do conteúdo. A controvérsia estabeleceu-se, em suma, na definição da competência jurisdicional, pois a empresa demandada era espanhola e o sítio eletrônico estava hospedado na Espanha, o que tinha gerado a extinção do processo sem apreciação do mérito na primeira instância.

Para definir a competência da justiça brasileira, o Tribunal inicialmente reconheceu que a evolução das tecnologias informáticas internacionalizou as relações humanas e relativizou distâncias geográficas, o que, dentre outros fatores, torna necessário

mudar a forma de entender conceitos jurídicos basilares como espaço, tempo e liberdade. Também identificou peculiaridades da interação social na rede mundial de computadores, nos seguintes termos:

> "a intangibilidade e mobilidade das informações armazenadas e transmitidas na rede mundial de computadores, a fugacidade e instantaneidade com que as conexões são estabelecidas, mantidas, encerradas, a possibilidade de não exposição física do usuário, o alcance global da rede, constituem-se em algumas peculiaridades inerentes a esta nova tecnologia que permitem a prática de possíveis condutas indevidas".

Assim, identificando a necessidade de que fosse possível o exercício da jurisdição nacional no caso analisado, sob pena de a internet constituir-se como zona de ausência de responsabilização, a Corte ainda reconheceu nova concepção de privacidade, atrelada à capacidade de dispor autonomamente das informações pessoais, figurando o consentimento como critério legalizador do uso daquelas informações.

Também em favor da tutela da privacidade do usuário, na apreciação do Recurso Especial nº 1.175.675, o Superior Tribunal de Justiça cominou a obrigação de servidor de conteúdo de retirar, mesmo em tutela de urgência, informação reputada difamante por parte do usuário demandante, ainda que este não apontasse com precisão o nome do domínio em que estavam situadas as informações. Na ocasião, a decisão que gerou o recurso continha determinação a Google Brasil Internet Ltda. de retirada "do *site* de relacionamentos Orkut toda e qualquer menção difamatória do nome do autor dentro do prazo de 48 horas" (fl. 128), sob pena de multa diária no valor de R$ 800,00 (oitocentos reais), limitada a R$ 8.000,00 (oito mil reais)". Ainda que a empresa demandada tenha alegado no bojo do recurso especial que a determinação genérica de exclusão de conteúdo atrelado a determinado assunto ou pessoa, sem indicação exata da URL impossibilitava o cumprimento da ordem e que disponibilizava aos usuários mecanismos de denúncia de abusos, o Tribunal concluiu pela existência de obrigação do provedor em excluir os conteúdos ofensivos, ainda que o pedido de exclusão feito pelo usuário seja genérico, tal como no caso julgado, em que o pleito foi de retirada de toda e qualquer menção difamatória do nome do autor.

Tal orientação foi reafirmada no Recurso Especial nº 1306157, no qual o Tribunal reconheceu que, mesmo em sede liminar, cabe ao provedor retirar informações difamantes com base em pedidos dos usuários, ainda que não haja indicação precisa das URLs, devendo o prestador do serviço desenvolver as ferramentas técnicas necessárias para a

solução de problemas advindos de seu serviço, sob pena de responsabilização. No caso, vídeo ofensivo à imagem de uma pessoa jurídica já tinha sido tornado indisponível pelo Youtube, mas isso não impediu o surgimento de outros com títulos que dificultavam reconhecer a relação com a empresa ofendida. Assim, os fundamentos da demandante consistiam, em suma, na inércia do provedor em adotar medidas suficientes para evitar novas exibições de vídeos ofensivos e em impossibilitar a indexação de conteúdo difamatório ao nome da autora no instrumento de buscas Google. Para o Tribunal, "se a Google criou um "monstro indomável", é apenas a ela que devem ser imputadas eventuais consequências desastrosas geradas pela ausência de controle dos usuários de seus *sites* - que na verdade são seus clientes -, os quais inegavelmente fomentam o lucro da empresa". Além disso, concluiu-se em prova pericial produzida no processo que é tecnicamente possível à Google realizar controle prévio do conteúdo dos vídeos, de modo que a empresa apenas não o realizava por conveniência.

Com base nesses fatores, foi reconhecida a obrigação de o provedor realizar varredura de conteúdo, o que, segundo a Corte, decorre de seu compromisso social, pois sua atividade gera sua corresponsabilidade nesse controle.

Em ambos os casos, apreciados em 2011 e 2013, deu-se prevalência aos direitos dos usuários de manutenção de sua honra e privacidade na rede, em detrimento das dificuldades operacionais alegadas pelas fornecedoras dos serviços e do interesse coletivo na manutenção da disponibilidade dos conteúdos. Apesar disso, a orientação jurisprudencial foi superada pelo Marco Civil da Internet, o qual passou a prever, no parágrafo único do artigo 19, a imprescindibilidade da indicação clara e específica do conteúdo a ser indisponibilizado, com a possibilidade de identificação inequívoca por parte do provedor ("a ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material"), o que vem sendo interpretado como necessidade de indicação da URL. A nova legislação também foi de encontro com a jurisprudência citada ao instituir a obrigação de exclusão do conteúdo tão somente após ordem judicial.

Também antes da criação do Marco Civil da Internet, a Corte, para viabilizar a tutela da privacidade de usuários vítimas da ação de outros usuários, cominava aos provedores a obrigação de manutenção dos dados pessoais pelo período mínimo de três anos, isto é, pelo prazo durante o qual seria possível a apresentação de pretensão indenizatória pela suposta vítima nos moldes do artigo 206, §3º, V, do Código Civil. O caso gerador de tal orientação referente ao prazo de guarda, Recurso Especial nº 1300161, foi

julgado em 2012 e consistia em demanda indenizatória em que a parte autora, usuário que se reputava ofendido em razão da veiculação de ofensas por meio de emails em serviço de correio eletrônico disponibilizado pelo réu, Microsoft Informática Ltda.

De forma conexa, foi ajuizada medida cautelar destinada não ao reconhecimento da responsabilidade civil, mas à obtenção dos dados para identificação do emitente das mensagens eletrônicas. Embora tenha sido reconhecida a ausência de responsabilidade do provedor, ao qual não poderia ser atribuída a obrigação de averiguação prévia do conteúdo de mensagens trocadas por email, firmou-se a necessidade de guarda de dados suficientes para identificar a autoria de mensagens, coibindo o anonimato (Constituição Federal de 1988, artigo 5º, IV), sob pena de responsabilização por culpa *in omittendo*.

Não se ignorou, porém, a necessidade de manutenção da privacidade dos usuários, pois a disponibilização da identificação somente seria possível quando constatada a prática de ilícito e somente por meio de ordem judicial.

Já em 2013, a demanda apresentada ao Tribunal para tutela da privacidade atraiu a análise do direito ao esquecimento, o qual foi reconhecido a despeito da existência do direito da coletividade ao conhecimento de informações que constituem sua história (Recurso Especial nº 1334097). O requerente tinha sido acusado da prática de atos criminosos na chacina da Candelária em 1993, tendo sido absolvido pelo Tribunal do Júri por negativa de autoria, mas, em 2006, no programa televisivo Linha Direta – Justiça, a demandada, TV Globo Ltda., pretendia veicular o caso, apontando o autor como um dos acusados. Um dos critérios empregados para análise do pedido foi a falta de contemporaneidade da notícia, o que, mesmo considerado, em contraposição, a história da sociedade como patrimônio imaterial do povo, permitiu afirmar o direito à não veiculação de informações verdadeiras, porém antigas, sobre o demandante.

Ainda que se tratasse de programa televisivo, a Corte utilizou a oportunidade do julgamento para destacar peculiaridades de a divulgação do programa ocorrer na internet, o que demanda soluções técnicas não existentes no plano físico. Ademais, foi destacada a progressiva redução da separação entre as esferas do público e do privado com as novas tecnologias. Assim, “o antigo conflito entre o público e o privado ganha uma nova roupagem na modernidade: a inundação do espaço público com questões estritamente privadas decorre, a um só tempo, da expropriação da intimidade/privacidade por terceiros, mas também da voluntária entrega desses bens à arena pública”.

Em seu voto, o Ministro Relator Luis Felipe Salomão destacou o arrefecimento da dicotomia público-privado nesses termos:

> **“**Essa tem sido uma importante - se não a mais importante - face do atual processo de esgarçamento da intimidade e da privacidade, e o que estarrece é perceber certo sentimento difuso de conformismo, quando se assiste a olhos nus a perda de bens caros ao ser humano, conquistados não sem enorme esforço por gerações passadas; sentimento difundido por inédita "filosofia tecnológica" do tempo atual pautada na permissividade, para a qual ser devassado ou espionado é, em alguma medida, tornar-se importante e popular, invertendo-se valores e tornando a vida privada um prazer ilegítimo e excêntrico, seguro sinal de atraso e de mediocridade”.

Vale registrar que sequer se tratava de informação pessoal, mas de pretensão de veiculação de informação pública, existente em processo criminal desprovido de segredo de justiça. Ainda assim, identificou-se a existência de uma vida útil da informação criminal e erigiram-se a dignidade humana, a honra, a privacidade e a intimidade como direitos e valores que se sobrepõem, no caso concreto, ao interesse da coletividade na informação.

Em todos esses julgamentos, o Superior Tribunal de Justiça pode delinear o direito à privacidade nos novos formatos de relação social viabilizados pelas novas tecnologias, em especial a internet, sendo úteis especialmente para permitir concluir pela subsistência da necessidade de tutela daquele direito ainda que as informações pessoais, atualmente, possuam sua função social e utilidade para a coletividade.

Apesar disso, na maioria dos julgados retornados na pesquisa, não houve limitação da publicização de informações ou dados relacionados aos usuários na rede, ou de ingerência, por algum método, na privacidade na rede. Embora não se possa asseverar, de plano, que essa tendência jurisprudencial revela a não consagração da privacidade na jurisprudência do Tribunal, é possível constatar a preponderância, na maior parte dos julgados, da disponibilização de dados em prol de atividades econômicas ou estatais e da participação dos provedores na esfera de privacidade dos usuários em detrimento desse direito individual.

No Habeas Corpus nº 26769, por exemplo, concluiu-se que a autoridade fiscal pode solicitar dos provedores, independentemente de autorização judicial, informações sobre declarações de imposto de renda falsas feitas por contribuintes e que se encontrem armazenadas pelos provedores. No caso concreto, a Receita Federal tinha colhido, perante provedor, informações sobre declaração de imposto de renda de contribuinte que, posteriormente, foi acusado em ação penal por crime contra a ordem tributária. A colheita

dos dados deu-se antes mesmo do inquérito policial e, portanto, sequer existia autoridade judiciária com competência para decidir sobre eventual pedido de quebra de sigilo de dados. Apesar disso, foi pronunciada a legalidade da prova posteriormente empregada em ação penal, uma vez que, a despeito de o Código Tributário Nacional não autorizar a quebra do sigilo dos dados fiscais, a Receita é a própria destinatária das declarações falsas armazenadas perante o servidor.

A decisão final, então, foi favorável ao Estado e à disponibilização dos dados pessoais em favor do exercício da atividade estatal, vislumbrando-se a utilidade das informações em prol da coletividade.

Além dessa situação referente à disponibilização de dados, a maior parte dos precedentes em que não foi acolhida a tese da parte que procurava valer-se do direito à privacidade tratou da hipótese de responsabilização dos servidores por atos originários de terceiros, outros usuários, a partir dos quais houve ofensa à privacidade do lesado.

Em uma das situações submetidas ao Tribunal (Recurso Especial nº 844736), um usuário ajuizou ação de obrigação de fazer e de indenização em desfavor de uma fornecedora de serviços, relatando que dela recebia emails publicitários com conteúdo pornográfico e reiterava essa conduta mesmo após ter sido solicitada, extrajudicialmente, a exclusão da lista de destinatários. O demandante argumentava que a propaganda era abusiva e o recebimento reiterado dessas mensagens pornográficas ofendia sua privacidade, além de sua honra, moral e dignidade, razão pela qual vindicada a paralisação dessa prática pela ré e a condenação ao pagamento de indenização por dano extrapatrimonial. Apesar disso, foi vencedor o voto que dava prevalência aos direitos do agente econômico, sob o fundamento de que o envio de *spam* não pode ser usado como justificativa para indenização por danos morais. Nada obstante o relator tenha fundamentado que "que o envio insistente de mensagens não solicitadas, que persistiram mesmo após pedido de cessação da atividade, viola o direito de privacidade do autor, pois implica intromissão na vida alheia, perturbando a paz e intimidade da pessoa", essa orientação foi minoritária.

Também em favor dos agentes econômicos, a jurisprudência tem orientação no sentido de não identificar responsabilidade dos provedores por conteúdo por meio deles disponibilizado na rede. Não se reconhece, ainda, a obrigação desses fornecedores de serviço pela fiscalização e triagem do conteúdo divulgado, sendo suficiente, para o cumprimento de suas obrigações, a criação e meios que permitam a identificação dos usuários e a fiscalização *a posteriori* em caso de acionamento (Recursos Especiais nº 1193764 e 1186616). No Recurso Especial nº 1193764, aliás, no qual foi demandado Google Brasil Internet Ltda. por

ofensas proferidas por outro usuário na rede Orkut, retirou-se do agente econômico a obrigação de controle sobre as informações veiculadas, modo a ser afastada sua responsabilidade objetiva por mensagem divulgada por outro usuário.

Por outro lado, cominava-se a obrigação desse fornecedor de excluir texto ou imagem alegadamente ofensivo, tão logo acionado pelo usuário, sob pena de responsabilidade solidária com o ofensor direto. Esse entendimento foi o predominante quando ainda havia inércia do legislador em regular a matéria, o que foi suprido com o advento do Marco Civil da Internet vigente desde 2014, no qual essa obrigação de exclusão foi limitada às ordens judiciais (art. 19).

Com mais ênfase após o início da vigência do Marco Civil da Internet, a exclusão de responsabilidade inicial dos provedores de conteúdo manteve-se na jurisprudência.

A mesma linha de orientação foi mantida no Recurso Especial nº 1568935, no qual um usuário apresentou pretensão indenizatória por danos extrapatrimoniais em face do provedor Google Brasil Internet Ltda. em razão de manifestações de outros usuários em comunidade na rede social Orkut. Na ocasião, reafirmou-se que a disponibilização do sítio não atrai a responsabilidade civil pelo mérito das manifestações dos usuários se não há controle editorial por parte do provedor.

No Recurso Especial nº 1352053, reafirmou-se que a responsabilidade do provedor de conteúdo - solidária - somente surge com sua inércia em excluir as informações depois de notificado. O autor demandou empresa jornalística por veicular, em seu sítio na internet, matéria propositadamente destorcida quanto à realidade, o que incitou a inclusão de diversos comentários ofensivos à honra do requerente. Após o pedido ser julgado procedente em primeiro e segundo graus, houve reforma no Tribunal Superior. Neste, reafirmaram-se as premissas de que o provedor de conteúdo não possui obrigação de realizar prévio controle das manifestações de seus usuários em sua página e de que também não tem como risco inerente à sua atividade empresária a ocorrência de ofensas entre usuários.

Igualmente, na Reclamação nº 5072, afastou-se a responsabilidade do provedor por conteúdo de terceiro, considerando indevido demandá-lo quando o suposto ofendido sabe quem é o criador do conteúdo e autor das ofensas. A possibilidade de cominação de alguma obrigação do provedor limitou-se à exclusão do conteúdo armazenado em cache. Foi afastada, também, a obrigação do provedor de busca em desindexar o nome do então autor a resultados que conduziam a páginas com conteúdo ilícito e violador de sua honra e privacidade. A premissa foi de que provedores de pesquisa apenas identificam

páginas públicas na rede onde estão localizados certos dados e informações, de sorte que a eles não pode ser cominada obrigação de eliminação de seu sistema resultados de buscas por certos termos e nomes.

De todo modo, na ponderação de interesses entre o benefício à coletividade e aos agentes econômicos na disponibilização dos serviços pelos provedores de conteúdo e o resguardo da privacidade ou da autodeterminação informacional dos usuários, na orientação jurisprudencial, já predominava, na maioria das situações, o interesse do coletivo como regra. Na citada Reclamação nº 5072, por exemplo, reconheceu-se expressamente a impossibilidade de dificultar a propagação de conteúdo na rede, ainda que ilícito e ofensivo, pois isso implicaria restringir o direito da coletividade à informação, de modo que "sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa".

O mesmo tem ocorrido quando a Corte aprecia situações de conflito entre a privacidade de um usuário e a liberdade de informação na internet, ambiente em que a proliferação do conteúdo dá-se de maneira muito mais rápida e abrangente que nos meios de comunicação tradicionais.

Nessa senda, a pesquisa retornou o Agravo Regimental no Agravo nº 928658, em que foi questionada a suficiência dos parâmetros tradicionais de ponderação ente conflito de privacidade e liberdade de expressão quando tal discussão trava-se no ambiente da internet. Dando prevalência às liberdades de informar e ser informado, não se vislumbrou a configuração de ofensa moral pela divulgação de notícia jornalística na internet na qual se vinculava um agente público a empresa fornecedora de software, ante a falta de sensacionalismo em seu conteúdo e o interesse público na informação.

A situação, porém, não foi de recusa ao reconhecimento do direito à privacidade do autor, envolvido e mencionado na notícia, mas apenas de corroboração de que a regra constitui a liberdade de informar e de ser informado, com excepcionalidade da vedação do exercício de tal liberdade e tão somente quando configurado seu abuso.

No mesmo sentido, o Recurso Especial nº 1330028 também permitiu ao Tribunal aplicar a regra geral de ponderação para avaliar os limites do exercício do direito de informação. Na situação julgada, o autor aduzia ter sofrido danos morais em razão da veiculação em sítio eletrônico do réu de nota referente ao demandante nos seguintes termos: "Em nome do pai: Uma mansão em condomínio de luxo em São Bernardo (SP) é o novo foco

de atenção de jornalistas investigativos (foto). Seria de filho esperto de pai idem". Na revista eletrônica, ainda havia menção ao autor com a alcunha “Lulinha” e a nota transcrita o vinculava a notícia de que tinha adquirido uma mansão ilicitamente. Fato é que, utilizando o parâmetro tradicional de ponderar entre o interesse público na informação, a possibilidade de intenção de ofender a honra sob o pretexto de exercício do direito de informar e a privacidade do autor, a Corte deixou de reconhecer a configuração do dano moral por falta de sensacionalismo e de afronta à privacidade no conteúdo disponibilizado.

Também na mesma linha, reafirmou-se, no Recurso Especial nº 1388994, a impossibilidade de limitação prévia de conteúdo passível de divulgação na rede, sob pena de configuração de censura. Na causa de pedir, o autor relatou que o réu, organizador e mantenedor de um *blog*, já tinha ofendido sua honra e imagem diversas vezes, histórico que foi reconhecido no acórdão, ao mencionar o comportamento temerário do réu, “muitas vezes extrapolando os limites da informação para promover ofensas à moral do recorrido, algumas delas reconhecidas judicialmente e outras perpetradas já durante o trâmite desta ação”. A Corte, assim, asseverou que esse passado permitia supor com considerável medida de certeza que novas ilicitudes seriam praticadas, o que era especialmente relevante por se tratar de ações praticadas na internet, a qual permite a propagação da informação com velocidade e penetração antes não imaginados, “elevando sensivelmente o potencial lesivo de conteúdos ofensivos”.

O pedido, porém, não se referia a tais situações pretéritas, antes se destinava a evitar ofensas futuras no mesmo sítio eletrônico. Diante desse cenário, os julgadores ponderaram entre os direitos fundamentais à moral e à liberdade de expressão. Mesmo considerado o fato de que a internet torna necessários novos paradigmas para tais julgamentos, em razão das inovações na dinâmica do relacionamento humano que provoca, concluiu-se que a tutela inibitória destinada a vedar futura ofensa à honra seria de impossível cumprimento. Isso porque impediria o exercício da liberdade de pensamento lícita e caracterizaria censura prévia, em afronta ao direito da população em geral à informação, o qual tem valor superior aos direitos individuais do requerente.

Em outra situação retornada na pesquisa por “internet e honra”, foi analisada a existência de direito de agentes públicos à não divulgação na internet de procedimento investigatório em que são apontadas irregularidades na conduta dos investigados. A União dos Municípios da Bahia e o Município de Pindobaçú impetraram os Mandados de Segurança nº 9744 e 9745, respectivamente, contra ato do Ministro de Estado do Controle e da Transparência, com o objetivo de retirar da página da então Controladoria-

Geral a União relatórios ainda preliminares em que eram apontadas ilicitudes no uso de verba federal em Municípios baianos. A contenda não dizia respeito, propriamente, à publicidade de tais relatórios, a qual sempre existiu como decorrência da publicidade dos atos administrativos, mas à licitude de sua divulgação na rede mundial de computadores, que possui amplo alcance, antes de finalizadas as investigações. Para a impetrante, essa prática ofendia os direitos de seus representados ao devido processo legal, à ampla defesa e à honra, pois ainda não comprovados, por investigação, os fatos a eles imputados. Apesar de, no voto minoritário, ter sido acolhida a pretensão da impetrante por não identificar, nos preceitos legais, obrigação da Controladoria em dar publicidade a procedimento investigatório inacabado, prevaleceu a orientação de que, acima dos direitos da privacidade, da honra e da moral dos investigados, encontra-se o direito da coletividade ao controle da licitude dos atos administrativos.

Discussão semelhante foi travada na apreciação do recebimento da Ação Penal nº 388. Nesta, o então Senador da República Jorge Konder Bornhausen apresentou queixa em face de Luiz Francisco Fernandes de Souza, Procurador Regional da República, e Cláudio Julio Tognolli, Jornalista, acusando-os da prática dos delitos de calúnia, injúria e difamação por meio de matéria jornalística divulgada no sítio “Consultor Jurídico" (*www.conjur.com.br*) na qual se reportavam atos de investigação do querelado e outras pessoas por crime de lavagem de *US$ 5 bilhões no exterior*. Novamente, a insurgência do sujeito considerado ofendido, o querelante, não se voltavam contra a existência do procedimento investigativo, tampouco à natureza pública dessa investigação, mas à sua divulgação na rede mundial de computadores.

O tribunal vislumbrou a necessidade de ponderar entre o direito da coletividade à informação e os direitos fundamentais individuais à honra, à privacidade e à presunção de não culpabilidade, sendo que, embora a queixa tenha sido recebida inicialmente, foi extinta sem condenação dos acusados.

Embora alguns dos precedentes mencionados não digam respeito expressamente aos direitos à privacidade e à tutela de dados pessoais, pois tratam de forma mais abrangente das liberdades de expressão e informação, pode-se perceber que foram raras as situações em que os tribunais decidiram em favor da privacidade de quem se sentia ofendido nesse direito. Essa defesa foi notada apenas nos Recursos Especiais nº 320958, 1168547, 1334097, de um total de 19 julgados encontrados, valendo destacar que a orientação de ordem de exclusão de conteúdo considerado ofensor à honra que tinha sido firmada nos Recursos Especiais nº 1175675 e 1306157 foi posteriormente modificada. Na

Corte Constitucional, somente no Recurso Extraordinário nº 673707 e no Inquérito nº 2245 assegurou-se a defesa do direito individual (direito de acesso a dados pessoais e direito da privacidade)

Foi notável, ainda, a raridade de demandas com envolvimento da tutela específica sobre dados pessoais e da autodeterminação informacional, o que se mostra coerente com as constatações de que os usuários sequer têm conhecimento sobre as práticas que envolvem seus dados na rede, mesmo tendo sido utilizados termos de busca como "privacidade e internet", "internet e dados", "dados pessoais", "autodeterminação informacional" e "autodeterminação sobre dados".

A realidade sobre coleta e uso de dados pessoais apresentada no início do trabalho e a insuficiência do consentimento formalizado nos moldes atuais evidenciam que a escassez de julgados referentes à defesa da autodeterminação sobre dados pessoais não decorre da baixa frequência de ofensa a esse direito. Nesse cenário, a ausência de consciência sobre tal realidade decorrente da assimetria informacional impede até mesmo que os usuários busquem a tutela jurisdicional de forma individual.

Por conseguinte, considerando que o paradigma constitucional é do Estado Democrático de Direito e que inexiste norma brasileira especificamente destinada à tutela desse direito, a falta de tutela jurisdicional como exercício do poder contramajoritário do Poder Judiciário reforça a falta de participação efetiva e consciente dos usuários na governança da internet no que concerne à tutela de seus dados pessoais no Brasil.

De fato, a análise dos referidos julgados de ambas as Cortes Superiores, obtidos a partir da busca jurisprudencial em seus sítios eletrônicos, resultou na localização de situações em que, em favor dos direitos individuais à privacidade e à tutela dos dados pessoais, foi reconhecida a necessidade de limitações ao exercício de outros direitos.

Assim, na defesa dos direitos individuais na internet, com prevalência da tutela do privado, foi determinada retratação na rede após a prática de delitos contra a honra (Recurso Especial nº 320958), fixou-se a competência da Justiça brasileira para determinar exclusão de conteúdo hospedado em servidor estrangeiro (Recurso Especial nº 1168547) e reconheceu-se o direito ao esquecimento quanto a informações que seriam veiculadas em programa televisivo divulgado na internet (Recurso Especial nº 1334097). Tais situações foram de prevalência dos direitos dos usuários de manutenção de sua honra e privacidade na rede, em detrimento das dificuldades operacionais alegadas pelas fornecedoras dos serviços e do interesse coletivo na manutenção da disponibilidade dos conteúdos.

No âmbito do Supremo Tribunal Federal, afirmou-se a existência de uma autodeterminação sobre dados pessoais (Recurso Extraordinário nº 673707), mas, ainda assim, limitada ao direito de acesso aos dados do próprio titular, sem reconhecimento da autodeterminação como direito de controle sobre quem acessa tais informações. Ainda na direção da preponderância do direito individual à privacidade, a Corte Constitucional, em 2007 (Inquérito nº 2245), decidiu ser necessária autorização judicial para utilização de informações pessoais financeiras em investigações conduzidas pelo Ministério Público e por Comissões Parlamentares de Inquérito, o que, no entanto, não foi posteriormente seguido pelo Superior Tribunal de Justiça no Habeas Corpus nº 26769.

Também em prol dos interesses individuais de usuários, a jurisprudência era direcionada ao reconhecimento das obrigações dos provedores de excluir conteúdo reputado difamante mesmo sem indicação precisa da URL, bastando a determinação genérica de exclusão de conteúdo atrelado a determinado assunto ou pessoa, e de realizar varredura de conteúdo como decorrência de seu compromisso social, como ocorrido nos citados Recursos Especiais nº 1175675 e 1306157. Quanto a esse tema, porém, em um segundo momento, verificou-se o redirecionamento da jurisprudência pelo afastamento da obrigação de provedores de fiscalização do conteúdo divulgado, pela necessidade de indicação precisa da localização do conteúdo a ser excluído e pela ausência de responsabilidade por informação criada por terceiro e disponibilizada por meio do provedor (Recursos Especiais nº 1193764, 1186616, 1352053, 1568935 e Reclamação nº 5072), a não ser quanto inerte o fornecedor diante de ordem judicial de exclusão do conteúdo com indicação exata da localização na rede.

Em outras situações nas quais o interesse da coletividade na divulgação da informação prevaleceu sobre o direito individual de limitação dessa propagação, tutelaram-se as liberdades de manifestação e informação, ainda que em detrimento de certa medida da privacidade e da honra de usuário considerado individualmente. O Superior Tribunal de Justiça realizou a ponderação entre tais direitos em conflito de modo a somente identificar a ilicitude do exercício dos direitos à informação e à manifestação de pensamento em caso de abusos como sensacionalismo (Agravo Regimental no Agravo nº 928658, Recursos Especiais nº 1330028, 1388994 e 1300161, e Ação Penal nº 388). Nesses casos, seja por uma utilidade pública sobre os dados ou pelo interesse social em assegurar direitos típicos do Estado Democrático, o interesse coletivo na propagação das informações sobrepôs-se ao interesse pessoal de manutenção de uma esfera privada.

No âmbito do Supremo Tribunal Federal, a relevância atribuída aos direitos à livre manifestação, à liberdade de imprensa, à criação, ao pensamento e à informação foi ainda mais enfática, pois a lhes foi conferida natureza de sobredireitos, com precedência sobre os direitos individuais, até mesmo quando se trate de histórias de vida pessoais (biografias) e mesmo que sejam exercidos no âmbito da internet (Ação de Descumprimento de Preceito Fundamental nº 130, Ação Direta de Inconstitucionalidade nº 4815 e Reclamações nº 9428 e 19548).

O mesmo ocorreu na tutela do direito da população em ter conhecimento, por meio da internet, de procedimentos administrativos inacabados, ainda que isso implique o comprometimento da imagem e da privacidade dos investigados (Mandados de Segurança nº 9744 e 9745). Também no sentido da disponibilização de informações, o acesso de dados perante provedores, por parte de autoridade administrativa e independentemente de ordem judicial, foi reconhecido em prol do interesse público sobre a informação privada (Habeas Corpus nº 26769 e). Perante a Suprema Corte a relevância de informações pessoais e de sua divulgação quanto a protestos tirados e cancelados diariamente, visando-se a extrair a utilidade desses dados para a economia da sociedade em massa, na qual a privacidade precisa conviver com as criações de conjuntos de dados produzidas pelos fornecedores (Ação Direta de Inconstitucionalidade nº 1790). Assim, ao passo que o Superior Tribunal de Justiça tutelou o interesse estatal sobre a informação acerca dos procedimentos administrativos pendentes, o Tribunal Constitucional o fez para proteger os interesses dos agentes econômicos sobre os dados pessoais, indicando, nas duas situações, a função social dessas informações.

Embora na maioria dos casos retornados na pesquisa tenha havido prevalência do público e do coletivo com a consequente amenização dos direitos individuais, dentre os quais a privacidade, não se pode concluir que os direitos individuais não foram tutelados de nenhuma maneira, mas é possível observar a escassez de situações em que essa tutela ocorreu. Ao lado disso, pode-se notar que, a despeito de várias das situações fáticas analisadas pelos Tribunais terem a peculiaridade de ocorrência no âmbito da rede mundial de computadores, na qual reconhecidamente a propagação da informação ocorre de forma muito mais abrangente e rápida, as ponderações entre direitos e interesses foram realizadas com base nos mesmos parâmetros tradicionais empregados para julgamento de fatos vivenciadas no mundo físico.

Essa orientação de manter os modos tradicionais de ponderação entre os direitos e os interesses em conflito não foi feita sem o prévio reconhecimento, em alguns casos expressos, de que a internet pode potencializar danos de direitos individuais como

honra e privacidade (Recurso Especial nº 320958), demanda soluções técnicas que não são desafios no ambiente físico (Recurso Especial nº 1334097), relativiza distâncias geográficas e constitui ambiente desafiador por ser submetida a autorregulação, demandando uma nova concepção de privacidade (Recurso Especial nº 1168547). Além disso, embora o tratamento dado à privacidade dos usuários tenha se pautado nos modos de análise e reconhecimento ordinários sobre esse direito, houve oportunidade de o Superior Tribunal de Justiça indicar um novo delineamento desse direito como decorrência da expansão da internet:

> "Cabe à sociedade se adequar à nova realidade criada pela Internet, em que o grau de exposição da vida pública e privada de cada indivíduo é bem maior. Conforme navegamos, transparecemos – muitas vezes sem perceber – nossas rotinas, hábitos, opiniões, enfim, revelamos diversos dados do nosso cotidiano e ficamos sujeitos a danos de difícil reparação, tudo em troca das vantagens e facilidades proporcionadas pela *web*. A incursão na era digital nos obriga a essas concessões." – página 14, Resp 138994

Na mesma direção, no Supremo Tribunal Federal, o Ministro Lewandowski destacou que essas questões são muito mais complexas quando se trata de informações veiculadas na internet, que se espalham rápida e amplamente e muitas vezes envolvem ações praticadas onde a jurisdição brasileira não alcança, o que demanda soluções para abusos que não são cometidos no mundo físico (ADI 4815).

Apesar disso e embora tenha sido realizada pesquisa referente a privacidade, sociedade da informação e internet, praticamente não foram encontrados julgados por meio dos quais se tenha buscado tutelar a privacidade e a tutela de dados pessoais no ambiente específico da internet. De fato, a maior parte da busca alcançou situações de tutela de dados na sociedade da informação como um todo, mas o âmbito jurisdicional ainda não se mostrou como ambiente de proteção assegurada aos usuários no que se refere à tutela de seus dados pessoais no contexto específico da rede mundial de computadores.

5.2 Análise do poder explicativo de teorias regulatórias

Identificadas as teorias regulatórias relevantes propostas pela doutrina aplicáveis ao ambiente da internet e examinado o contexto fático dos discursos do estado, do

mercado e dos usuários sobre a temática da tutela dos dados pessoais na internet, busca-se analisar qual modelo tem maior poder explicativo para a compreensão da realidade brasileira.

Isso contribuirá para a identificação do papel dos usuários nesse contexto regulatório e, ao fim, poderá auxiliar no encontro de instrumentos para seu empoderamento nesse contexto. Por conseguinte, identificada a maior ou menor participação de tais indivíduos como elemento capaz de influenciar o contexto governado, será possível associar essa percepção com as conclusões sobre as ingerências do Estado e dos fornecedores sobre os direitos a privacidade e tutela de dados pessoais daqueles usuários.

A partir disso, a tarefa consistirá em analisar se o tratamento conferido à privacidade pelos Tribunais e pelos demais *stakeholders* atuantes na rede coaduna com a aceitação, por parte dos usuários, da reconfiguração desse seu direito individual ou, em verdade, caracteriza afronta à privacidade e à tutela de dados pessoais desses usuários.

Os estudos mencionados no tópico "Percepção dos usuários sobre as práticas com seus dados pessoais" permitem verificar que os usuários não têm conhecimento suficiente acerca das tecnologias que fazem parte do fluxo de informações na internet para tomarem suas decisões acerca das práticas com seus dados pessoais, isto é, para exercer sua autodeterminação sobre os dados. A ausência dessa competência coloca em questionamento a capacidade de tais indivíduos, no contexto de governança da internet, de efetivamente participarem como um dos atores com capacidade de moldar os comportamentos nesse ambiente.

Essa capacidade fica limitada às vias de representação na criação de normas formais sobre o contexto da internet, como parlamentares e algumas pessoas jurídicas representantes da sociedade civil, valendo notar que sequer há representante dos usuários consumidores no Comitê Gestor da Internet de acordo com a composição prevista no Decreto nº 4.829/2003.

Não se ignora que, na criação do Marco Civil da Internet, por exemplo, houve participação popular. Aliás, aponta-se como início concreto da criação dessa Lei a reação social contra o Projeto de Lei nº 84/99, chamado "Lei Azeredo", que criminalizava condutas já arraigadas entre os usuários, tais como transferir músicas de CD para um dispositivo. Assim, a mobilização social levou à conclusão de uma petição on-line com mais de 150.000 assinaturas[42].

42 Registro da mobilização disponível em < https://www.cartamaior.com.br/?/Editoria/Politica/Em-defesa-daliberdade-e-do-conhecimento-na-Internet-brasileira/4/14135>. Acesso em 11 de abril de 2018.

A partir disso, em 2009, concretizaram-se as iniciativas governamentais destinadas a regulamentar a internet no país com a consideração sobre as práticas consolidadas nesse ambiente e mais no intuito de reconhecer os direitos dos participantes da rede, menos do que criminalizar condutas que já faziam parte desse ambiente de relacionamento. O Ministério da Justiça criou, então, grupo de acadêmicos para criar um processo multissetorial para apresentação de uma proposta legislativa e o início dos trabalhos deu-se, justamente, com o desenvolvimento da plataforma on-line "Cultura Digital", destinada a consulta sobre um anteprojeto de lei (SOUZA; LEMOS, 2016), a qual, em dois períodos de consulta, recebeu cerca de 2000 propostas da população.

A apresentação de propostas, todavia, não significa, por si só, que tenham sido acolhidas as demandas sociais no anteprojeto e, ao fim, na Lei criada, tampouco que os direitos dos usuários, e não de outros setores da sociedade civil como provedores, foram abrangidos na proposta legislativa na mesma linha pretendida nas manifestações na plataforma.

Ao lado disso, a concretização da efetiva participação direta dos usuários também precisava ocorrer na regulamentação do MCI. Nessa regulamentação, o Ministério da Justiça proporcionou debates no sítio eletrônico Pensando o Direito para três linhas temáticas (neutralidade da rede, guarda de registros e privacidade da rede), em janeiro de 2015 e em fevereiro de 2016, nos quais foi possível participar como pessoa física ou representante de instituições ou empresas. Constatou-se, porém, que, apesar da iniciativa governamental, houve pouca interação entre os usuários e o próprio Ministério da Justiça sequer possuía um perfil para dialogar com os participantes, o que reduziu o potencial democrático do sítio eletrônico (COIRO-MORAES; FARIAS, 2017).

No portal e-Democracia, desenvolvido pela Câmara dos Deputados como instrumento para participação cidadã em processos de tomada de decisão, também foi disponibilizado espaço para interação dos cidadãos na elaboração do MCI. Apesar disso, constatou-se que a ferramenta foi muito pouco divulgada, além de que somente poderia ser utilizada pela parcela populacional que possui acesso aos recursos informacionais e à internet (FREITAS; LIMA, Fernanda F.; LIMA , Fernanda Q., 2015). Além disso, mesmo entre as poucas pessoas participantes, observou-se uma representatividade de apenas um grupo populacional com características socioeconômicas bem específicas - pessoas brancas, com alto grau de escolaridade e renda - de modo que, para a finalidade de fomento da participação democrática no diálogo do qual resultou o MCI, a iniciativa permitiu reforçar a percepção da baixa participação direta dos usuários na governança da rede.

Apesar de tais tentativas de avanço na participação popular, a capacidade de atuar como real *stakeholder* no contexto da governança da internet poderia decorrer não apenas da participação na criação de leis formais, mas também dos efeitos das escolhas realizadas nesse ambiente regulado.

Com efeito, não apenas o direito é capaz de exercer influência sobre os comportamentos na rede, o mercado e a estrutura de composição da internet, mas também as escolhas e a ação dos usuários nesse cenário devem ser capazes de fazer parte da malha regulatória e de governança para que as teorias corregulatórias que reconhecem o papel ativo dos usuários tenham poder explicativo no contexto analisado.

Essa participação poderia ocorrer, por exemplo, por meio do exercício de escolhas conscientes sobre a contratação de produtos e serviços disponibilizados por meio das aplicações em computadores ou *smartphones*, o que afetaria o mercado baseado na economia de dados e permitiria essa participação com percepção real do contexto em que é feita essa escolha de consumo. Assim, sem a assimetria informacional ainda existente quanto às práticas com seus dados pessoais, os indivíduos poderiam se posicionar conscientemente em face dos produtos e serviços contratados na rede.

Ocorre que, como apontado na leitura dos estudos descritos, tal participação não tem tido como um dos critérios o exercício do direito à autodeterminação sobre os dados pessoais, mas apenas a riqueza de funcionalidades das aplicações. Em outros termos, no contexto atual brasileiro, os produtos e serviços disponibilizados no ambiente da internet não têm como um dos medidores de sua qualidade no mercado o grau de obediência aos direitos basilares dos usuários relacionados à sua privacidade e à tutela dos dados.

Assim, ainda que o usuário possa ser reconhecido como um componente do *node* mercado, em verdade, encontra-se sem poder decisório efetivo no que tange à tutela de seus dados. Mesmo se identificado como um ator independente no contexto regulado - tal como se faz nos pensamento cypherpunk e do comunitarismo em rede-, a ausência de uma escolha consciente pelo usuário, baseada em seu conhecimento sobre as práticas com seus dados pessoais e fundada na possibilidade de escolha entre alternativas e expressada por meio de consentimento efetivo, faz com que a capacidade de influenciar esse contexto fique prejudicada e sua posição passe a ser de submissão em relação aos desenvolvedores das tecnologias, às empresas privadas e aos governos.

Especificamente no que tange à teoria cypherpunk, não há capacidade explicativa para a realidade brasileira no que tange à tutela de dados pessoais na internet.

De fato, os usuários, de modo geral, sequer conhecem o que se faz com seus dados na rede, o que lhes impossibilita modificar a realidade social e política desse contexto por meio do uso de tecnologias como criptografia. Ademais, mesmo para o uso dessa tecnologia, somente 17% dos brasileiros participantes da pesquisa promovida pelo Centro Internacional para Inovação em Governança (Centre for International Governance Innovation – CIGI) afirmou ser provável seu uso no ano seguinte.

Ao lado disso, a ingerência governamental sobre as práticas com dados pessoais já teve início, o que significa ter reconhecido que a lei constitui mecanismo regulatório que se pretende eficaz, diferentemente sustentado pelos defensores de tal teoria.

A teoria ciberlibertarianista, na mesma linha, não mais explica o contexto brasileiro nessa temática. Com efeito, a despeito da extraterritorialidade da internet, essa ausência de fronteiras físicas do ciberespaço não tem constituído impedimento para que o estado, como ator regulatório, participe da formatação de comportamentos na rede. Assim, já há iniciativas regulatórias formais pelo estado, como a criação do Decreto nº 8.771/16 e a cominação de condutas por meio de decisões judiciais.

Não se ignora que o manejo das tecnologias e a capacidade de modificar a arquitetura da rede constituem grandes forças regulatórias nesse ambiente. Também se sabe que essa atuação formal pelo estado encontra desafios, como a limitação de sua soberania ao território nacional, a desobediência de normas instituidoras de direitos individuais desacompanhada da fiscalização e punição, bem como a resistência de companhias privadas ao cumprimento de ordens estatais.

De fato, as dificuldades com cumprimento de ordens judiciais que levaram aos bloqueios do WhatsApp constituem exemplo desses desafios, encontrados também em outros países onde o estado pretende atuar ativamente no controle das práticas na internet. Na disputa entre *Equustek Solutions Inc. (Equustek) e Datalink Technologies Gateway LLC* (JOLT DIGEST, 2017) perante a Suprema Corte do Canadá, por exemplo, este tribunal ordenou que o buscador Google desindexasse informações da autora nas buscas realizadas não somente naquele país, mas em todo o mundo (COLUMBIA, 2017), o que gerou reações da empresa perante tribunais de outros países. Assim, em uma disputa de soberania por meio das forças de decisões judiciais nacionais, o Tribunal do Distrito Norte da Califórnia concedeu medida cautelar contra a decisão judicial canadense, aos argumentos de que aquela ordem judicial estrangeira violava normas locais dos Estados Unidos e privava o Google de benefícios reconhecidos no ordenamento jurídico norte-americano.

A despeito dessas dificuldades, a atuação estatal não mais é inerte em face dos problemas e conflitos existentes nas práticas com dados pessoais na rede, isto é, não mais se deixa a regulação desse ambiente para um contrato social espontâneo entre usuários e fornecedores das tecnologias. Em verdade, o reconhecimento da "falácia do ciberespaço" e da vulnerabilidade de alguns grupos na rede - como dos usuários em relação às práticas com seus dados pessoais – apenas reforçam a necessidade de iniciativas regulatórias formais.

A realidade brasileira, então, mais se aproxima do ciberpaternalismo, dado o reconhecimento da necessidade e da viabilidade de regulação do ciberespaço. Ademais, a instituição de um Marco Civil destinado especificamente a regular comportamentos na internet também indica a tentativa de adaptação regulatória para esse espaço de interação. Ainda, a existência de dispositivos legais por meio dos quais se busca realizar tal regulação a partir de ingerências na arquitetura da rede - como a instituição do objetivo de adesão a padrões tecnológicos abertos (art. 4º, IV), a obrigação do tratamento igualitário dos pacotes de dados por parte dos responsáveis por transmissão, comutação ou roteamento (art. 9º) – aproxima-se da identificação de Reidenberg sobre a arquitetura da rede como estrutura física que auxilia a moldar a arquitetura regulatória, com a criação de uma *Lex Informática*.

A despeito disso, a teoria de LESSIG, expoente do ciberpaternalismo, não ilustra o ambiente regulatório brasileiro sobre tutela de privacidade e dados pessoais na rede no que tange à situação do usuário como *pathetic dot*. Isso porque, a despeito de o mercado, a arquitetura da rede e o governo terem atuado, cada um em sua medida, no contexto regulatório, o usuário já não pode ser visto tão somente como alvo dessas forças regulatórias. Apesar de a posição desses usuários ainda ser de vulnerabilidade em relação àquelas outras fontes, é viável a atuação dos usuários como origem de motivações de comportamentos com seus dados. Nessa direção, por exemplo, houve reações de usuários do Facebook após o escândalo envolvendo a *Cambridge Analytica*, incluindo-se os usuários brasileiros[43], em especial por meio da campanha #DeleteFacebook. Dentre outras razões, essa reação conduziu os gestores da rede social a modificar padrões da plataforma, como disponibilizar atalho para controle sobre as informações compartilhadas e interromper a possibilidade de busca de usuários pelo número de telefone. Assim, os usuários puderam, de alguma maneira, contribuir para modificar comportamentos e práticas que envolvem seus dados pessoais.

43 Sobre a liderança do Ceará no movimento no Brasil: http://br18.com.br/ceara-lidera-interesse-pelo-movimento-deletefacebook/.

No comunitarismo em rede de Murray, por outro lado, a capacidade participativa do usuário é igualada à dos demais sistemas que compõem a malha regulatória, isto é, da arquitetura, do estado (leis), das normas sociais e do mercado.

Porém, na verdade, na temática da tutela de dados pessoais, pode-se notar que os usuários preocupam-se com sua proteção na rede, mas não escolhem entre aderir ou não a um novo serviço ou produto com base na capacidade de proteção ou violação desse seu direito, mas apenas com base na funcionalidade da aplicação. Pode-se observar, ainda, que essa postura não advém de sua concordância com todas as práticas governamentais e empresariais com seus dados, mas de uma resignação por falta de vislumbrar alternativas de comportamento. Portanto, a verificada resignação dos usuários quanto à exploração baseada em seus dados pessoais indica a impossibilidade de reconhecer o papel ativo desses atores.

Ainda que a informação sobre a realidade chegue ao consumidor, constatou-se nas pesquisas a ausência de modificação de seu comportamento real, isto é, continua a contratar e utilizar os produtos e serviços na internet independentemente do nível de ingerência sobre seus dados pessoais (HSING, 2016). Verificou-se que tal complacência decorre da maior valorização das funcionalidades das aplicações disponibilizadas na internet do que da possível ofensa futura aos seus dados ou à sua privacidade, violação esta que não é fácil e imediatamente visualizada e sentida pelo consumidor.

Além dessa distância em relação aos efeitos da disponibilização dos dados pessoais, a resignação dos usuários decorre também da inexistência de alternativa diversa da mera não contratação do serviço por meio da adesão à aplicação ou do acesso ao sítio eletrônico com aceitação dos “cookies”, por exemplo. Por conseguinte, resta ao usuário escolher apenas entre aderir ou não à aplicação, acessar ou não certo conteúdo etc., já que é insuficiente a variedade de opções de privacidade aos usuários (isto é, mais específicas opções de *opt-in* e *opt-out*), como uma alternativa de pagamento mensal para evitar a coleta dos dados (REIDENBERG, 2000).

Na concepção de Murray, o usuário não apenas participa ativamente do contexto regulatório, mas também suas escolhas são consideravelmente proeminentes no alcance de objetivos regulatórios, gerando-se uma situação de simbiose com os demais sistemas (direito, normas sociais e mercado). Ocorre que, a despeito de os usuários serem mais que meros *pathetic dots*, ainda não se retira a legitimidade de atuação dos agentes de mercado e do governo necessariamente de um diálogo com aqueles usuários. As práticas de mercado com dados pessoais, por exemplo, são simplesmente aceitas pelos consumidores, de

modo geral, ao menos enquanto não são criados instrumentos para incrementar a legitimação da atuação de governos e mercados por meio do citado diálogo.

No comunitarismo em rede, o papel que a comunidade de usuários pode assumir é considerado essencial para o processo regulatório da internet. Vale registrar que essa prescrição de um bom modelo sugerido não é o que atrai a dificuldade explicativa dessa teoria para o contexto brasileiro da tutela de dados pessoais na internet. Em verdade, a análise que se propôs realizar neste trabalho não é prescritiva, mas apenas descritiva dessa realidade e a postura do mercado e do governo que permite identificar seus discursos sobre esse tema, ao lado do posicionamento dos usuários identificado nas pesquisas apenas não permitem identificar a efetiva concretização do modelo regulatório proposto.

Uma das contraposições do comunitarismo em rede em face do ciberlibertarianismo reside, justamente, no afastamento da crença de que apenas constructos autorregulatórios têm forças no ambiente da rede mundial de computadores (MURRAY, 2011). Aproxima-se, assim, do ciberpaternalismo quanto ao reconhecimento da viabilidade de regulação nesse cenário. Por outro lado, o comunitarismo afasta-se da teoria ciberpaternalista por não considerar o usuário como alvo de um modelo regulatório a ele imposto por mercado, leis e normas sociais. Em verdade, o comunitarismo tem como premissa a formação do processo regulatório por um diálogo, e não apenas um conjunto de restrições externamente impostas ao usuário.

Assim, menciona-se como exemplo de concretização do comunitarismo a não aceitação dos sistemas de Gerenciamento de Direitos Autorais (DRM - *Digital Rights Management*), conjunto de tecnologias destinado a controlar a utilização, a alteração e a distribuição de obras protegidas por direitos autorais. Apesar de sua criação ter sido destinada a tutelar os direitos autorais nesse universo online, os consumidores principalmente de música os consideraram restrição prejudicial à liberdade de utilização de produtos adquiridos mediante contraprestação, o que levou ao insucesso do mecanismo como decorrência de reação dos próprios usuários (MURRAY, 2011).

Na situação do DRM, por exemplo, a existência do mecanismo era notável a todo consumidor que pretendesse disseminar, usar e modificar as obras, diante do que puderam reagir.

Por outro lado, a insurgência contra as práticas com dados pessoais consideradas abusivas não possui tal facilidade, na medida em que as formas de coleta, uso, tratamento e disseminação dos dados não são ostensivas e, como indicado na pesquisa acima

reportada referente ao projeto Quem Defende Seus Dados? (INTERNETLAB, 2016), não são sequer adequadamente informadas aos usuários.

Já a regulação responsiva não se pauta na identificação dos participantes do contexto regulatório. Partindo da premissa de que o estado é um dos atores centrais nessa tarefa, propõe-se a aplicação em primeiro lugar de medidas de persuasão, apelando-se para as dissuasórias apenas subsidiariamente e somente quando a resposta dos regulados aos instrumentos persuasivos não for suficiente para o alcance do resultado regulatório pretendido.

Para o bom funcionamento dessa teoria, esse regulador precisa deixar evidente ao agente econômico a possibilidade de uso de instrumentos de dissuasão, sem deixar de evidenciar que, com a colaboração dos regulados, as técnicas não punitivas serão empregadas preferencialmente.

No Brasil, no âmbito da tutela de dados, as medidas que já foram aplicadas pelo estado consistiram na emissão de decisões judiciais e na criação de normas legais principiológicas. Embora pudessem ser reconhecidas como instrumentos persuasórios de início do movimento regulatório, ainda não há uma autoridade responsável por avaliar a responsividade a essas medidas de persuasão.

Outrossim, se não há fiscalização do cumprimento das poucas normas existentes sobre o tema da tutela de dados pessoais na internet, tampouco há reação pelo estado regulador por meio da utilização de meios mais incisivos, de dissuasão. Aliás, sequer é possível reconhecer o início de um caminho regulatório desse tema no sentido da teoria responsiva, pois, embora já haja ingerência estatal em relação a alguns dos serviços e produtos disponibilizados na rede, a Lei Complementar nº 157/16 já prevê a incidência do imposto sobre serviços de qualquer natureza sobre a "disponibilização, sem cessão definitiva, de conteúdos de áudio, vídeo, imagem e texto por meio da internet" e o Superior Tribunal de Justiça já tem orientação da obrigação dos fornecedores de streaming de música de pagamento por direitos autorais ao Escritório Central de Arrecadação e Distribuição -, ainda inexiste autoridade destinada a fiscalizar o cumprimento das normas de proteção dos dados dos usuários na rede.

Ao lado disso, não é possível observar a gradação nessa atuação do estado regulador entre as medidas de persuasão e dissuasão. Em verdade, em muitas situações, ante a ausência de norma no ordenamento jurídico e de instrumentos de colaboração e persuasão, a atuação estatal dá-se por meio do Poder Judiciário, sem que os mecanismos acusatórios e punitivos sejam empregados de forma subsidiária aos cooperativos. Em alguns casos,

decisões judiciais são bastante incisivas e chegam ao ápice da ingerência regulatória proposta na regulação responsiva, isto é, a paralisação do serviço. É o que se deu, a título de exemplo, nos casos de suspensão do aplicativo WhatsApp.

A regulação responsiva ainda é pouco explicativa com relação ao princípio segundo o qual deve ser conferida aos atores do ambiente regulatório a possibilidade de participação na regulação, com identificação de suas motivações. Até o momento do contexto brasileiro, porém, na temática deste trabalho, a maioria dos usuários sequer conhece a realidade das práticas com seus dados, como observado nas pesquisas. Isso dificulta sua participação consciente nesse processo de responsividade, na medida em que a teoria preconiza um processo de regulação colaborativo em que todos os envolvidos possam dialogar.

No Brasil, a concretização do princípio da responsabilidade ativa mostra-se dificultada, seja pela ausência de normas com suficiente especialização na temática dos dados pessoais, seja pela inexistência de previsão de medidas de persuasão e de dissuasão quando há previsão genérica da tutela dos dados. De fato, a inexistência de regulamentação específica destinada à tutela dos dados pessoais indica que o estado brasileiro ainda não definiu e declarou como pretende direcionar os regulados e em que termos buscaria uma responsabilização ativa. Ao mesmo tempo, mesmo nas situações em que há previsão genérica da proteção desse direito, como no artigo 7º, VII a X, do Marco Civil da Internet, a carência de mecanismos dissuasórios no sistema regulatório e de um órgão com competência específica de fiscalizar o cumprimento das normas também inviabiliza a responsabilização passiva.

Aliás, a proposta de Ayres e Braithwaite (2006) foi questionada quanto à aplicabilidade em países em desenvolvimento, pois, nestes países, a força de grandes empresas sobre o próprio estado regulador arrefeceria a capacidade de orientação e coerção de comportamentos pelo governo. Além disso, tais países não teriam recursos materiais e humanos em órgãos reguladores suficientes para a aplicação adequada da teoria.

No contexto brasileiro – e especificamente na temática da tutela de dados pessoais de usuários da internet – sequer há órgão ou agência com competência específica de instituir normas persuasórias ou dissuasórias, tampouco de auditar e fiscalizar o cumprimento das normas genéricas já existentes no ordenamento jurídico. Essa carência inviabiliza a avaliação do quanto os demais agentes são responsivos e de que mecanismos de persuasão ou dissuasão são pertinentes a partir da autorregulação e das respostas dos regulados.

Para se contrapor à alegação de que, nos países em desenvolvimento, falta capacidade regulatória dos agentes estatais, BRAITHWAITE defende a participação de terceiros, agentes não estatais ou empresas, na rede regulatória. Em outros termos, o autor reconhece organizações da sociedade civil como atores participantes do ambiente regulatório (BRAITHWAITE, 2006). Essa efetiva participação da sociedade civil, porém, depende do fim da assimetria informacional quanto às práticas de coleta, uso e disseminação dos dados pessoais, na medida em que, ao menos por enquanto, a própria falta de ciência da sociedade (MENDES, 2015) quanto a essas práticas impede sua reação e efetiva participação no contexto regulatório.

Tal assimetria aliás, caracteriza-se não apenas entre empresas e usuários (ou entidades coletivas criadas para sua defesa), mas também entre tais agentes econômicos privados e o Estado. A título de exemplo, nota-se que, em processos judiciais, as empresas recusam a viabilidade de tomada de medidas necessárias à tutela de direitos dos usuários, como a possibilidade de filtragem de conteúdo pelo Youtube, e reitera tal negativa ao Poder Judiciário, mesmo em face de evidência pericial da possibilidade, a exemplo do constatado no Recurso Especial nº 1306157. Similarmente, quando ordenado por autoridades judiciais no exercício da persecução criminal a prestar informações sobre trocas de informações entre usuários, a companhia Facebook recusa-se a cumprir ordens de autoridades brasileiras ao argumento de inviabilidade técnica. Não esclarece, porém, como tal inviabilidade se caracteriza ou se decorre simplesmente de questões negociais da empresa, o que situa a autoridade estatal em posição de vulnerabilidade em face do próprio agente econômico privado.

Não se ignora que algumas entidades civis organizadas já têm reagido, sobretudo a abusos prejudiciais à tutela de dados pessoais de consumidores na rede, seja por meio de processos judiciais (como as Ações Civis Coletivas nº 2015.01.1.039791-9 e 2015.01.1.040448-5 ajuizadas por associação civil perante o Tribunal de Justiça do Distrito Federal e dos Territórios) ou de estudos e tentativas de informação aos usuários (como os desenvolvidos pelo Instituto InternetLab[44]). A despeito do crescimento da participação dessas entidades de pesquisa e associações, ainda é pouco expressiva sua ingerência do ponto de

44 Trata-se de um centro de pesquisa interdisciplinar para promoção de debate acadêmico e produção de conhecimento conjugando direito e tecnologia, em especial nos temas que envolvem internet, do qual participam acadêmicos, representantes do setor público, do setor privado e da sociedade civil. Além de manter página na rede Facebook com informações sobre as temáticas de privacidade, liberdade de expressão, dentre outros temas afetos às interações na internet, o grupo realiza pesquisas e as disponibiliza na rede (http://www.internetlab.org.br/pt/), disseminando o conhecimento e o debate sobre essas novas temáticas. É o responsável, por exemplo, pelo estudo Quem Defende Seus Dados? e pelo Congresso Direitos Fundamentais e Processo Penal na Era Digital.

vista de efetivamente modificar o comportamento dos demais atores do ambiente regulatório e de levar ao usuário conhecimento sobre as práticas com seus dados.

Soma-se a isso o fato de que tal teoria, de modo geral, chega a sofrer a crítica de que poucos estados possuem poder regulatório suficiente para sustentar a manipulação dos regulados de forma segura em direção aos seus objetivos regulatórios estatais. Aponta-se, por exemplo, não ser incomum que poderes regulatórios sejam identificados com atores não estatais como decorrência de capacidades oriundas de maior informação, organização e riqueza em determinada área de atuação.

Nesse caso, grandes empresas dominam a interpretação e a aplicação dos mecanismos regulatórios existentes, ainda que, nos moldes da lei formal, lhes falte legitimidade para essa dominação regulatória (JORDANA; LEVI-FAUR, 2004). Assim, percebe-se que, para corroborar a viabilidade da regulação responsiva nos países em desenvolvimento, Braithwaite sugere a atuação em rede de agentes estatais e não estatais, em cooperação, mas a realidade brasileira quanto ao tema deste estudo tem sido de prevalência da capacidade regulatória das grandes empresas que coletam, usam e disseminam os dados pessoais dos usuários.

Nessa linha, dentre as teorias estudadas neste trabalho, aquela que mais se aproxima do contexto regulatório brasileiro na temática de tutela dos dados pessoais na internet consiste na regulação descentrada proposta por Black.

5.3 Poder explicativo da teoria da regulação descentrada

A existência de um espaço não vivenciado até a criação da internet, isto é, de um ciberespaço que, além de inovador quanto ao seu formato – virtual -, não foi inicialmente criado para viabilizar interações sociais e econômicas, mas acadêmicas e militares parece ter acarretado, por si só, a descentralização das fontes de sua regulação. Ainda que a criação de uma rede mundial de computadores tenha sido fomentada pelo Departamento de Comércio dos Estados Unidos, o desenvolvimento da tecnologia foi feito na academia e, posteriormente, com a identificação de seu potencial para o desenvolvimento de atividades econômicas, foi incrementado e expandido quanto à sua estrutura física por agentes de mercado, visando ao lucro.

Trata-se de ambiente extremamente influenciado pela tecnologia, a qual, se modificada, pode alterar as formas de interação, o potencial para desenvolvimento de atividades econômicas, o exercício de direitos e até o modo de atuação política. Em face disso, naturalmente a força regulatória inicial desse contexto adveio dos desenvolvedores dessa tecnologia de hardwares e softwares. Significa que a regulação já se iniciou de forma descentrada, nos termos da teoria de Black, isto é, partiu de fora dos fóruns tradicionais de regulação.

Ainda após algumas décadas de desenvolvimento e expansão da rede, o discurso dos agentes de mercado prevalece. A despeito da existência de normas legais para tutela dos dados pessoais – que impõem limites às práticas com esses dados e condições de sua legalidade, como o consentimento expresso e informado (artigos 7º, VI e 10 a 17 do Marco Civil da Internet; Decreto nº 8.771/2016), as atividades componentes da microeconomia de dados e de modulação de comportamento ainda são realizadas sob a luz do discurso da extinção da privacidade (neste discurso, fala-se em privacidade com abrangência do direito à tutela sobre dados pessoais) como consequência de escolhas dos próprios usuários. Essa fala, associada à ausência de fiscalização do cumprimento das normas de tutela de dados conduz à prevalência da força regulatória dos agentes econômicos atuantes na parte de desenvolvimento das tecnologias que compõem a internet.

Assim, os desenvolvedores de tecnologias e, de modo especial, aqueles que dominam as camadas de base da rede, ao formatarem toda a estrutura operacional e dominarem as capacidades técnicas para isso e se verem praticamente livres de ingerência regulatória dos usuários e formal do estado, fazem com que a regulação desse ambiente seja feita principalmente por seus interesses de mercado. Essa capacidade de ingerência regulatória ocorre, por exemplo, nos interesses comerciais que envolvem os contratos de ponto de troca de tráfego e outras formas de interação entre sistemas autônomos.

Neste aspecto, vale mencionar que mesmo o Estado, por meio de seus agentes regulatórios, pode vir a atuar de forma mais sintonizada com os interesses do mercado em detrimento dos usuários. Assim, por exemplo, atribuiu-se à Anatel o papel de estabelecer parâmetros para gerenciamento que assegure a neutralidade da rede, nos moldes do artigo 6º do Decreto nº 8.771/2016[45].

[45] Decreto nº 8.771/2016. Art. 6º. Para a adequada prestação de serviços e aplicações na internet, é permitido o gerenciamento de redes com o objetivo de preservar sua estabilidade, segurança e funcionalidade, utilizando-se apenas de medidas técnicas compatíveis com os padrões internacionais, desenvolvidos para o bom funcionamento da internet, e observados os parâmetros regulatórios expedidos pela Anatel e consideradas as diretrizes estabelecidas pelo CGIbr.

Logo, embora ainda seja controvertida a inclusão do serviço de conexão à internet como objeto de regulação por aquela Agência, na medida em que a Lei Geral de Telecomunicações exclui o serviço de valor adicionado da concepção de serviço de telecomunicações (art. 61), fato é que à ANATEL já foi atribuída a competência de fixar padrões regulatórios necessários à "adequada prestação de serviços e aplicações na internet" (art. 6º, Decreto nº 8.771/2016).

Na prática vivenciada atualmente, atribui-se à ANATEL postura de pouca proteção dos direitos dos consumidores e complacência com os interesses das grandes operadoras de telecomunicações também fornecedoras de serviço de conexão à internet (LEFEVRE, 2017b). Esse posicionamento é especialmente relevante para a tutela dos direitos dos usuários da rede, na medida em que a internet funciona sobre as redes de telecomunicações e depende da interação entre empresas fornecedoras da infraestrutura dessas redes, como indústrias de equipamentos, provedores de acesso e de conteúdo, centros de pesquisa, estado e usuários. Nesse caso, assumir um viés protecionista do mercado implica distribuir desigualmente capacidade de ingerência regulatória.

Essa capacidade de desenvolvimento da arquitetura legal torna inviável a regulação no formato de comando e controle, o qual pressupõe a apresentação, pelo estado, de comandos prévios à atuação dos regulados. No ciberespaço, de fato, a regulação estatal deve ser feita sobre a autorregulação já iniciada espontaneamente e que a arquitetura da rede proporciona e tende a fomentar, tal como preconizado na regulação descentrada.

Por conseguinte, uma vez que o contexto a ser regulado estava formado quando o estado passou a observar a necessidade de ingerência no ciberespaço, incluindo-se as necessidades para efetiva tutela dos direitos individuais relacionados aos dados pessoais, a regulação por meio de mecanismos diretos de comando e controle não foi reconhecida como a mais eficiente. Em face disso, no tema da tutela dos dados pessoais, optou-se pela criação de lei com caráter principiológico, o MCI. Ainda que esta Lei contenha previsão de comportamentos específicos em relação a esta temática, tais como a vedação de guarda de registros de acesso a aplicações na provisão de conexões (art. 14), não previu, desde o início, medidas punitivas para aplicação imediata contra tais provedores.

Além disso, no Comitê Gestor de Internet, do qual emanam orientações para atuação na rede, há considerável espaço para participação de representantes do setor empresarial (8 de 21 membros), de modo que esta participação incentiva o estabelecimento de diretrizes de forma dialogada e negociada. Dentro desse Comitê, então, em relação aos atores empresariais e à comunidade científica, o governo, por meio do Decreto nº 4.829/2003,

estabeleceu um fórum de tomada de decisões sobre as diretrizes das práticas na internet no Brasil na qual participam outros atores além dos representantes governamentais.

A fragmentação do conhecimento e do poder decorrente do controle também se aplica no ambiente estudado, na medida em que a atuação de cada ator desse cenário de regulação pressupõe que os demais participantes têm informações e capacidades distintas para obter a solução de alguns problemas ou orientar algumas práticas em algum sentido desejado.

Assim, sobretudo a arquitetura da rede e seus desenvolvedores - os quais são, atualmente, agentes de mercado - possuem conhecimento e instrumentos para moldar os comportamentos na rede, isto é, para, por meio de ações sustentadas e focalizadas, buscar certos resultados pretendidos. Essa capacidade está, por exemplo, na possibilidade de acesso aos dados pessoais, de seu tratamento e disseminação, resultando em modulação de comportamentos na rede e nas práticas de marketing especializado. Encontra-se, ainda, na própria capacidade de ampliar ou reduzir acesso à rede e a conteúdos, por meio de acordos comerciais entre operadores de sistemas autônomos. Pode ser identificada, também, na viabilidade de conferir tratamento diverso aos pacotes de informações trocados na rede, daí a necessidade de posicionar a neutralidade de rede como regra.

O estado também conta com essa possibilidade de emissão de comandos, como regulador tradicional dotado de instrumentos, reconhecidos como legítimos, para impor restrições e penalidades e de criar incentivos para ações em um ou outro sentido. Assim, normas legais são criadas pelo Legislativo, tais quais as do Marco Civil da Internet, regulamentadas e implementadas por atos do Poder Executivo e tem seu cumprimento forçado pelo Poder Judiciário, como quando se exige a apresentação de registros de conexão e de acesso a aplicações com base no artigo 10 do MCI.

Na mesma linha, quanto aos usuários, em especial no tema de estudo, pressupõe-se que possuem capacidades para manifestar sua vontade acerca de seu direito à tutela sobre dados pessoais. Não fosse esse pressuposto, o consentimento não seria legalmente previsto como requisito para a legalidade das práticas com esses dados, tampouco os provedores incluiriam em seus procedimentos de adesão aos serviços e produtos a necessidade de aceitação de seus termos e condições.

Neste ponto, vale registrar que, a despeito de ter sido notada a insuficiência atual dos modelos de concessão de consentimento para que haja a efetiva expressão da vontade dos usuários, fato é que se pressupõe essa capacidade de cada um deles em aderir, ou não, às condições dos provedores.

Além disso, embora por meio de representatividade e sem a efetividade que se idealiza, os usuários contam com a possibilidade de influenciar as normas de comando sobre as práticas com seus dados quando contam com representantes nos Poderes Executivo e Legislativo.

É preciso ponderar, no entanto, que, ao preconizar uma concepção de atividade regulatória como conduta intencional, sustentada e focalizada de modificar os comportamentos com base em propósitos definidos, a teoria da regulação descentrada reduz sua identificação com o cenário brasileiro no que tange ao papel do usuário na temática de tutela de dados pessoais.

Neste aspecto, até o momento, tem-se compreendido que a expressão do discurso do usuário ocorre por meio da concessão de consentimento no momento da adesão a produtos e serviços, uma anuência que, no entanto, carece da efetiva ciência quanto àquilo a que se adere na medida em que esses indivíduos não têm plena consciência sobre as práticas com seus dados, como observado nas pesquisas analisadas no item 4.3 Além disso, mesmo quando comunicados do real conteúdo dessas práticas, os fornecedores dos dados pessoais mostraram-se não concordantes com a realidade sobre essas práticas, mas apenas conformados. De todo modo, a despeito dessa resignação – em vez de aceitação -, também se constatou, e especial na pesquisa de Hsing na análise do comportamento real das pessoas, que a preferência declarada pelos participantes daquele estudo está na valoração das funcionalidades das aplicações, em detrimento de um maior valor à tutela de seus dados e de sua privacidade.

De toda forma, a incipiência da percepção dos usuários sobre sua capacidade de participação como coprodutor da regulação desse ambiente, especificamente na temática da tutela de seus dados pessoais, não afasta o fato de que essa sua capacidade é real e atrai o poder explicativo da teoria da regulação descentrada.

Com efeito, ainda que a quantidade de pessoas conectadas na rede venha crescendo, já foi possível perceber que esse acréscimo da população conectada é acompanhado do aumento de sua preocupação com questões de privacidade e segurança na rede. Essa preocupação, porém, ainda se dá em uma posição de vulnerabilidade dos usuários em relação às demais forças regulatórias, como o estado, os agentes econômicos e a arquitetura da rede.

Nota-se, por exemplo, que, diante da possibilidade de reconhecer tal situação de subjugação, o estado atribuiu aos próprios indivíduos – não ao modelo de mercado da microeconomia de dados e da modulação de comportamentos – a

responsabilidade pelo atual estado de usos e abusos com os dados pessoais quando, no julgamento do Recurso Especial nº 1334097, o Ministro Relator atribuiu aos usuários um "sentimento difuso de inconformismo" de perda de intimidade e privacidade, além de uma permissividade em ser devassado e espionado. As pesquisas empíricas, porém, contradizem essa postura e indicam um crescente estado de preocupação por parte dos usuários, o que se revelou, por exemplo, na campanha #DeleteFacebook em março de 2018, após o escândalo da rede social com envolvimento de disseminação de dados pessoais sem anuência dos titulares.

O discurso estatal também coadunou com o discurso do mercado de redução da privacidade e da autodeterminação sobre dados na sociedade informacional quando modificou-se a jurisprudência do Supremo Tribunal Federal para admitir o acesso direto, por autoridades fiscais, a dados de instituições financeiras independentemente de decisão judicial, ou mesmo quando, dentre os 11 julgados identificados a partir dos termos de busca propostos, apenas 1 consagrou a prevalência do direito individual à privacidade.

A mesma Corte reforçou esses discursos do estado e dos agentes de mercado quanto à utilidade social, econômica e política da divulgação das informações pessoais em detrimento da autodeterminação sobre os dados, quando se reconheceu que, a despeito da existência dos direitos individuais à privacidade e aos dados pessoais, a função social e a utilidade pública sobre as informações pessoais têm conduzido à prevalência da sua publicidade em detrimento da autodeterminação sobre esses dados. Isso ocorreu, por exemplo, com dados que compõem biografias, informações sobre remunerações de agentes públicos ou dados fiscais.

Esse tipo de discurso – emanado não apenas dos agentes econômicos, mas, como se vê, também pelo estado – reforça um estado de coisas não apenas de incremento do valor dos dados pessoais, mas também de abusos contra o direito individual à sua tutela, notadamente ante a carência de uso de instrumentos estatais para fiscalização e punição de práticas que contrariam o discurso estampado nas normas legais destinadas a essa tutela.

Apesar disso tudo, o fato de, atualmente, os usuários não contarem com instrumento mais eficiente que o consentimento para interferirem como verdadeiros agentes participantes da regulação descentrada não lhes retira essa capacidade de participação. Esse quadro de deficiência na participação dos usuários como autorreguladores/reguladores permanecerá enquanto existir a assimetria informacional quanto às práticas que envolvem seus dados.

6 CONCLUSÃO

Compreender melhor como dados pessoais de usuários disponibilizados e coletados na internet são utilizados em práticas empresariais e governamentais tem se tornado uma preocupação cada vez mais disseminada não apenas no ambiente acadêmico, mas também empresarial, profissional e na vivência de cada indivíduo nessa sociedade em rede. As recorrentes menções, na mídia, sobre práticas com dados pessoais que não eram de conhecimento dos titulares dessas informações e sobre vazamentos e ilegalidades cometidas por companhias privadas e governos têm despertado o interesse pela temática no dia-a-dia de cada indivíduo, sobretudo da grande maioria que já não consegue se esquivar de ter uma vida, exercer direitos e construir sua cidadania no ciberespaço.

Inicialmente, a percepção da utilidade e do crescente uso dos dados pessoais trouxe preocupações com a privacidade. Em razão disso, buscou-se, neste trabalho, abordar como a concepção desse direito subjetivo moldou-se no tempo e alcançou um novo formato a partir da compreensão de público-privado na pós-modernidade. Não apenas por isso a privacidade precisou ser abordada neste estudo, mas também para permitir perceber que, no ciberespaço atual, ela se diferencia, como direito, de um direito subjetivo autônomo à autotutela dos dados pessoais, bem como de um direito à extimidade. Além disso, observou-se que tecnologias de informação e comunicação constituem um relevante fator na redefinição atual da fronteira entre o público e o privado.

Assim, a partir desse desenvolvimento da concepção de privacidade, foi possível diferenciá-la dos direitos autônomos à tutela dos dados pessoais e à extimidade, o que constituiu uma das premissas do presente estudo, voltado mais especificamente para a realidade brasileira da tutela dos dados pessoais.

Notou-se que uma concepção de racionalidade passou a ser demandada para legitimar normas jurídicas, ainda que tal racionalidade seja reconhecidamente limitada e sem respaldo em verdades absolutas. Nesse contexto, adotou-se o paradigma do Estado Democrático de Direito, em uma pós-modernidade pautada em uma racionalidade que se vê limitada e inacabada. Em razão disso, a atuação do Poder Judiciário passou a ser essencial para o reconhecimento e a concretização de direitos, pois a criação das normas formais passou a ser orientada por aquele reconhecimento de limitação e, nessa linha, princípios adquiriram força normativa ao lado das regras e deixou-se de identificar apenas o ordenamento jurídico formalizado como fonte de direitos.

Como, no contexto normativo brasileiro atual, vivencia-se a deficiência da legislação destinada à tutela específica dos dados pessoais, verificou-se, a partir de pesquisa jurisprudencial no Supremo Tribunal Federal e no Superior Tribunal de Justiça, que essas Cortes não têm sido capazes de compensar a deficiência dos usuários no exercício de sua autonomia na criação de normas destinadas à tutela de seus dados pessoais na sociedade da informação estudada.

Paralelamente a isso, analisando os valores que orientam a formação dos discursos das empresas, dos estados e dos usuários sobre essa temática, observou-se que aqueles (empresas e estados) buscam legitimar suas práticas com dados pessoais na utilidade coletiva, social, política e econômica dessas informações, sobrepondo-as, em relevância e valor, ao direito de autodeterminação sobre os dados.

Uma vez que o atual modelo de relação entre público e privado dá-se sob a luz do paradigma do neoconstitucionalismo, examinou-se como esses discursos têm sido acolhidos, ou não, na jurisprudência do Superior Tribunal de Justiça e do Supremo Tribunal Federal. Nisso, notou-se que, no exercício de seu poder contramajoritário, os direitos individuais à privacidade na rede e à autodeterminação sobre os dados estão sendo, de alguma maneira, reconhecidos, mas ainda em medida insuficiente perante as demandas surgidas com as transformações tecnológicas nessa sociedade em rede. Mesmo nesse contexto de inovações, as demandas relacionadas especificamente à proteção dos dados pessoais ou ainda não chegaram a essas Cortes ou nelas são tratadas com base nos parâmetros tradicionais de cotejo entre interesse público e interesse privado aplicados ao ambiente físico, fora do ciberespaço.

Esse exame jurisprudencial permitiu constatar que ainda há notável deficiência no exercício do poder contramajoritário daquelas Cortes no que concerne à tutela de dados pessoais no Brasil, o que se deve não apenas ao fato de que o exame sobre consequências de práticas de coleta, armazenamento, tratamento e disseminação de dados pessoais no ambiente da internet ainda é analisado sob as mesmas premissas com as quais se julgam as causas de afronta ao direito à privacidade no mundo físico. Deve-se, também, ao fato de que os efeitos nocivos das práticas com dados pessoais sobre direitos individuais não são ostensivos e rapidamente percebidos pelos usuários, o que, ao menos por enquanto, tem conduzido poucas demandas até aqueles Tribunais acerca dessa temática.

Após investigada a capacidade de cada um desses múltiplos *stakeholders* em legitimar seu discurso, destaca-se a percepção de que, como notado em pesquisas realizadas com os usuários da internet, há uma crescente preocupação com a tutela sobre seus dados pessoais. Por outro lado, por não vislumbrar alternativas à adesão incontestada das

aplicações que levam à coleta, ao armazenamento, ao processamento e à disseminação de seus dados, esses mesmos usuários preocupados continuam a, progressivamente, disponibilizar tais informações na rede.

E, assim, vai se reforçando o discurso explícito do mercado no sentido de que a privacidade, no mundo atual, não pode ser exigida como antes. O fundamento desse reforço discursivo consiste em que esse cenário seria consequência da escolha dos usuários e não simplesmente de estratégias comerciais, pois os novos produtos e serviços baseados nos dados pessoais somente seriam acolhidos no mercado por opção de adesão formalizada por meio de um consentimento.

Essa insuficiente força da perspectiva do usuário reforçou-se nas pesquisas empíricas, em que se constatou que a crescente preocupação desses indivíduos com a indiscriminada coleta, tratamento e disseminação de seus dados pessoais não tem impedido a crescente adesão a novas aplicações na rede. Por outro lado, sua incapacidade de fazer valer seu discurso – que demanda uma tutela desse direito, mas é distorcido sob o pretexto do consentimento – decorre não apenas da falta de conhecimento suficiente acerca das tecnologias que fazem parte do fluxo de informações na internet, mas também da ausência de alternativas a não ser a adesão aos modelos propostos pelas empresas, bem como da inexistência de uma autoridade com competência para fiscalizar as práticas com os dados e da falta de transparência sobre essas práticas.

Por outro lado, há válidas tentativas governamentais de buscar transparência na atuação dos agentes econômicos e dos desenvolvedores de tecnologia, ao mesmo tempo em que agentes econômicos demonstram sua capacidade de fazer prevalecer seus interesses, independentemente do conteúdo das normas estatais, na medida em que têm efetivamente participado da governança da internet por meio do controle da arquitetura da rede.

Analisando esse cenário sob a luz das teorias regulatórias abordadas - ciente de que são apenas algumas das teorias que se pode adotar como referencial teórico -, nota-se como aquelas que envolvem a autorregulação não explicam a realidade brasileira, ao menos sob a perspectiva dos usuários.

Nem mesmo o comunitarismo em rede, que tem como um de seus pontos fortes o reconhecimento do usuário como efetivo ator com poder na malha de pontos regulatórios, explica essa realidade brasileira, valendo reforçar que esse exame está sendo realizado especificamente na temática da tutela de dados pessoais na rede por usuários do Brasil, e não sobre todo o contexto de regulação da internet. De fato, a vulnerabilidade dos usuários em face do domínio da técnica da arquitetura da rede pelas corporações e estados e a

assimetria informacional sobre essa realidade implicam, atualmente, a pouca consciência sobre essas práticas com seus dados pessoais, o que reduz sua capacidade de agir em igualdade de forças com o mercado, as leis, a arquitetura da rede e as normas sociais, colocando em cheque a concretização do comunitarismo em rede, da teoria cyberphunk e a legitimidade do ciberlibertarianismo. Outrossim, o ciberpaternalismo de Lessig também não se mostrou explicativo porque os usuários, embora ainda hipossuficientes em face das outras fontes normativas, tem passado a se apresentar como uma origem de regulabilidade, a qual não provem exclusivamente do código.

De fato, apesar dessa disparidade de forças, há uma incipiente percepção dos indivíduos sobre sua capacidade de participação como coprodutor da regulação desse ambiente, o que tem começado com o aumento de sua preocupação com questões de privacidade e segurança na rede. Isso, ao lado da crescente preocupação estatal na criação de normas específicas e de uma autoridade reguladora própria para essa temática, permite identificar a teoria da regulação descentrada como a que, dentre as estudadas, explica, no momento, esse contexto.

Nada obstante a teoria responsiva possa ser identificada como uma das formas de regulação descentrada, o atual cenário brasileiro ainda sequer permite aferir a responsividade dos múltiplos atores envolvidos, já que a atuação estatal nessa temática ainda é muito tímida.

Reconhecer o poder explicativo dessas formulações teóricas no ambiente estudado foi uma maneira de buscar contribuir com reflexões sobre o contexto regulatório brasileiro na temática da tutela dos dados pessoais, notadamente na internet. Com isso, pretende-se subsidiar novas análises destinadas principalmente à construção do arsenal normativo formal brasileiro nesse tema, o qual ainda é incipiente, mas que tem sido uma preocupação do legislador, como se pode observar com a recente aprovação, na Câmara dos Deputados, do Projeto de Lei nº 4060/2012.

Esse diagnóstico voltado à perspectiva do usuário e de sua capacidade de participação no ambiente regulatório, juntamente com a análise da situação regulatória de outros países e dos impactos de outros conjuntos normativos - como o agora vigente Regulamento Geral de Proteção de Dados da União Europeia -, poderá ajudar, também na conscientização sobre a premente criação, no contexto normativo brasileiro, de mecanismos de transparência e redução da assimetria informacional sobre as práticas com dados pessoais.

Fica, ainda, o ensinamento de que formas como o ciberphunk e o ciberlibertarianismo não apenas deixam de explicar o contexto estudado, mas também não se

mostram suficientes para a tutela dos direitos individuais dos usuários na rede, dentre os quais a autodeterminação sobre os dados, uma vez que a legitimidade das normas regulatórias depende da observância de um procedimento dialogado em que se viabilize a participação dos atingidos. Assim, a assimetria informacional e a atual prevalência da governança pela arquitetura da rede impedem, neste momento, reconhecer a legitimidade de uma opção de ausência estatal neste estado que se apresenta como democrático de direito, mas que, no tema de estudo, está pautado apenas em uma lógica de consentimento que se mostra insuficiente.

De todo modo, uma vez que o modelo, até o momento, é pautado no consentimento, conhecer melhor o que os usuários brasileiros da internet realmente sabem sobre as práticas que envolvem seus dados ainda constitui possível pesquisa a ser explorada. Essa possibilidade de continuidade de estudo mostra-se relevante não apenas porque os arranjos normativos atuais ainda estão fundados na manifestação de vontade dos usuários – ao menos até que se delineie um paradigma mais eficiente em termos protetivos -, mas também porque, embora já se reconheça a inviabilidade de adoção de ideais libertários e tecnodeterministas quanto à regulação do ciberespaço, ainda não se alcançou um modelo regulatório que compatibilize na medida necessária todos os interesses (interesse público, autodeterminação informacional, inovação e liberdade na internet etc.) decorrentes dos valores dos dados pessoais.

BIBLIOGRAFIA

ADFOR US. “Behind the Banner”. 2014. Disponível Em < https://www.youtube.com/watch?v=BNl38J0PZsQ>. Acesso em 22 de março de 2018.

ANDERSON, Janna; RAINIE, Lee. “The Future of Privacy”. 2014. Disponível em http://www.pewinternet.org/2014/12/18/future-of-privacy/. Acesso em 7 de junho de 2016.

ARENDT, Hannah. Reflections on little rock. In: Dissent, 6 (1), New York, 1959.

ASCQUISTI, Alessandro; BÖHME, Rainer; HUI, Kai-Lung; SPIEKERMANN, Sarah. **The challenges of personal data markets and privacy**. Electron Markets, Institute of Information Management, University of St. Gallen, 2015. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em 14 de maio de 2016.

_____. TAYLOR, Curtis; WAGMAN, Liad. “The Economics of Privacy”, 2016, Journal of Economic Literature, 442. Disponível em < https://pubs.aeaweb.org/doi/pdfplus/10.1257/jel.54.2.442>. Acesso em 16 de março de 2018.

ASSANGE, Julian et all. **Cypherpunks: liberdade e o futuro da internet**. São Paulo: Boitempo Editorial, 2013.

AYRES, Ian; BRAITHWAITE, John. **Responsive Regulation. Transcending the deregulation debate**. Oxford Socio-Legal Studies. New York Oxford OXFORD UNIVERSITY PRESS, 1992.

BARLOW, John Perry. “A Declaration of the Independence of Cyberspace”. Davos, Switzerland, 1996. Disponível em <https://www.eff.org/cyberspace-independence>. Acesso em 4 de abril de 2018.

BARROSO, Luís Roberto. “A razão sem voto: a função representativa e majoritária das cortes constitucionais”. 2016. Disponível em <https://estudosinstitucionais.com/REI/article/view/79/98>. Acesso em 31 dez 2017.

BARTLETT, Jamie. **The People Vs Tech: How the internet is killing democracy (and how we save it)**. Ebury Press, 2018, 256 p.

BELL, D. **O Advento da Sociedade Pós-Industrial**. São Paulo. Cultrix. 1974.

BASTOS, Cristina Silva. “Da eco-inovação à tentação do greenwashing: a fraude ambiental da Volkswagen”. DINÂMIA’CET – IUL, Centro de Estudos sobre a Mudança Socioeconómica e o Território ISCTE-IUL – Av. das Forças Armadas, 1649-026 Lisboa, PORTUGAL, 2016. Disponível em < https://repositorio.iscte-iul.pt/bitstream/10071/11946/3/DINAMIA_WP_2016-02.pdf. Acesso em 23 de abril de 2018.

BICKEL, Alexander. **The Least Dangerous Branch: the Supreme Court at the bar of Politics**. New Haven, CT: Yale University Press, 1986.

BIONI, Bruno R. “Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet”. 2016. Dissertação (Mestrado). Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 5. ed. Rio de Janeiro: Forense Universitária, 2001.

BLACK, Julia. “Critical reflections on regulation”. Australian Journal of Legal Philosophy, 27. pp. 1-35. 2002.

_____. “Decentring regulation: understanding the role of regulation and self-regulation in a 'post–regulatory' world”. 2001. Disponível em: <http://disciplinas.stoa.usp.br/pluginfile.php/287328/mod_folder/content/0/Black,%20Decentring%20regulation.pdf?forcedownlad=1>. Acesso em 22 de maio de 2018, p. 105.

BOLESINA, Iuri. “O direito à extimidade no ciberespaço e a transformação do binômio público-privado”. II Mostra de Pesquisa de Direito Civil Constitucionalizado, 2015.

BONIFAZ, Rafael; DELGADO-RON, Andrés. “Casos verificados de uso ilegítimo de software de vigilância por parte de governos da América Latina 2015-2016”. Revista Puce. ISSN: 2528-8156. N. 106. Maio de 2018, pp. 315-333.

BOURDIEU, Pierre. **A economia de trocas simbólicas**. São Paulo: Perspectiva, 1987.

BRADSHAW, Samantha; DENARDIS, Laura. “The politicization of the Internet’s Domain Name System: Implications for Internet security, universality, and freedom”. New Media & Society, 2016.

BRAITHWAITE, John. “Responsive Regulation and Developing Economies”. World Development Vol. 34, No. 5, 2006, p. 884. Disponível em < http://johnbraithwaite.com/wp-content/uploads/2016/03/Responsive%20Regulation%20and%20Developing%20Economies.pdf>. Acesso em 9 de abril de 2018.

_____. “The essence of responsive regulation”. UBC Law Review, v. 44. 3, p. 475 - 520, 2011.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em 24 de maio de 2018.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. 292 p.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRIAN, H. “Privacy Paradox 2.0”, 2010. Disponível em: <http://ssrn.com/abstract=1584443>. Acesso em: 09 de setembro de 2015.

BROEDERS, Dennis; SCHRIJVERS, Erik; SLOOT, Bart van der. Exploring the Boundaries of Big Data. Amsterdam University Press, 2016.

CANABARRO, Diego. “Governança Global da Internet: tecnologia, poder e desenvolvimento”. Tese (Doutorado) Universidade Federal do Rio Grande do Sul, 2014.

CARMO, T. G. . “Novos rumos da dicotomia entre o público e o privado no Estado brasileiro do século XXI”. Âmbito Jurídico , v. 76, p. 1-16, 2010.

CARVALHO NETTO, Menelick de. “A hermenêutica constitucional sob o paradigma do Estado Democrático de Direito”. In. **Jurisdição e hermenêutica constitucional no Estado Democrático de Direito**. Coord. Marcelo Andrade Carroni de Oliveira, Balo Horizonte: Mandamentos, 2004.

_____; SCOTTI, Guilherme. **Os direitos fundamentais e a (in) certeza do direito: a produtividade das tensões principiológicas e a superação do sistema de regras**. Belo Horizonte: Fórum, 2011.

_____. FERREIRA, Gianmarco Loures. “O Supremo Tribunal Federal e as Ações Afirmativas: cotas raciais para a educação superior” IN: “Acusações de racismo na capital da República : obra comemorativa dos 10 anos do Núcleo de Enfrentamento à Discriminação do MPDFT “. coordenador, Thiago André Pierobom de Ávila ; autores, Ana Claudia Farranha ... [et al.]. – Brasília : MPDFT, Procuradoria Geral de Justiça, 2017. Disponível em < http://www.mpdft.mp.br/portal/pdf/nucleos/ned/Acusacoes_de_racismo_na_capital_da_Republica.pdf>. Acesso em 31 dez 2017.

CASTELLS, Manuel. **A Era da Informação: Economia, Sociedade e Cultura. Vol. I. A sociedade em rede**. São Paulo: Paz e Terra, 1999.

____. **O Poder da Comunicação**. São Paulo/Rio de Janeiro: Paz e Terra, 2015.

CHATELARD, Daniela Scheinkman; SEGANFREDO, Gabriela de Freitas Chediak. “Das Ding: o mais primitivo dos êxtimos”. Caderno de Psicanálise.-CPRJ, Rio de Janeiro, v. 36, n. 30, p. 61-70, jan./jun. 2014.

CIGI IPSOS - Centre for International Governance Innovation. “Global Suervey on Internet Security & Trust”. 2017 Survey Results. Disponível em < https://www.cigionline.org/internet-survey>, acesso em 5 de março de 2018.

COIRO-MORAES, Ana Luiza; FARIAS, Victor Varcelly Medeiros. O exercício da cidadania da ágora grega ao site de rede social digital. Revista Extraprensa, São Paulo, v. 11, n. 1, p. 74-91, dec. 2017. ISSN 2236-3467. Disponível em: <https://www.revistas.usp.br/extraprensa/article/view/122629>. Acesso em 11 de abril de 2018. doi:http://dx.doi.org/10.11606/extraprensa2017.122629.

COMISSÃO EUROPEIA. “Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector”. Final Report. A study prepared for the European

Commission DG Communications Networks, Content & Technology by Deloite. 2017. Disponível em < file:///C:/Users/m318807/AppData/Local/Temp/1-Finalreportofthestudy.pdf>. Acesso em 24 de maio de 2018.

CORREIA, Victor. "A Dicotomia Público-Privado. Poliética". Revista de Ética e Filosofia Política. ISSN 2318-3160, [S.l.], v. 3, n. 1, p. 7-44, nov. 2015. ISSN 2318-3160. Disponível em: <https://revistas.pucsp.br/index.php/PoliEtica/article/view/19492>. Acesso em 4 de janeiro de 2018.

DENARDIS, Laura. **The global war for Internet governance**, New Haven, CT: Yale University Press, 2014.

_____. "Protocol Politics - The Globalization of Internet Governance". The MIT Press Cambridge, 2009.

_____. "Multi-Stakeholderism - The Internet Governance Challenge to Democracy". Harvard International Review, 2013. Disponível em < http://hir.harvard.edu/article/?a=10351>. Acesso em 10 de janeiro de 2018.

DINIZ, Maria Helena. **Curso de direito civil brasileiro.** 18. ed. São Paulo: Saraiva, v 1. 2002.

DLA PIPER. DLA Piper's Data Protection Laws of the World Handbook. Disponível em < https://www.dlapiperdataprotection.com/index.html?t=definitions&c=AO>. Acesso em 20 de maio de 2018.

DOMINGO-FERRER, J; TORRA, V. "A Critique of K-Anonymity and Some of Its Enhancements". Third International Conference on Availability, Reliability and Security 2008. Disponível em < https://crises-deim.urv.cat/webCrises/publications/bcpi/DomingoTorraPSAI2008.pdf>. Acesso em 16 de abril de 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DPDC – DEPARTAMENTO DE PROTEÇÃO E DEFESA DO CONSUMIDOR. Decisão de Aplicação de Sanção Administrativa. Processo nº 08012.002116/2016-21.Representada: Decolar.com Ltda. Diário Oficial da União, Brasília, DF, 18 jun. 2018. Edição 115, Seção 1, p. 73.

EVANS, Dave, "How the Internet of Everything Will Change the World". 2012. Disponível em <http://blogs.cisco.com/digital/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic>. Acesso em 19 de junho de 2016.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de direito civil: parte geral e LINDB**, volume 1. 13. ed. rev., ampl. e atual. – São Paulo: Atlas, 2015.

FINANCIAL POST. "Mark Zuckerberg lost a massive $4.9 billion yesterday, and other tech titans didn't fare much better", 2018. Disponível em http://business.financialpost.com/technology/mark-zuckerberg-just-lost-3-8-billion-over-

misused-data-affecting-50-million-facebook-users. Acesso em 24 de maio de 2018.FOUNTAIN, Jane. “Construindo um Estado Virtual”. Editora ENAP, 2005.

FOGG, B.J. “Persuasive Computers: Perspectives and Research Directions”. Stanford University, Box 8338, Stanford, CA, Estados Unidos, 1998. Disponível em < http://www.cse.chalmers.se/research/group/idc/ituniv/kurser/07/idproj/papers/fogg.pdf>. Acesso em 6 de junho de 2018.

FOLHA DE S. PAULO. “Quem instala o app escolhe ceder os dados, diz Facebook”, 2018. Disponível em https://www1.folha.uol.com.br/mercado/2018/03/quem-instala-o-app-escolhe-ceder-os-dados-diz-facebook.shtml. Acesso em 15 de maio de 2018.

FOLHA DE S. PAULO. “Planalto usa dados de agência para monitorar política em redes sociais”, 2017. Disponível em <http://www1.folha.uol.com.br/poder/2017/04/1874399-planalto-usa-dados-de-agencia-de-sp-para-monitorar-redes-sociais.shtml>. Acesso em 25 de maio de 2018.

FOLHA DE S. PAULO. “PF quer instalar vírus em telefone grampeado para copiar informações”, 2015. Disponível em < http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml>. Acesso em 15 de maio de 2018.

FÓRUM ECONÔMICO MUNDIAL. “Personal Data: The emergence of a New Asset Class”. 2011. Disponível em: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em 14 de maio de 2016.

FREITAS, Christiana Soares de; LIMA, Fernanda Fiuza; LIMA, Fernanda Queiroz. “Os Desafios ao Desenvolvimento de um Ambiente para Participação Política Digital: o Caso de uma Comunidade Virtual Legislativa do Projeto e-Democracia no Brasil”. Organizações & Sociedade. Salvador, v. 22, n. 75, p. 639-658, Dez. 2015. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1984-92302015000400639&lng=en&nrm=iso>. Acesso em 23 de maio de 2018. http://dx.doi.org/10.1590/1984-9230759.

GAMA, Guilherme Calmon Nogueira da. **Função social no Direito Civil**, São Paulo: Atlas, 2007.

GETSCHKO,Demi; MOREIRAS, Antonio M. ”Os Pontos de Troca de Tráfego, o PTTMetro e a Internet Brasileira”, 2008. Disponível em < http://www.ceptro.br/pub/CEPTRO/PalestrasPublicacoes/Os_Pontos_de_Troca_de_Trfego_o_PTTMetro_e_a_Internet_Brasileira.pdf >. Acesso em 23 de abril de 2018.

GOMES, Rodrigo Dias de Pinho. “Desafios à privacidade: Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais”, 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf>. Acesso em 24 de maio de 2018.

GORMLAY, Ken. “One Hundred Years of Privacy”, Wisconsin Law Review, 1992(5): 1335-1441, 1992. Disponível em https://cyber.harvard.edu/privacy/Gormley--100%20Years%20of%20Privacy.htm. Acesso em 25 de maio de 2018.

HABERMAS, Jünger. **A inclusão do outro – estudos de teoria política**. Trad. George Sperber e Paulo Astor Soethe. São Paulo: Edições Loyola, 2002.

_____. **Mudança estrutural da esfera pública**, Rio de Janeiro, Ed. Tempo Brasileiro, 2003.

HSING, Chen Wen. “Coleta de dados pessoais e paradoxo da privacidade: um estudo entre usuários de aplicativos móveis”. Tese (doutorado), Departamento de Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, São Paulo, 2016.

HUGUES, Eric. “A Cypherpunk’s Manifesto”. 1993. Disponível em <http://www.activism.net/cypherpunk/manifesto.html>. Acesso em 9 de março de 2018.

IBGE – Instituto Brasileiro de Geografia e Estatística. Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua. 2017. Disponível em <https://www.ibge.gov.br/estatisticas-novoportal/sociais/trabalho/17270-pnad-continua.html?&t=downloads>. Acesso em 12 de janeiro de 2018.

INTERNETLAB - Associação Internetlab de pesquisa em Direito e Tecnologia. “O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais”. 2016. Disponível em < http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>, Acesso em 17 de maio de 2016.

_____. “Quem defende seus dados?” 2015. Disponível em < http://quemdefendeseusdados.org.br/pt/>. Acesso em 4 de agosto de 2016.

ISOC - INTERNET SOCIETY. “Brief History of the Internet”, 1997. Disponível em < https://cdn.prod.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf>. Acesso em 24 de maio de 2018.

JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada: conflitos entre direitos da personalidade**. São Paulo: Revista dos Tribunais, 2000.

JAKOBSSON, Markus (ed.). **The death of the internet**. Wiley, 2012.

JOLT DIGEST. “Google v. Equustek: United States Federal Court Declares Canadian Court Order Unenforceable”, 2017. Disponível em <https://jolt.law.harvard.edu/digest/google-v-equustek-united-states-federal-court-declares-canadian-court-order-unenforceable>. Acesso em 23 de maio de 2018.

JORDANA, Jacint; LEVI-FAUR, David. **The politics of regulation: institutions and regulatory reforms for the age of governance**. Cheltenham: Edward Elgar cop. 2004.

KERBER, Wolfgan. “Digital markets, data, and privacy: competition law, consumer law and data Protection”. Journal of Intellectual Property Law & Practice, 2016.

KOSINSKI, Michal, STILLWELL, David; YOUYOU, Wu. “Computer-based personality judgments are more accurate than those made by humans”. PNAS January 27, 2015. 112 (4) 1036-1040. Disponível em <http://www.pnas.org/content/112/4/1036>. Acesso em 10 de abril de 2018.

KUHN, Thomas. S. **A estrutura das revoluções científicas**. São Paulo: Perspectiva, 1991.

LATOUR. **Reagregando o Social: uma introdução a Teoria Ator-Rede**. São Paulo: EDUSC. Bahia: EDUFBA, 2012.

LEFÈVRE, Flávia. “Zero-rating - A Internet dos Pobres”. Palestra na IX Escola do Sul de Governança da Internet – SSIG 2017 – 4 de março de 2017 – Rio de Janeiro. Disponível em <http://flavialefevre.com.br/pt/blog/zero-rating-a-internet-dos-pobres>. Acesso em 23 de abril de 2018, 2017a.

_____. “O STF, a Internet e as telecomunicações”. Disponível em <http://flavialefevre.com.br/pt/blog/o-stf-a-internet-a-as-telecomunicacoes>. Acesso em 17 de julho de 2018, 2017b)

LESSIG, Lawrence. **Cultura Livre: Como a mídia usa a tecnologia e a lei para barrar a criação cultural e controlar a criatividade**. Estados Unidos, 2004.

_____. **Code: version 2.0.** New York: Basic Books, 2006. Disponível em <http://pdf.codev2.cc/Lessig-Codev2.pdf>. Acesso em 13 de junho de 2017.

LOPES, Ana Frazão de Azevedo. **Empresa e Propriedade - Função Social e Abuso de Poder Econômico**. Editora Quartier Latin, 2006.LOURENÇO, Cíntia Azevedo. “METADADOS: o grande desafio na organização da Web”. Inf. & Soc.: Est., João Pessoa, v.17, n.1, p.71-80, jan./abr. 2007.

LUNARDI., Fabrício Castanha. “A hermenêutica dos direitos fundamentais à luz do pós-positivismo e do neoconstitucionalismo”. Revista de Direitos e Garantias Fundamentais, vol. 12, 2012.

MACHADO, Diego Carvalho; PACÍFICO, Leandro. “Proteção de dados pessoais no cenário internacional: breves comentários sobre os modelos norte-americano e europeu e o direito brasileiro”, 2016. Disponível em < http://irisbh.com.br/protecao-de-dados-pessoais-no-cenario-internacional-breves-comentarios-sobre-os-modelos-norte-americano-e-europeu-e-o-direito-brasileiro/>. Acesso em 10 de junho de 2018.

MACHLUP, Fritz. **The production and distribution of knowledge in the United States**. Princeton, Nova Jersey: Princeton University Press, 1962.

MAIA, Paulo Eduardo Assis; MIRA, Gustavo Fernandes Paravizo; PINHEIRO, Marta de Araújo. “O discurso de segurança e a privacidade no marco civil da internet”. IV Simposio Internacional LAVITS, Buenos Aires, 2016.

MANDIANT. “Exposing One of China’s Cyber Espionage Units”, 2013. Disponível em <https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html>. Acesso em 10 de abril de 2018.

MARINI apud BAIÃO, C.Sampaio e GONÇALVES Kalline Carvalho. “A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana”. Civilistica.com. a. 3. n. 2. 2014.

MARSDEN. “Internet Co-Regulation and Constitutionalism: Towards a More Nuanced View”. 2011. Disponível em <http://ssrn.com/abstract=1973328>. Acesso em 1º de agosto de 2016.

MASCENA, Keysa Manuela Cunha de. “Priorização de stakeholders: um estudo em empresas que divulgam relatórios com a estrutura da Global Reporting Initiative – GRI no Brasil. São Paulo. Dissertação (Mestrado), Universidade de São Paulo, 2013.

MAY, Thimoty. “The Cyphernomicon”, 1994. Disponível em <http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.txt>. Acesso em 9 de março de 2018.

MAYER-SCHNONBERGER, Viktor. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Trad. Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013.

_____. CUKIER, k. **Big Data. A Revolution that Will Transform How We Live, Work, and Think**. London: John Murray Publishers, 2013.

MAYER, Jonathan; MUTCHLER, Patrick; MITCHELL, John C. “Evaluating the privacy properties of telephone metadata”. PNAS May 16, 2016. Disponível em < https://doi.org/10.1073/pnas.1508081113>. Acesso em 21 de maio de 2018.

MEMORANDUM of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. Disponível em < https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en>. Acesso em 21 de maio de 2018.

MENDES, Laura Schertel. “A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais”. Revista de Direito do Consumidor , v. 102, p. 19-43, 2015.

MORATO, Antonio Carlos. “Quadro geral dos direitos da personalidade”, Revista da Faculdade de Direito da Universidade de São Paulo. v. 106/107 p. 121 - 158 jan./dez. 2011/2012.

MOUNIER, Pierre. **Donos da rede – As tramas políticas da internet**. Edições Loiola, 2006.

MURRAY, Andrew D. **The regulation of cyberspace: control in the online environment**, xxii, 274 p. Abingdom: Routledge Cavendish, 2007.

_____. **Internet Regulation**. London School of Economics and Political Science. Spring 2011.

_____. “Finding Proportionality in Surveillance Laws”. 2015. Disponível em https://paulbernal.wordpress.com/2015/12/11/finding-proportionality-in-surveillance-laws-guest-post-by-andrew-murray/. Acesso em 13 de maio de 2016.

_____. **Information technology law: the law and society**. Oxford: Oxford University Press, 2013, 602 p.

NORIJI, Sergio. “Direito à privacidade na era da informática algumas considerações”. R. Jur. UNIJUS, Uberaba MG, v.8, nº 8, p. 99106, maio2005. Disponível em < http://www.egov.ufsc.br/portal/sites/default/files/privacidade_informatica.pdf>. Acesso em 4 janeiro 2018.

OECD ECONOMIC PAPERS. “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value”, OECD Digital Economy Papers, No. 220, OECD Publishing, 2013. Disponível em <http://dx.doi.org/10.1787/5k486qtxldmq-en>. Acesso em 15 de maio de 2016.

O’NEIL, Cathy. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**, Crown, 2016.

OPINION BOX. “Opinion Box pesquisa: privacidade e segurança na internet”, 2016. Disponível em https://blog.opinionbox.com/opinion-box-pesquisa-privacidade-na-internet/. Acesso em 20 de janeiro de 2018.

O’SULLIVAN, K.P.V.; FLANNERY, Darragh J. “A discussion on the resilience of command and control regulation within regulatory behaviour theories”. Set. 1, 2011, p. 4. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1927500>. Acesso em 9 de abril de 2018.

PINHEIRO, Alexandre Pereira. “Reversibilidade de bens na concessão do serviço telefônico fixo comutado: uma análise crítica na perspectiva da teoria responsiva da regulação”. Dissertação (Mestrado). Faculdade de Direito, Universidade de Brasília, Brasília, 2017.

PRIVACY COMMISSIONER FOR PERSONAL DATA. 2016. “Upward Trend in Privacy Complaints Sees Need for Personal Data Protection and Respect amongst Individuals and Organisations”. Disponível em <https://www.pcpd.org.hk/english/news_events/media_statements/press_20160126a.html>. Acesso em 16 de maio de 2016.

"PRIVACY INTERNATIONAL. "State of Privacy Brazil: Communication Surveillance, Data Protection, Right to Privacy". 2016. Disponível em: <https://www.privacyinternational.org/node/979>. Acesso em 19 de novembro de 2016.

REED, Chris. **Internet Law: text and materials**. Cambridge University Press, 2004.

REIDENBERG, Joel. "Governing Networks and Rule-Making in Cyberspace". 45 Emory L.J. 911, 1996. Disponível em <http://ir.lawnet.fordham.edu/faculty_scholarship/29>. Acesso em 4 de abril de 2018.

_____. **Resolving Conflicting International Data Privacy Rules in Cyberspace**. Stanford Law Review, vol. 52, no. 5, 2000, pp. 1315–1371. www.jstor.org/stable/1229516.

ROCHFELD, Judith. "Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet". Revista de Direito, Estado e Telecomunicações / The Law, State and Telecommunications Review, [S.l.], v. 10, n. 1, p. 61-84, maio 2018. ISSN 1984-8161. Disponível em: <http://www.ndsr.org/SEER/index.php?journal=rdet&page=article&op=view&path%5B%5D=326>. Acesso em: 24 de junho de 2018.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Leo Peixoto; NEVES, Fabrício Monteiro. "Niklas Luhmann: a sociedade como sistema". Porto Alegre: Edipucrs, 2012, p. 60/61.

ROHRMANN, Carlos Alberto; SILVA, Denis Franco. "Tensões entre o direito público e o direito privado na regulamentação de contratos eletrônicos de browsewrap" in **Novas perspectivas do direito: diálogos ou disjunções entre o direito público e o direito privado**. Organização CONPEDI/UNA/UCR/IIDH/IDD/UFPB/UFG/Unilasalle/UNHwN; Coordenadores: Luiz Gustavo Gonçalves Ribeiro, Maria Cristina Vidotte Blanco Tarrega - Florianópolis: CONPEDI, 2017. Disponível em < https://www.conpedi.org.br/publicacoes/c7yrg601/k2gxp024/j7ND0G2nU4q1sn44.pdf>. Acesso em 24 de maio de 2018.

ROMA, Bruno Marques Bensal; SILVA, Rodrigo Freitas de. "O desafio legislativo do bitcoin". Revista de Direito Empresarial, vol. 20. ano 4. p. 109-128. São Paulo: Ed. RT, novembro, 2016.

RUBENFELD, Jed, "The Right of Privacy" (1989). Faculty Scholarship Series. 1569. Disponível em http://digitalcommons.law.yale.edu/fss_papers/1569. Acesso em 4 de janeiro de 2018.

RUBINSTEIN, I. **Big Data: The End of Privacy or a New Beginning? International Data Privacy Law**, Volume 3, Issue 2, 1 May 2013, Pages 74–87. Disponível em: https://doi.org/10.1093/idpl/ips036.

SARMENTO, Daniel. “Interesses Públicos vs. Interesses Privados na Perspectiva da Teoria e da Filosofia Constitucional.”. In **Interesses Públicos versus Privados: desconstruindo o princípio da supremacia do interesse público**. SARMENTO, Daniel (org.). Rio de Janeiro: Lumen Juris, 2005.

SARTI, Gustavo Mescoki. “Uma abordagem sociológica da governança da internet – a Conferência Mundial de Telecomunicações Internacionais“, Dissertação (Mestrado). Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas, 2017.

SCHEWICK, Barbara van. **Internet architecture and Innovation**. Cambridge: The MIT Press, 2010.

SCHNEIER, Bruce. **Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World**. W. W. Norton & Company, 2016, 448 p.

SCHÖNBEGER, Viktor Mayer. **Generational development of data protection in Europe**. Technology and privacy. MIT Press Cambridge, MA, USA ©1997.

SEMINÁRIO INTERNACIONAL “A Economia Movida a Dados: Desafios Regulatórios para a Garantia da Inovação e a Proteção da Personalidade”. Brasília, Centro de Estudos em Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (Cedis/IDP), do Grupo de Estudos em Direito das Telecomunicações da Universidade de Brasília (GETEL/UnB) e do Instituto Brasileiro de Direito Civil (IBDCivil), informações verbais, 2018.

SILVA, Filipe Carreira da. “Habermas e a esfera pública: reconstruindo a história de uma ideia”. Sociologia, Problemas e Práticas, Oeiras, n. 35, p. 117-138, abr. 2001. Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0873-65292001000100006&lng=pt&nrm=iso>. Acesso em 4 de janeiro de 2018.

SILVEIRA, Sérgio Amadeu. “A disseminação dos coletivos cypherpunks e suas práticas discursivas“. II Encontro Internacional Participação, Democracia e Políticas Públicas, UNICAMP, Campinas (SP), 27 a 30 de abril de 2015.

_____. “Governo dos Algoritmos”, Revista de Políticas Públicas, v. 21, n. 1, 2017a.

_____. **Tudo sobre tod@s**. São Paulo: Edições SESC SP, 2017b.

SMITH, Michael S. “Protecting Privacy in an IoT-Connected World”. Information Management, vol. 49, n. 6, November 2015.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016.

STALLMAN, Richard. **Free Software, Free Society: Selected Essays of Richard M. Stallman**. Boston: GNU Press, 2002.

STONE, Brad. Our Paradoxical Attitudes toward Privacy. New York Times, 02 de julho de 2008. Disponível em: <http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-

towards-privacy/.>. Acesso em 09 de setembro de 2015. BRIN, David. “The Transparency Society”. Basic Books, 1999, 384 p.

TEPEDINO, Gustavo. **Temas de Direito Civil - Tomo III**, Editora Renovar. 2009.

_____. “Notas sobre a função social dos contratos “. Disponível em < http://www.tepedino.adv.br/wpp/wp-content/uploads/2017/07/Notas_Sobre_Funcao_Social_Contratos_fls_395-405.pdf>. Acesso em 7 fev 2018.

THE GUARDIAN. “Google will stop scanning content of personal emails”. 2017. Disponível em https://www.theguardian.com/technology/2017/jun/26/google-will-stop-scanning-content-of-personal-emails. Acesso em 24 de maio de 2018.

THE NEW YORK TIMES. “How Trump Consultants Exploited the Facebook Data of Millions”, 2018a. Disponível em <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em 25 de maio de 2018.

THE NEW YORK TIMES. “You Are the Product’: Targeted by Cambridge Analytica on Facebook”, 2018b. Disponível em < https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html>. Acesso em 25 de maio de 2018.

THE WALL STREET JOURNAL. “Sites Feed Personal Details To New Tracking Industry”, 2010, Disponível em < https://www.wsj.com/articles/SB10001424052748703977004575393173432219064>. Acesso em 20 de maio de 2018.

TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. “The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation”, 2015. Disponível em: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>. Acesso em 5 de março de 2018.

UNIÃO EUROPEIA. Comissão Europeia. DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em <http://data.consilium.europa.eu/doc/document/ST-5418-2016-REV-1/pt/pdf>. Acesso em 4 de agosto de 2016.

UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Regulamento Geral sobre a Proteção de Dados. Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acesso em 20 de julho de 2016.

UNISYS. “Unysis Security Index. Brasil”. 2017. Disponível em < http://www.unisys.com/unisys-security-index/brazil>. Acesso em 5 de março de 2018.

WARREN; BRANDEIS. “The Right to Privacy”. Harvard Law Review, 1980, nº 5, vol IV.

WIKILEAKS. “Vault 7: CIA Hacking Tools Revealed”. 2017. Disponível em < https://wikileaks.org/ciav7p1/>. Acesso em 6 de junho de 2018.

ZANINI, Estevam de Assis Zanini. “O surgimento e o desenvolvimento do right of privacy nos Estados Unidos”. Revista Brasileira de Direito Civil | ISSN 2358-6974 | Volume 3 – Jan / Mar 2015.

ZITTRAIN, Jonathan; CRAWFORD, Susan; BREM, Lisa. “Game changers: mobile gaming apps and data privacy”; Harvard Law School: The Case Studies. 2012.

ZUCKERBERG, Mark. 2018. Disponível em <https://www.facebook.com/zuck/posts/10104712037900071>. Acesso em 10 de abril de 2018.

JURISPRUDÊNCIA

BRASIL. Supremo Tribunal Federal. Inquérito nº 2245/MG, Min. JOAQUIM BARBOSA, Tribunal Pleno, julgado em 28/08/2007, DJe-139 DIVULG 08-11-2007 PUBLIC 09-11-2007 DJ 09-11-2007 PP-00038 EMENT VOL-02298-01 PP-00001 RTJ VOL-00203-02 PP-00473.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 1790. Relator(a): Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 23/04/1998, DJ 08-09-2000 PP-00004 EMENT VOL-02003-01 PP-00199).

BRASIL. Supremo Tribunal Federal. Ação de Descumprimento de Preceito Fundamental nº 130. Relator(a): Min. CARLOS BRITTO, Tribunal Pleno, julgado em 30/04/2009, DJe-208 DIVULG 05-11-2009 PUBLIC 06-11-2009 EMENT VOL-02381-01 PP-00001 RTJ VOL-00213-01 PP-00020).

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade. Min. OCTAVIO GALLOTTI, Relator(a) p/ Acórdão: Min. GILMAR MENDES, Tribunal Pleno, julgado em 26/05/2010, DJe-047 DIVULG 11-03-2011 PUBLIC 14-03-2011 EMENT VOL-02480-01 PP-00008 RTJ VOL-00220-01 PP-00050).

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 766390. Relator(a): Min. RICARDO LEWANDOWSKI, Segunda Turma, julgado em 24/06/2014, PROCESSO ELETRÔNICO DJe-157 DIVULG 14-08-2014 PUBLIC 15-08-2014).

BRASIL. Supremo Tribunal Federal. Suspensão de Segurança nº 3902. Relator(a): Min. AYRES BRITTO Julgamento: 09/06/2011, Órgão Julgador: Tribunal Pleno.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 4815. Relator(a): Min. CÁRMEN LÚCIA, Tribunal Pleno, julgado em 10/06/2015, PROCESSO ELETRÔNICO DJe-018 DIVULG 29-01-2016 PUBLIC 01-02-2016).

BRASIL. Superior Tribunal de Justiça. REsp 1567780/RJ, Rel. Ministro RICARDO VILLAS BÔAS CUEVA, TERCEIRA TURMA, julgado em 14/03/2017, DJe 21/03/2017.

COLUMBIA. Corte de Apelação. Google Inc. versus Equustek Solutions Inc., Robert Angus e Clarma Enterprises Inc. 2017. Disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do. Acesso em 13 de fevereiro de 2018.