A PROTEÇÃO DE DADOS PESSOAIS ENTRE LEIS, CÓDIGOS E PROGRAMAÇÃO: OS LIMITES DO MARCO CIVIL DA INTERNET[1]

Rafael A. F. Zanatta[2]

Introdução

Este artigo é uma versão adaptada de uma palestra proferida na Escola Politécnica da Universidade de São Paulo, a convite do Instituto Brasil-Europa, em julho de 2014. O objetivo da palestra era apresentar um panorama geral da proteção de dados pessoais no Brasil e discutir a possibilidade de construção de um "sistema regulatório híbrido", capaz de unir a regulação estatal (leis e autoridades administrativas), a autorregulação (produção de *standards* e códigos de conduta por empresas do setor privado) e a regulação pela tecnologia (modificação do comportamento humano pela arquitetura virtual).

A partir da aprovação do Marco Civil da Internet (Lei 12.965/2014),[3] a palestra tinha como fio condutor uma pergunta central: quais as possibilidades de construção, no Brasil, de um modelo regulatório capaz de unir Estado, mercado e sociedade civil? Em outras palavras: de que modo direito estatal (*hard law*), recomendações e códigos de melhores práticas (*soft law*) e a própria tecnologia (programações e aparelhos) podem garantir a devida proteção dos dados pessoais dos cidadãos brasileiros?

Nesse texto, busco uma reflexão para além do discurso dogmático e interno do direito. Diferentemente dos estudos jurídicos que tratam da proteção de dados pessoais por

[1] Publicado na coletânea *Direito & Internet III: Marco Civil da Internet* (Quartier Latin, 2015). Referência para citação: ZANATTA, Rafael A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. *Direito e Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, 2015, p. 447-470.

[2] Mestre pela Faculdade de Direito da Universidade de São Paulo. Pesquisador da FGV Direito SP e do Núcleo de Direito, Internet e Sociedade. As ideias apresentadas nesse artigo são resultantes de debates e conversas com Dennys Antonialli, Francisco Brito Cruz, Pedro Ramos e Piedade Costa.

[3] Para um panorama geral da Lei 12.965/2014, ver a coletânea de artigos organizada por Ronaldo Lemos e George Salomão Leite, que contém textos de Demi Getschko (origens do Marco Civil), Pedro Henrique Ramos (neutralidade de rede), Cláudia Lima Marques (contratos de prestação de serviços de internet), Marcel Leonardi (direito à privacidade e liberdade de expressão), Carlos Affonso Souza (responsabilidade civil dos provedores de acesso e de aplicações), entre outros. LEMOS, Ronaldo; SALOMÃO LEITE, George (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.

uma perspectiva dogmática de "direito fundamental do consumidor"[4], apresento nesse texto uma perspectiva sócio-jurídica sobre a construção do modelo regulatório brasileiro para proteção de dados pessoais, analisando os interesses de diferentes atores acerca da necessidade de adoção do "modelo europeu" de regulação – caracterizado pelo reconhecimento do direito à proteção de dados pessoais, a existência de uma Autoridade Garantidora para monitoramento do cumprimento das regras de tratamento de dados pessoais, e o incentivo à elaboração de códigos de conduta pelo setor privado, que, após validação pela autoridade de proteção de dados, ganha caráter normativo.[5]

A partir da observação do posicionamento de diferentes atores na discussão do anteprojeto de lei de proteção de dados pessoais, discuto a tentativa de implementação de um modelo de "corregulação" no Brasil, no qual "governo e indústria compartilham responsabilidade pela elaboração e cumprimento de *standards* regulatórios" (Hirsch, 2011, p. 441). Discuto ainda as limitações desse modelo e a necessidade de enxergar a proteção de dados pessoais no Brasil sob um prisma mais amplo, a partir de uma "caixa de ferramentas de governança" que inclui (i) regulação estatal (leis, agências, autoridades administrativas), (ii) instrumentos de autorregulação (códigos técnicos, códigos de conduta, certificação), (iii) normas internacionais (acordos bilaterais e multilaterais), e (iv) tecnologia (criptografia, *privacy by design*, programação).

O artigo está dividido em quatro partes. Na primeira, apresento brevemente o "estado da arte" da regulação de proteção de dados pessoais no Brasil, ainda bastante atrasado em comparação com outros países latino-americanos. Na segunda, discuto as tentativas do governo de discutir um anteprojeto de lei de proteção de dados pessoais em 2010 e 2011. Nessa parte, destaco o posicionamento dos atores com relação à criação da Comissão Nacional de Proteção de Dados Pessoais no Brasil. Na terceira parte, faço uma breve análise da Lei 12.965/2014 e busco identificar os limites do Marco Civil da Internet para a devida proteção de dados pessoais. Por fim, retomo a ideia de um "sistema regulatório híbrido" e exploro possibilidades de construção dessa agenda, identificando os papéis e responsabilidades de diferentes atores.

---

[4] Ver, como estudos representativos dessa vertente, DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006; MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, v. 79, p. 45-81, 2011.

[5] Para um estudo detalhado da experiência holandesa de governança colaborativa para proteção de dados pessoais (lei geral estatal combinada com produção de códigos pelo setor privado) e a influência dessa abordagem nas propostas da administração Barack Obama para regulação da privacidade, cf. HIRSCH, Dennis. Going Dutch? Collaborative Dutch privacy regulation and the lessons it holds for U.S. privacy law, *Michigan State Law Review*, 83, 2013, p. 85-162.

1. O problema do atraso regulatório brasileiro para proteção de dados pessoais

A. O debate teórico sobre regulação e direito

Antes de discutir a questão do "atraso regulatório"[6] para proteção de dados pessoais no Brasil, é preciso ter em mente um debate teórico sobre o assunto.[7] Afinal, o que é regulação? Obviamente, não pretendo responder essa questão com precisão conceitual e ontológica. Entretanto, é preciso um mínimo de compreensão das concepções teóricas que estruturam os debates sobre direito e regulação.

Existe um amplo debate na literatura sobre diferentes "concepções de regulação"[8]. Para alguns, "a regulação é algo que é feito exclusivamente por governos, uma questão de *enforcement* jurídico e estatal; para outros, regulação é principalmente um trabalho de atores sociais que monitoram outros atores, incluindo governos" (Levi-Faur, 2010, p. 4). Como nota a professora Julia Black, existem visões "centradas no Estado", que privilegiam o controle focado e sustentado por uma agência pública sobre atividades que são valorizadas por uma comunidade, e visões "não centradas no Estado", que consideram qualquer tipo de influência social e econômica, inclusive cultural, privilegiando atores não estatais.[9] Uma é mais jurídica, outra é sociológica.

Para simplificar a discussão sobre regulação e proteção de dados pessoais no Brasil, adoto primeiramente uma concepção mais tradicional, centrada no Estado e nas agências governamentais. Assim, quando uso o termo "regulação", refiro-me a formas de influência da sociedade e dos atores sociais por agentes públicos, especialmente através do uso de instrumentos jurídicos. A regulação, nesse sentido, pode ser entendida como instrumentos de governança ligados a agentes públicos, o que inclui legislação, licenças, códigos, normas e atos administrativos. Nas palavras de Egon Moreira, regulação é

---

[6] Para uma breve análise da situação brasileira e da crescente judicialização das questões que envolvem proteção de dados pessoais, cf. ZANATTA, Rafael; GLEZER, Rubens. Atraso Regulatório para Proteção de Dados no Brasil, *Valor Econômico*, Opinião, p. A-13, 01/10/2014.

[7] Ver, por todos, BALDWIN, Robert; CAVE, Martin; LODGE, Martin. *Understanding Regulation: theory, strategy, and practice*. Oxford: Oxford University Press, 2012. Para um panorama de diferentes debates teóricos sobre regulação e democracia no contexto europeu e americano, cf. MATTOS, Paulo *et al.* (org.). *Regulação Econômica e Democracia: o debate norte-americano*. São Paulo: Editora, v. 34, 2004; MATTOS, Paulo *et al.* (org.). *Regulação Econômica e Democracia: o debate europeu*. São Paulo: Editora Singular, 2006.

[8] Cf. LAVI-FAUR, David. Regulation & Regulatory Governance, *Jesuralem Papers in Regulation & Governance*, working paper n. 1, feb. 2010, p. 4-9. Disponível em: http://regulation.huji.ac.il/papers/jp1.pdf

[9] BLACK, Julia. Decentring Regulation: understanding the role of regulation and self-regulation in a "post regulatory" world, *Current Legal Problems*, n. 54, p. 103-147, 2001.

"aquele conjunto de ações jurídicas que visam estabelecer parâmetros de conduta em determinado espaço-tempo"[10].

Em termos gerais, para fins meramente didáticos, é possível compreender alguns "tipos de regulação", a partir de uma perspectiva centrada no Estado e sua relação com a sociedade (influência no comportamento humano). Essa distinção meramente ideal-típica ajuda a compreender os papéis do setor privado e do Estado na criação de comandos ou técnicas normativas em determinados setores passíveis de regulação.

No tipo "não-regulação", atores públicos e privados teoricamente não interferem e não tentam moldar o comportamento humano. Na "autorregulação", o setor privado se organiza e cria "standards" e normas procedimentais para a conduta dos atores, independentemente do Estado. Em termos gerais, é o que ocorre na regulação da propaganda (CONAR) e da bolsa de valores (Bovespa). Na "corregulação", o Estado reconhece a importância da produção espontânea de normas pelo setor privado, mas monitora e valida tais normas. Por fim, o tipo da "regulação tradicional" consiste na criação de regras e comandos mediante ameaça de sanções (sanções penais ou multas punitivas).

Tabela 1. Quadrantes da regulação		
+ *Setor Privado*	Autorregulação	Corregulação
- *Setor Privado*	Não regulação	Regulação Tradicional
	- Setor Público	*+ Setor Público*

Fonte: Elaboração própria

Obviamente, os tipos não representam fielmente a realidade. É praticamente impossível pensar em alguma esfera da vida que não sofra influência do setor privado e do Estado. De todo modo, essa tipologia pode ser útil para pensar em formas de governança que atribuam funções ao Estado e ao setor privado. Como ficará evidente nesse artigo, o

[10] MOREIRA, Egon. Qual é o Futuro do Direito da Regulação no Brasil?, in: SUNDFELD, Carlos Ari; ROSILHO, André (org.), *Direito da Regulação e Políticas Públicas*. São Paulo: Malheiros, 2014, p. 114.

Brasil enfrenta um sério problema em avançar um modelo de corregulação para proteção de dados pessoais, tal como existente na Holanda e nos países na União Europeia.[11]

B. A "colcha de retalhos jurídica" para proteção de dados pessoais no Brasil

Quais normas jurídicas regulam a proteção de dados pessoais no Brasil? A ideia de "colcha de retalhos jurídica" serve para entender, em primeiro passo, o que já existe no Brasil em termos de proteção de dados pessoais. Seria muita ingenuidade dizer que não há algum tipo de proteção de dados pessoais no Brasil. Antes mesmo da aprovação da Lei 12.965/2014, já existiam normas jurídicas e regulações setoriais para proteção de dados. O problema é que tais normas são fragmentadas e não tratam do direito à proteção de dados pessoais de forma explícita.[12]

Há na Constituição Federal o reconhecimento de um direito fundamental à vida privada e à liberdade. Naquele momento de transição de um regime ditatorial para uma democracia, foi construído o instrumento do "habeas data", que é um remédio constitucional para que os cidadãos brasileiros possam entender ou saber por que existem bancos de dados em órgãos públicos.[13] Isso aconteceu em um momento muito específico, em que existia um serviço de inteligência nacional, que criava bancos de dados de "subversivos" ou militantes de esquerda no Brasil. O habeas data surgiu como um remédio constitucional para isso. No entanto, o habeas data não tratava de bancos de dados de pessoas jurídicas privadas.[14] Não é possível usar o habeas data para entender como que uma empresa está utilizando um banco de dados – um problema central no mundo informatizado e conectado de hoje. Apesar de ser uma "importante inovação institucional latino-americana" (Guadamuz, 2001), tal instrumento é bastante limitado para a proteção de dados pessoais.[15]

---

[11] Ver o estudo do professor Dennis Hirsch citado na nota 4.

[12] Apesar de pouco comentado na literatura, no final da década de 1970 tentou-se criar uma comissão nacional para proteção de dados (aos moldes da *Commission nationale de l'informatique et des libertes*) e garantir direitos dos cidadãos brasileiros para identificação, compreensão e correção dos bancos de dados produzidos por empresas privadas e órgãos do governo. O projeto de lei 4.365/1977 foi apresentado por José Roberto Faria Lima (Arena/SP) à Câmara dos Deputados, mas foi arquivado no ano seguinte.

[13] Os argumentos desse parágrafo baseiam-se em: DALLARI, Dalmo A. O Habeas Data no Sistema Jurídico Brasileiro, *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 97, p. 239-253, 2002.

[14] Constituição Federal, art. 5º, LXXII: "conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público".

[15] Além do artigo 5º, inciso LXXII, a Lei nº 9.507/1997 – que regulou o "direito de acesso a informações e disciplina o rito processual do habeas data" – garantiu o direito de conhecimento de informações relativas ao cidadão e retificação dos dados, mas não tutelou o direito à destruição de dados pessoais falsos.

Nos primeiros anos de regime democrático e civil, nós tivemos no Brasil uma legislação muito avançada para proteção do consumidor: o Código de Defesa do Consumidor (Lei 8.078/1990). No artigo 43 existem regras para obtenção de consentimento para criação de bancos de dados. Nesta lei, dispõe-se que o consumidor "terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivoados sobre ele, bem como sobre suas respectivas fontes". Além disso, diz que a abertura de cadastros e dados pessoais "deverá ser comunicada por escrito ao consumidor, quando não comunicada por ele" (Art. 43, § 2°). Não há, no entanto, a estipulação clara de direitos à proteção de dados pessoais, como acesso, transparência, respeito à finalidade de uso e remoção.[16]

Depois de 1990, outra norma que tratou da proteção de dados pessoais foi a Lei de Telecomunicações, de 1997, criada no governo Fernando Henrique Cardoso no período de privatizações e concessões, em que o governo criou regras específicas e um dever de sigilo no manejo de dados dos clientes.[17] O art. 3º dessa lei fala do "direito ao respeito de sua privacidade" na "utilização de seus dados pessoais pela prestadora de serviços" (art. 3º, IX). Recentemente, tivemos uma decisão da Secretaria Nacional do Consumidor, que aplicou uma multa de 3,5 milhões de reais na empresa Oi pela utilização de um software (*Velox*) que criava ilegalmente bancos de dados e revendia para terceiros. A Lei de Telecomunicações foi utilizada na decisão juntamente com outras legislações.[18]

Em 2001 veio a Lei de Sigilo Bancário, a Lei Complementar 105, que criou normas para as instituições financeiras com relação aos bancos de dados. O Código Civil de 2002 também reafirmou as regras de responsabilização e explicitou a proteção da vida privada no capítulo que trata dos direitos da personalidade.[19]

Havia, há cinco anos, um quadro geral que foi avançado em 2011 com a Lei 12.414, que criou regras específicas para bancos de dados do setor privado, especialmente para proteção do consumidor e a necessidade de consentimento prévio para criação do

---

[16] MENDES, Laura Schertel. O Direito Fundamental à Proteção de Dados Pessoais. *Revista de Direito do Consumidor*, v. 79, p. 45-81, 2011.

[17] Lei nº 9.472, de 16 de julho de 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm

[18] "Oi é multada em R$ 3,5 milhões por invasão de privacidade feita por Velox", *Jornal O Globo*, 23/07/2014. Disponível em: http://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505

[19] Lei 10.406/2002, Art. 21: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

cadastro positivo.[20] Essa é a "colcha de retalhos jurídica" que existia até o Marco Civil da Internet.

Com a Lei 12.965/2014, alguns avanços são feitos no plano normativo para a proteção de dados pessoais. No entanto, tais avanços mostram-se limitados. Por exemplo, declara-se o princípio da proteção dos dados pessoais (art. 3º, III), porém não há definição conceitual de "dados pessoais". Garante-se o direito ao "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet" (art. 7º, VII), porém permite-se o repasse de tais informações mediante decisão judicial. Por fim, garante-se a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet" (art. 7º, X), ressalvadas as hipóteses de guarda obrigatória de registros previstas na lei.[21]

C. O atraso brasileiro em perspectiva comparada: emergência das autoridades garantidoras na América Latina

É espantoso observar a situação regulatória brasileira em comparação com outros países latino-americanos. Nos últimos anos, houve uma difusão de legislações gerais de proteção de dados pessoais em toda a América Latina, com a definição de direitos dos cidadãos e criação de mecanismos de cumprimento de tais direitos via agências reguladoras (autoridades administrativas de proteção de dados pessoais). Um levantamento feito pelo professor Nelson Angarita Remolina, da Universidade de Los Andes (Colômbia), mostra tal situação e destaca o avanço recente da proteção de dados pessoais em tais países.

Tabela 2. Proteção de dados pessoais na América Latina		
País	*Norma Constitucional*	*Legislação infraconstitucional*
Argentina	Art. 43, Constituição (1994)	Lei 25326/2000

[20] Danilo Doneda e Laura Schertel Mendes produziram um artigo recentemente afirmando que a proteção de dados no Brasil está virando um campo autônomo de regulação, sendo puxado principalmente pela proteção do direito do consumidor. As novas legislações de consumidor no Brasil, especialmente a de 2011, que trata de banco de dados, tenta positivar valores de transparência e controle, ao invés de privacidade como liberdade negativa. DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: *Reloading Data Protection*. Springer Netherlands, 2014. p. 3-20.
[21] LOURENÇO, Cristina; BALHE GUEDES, Maurício. A Internet e o Direito à Exclusão Definitiva de Dados Pessoais na Experiência Brasileira, in: LEMOS, Ronaldo; SALOMÃO LEITE, George (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014, p. 560-573.

		Decreto 1558/2001
Bolívia	Art. 130, Constituição (2004)	-
Chile	-	Lei 19628/1999 Lei 19812/2002 Lei 20575/2012
Colômbia	Art. 15, Constituição (1991)	Lei 1581/2012
Costa Rica	-	Lei 8968/2011
México	Art. 16, Constituição (2009)	Lei Federal 05-07-2010
Nicarágua	Art. 26, Constituição (1987)	Lei 787/2012 Decreto 36/2012
Paraguai	Art. 135, Constituição (1992)	Lei 1682/2001 Lei 1691/2002
Peru	Art. 2 e 200, Constituição (1993)	Lei 29733/2011 Decreto 003-2013-JUS
Uruguai	-	Lei 18331/2008 Decreto 414/2009

Fonte: Angarita Remolina (2014)

Os dados compilados por Angarita apontam, pelo menos, três tendências na América Latina: (i) a positivação de direitos de proteção de dados pessoais,[22] (ii) a criação de autoridades administrativas independentes ou semi-independentes para proteção de dados pessoais, e (iii) a criação de instrumentos jurídicos específicos para proteção de tais direitos.[23]

No Brasil, discute-se desde 2010 a criação de uma lei geral de proteção de dados pessoais. No entanto, tal projeto normativo está paralisado e encontra fortes resistências do setor privado, como será explicado na próxima seção.

[22] No México, tem-se utilizado a expressão "derechos ARCO" para denominar os direitos de acesso, retificação, cancelamento e oposição ao tratamento de dados pessoais.

[23] Na Nicarágua, por exemplo, criou-se a "ação para proteção de dados pessoais" que deve ser direcionada à *Dirección de Protección de Datos Personales*, órgão encarregado de conhecer e julgar a ação. Tal ação é cabível para: (i) conhecer os dados pessoais que foram objeto de tratamento em banco de dados, (ii) verificar violação de garantias de confidencialidade, integridade e segurança no tratamento de dados, (iii) conhecer a lesão de alguns princípios que gerem a qualidade do tratamento dos dados pessoais, no âmbito público e privado, (iv) acessar informações que se encontrem em poder de qualquer entidade público ou privada, (v) exigir a retificação, atualização, modificação, inclusão, complementação, supressão, bloqueio ou cancelamento de dados pessoais tratados em bancos de dados de entidade públicas ou instituições privadas (art. 48, Lei 787/2012, República da Nicarágua).

2. A discussão do anteprojeto de dados pessoais no Brasil

A. A construção do consenso na academia e no governo

As discussões sobre um anteprojeto de lei de proteção de dados pessoais foram resultantes de uma parceria do Ministério da Justiça com o Observatório Brasileiro de Políticas Digitais da Fundação Getulio Vargas do Rio de Janeiro, firmada há quase cinco anos.[24] Porém, antes do início da discussão pública do anteprojeto de lei de proteção de dados pessoais em novembro de 2010, algumas articulações foram importantes para a construção de consenso sobre o tema, ao menos dentro da comunidade especializada no assunto.

A primeira articulação, ao menos no plano intelectual, foi feita por alguns juristas brasileiros da área de direito civil e direito do consumidor. Os trabalhos de Danilo Doneda (2006) e Laura Schertel Mendes (2009), pelo que sei, foram os primeiros a tentar traçar um panorama da legislação brasileira e defender a ideia da adoção do "modelo europeu" (declaração de direitos e criação de órgãos reguladores independentes). Em razão dessa agenda normativa, tais juristas assumiram posições no governo (Ministério da Justiça) e em instituições privadas de formulação de políticas (Fundação Getulio Vargas). Uma vez que esses juristas assumiram determinadas funções no governo, passaram a divulgar a tese da necessidade de afirmação de direitos e regulação por uma autoridade administrativa especializada em proteção de dados pessoais.

Uma segunda articulação importante foi feita pelo Comitê Gestor da Internet (CGI.br). Além de tratar do tema em suas reuniões internas multissetoriais (governo, setor privado, comunidade técnica, academia e sociedade civil), o CGI.br passou a organizar um seminário anual sobre proteção à privacidade e aos dados pessoais, com participação de acadêmicos internacionais e profissionais de diferentes áreas de atuação.[25] Desde 2010, tal seminário tem servido como ponto nodal para a discussão da proteção de dados pessoais no Brasil e avaliação das políticas regulatórias propostas pelo governo.

Paralelamente ao Marco Civil da Internet, formou-se um relativo consenso no ano de 2010 – ao menos no Comitê Gestor da Internet, na academia e em setores

[24] Para um relato dessa iniciativa, cf. FGV-CTS, *Relatório de Políticas de Internet: Brasil 2011*. São Paulo: Comitê Gestor da Internet no Brasil, 2012, p. 53-59 (elaborado por pesquisadores do Centro de Tecnologia e Sociedade do Rio de Janeiro em parceria com o Comitê Gestor da Internet).

[25] Todas as informações sobre o evento estão disponíveis em: http://seminarioprivacidade.cgi.br/sobre-o-evento/

especializados do governo – sobre a necessidade de uma "lei abrangente para tutela do cidadão com relação a dados pessoais". Iniciou-se, então, o processo pré-legislativo de construção de um anteprojeto de lei que seria enviado pelo Executivo ao Congresso Nacional.

O governo federal utilizou o blog "Cultura Digital"[26] para publicar uma minuta para discussão desse anteprojeto. Com isso, mobilizou a sociedade civil e as empresas para participação ativa na elaboração do anteprojeto, fortalecendo um aspecto procedimental democrático.[27] Isso aconteceu entre novembro de 2010 a janeiro de 2011, com prorrogação do período de discussão para abril de 2011.

Segundo Juliana Pereira, da Secretaria Nacional do Consumidor, foram 700 contribuições de pessoas de diferentes setores: academia, ativistas, empresas do setor privado, associações, lobistas.[28] Assim, é crucial entender quem são esses atores e quais foram os posicionamentos relevantes na discussão da versão inicial proposta pelo Ministério da Justiça em parceria com os acadêmicos da FGV.

B. Avaliando a participação dos atores na discussão do anteprojeto de lei de proteção de dados pessoais

A partir de dados disponibilizados pela Associação Brasileira de Marketing Direto,[29] foi possível mapear alguns posicionamentos estratégicos de atores privados na discussão do anteprojeto. A ABEMD produziu um relatório de 250 páginas compilando as manifestações das empresas e entidades que apresentaram propostas de forma específica para os artigos, parágrafos, incisos ou alíneas do projeto de lei.[30] É partir desta fonte que as análises desta seção foram feitas.

Das vinte "entidades e empresas" participantes das discussões de 2010 e 2011, é possível segmentá-las em algumas categorias e avaliar a grau de influência formal de cada grupo (considerado a presença em tais discussões). No caso da discussão do APL de proteção de dados pessoais, tem-se o seguinte quadro de atores participantes:

---

[26] http://culturadigital.br/

[27] Nesse sentido, cf. VAZ, Ana Carolina. Neutralidade da Rede, Proteção de Dados Pessoais e Marco Regulatório da Internet no Brasil. *Revista Democracia Digital e Governo Eletrônico*, n. 5, 2011.

[28] Informação disponível em: http://www.conjur.com.br/2013-jan-28/texto-lei-protecao-dados-pessoais-ficar-pronto-janeiro

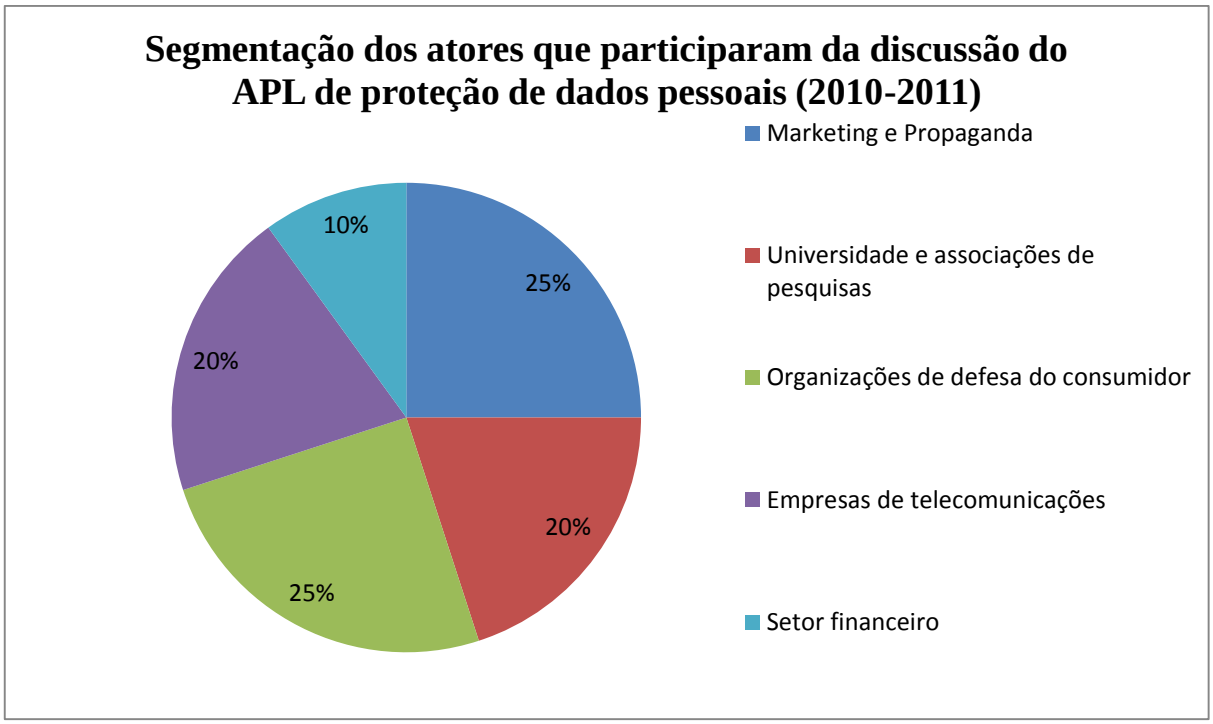
[29] http://www.abemd.org.br/

[30] O relatório produzido pela ABEMD, assinado por Efraim Kapulski, está disponível em: http://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf

Tabela 3. Segmentação dos atores no debate do APL de proteção de dados pessoais				
Empresas de marketing e propaganda	*Universidades e associações de pesquisa*	*Organizações de Defesa do Consumidor*	*Empresas de telecomunicações*	*Empresas do setor financeiro*
Associação Brasileira de Marketing Direto; Associação Brasileira das Relações Empresa Cliente; Qualidade de Informação Brasil; Associação Brasileira de Anunciantes; Equifax Brasil;	Comissão de Informática, Internet e Tecnologia; Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da USP; Câmara Brasileira de Direito Eletrônico; Organização Transparência Hacker	Comissão de Ciência e Tecnologia da OAB/SP; Instituto Brasileiro de Defesa do Consumidor; Fundação Procon São Paulo; Associação Brasileira de Defesa do Consumidor; Morrison & Foerster – Global Privacy Alliance (GPA)	Nokia S.A.; Associação Brasileira de Televisão por Assinatura; Telemar Norte-Leste S.A. (“Oi”); Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal;	Confederação Nacional das Instituições Financeiras; Associação Brasileira das Empresas de Cartões de Crédito e Serviços;
5 atores	4 atores	5 atores	4 atores	2 atores

Fonte: ABEMD (2011)

A partir da segmentação dos participantes, é possível visualizar a porcentagem de influência formal de cada grupo. Obviamente, essa análise compreende apenas aspectos quantitativos (quais atores em que número). Não é possível mensurar o grau de influência de cada um ou mesmo a capacidade de organização e lobby desses grupos. Ao menos no aspecto formal, é possível identificar uma distribuição relativamente equânime entre os atores, o que reforça o caráter democrático e multissetorial da discussão do anteprojeto de lei de proteção de dados pessoais em 2010 e 2011.



Fonte: ABEMD (2011)

A participação de tais atores proporcionou diversas polarizações e divergências em torno de conceitos e propostas normativas feitas pelo Ministério da Justiça em 2010.

Primeiro, houve divergência com relação ao conceito de "dado pessoal". O anteprojeto definia tal dado pessoal como "qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores". Tal definição foi combatida por alguns grupos. A ABEMD e a ABTA, por exemplo, opinaram pela supressão da parte final do inciso, por considerar que várias pessoas podem fazer uso do mesmo IP (*internet protocol*). A Equifax Brasil sustentou que seria inadequado que informações que identificassem indivíduos apenas de forma indireta fossem incluídas no texto legal, uma vez que trariam "sensível insegurança jurídica". Empresas de telefonia e a Câmara Brasileira de Comércio Eletrônico foram contrárias à inclusão do IP como dado pessoal.

Uma segunda discussão calorosa se deu em razão do artigo 9º do anteprojeto, que dizia: "o tratamento de dados pessoais somente pode ocorrer após o *consentimento livre, expresso e informado do titular*, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11". Nessa discussão, os atores se posicionaram de diferentes formas para defender conceitos

do que é "consentimento". Empresas de marketing defenderam a ideia de que consentimento é "qualquer meio que certifique a ciência do titular". A Confederação Nacional das Instituições Financeiras defendeu que o termo "notificação" era impróprio e deveria ser substituído pelo termo "comunicação". A Global Privacy Alliance (GPA) criticou o texto da lei e sustentou que o sistema de adesão expressa (*opt-in*) deveria ser reservado para situações nas quais mau uso dos dados possa gerar danos severos aos titulares. A OAB/SP, por outro lado, defendeu uma redação focada da publicização e transparência dos termos de coleta de dados.[31]

Tais discussões mostram a ausência de consenso em questões conceituais básicas do anteprojeto, como a própria definição de "dados pessoais" e "consentimento" para coleta e tratamento de dados. No entanto, o debate mais rico do anteprojeto é a questão da criação de uma autoridade garantidora para proteção de dados pessoais. É nesse tópico que determinados atores do setor privado se organizam para frear a iniciativa do governo.

C. Corregulação e autorregulação: mobilizações em torno do desenho regulatório

Desde o início das discussões do anteprojeto de proteção de dados pessoais, o Ministério da Justiça sustentou a necessidade de se criar um Conselho Nacional de Proteção de Dados Pessoais (ou uma Comissão Nacional), que figuraria como autoridade administrativa para garantia dos direitos de proteção de dados pessoais e monitoramento do setor privado e do governo.[32] O titulo II do anteprojeto (tutela administrativa) apresentava os seguintes artigos:

> Art. 38. É criado o Conselho Nacional de Proteção de Dados Pessoais, com autonomia administrativa, orçamentária e financeira, com a atribuição de atuar como Autoridade de Garantia quanto à proteção de dados pessoais, cuja estrutura e atribuições serão estabelecidas em legislação específica.
> Art. 39. Compete ao Conselho Nacional de Proteção de Dados Pessoais: I – zelas pela observância desta lei, de seu regulamento e do seu regimento interno; II – planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais; III – editar normas e provimentos sobre matérias de sua competência; IV – aprovar seu regimento interno; V – receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais,

[31] Redação sugerida pela OAB/SP: "O tratamento de dados pessoais somente pode ocorrer após autorização expressa do titular dos dados, através de documento ou outro meio qualquer afixado ou informado em local claro, de forma destacada e nítida dos demais contextos, indicando o fim que será utilizado".
[32] "Executivo elabora anteprojeto para proteção de dados pessoais", *Câmara dos Deputados*, 20/01/2011. Disponível em: http://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/192809-EXECUTIVO-ELABORA-ANTEPROJETO-PARA-PROTECAO-DE-DADOS-PESSOAIS.html

> nos termos do regulamento; VI – aplicar, de ofício ou a pedido da parte, conforme o caso, sanções, medidas corretivas e preventivas que considere necessárias, na forma desta lei; VII – criar, manter e publicar, para fins de transparência, um registro de banco de dados pessoais de caráter de categorias e setores que considere relevantes, nos termos do regulamento; VIII – verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados; IX – promover o conhecimento entre a população das normas da matéria e de suas finalidades, bem como das medidas de segurança dos dados; X – vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos do regulamento; XI – reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros que não contém com este nível adequado; XII – determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento, XIII – desenvolver outras atividades compatíveis com suas finalidades.

Na discussão do anteprojeto de dados pessoais ocorreu uma movimentação peculiar sobre esse tópico. A tabela abaixo sintetiza os argumentos apresentados por diferentes grupos com relação à criação do Conselho Nacional de Proteção de Dados.

Tabela 3. Posicionamento sobre a criação do Conselho Nacional de Proteção de Dados

Atores	*Posição*	*Argumentos e críticas*
ABEMD, ABRAREC, QIBRAS	Contra	"Entendemos desnecessária a criação da Autoridade de Garantia em razão de já existirem órgãos e entidades com capacidade de controle, fiscalização e sanção das normas estabelecidas neste projeto lei. (...) Opinamos pela total supressão do preceito".
ABDI	A favor	"Necessária a convocação da iniciativa privada para participar, inclusive do processo de elaboração de eventual regulamento".
ABTA	Contra	"Diversos órgãos do Estado podem cumprir esta função, tais como o DPDC, o Ministério Público, o PROCON. (...) A criação de tal instituição significa a criação de uma estrutura extremamente custosa e complexa, com poderes regulatórios que podem até mesmo embaraçar a garantia dos direitos fundamentais".
OAB/SP	A favor	"Defende que deve ser explicitada no próprio da lei a estrutura da Autoridade de Garantia" (composta por integrantes da sociedade civil e integrantes do Poder Judiciário).
GEPOPAI	A favor	"Inclusão de um parágrafo único dando um caráter

		multistakeholder para o Conselho, seguindo o modelo do Comitê Gestor da Internet".
Procon	A favor	"De suma importância a definição clara de sua estrutura e atribuições"
PROTESTE	A favor	"A entidade sugere que seja adotado um modelo de composição paritária, viabilizando a participação direta de órgãos governamentais, empresariais e entidades da sociedade civil, indicadas de forma democrática por cada um dos setores participantes".
SindiTeleBrasil	Contra	"Apresenta sua discordância em relação à criação de uma Autoridade Garantidora, entendendo que os direitos previstos neste projeto poderão ser adequadamente resguardados pela atuação de órgãos já existentes".

Fonte: ABEMD (2011)

Como visto acima, houve uma forte mobilização do setor privado e empresarial contra a criação da Autoridade Garantidora de proteção de dados pessoais. Segundo tais atores, já existem órgãos que poderiam executar as políticas de proteção de dados e garantir os direitos estabelecidos nesta lei. Com relação às posições da OAB e as instituições da sociedade civil, a crítica foi formulada no sentido de déficit participativo e democrático do arranjo institucional proposto. Para a OAB, juízes e membros da sociedade civil deveriam compor a estrutura da Comissão. Para os centros de pesquisa e de defesa do consumidor, o melhor modelo a ser adotado seria o do Comitê Gestor da Internet – conhecido pelo formato "multissetorial"[33] de deliberação, no qual empresas privadas, comunidade acadêmica, membros do governo e representantes da sociedade civil têm espaço para discussão horizontal.

Uma segunda discussão importante do modelo regulatório brasileiro centrou-se no artigo 45, que previa a possibilidade de elaboração de "códigos de boas práticas"[34] por parte do setor privado. Além de definir o caráter vinculante de tais códigos (entre os membros de uma determinada classe profissional), o anteprojeto estabelecia que os

[33] Para uma análise do arranjo institucional do CGI, cf. ADACHI, Tomi. *Comitê Gestor da Internet no Brasil (CGI. br): uma evolução do sistema de informação nacional moldada socialmente*. Tese de Doutorado. Universidade de São Paulo, 2009.

[34] Art. 45: "Os responsáveis pelo tratamento de dados pessoais, individualmente ou através de organizações de classe, poderão formular códigos de boas práticas que estabeleçam as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento e no uso de dados pessoais e demais quesitos e garantias para as pessoas, com pleno respeito aos princípios e disposições da presente lei e demais normas referentes à proteção de dados".

códigos deveriam ser "depositados na Autoridade de Garantia, que poderá não aprová-los em desconformidade com as disposições legais e regulamentares sobre a matéria, ao que seguirá uma solicitação para que sejam feitas as modificações necessárias e indicadas".

Contrariamente ao modelo existente na Europa e em países da América Latina, associações de direito de informática e de empresas de televisão e telecomunicações foram contrários ao modelo de "corregulação"[35] proposto pelo governo. Para tais atores, a Autoridade deveria ser apenas *comunicada de eventuais códigos formulados*, sem possibilidade de ingerência sobre o conteúdo.

Percebe-se, assim, uma tentativa de criação de um regime regulatório diferente do Europeu, mais pautado na autorregulação e na redução do papel da autoridade administrativa. Isso pode sugerir uma desconfiança por parte do setor privado com relação ao governo e suas autoridades administrativas. Parece não haver consenso para criação do modelo de corregulação – onde o Estado estimularia a produção de códigos de conduta pelo setor privado, validando tais regras e tornando-as vinculativas após a verificação de compatibilidade de seu conteúdo com a lei geral de proteção de dados pessoais.[36]

3. Para além do texto legal: desafios para a construção do modelo regulatório híbrido

A. Limites do Marco Civil da Internet

O Marco Civil da Internet é uma legislação baseada em princípios. Foi propositalmente concebida para esse fim: definir os valores básicos que a sociedade pretende proteger no uso da internet no Brasil. É ilusório pensar que a solução para os vários problemas jurídicos do uso da internet está na Lei 12.965/2014. A proteção de dados pessoais, por exemplo, está apenas definida como direito. Não há, por enquanto, garantia suficiente para uma adequada tutela dos dados pessoais no Brasil.

Tome-se, por exemplo, a questão da retenção de dados pessoais e a possibilidade de uma autoridade administrativa obter os dados guardados por provedores de aplicações de internet (art. 15, Lei 12.965/2011). Definiu-se como regra geral a retenção, para fins de

[35] "Um sistema de corregulação se caracteriza quando a autorregulação ocorre num segmento em que o Estado não abdica de suas funções normativa e supervisora. A atuação regulatória, privada e pública, neste sistema terá maior eficácia na medida em que a ação privada for complementar à pública e vice-versa". SANTANNA, Luciano. Autorregulação Supervisionada pelo Estado, *Revista de Direito Administrativo*, Rio de Janeiro, v. 257, maio/ago, 2011, p. 195-196.

[36] Para uma defesa da corregulação no Brasil, cf. SILVA, Rosane Leal. Cultura Ciberlibertária x Regulação da Internet: a corregulação como modelo capaz de harmonizar este conflito. *Revista Brasileira de Estudos Constitucionais*. Belo Horizonte, v. 6, n. 21, jan./mar. 2012.

investigação e finalidades policialescas.[37] No entanto, não há clareza sobre quais argumentos que a "autoridade policial ou administrativa ou o Ministério Público" devem oferecer para "requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações sejam guardados" (Art. 15, § 2º).

Determinou-se que tanto a extensão da retenção quanto a obtenção dependerão de ordem judicial. Porém, os critérios definidos no art. 22 são muito amplos ("fundados indícios da ocorrência do ilícito", "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória") e cabíveis para todo o tipo de ação ("processo judicial cível ou penal, em caráter incidental ou autônomo"). Isso abre espaço para pedidos e decisões não fundamentadas, que tornam a obtenção de dados a regra, ao invés da exceção.

É função da Autoridade Garantidora monitorar esses pedidos, fazendo com que os juízes apresentem fundamentações convincentes para disponibilização de dados pessoais por ordem judicial. A Lei de Proteção de Dados Pessoais precisa estipular, com maior precisão possível, quais são as autoridades administrativas que podem realizar os pedidos cautelares e sob quais justificativas. Não se pode criar um sistema frouxo no qual qualquer pedido é acatado, sob qualquer justificativa. A tutela constitucional da inviolabilidade das comunicações aplica-se igualmente aos dados pessoais, dados de conteúdo e dados de tráfego.[38]

Ainda, o Marco Civil da Internet não trata do uso indevido de dados pessoais por empresas privadas, para fins de propaganda comportamental.[39] A mera definição do "direito à proteção de dados pessoais" é insuficiente para proteger tal direito. É preciso pensar para além do direito positivo estatal.

---

[37] A adoção desse modelo único de retenção de dados tem sido criticada por acadêmicos da área, como Marcel Leonardi: "Lamentavelmente, o Marco Civil da Internet impôs um modelo de guarda obrigatória de dados para os provedores de aplicações, e não *facultativa*, como originalmente previsto. Adotou, assim, um modelo de preservação dos dados de forma indiscriminada, em oposição a um modelo de preservação dos dados efetivamente ligados a um ato ilícito praticado, o que implica tratar todos os usuários de Internet como suspeitos da prática de atos ilícitos, com sérias implicações para sua privacidade". LEONARDI, Marcel. A Garantia Fundamental do Direito à Privacidade e à Liberdade de Expressão nas Comunicações como Condição ao Pleno Exercício do Direito de Acesso à Internet, in: LEMOS, Ronaldo; SALOMÃO LEITE, George (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014, p. 624.

[38] Cf., como estudo representativo, GUARDIA, Gregório. *Comunicações Eletrônicas e Dados Digitais no Processo Penal*. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2012.

[39] HOOFNAGLE, Chris Jay *et al*. Behavioral Advertising: The Offer You Can't Refuse, *Harvard Law & Policy Review*, v. 6, p. 273-296, 2012. ANTONIALLI, Dennys. Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes. *Stanford Journal of Civil Rights & Civil Liberties*, v. 8, p. 323-367, 2012 (analisando as políticas de privacidade oferecidas por empresas localizadas nos EUA e o conflito de tal abordagem contratual e voluntarista com relação ao modelo constitucional de proteção à privacidade da Alemanha).

B. Enxergando a caixa de ferramentas do sistema regulatório híbrido

É importante discutir a possibilidade de outro modelo de proteção: o modelo regulatório híbrido. Nesta estratégia regulatória, pensamos a proteção de dados não somente por autoridades administrativas e lei, que seria apenas a categoria de "instrumentos regulatórios" (agências reguladoras, leis nacionais e uma estrutura administrativa). A ideia é pensar também em (i) acordos internacionais que vão tratar de proteção de dados, (ii) autorregulação via utilização de códigos de ética pelo setor privado, e uma coisa que é muito pouco discutido nas faculdades de direito ou no Ministério da Justiça, que é (iii) *a tecnologia e criptografia*. Ou seja, como é que nós conseguimos proteger privacidade e dados pessoais via programação, via códigos e via tecnologia.[40] É a ideia do *privacy by design*: imbuir na própria programação valores, como privacidade e a proteção de dados pessoais.[41]

O modelo regulatório híbrido baseia-se nessa caixa de ferramentas. Essa ideia é inspirada nos textos recentes do professor Colin Bennett e consistente com um influente ensaio de Jean-François Blanchette e Deborah Johnson escrito em 1998 e publicado em 2002, no qual se propõe:

> (...) que uma política compreensiva de proteção de dados seja pensada não como um único pedaço de legislação, a "bala de prata" que será aplicada para todos os domínios e resolver todos os problemas. Ao invés, uma política compreensiva deveria ser entendida como uma abordagem de política pública que faz uso de uma variedade de estratégias consistentes umas com as outras e que se reforçam mutuamente. Em outras palavras, uma política compreensiva é aquela que começa com um quadro de princípios gerais que definem padrões amplos para a proteção de dados. Os princípios gerais são então implementados em uma variedade de estratégias que incluem leis em domínios específicos, mercados estruturados, práticas de autorregulação e tecnologias que aumentem a privacidade (*privacy-enhancing technology*). Tal proposta é consistente com o insight de Lawrence Lessig de que o comportamento individual é regulado em quatro formas: pelo direito, pelas normas, pela tecnologia e pelo mercado. Lessig

[40] RUBINSTEIN, Ira S. Regulating Privacy by Design. *Berkeley Technology Law Journal*, v. 26, 2011, p. 1411 (discutindo a proposta política da Federal Trade Commission de incentivo ao *privacy by design*, escolha do consumidor simplificada e aumento da transparência para manejo dos dados).

[41] WORLF, Ralf *et al.*, Privacy by Design Through a Social Requirements: analysis of social network sites from a user perspective, in: GUTWIRTH, Serge *et al.*, *European Data Protection: coming of age*. London: Springer, 2013, p. 241-265 (enxergando uma tendência de proteção da privacidade pela programação, porém com enfoque na opção de privacidade feita pelo usuário ao utilizar um serviço como uma rede social).

> enfatiza como as quatro formas trabalham conjuntamente em formas de suporte mútuo (Blanchette & Johnson, 2002, p. 40).

Desde modo, é possível pensar a proteção de dados pessoais no Brasil a partir da perspectiva desse modelo regulatório híbrido, capaz de unir acordos internacionais, regulação estatal, autorregulação/corregulação e tecnologia. A tabela abaixo, baseada na proposta de Colin Bennett, exemplifica cada um desses elementos.

Tabela 5. Modelo regulatório híbrido para proteção de dados pessoais

Categoria	*Atores responsáveis*	*Instrumentos*
Acordos internacionais	Organizações de Estados	OECD Guidelines, Princípios da ONU, Acordos de comércio (*internet economy*)
Instrumentos regulatórios	Estado administrativo	Leis nacionais, agências reguladoras, autoridades garantidoras
Autorregulação	Empresas privadas e associações civis	Códigos de ética, códigos de conduta, selos de privacidade, standards técnicos
Tecnologia	Empresas privadas e programadores independentes	Criptografia, *privacy by design*, *privacy enhancing technologies*

Fonte: Bennett & Raab (2003)

Nesse modelo, há uma responsabilidade compartilhada para a proteção de dados pessoais. Estados nacionais podem elaborar acordos e criar instrumentos regulatórios específicos, porém as empresas privadas e a sociedade civil também assumem papéis importantes para a proteção de dados pessoais, via códigos deontológicos ou tecnologias que podem, por *default*, proteger os dados pessoais (anonimizando os dados ou criando ferramentas técnicas do tipo *do not track me*[42] ou *disconnect*[43]). Tal perspectiva também foi notada por Dennys Antonialli e Francisco Brito Cruz, reconhecendo as insuficiências e limites de uma abordagem regulatória pautada exclusivamente em instrumentos jurídicos, bem as insuficiências da tecnologia de proteger os cidadãos de violações e ofensas a direitos fundamentais:

[42] https://chrome.google.com/webstore/detail/donottrackme-online-priva/epanfjkfahimkgomnigadpkobaefekcd
[43] https://disconnect.me/

> Sozinha, a tecnologia não dá conta de imunizar cidadãos contra violações e abusos. Novos mecanismos para burlar eventuais barreiras tecnológicas sempre podem ser criados. É nesse sentido que o uso da tecnologia deve se aliar ao direito nacional ou internacional. Limites devem impor não só deveres aos Estados - como o respeito à vida privada -, mas também assegurar ao cidadão mecanismos de controle sobre suas informações pessoais. Democracias devem usar o direito como ferramenta de regulação, servindo de escudo para a tutela do direito à privacidade em detrimento de modelos de negócio que possibilitem o acúmulo desse enorme volume de dados pessoais (...). A possibilidade de formação desses bancos de dados expõe o usuário às mesmas lentes nefastas da "teletela orwelliana". O fato é que os modelos de negócio que imperam na rede hoje propiciam campo livre para a vigilância governamental. Deixar de regulamentar a coleta de dados (privadas e estatais) por meio da criação de barreiras tecnológicas ou jurídicas é negar uma ferramenta preciosa à autonomia do indivíduo e à sociedade democrática (Antonialli & Brito Cruz, 2013).

Nessa proposta, global e local se unem, reconhecendo também que a arquitetura dos dispositivos na internet moldam condutas e regulam o comportamento humano – conforme pensou Lawrence Lessig.[44] Direito e tecnologia assumem papéis complementares para a proteção de valores sociais.[45]

C. Desafios de uma agenda: atores e papéis

Quais são os desafios para a construção desse modelo de proteção de dados pessoais capaz de unir leis, códigos de conduta e programação? No Brasil, eles são vários. Primeiramente é preciso enxergá-los para, em seguida, traçarmos estratégias de superação de tais obstáculos.

Primeiro, é preciso superar o "ocultismo" do debate sobre proteção de dados pessoais. Ele ainda é muito restrito e muito pouco conhecido.[46] Em geral, a população brasileira ainda não percebe a importância da proteção de dados pessoais. Por tal motivo, é fundamental a existência de uma (i) política nacional de proteção de dados pessoais e de uma (ii) agência especializada na disseminação desses valores. Nós precisamos de um órgão que crie políticas públicas para proteção de dados pessoais, em termos de educação e de conscientização. Precisamos de campanhas educacionais (o que muitos chamam de

[44] LESSIG, Lawrence. *Code 2.0*. New York: Basic Books, 2006, p. 83-156 (capítulo "regulation by code").
[45] MOSES, Lyria Bennett. How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target, *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013.
[46] É certo que as relevações de Edward Snowden em junho de 2013 tiveram efeito na esfera pública. No entanto, a proteção de dados pessoais ainda é discutida em poucos centros de pesquisa em direito e tecnologia e em alguns departamentos de direito civil e direito do consumidor.

"data literacy").[47] A Comissão Nacional de Proteção de Dados Pessoais poderá funcionar como fomentadora de debates na esfera pública com relação à garantia de tal direito em um ambiente virtual descentralizado e crescentemente complexo.

Em segundo lugar, é preciso um mínimo de esforço para que ciências sociais e ciências exatas possam dialogar. É impossível uma discussão adequada sobre proteção de dados pessoais sem conhecimento dos aspectos técnicos que envolvem a criação, manejo e tratamento de bancos de dados por empresas e governos. Programadores e técnicos de informática precisam dialogar com juristas e reguladores. Infelizmente, ainda não há instâncias que fomentem esses debates no Brasil.

Terceiro, as empresas privadas precisam assumir papéis de transparência e conscientização de seus usuários e clientes. Os "termos de uso" são anunciados em letras miúdas e pouco atrativas.[48] A preocupação com o consentimento tem que ser substituída pelo diálogo e transparência sobre o uso de dados pessoais para finalidades diversas. As empresas podem – e devem – assumir posturas éticas, fazendo uso legítimo de dados pessoais. O *Chief Privacy Officer* de uma empresa deve assumir responsabilidades para cumprimento das regras colocadas pelo governo. Além disso, a sociedade civil pode se organizar e criar veículos de monitoramento de empresas e governos com relação à privacidade e proteção de dados pessoais.[49] Nos Estados Unidos da América, esse monitoramento da sociedade civil é feito de forma organizada e estratégica por associações como a *American Civil Liberties Union* (ACLU), a *Eletronic Frontier Foundation* (EFF), o *Center for Digital Democracy* (CDD) e a *Electronic Privacy Information Center* (EPIC). No Brasil, não há organizações da sociedade civil atuando de forma estratégica para proteção da privacidade. A questão ainda é tratada como uma pauta de direito do consumidor.

Toda a sociedade possui papéis para a construção dessa agenda. A responsabilidade não é somente de agentes públicos, mas também de acadêmicos, empresários, programadores e ativistas. Sem esse engajamento, não há possibilidade de uma "governança da proteção dos dados pessoais" no Brasil.

---

[47] A agência de proteção de dados pessoais do Uruguai, por exemplo, realiza campanhas de educação de proteção de dados no país e criou um concurso entre os professores sobre a melhor forma de ensinar esse assunto.

[48] Não é sem razão que a sociedade civil tem se mobilizado para atacar a "maior mentira da história da internet", como defendem os criadores do *Terms of Service Didn't Read*, na França. Cf. https://tosdr.org/

[49] BENETT, Colin. *The Privacy Advocates: resisting the spread of surveillance*. Cambridge: MIT Press, 2008.

Conclusão

Os juristas brasileiros tendem a acreditar que as leis são as únicas soluções para problemas sociais. No caso da proteção de dados pessoais, está claro que a Lei 12.965/2014 oferece apenas as diretrizes normativas para garantia desse direito. A proteção do cidadão diante da constante criação e utilização de bancos de dados, públicos e privados, dependerá de uma série de instrumentos à disposição da sociedade contemporânea: acordos internacionais, instrumentos regulatórios, códigos de conduta e a própria tecnologia. Não se trata de encontrar uma solução no Estado ou no mercado. A ideia de um modelo regulatório híbrido inclui agentes públicos e privados, tendo em mente o papel modulador da tecnologia e o papel mobilizador da sociedade civil.

O desafio brasileiro é muito grande. Além do atraso regulatório para proteção de dados pessoais, ainda há dissenso sobre (i) os conceitos que estruturaram o anteprojeto de lei de proteção de dados pessoais e (ii) o arranjo institucional da Comissão Nacional de Proteção de Dados Pessoais. Há resistência do setor privado para o modelo de corregulação.

Como argumentado, é fundamental que o Brasil tenha uma lei de proteção de dados pessoais e uma autoridade garantidora capaz de monitorar usos ilegítimos de dados de cidadãos por parte de governos e empresas. No entanto, a solução não está na simples adoção do modelo europeu. Códigos – sejam eles de conduta ou de programação – também regulam. Em um mundo digitalizado, o direito é insuficiente para a garantia de direitos. Reconhecer esse limite parece fundamental hoje.

Referências

ADACHI, Tomi. *Comitê Gestor da Internet no Brasil (CGI. br): uma evolução do sistema de informação nacional moldada socialmente*. Tese de Doutorado. Universidade de São Paulo, 2009.

ANGARITA REMOLINA, Nelson. Latin America and Protection of Personal Data: Facts and Figures (1985-2014), *University of Los Andes Working Paper*, 2014. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412091.

ANTONIALLI, Dennys. Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes. *Stanford Journal of Civil Rights & Civil Liberties*, v. 8, p. 323-367, 2012.

ANTONIALLI, Dennys; BRITO CRUZ, Francisco. Por Que a Privacidade Importa, *O Estado de São Paulo*, 16/06/2013.

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. *Understanding Regulation: theory, strategy, and practice*. Oxford: Oxford University Press, 2012.
BENNETT, Colin J.; RAAB, Charles D. *The Governance of Privacy*. Hampshire GB: Ashgate, 2003.
BENNETT, Colin. *The Privacy Advocates: resisting the spread of surveillance*. Cambridge: MIT Press, 2008.
BLACK, Julia. Decentring Regulation: understanding the role of regulation and self-regulation in a "post regulatory" world, *Current Legal Problems*, n. 54, p. 103-147, 2001.
BLANCHETTE, Jean-François; JOHNSON, Deborah G. Data retention and the panoptic society: The social benefits of forgetfulness. *The Information Society*, v. 18, n. 1, p. 33-45, 2002.
DALLARI, Dalmo A. O Habeas Data no Sistema Jurídico Brasileiro, *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 97, p. 239-253, 2002.
DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006.
DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: *Reloading Data Protection*. Springer Netherlands, 2014. p. 3-20.
FGV-CTS, *Relatório de Políticas de Internet: Brasil 2011*. São Paulo: Comitê Gestor da Internet no Brasil, 2012.
GUADAMUZ, Andrés. Habeas Data vs the European Data Protection Directive, *The Journal of Information, Law and Technology*, n. 3, 2001. Disponível em: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz/#fn17
GUARDIA, Gregório. *Comunicações Eletrônicas e Dados Digitais no Processo Penal*. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2012.
GUTWIRTH, Serge *et al.*, *European Data Protection: coming of age*. London: Springer, 2013.

HIRSCH, Dennis. The Law and Policy of Online Privacy: regulation, self-regulation, or co-regulation? *Seattle University Law Review*, v. 34, 2011, p. 441.
HOOFNAGLE, Chris Jay *et al*. Behavioral Advertising: The Offer You Can't Refuse, *Harvard Law & Policy Review*, v. 6, p. 273-296, 2012.
LAVI-FAUR, David. Regulation & Regulatory Governance, *Jesuralem Papers in Regulation & Governance*, working paper n. 1, feb. 2010, p. 4-9. Disponível em: http://regulation.huji.ac.il/papers/jp1.pdf
LEMOS, Ronaldo; SALOMÃO LEITE, George (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.
LESSIG, Lawrence. *Code 2.0*. New York: Basic Books, 2006.
MATTOS, Paulo *et al.* (org.). *Regulação Econômica e Democracia: o debate norte-americano*. São Paulo: Editora, v. 34, 2004.
MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, v. 79, p. 45-81, 2011.
MOREIRA, Egon. Qual é o Futuro do Direito da Regulação no Brasil?, in: SUNDFELD, Carlos Ari; ROSILHO, André (org.), *Direito da Regulação e Políticas Públicas*. São Paulo: Malheiros, 2014.
MOSES, Lyria Bennett. How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target, *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013.

RUBINSTEIN, Ira S. Regulating Privacy by Design. *Berkeley Technology Law Journal*, v. 26, 2011, p. 1411.

SANTANNA, Luciano. Autorregulação Supervisionada pelo Estado, *Revista de Direito Administrativo*, Rio de Janeiro, v. 257, maio/ago, p. 183-211, 2011.

SILVA, Rosane Leal. Cultura Ciberlibertária x Regulação da Internet: a corregulação como modelo capaz de harmonizar este conflito. *Revista Brasileira de Estudos Constitucionais*. Belo Horizonte, v. 6, n. 21, jan./mar. 2012.

VAZ, Ana Carolina. Neutralidade da Rede, Proteção de Dados Pessoais e Marco Regulatório da Internet no Brasil. *Revista Democracia Digital e Governo Eletrônico*, n. 5, 2011.

ZANATTA, Rafael; GLEZER, Rubens. Atraso Regulatório para Proteção de Dados no Brasil, *Valor Econômico*, Opinião, p. A-13, 01/10/2014.