O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE)

The Brazilian Personal Data Protection Bill in comparison to the new European Community Regulation 2016/679

Alexandre Veronese

Professor Adjunto de Teoria Social e do Direito da Faculdade de Direito da Universidade de Brasília - UnB. Doutor em Sociologia pela Universidade do Estado do Rio de Janeiro - UERJ. Coordenador do Grupo de Estudos em Direito das Telecomunicações (GETEL) da UnB.
veronese@matrix.com.br

Noemy Melo

Pesquisadora Associada do Grupo de Estudos em Comércio e Direito da Concorrência da Universidade de Brasília. Doutora em Direito pela Université de Paris II (Panthéon-Assas).
noemyaraujo@hotmail.com

Recebido em: 22.04.2017
Aprovado em: 21.07.2017

Áreas do Direito: Civil; Consumidor; Constitucional

Resumo: O artigo descreve as origens das normas referentes à proteção de dados pessoais no Brasil para comparar o atual Projeto de Lei 5.276/2016 com o Regulamento 2016/679 da União Europeia. O objetivo do artigo é estabelecer uma crítica ao Projeto de Lei brasileiro, sem descuidar de mencionar a necessidade de sua aprovação. Na primeira parte, é descrita a origem do conceito jurídico de informação, no âmbito da legislação referente aos arquivos estatais e privados. Depois, é evidenciada a construção do conceito de proteção à personalidade e às informações nas relações de consumo, no cerne do direito civil e do direito do consumidor. É indicado que o debate brasileiro houve por construir os conceitos jurídicos pertinentes à proteção de dados pessoais com foco na interpretação constitucional, culminando com o Marco Civil da Internet, que se

Abstract: The article describes the sources of the statutory legal norms that deal with personal data protection and the Brazilian Bill under debate in the Parliament in order to compare them with the actual European Union Regulation 2016/679. The main goal of the article is to provide some criticism over the Brazil Federal Bill 5,276/2016 without losing sight about its enactment importance. The first section describes the origin of the Brazilian legal concept of information, which was driven from administrative legal statutes concerning public and private archives. Afterwards, the next section shows the construction of the legal concept of personality rights in the Civil Code and the concept of the personal information protection in the Consumer Relations Code. A remark is made to demonstrate that the Brazilian legal community built such legal

afigura como uma norma eclética, uma vez que incide em diferentes ramos do direito público e do direito privado. Por fim, é descrito o Projeto de Lei de Proteção dos Dados Pessoais, sendo este comparado com o Regulamento 2016/679. São feitas três críticas. A primeira é a ausência de previsão no Projeto de Lei de meios administrativos para efetivação dos direitos previstos. A segunda está centrada na baixa capacidade de construir modelos legais que sejam hábeis a forçar as condutas das empresas. Por fim, a terceira se refere a vácuos normativos, em especial aos referentes à regulação do tratamento de dados pessoais para fins criminais, que é matéria regulada no direito comunitário europeu. A conclusão indica que o Brasil está atrasado na construção de uma legislação para proteção dos dados pessoais e que o debate legislativo deveria buscar o incremento de uma sinergia regulatória entre Internet, telecomunicações e comunicação social.

Palavras-chave: Direitos da personalidade – Dados pessoais – Projeto de Lei 5.276/2016 – Regulamento 2016/679 – União Europeia.

concepts with a fierce use of the constitutional law and that such operation culminated in the enactment of the Internet Civil Legal Framework, which can be tagged as an eclectic statute, because it covers a wide array of legal areas, both public and private. At last, the article details the Brazil Personal Data Protection Bill, which is compared to the European Union Regulation 2016/679. Three critics are made. The first is the absence of the administrative means to enforce the legal rights of the future statute. The second is the low capacity that the Brazilian system has to build legal models to regulate the private enterprises behavior. The third cover some absent legal topics, with special regard to the necessity of regulate the personal data treatments for criminal purposes, as European Union does. The conclusion indicates that Brazil is late about the enactment of a bill to build a system of personal data protection. In addition, it criticizes that would be important whether the legislative debate included some other communications' fields like telecommunications and broadcasting in a manner to bring more regulatory synergy.

Keywords: Personality rights – Personal data – Brazilian Federal Bill 5,276/2016 – Regulation 2016/679 – European Union.

1. Introdução: do direito público à proteção de dados pessoais privados

O objetivo[1] do presente trabalho é expor a existência de normas e conceitos jurídicos em uso no Brasil para a proteção de dados pessoais na Internet, em

1. O presente trabalho é derivado da apresentação realizada pelos autores em 13 de dezembro de 2016 na Université Paris Descartes, no colóquio *Propriété(s) et données*. Os autores

cotejo com a legislação da União Europeia sobre o tema, em especial o recente Regulamento Geral da Proteção de Dados– Regulamento 2016/679 UE. O tema guarda grande importância, a ponto de Judith Rochfeld considerar a possibilidade da emergência, no âmbito dos direitos da personalidade, do conceito de "pessoa e identidade digital" (*personne et identité numérique*), sobreposta à personalidade e à identidade social[2]. O panorama é similar no caso brasileiro. José Antônio Peres Gediel e Adriana Espíndola Corrêa elucidam que os riscos à violação da privacidade são concretos, seja pela ação potencial e lesiva do Estado, seja pela atuação das empresas[3]. No caso do Brasil, a ausência de uma legislação específica para proteção de dados pessoais na Internet não quer dizer que inexistam prescrições constitucionais e legislativas sobre o tema.

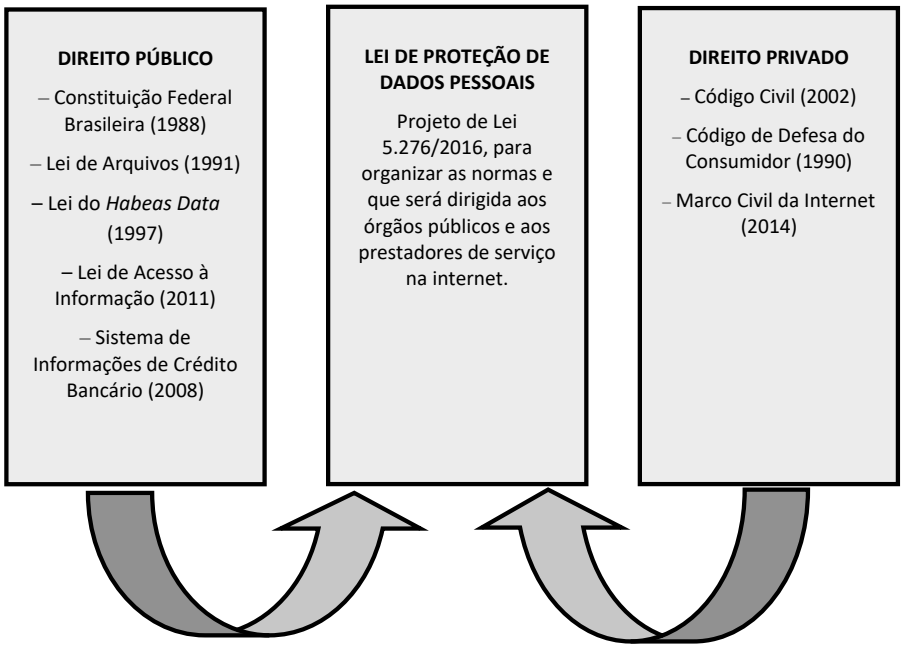
O Brasil recentemente aprovou uma lei para regulação geral da internet, chamada de Marco Civil da Internet (Lei Federal 12.985/2014), que possui a precisão de uma futura lei para proteção de dados pessoais. Para suprir tal lacuna, existe o Projeto de Lei 5.276/2016, que pretende criar novas bases à proteção de dados no país[4]. Porém, para compreender o atual Projeto de Lei, é necessário analisar a recente evolução histórica da legislação brasileira. Também é necessário compreender a construção interpretativa feita por parte da comunidade jurídica brasileira que, à míngua de uma legislação clara, alça os direitos da personalidade a um conjunto aberto de direitos, sem uma forma previamente definida, com amparo na aplicação

agradecem ao convite das organizadoras, Profa. Nathalie Marthial-Braz (Université Paris Descartes) e Profa. Célia Zolynski (Université de Versailles Saint-Quentin-en-Yvelines). Também agradecem à Fundação de Apoio à Pesquisa do Distrito Federal (FAP-DF) e à Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que viabilizaram o fomento à participação no referido evento.

2. ROCHFELD, Judith. *Les grands notions du droit privé*. 2. ed. Paris: Presses Universitaires de France, 2013. p. 71-72.
3. KLEE, Antonia Espíndola Longoni. A regulamentação do uso da Internet no Brasil pela Lei 12.965/2014 e a proteção dos dados e dos registros pessoais. *Direito & Justiça*, Porto Alegre, v. 41, n. 2, p. 126-153, jul.-dez. 2015.
4. Existem três projetos de lei no Congresso Nacional. O primeiro e mais antigo é o Projeto de Lei 4.060/2012, que é o mais incompleto de todos. O segundo é o Projeto de Lei do Senado 330/2013, que possui um texto mais elaborado que o primeiro, incluindo mais elementos da experiência internacional. Por fim, o terceiro é o Projeto de Lei 5.276/2016, cuja elaboração foi mais detalhada e próxima do modelo europeu. Ele é o melhor texto em tramitação, apesar de possuir alguns problemas e lacunas. Para uma análise comparada dos três projetos, cf. ARTIGO 19. *Proteção de dados pessoais no Brasil*: análise dos projetos de lei em tramitação no Congresso Nacional. São Paulo: Artigo 19 / Fundação Ford, nov. 2016, 35p.

direta de normas constitucionais ao direito civil[5]. Ao final dessa análise histórica, ficará evidente que a proteção de dados pessoais no direito brasileiro atual pode ser entendida a partir da seguinte imagem:

Figura 1. Imagem gráfica das origens jurídicas da proteção de dados pessoais



Fonte: autoria própria

A imagem *supra* evidencia que o tratamento e a proteção de dados pessoais, no Brasil, possuem duas origens diversas – o direito público e o direito privado –, e que estas não possuíam um espaço de conjugação analítica. Essa conjugação se deu pela ação dos intérpretes, a exemplo do que ocorreu em outros sistemas jurídicos, como bem elucida Danilo Doneda, ao examinar os ordenamentos italiano e português, no quais houve a expansão do direito à privacidade em direção aos direitos da personalidade e à proteção dos dados pessoais. Ambos os países fizeram tal expansão com amparo em textos constitucionais nacionais e na Carta dos Direitos Fundamentais da União Europeia. Esses textos constitucionais apresentavam disposições claras e específicas sobre o tema. No caso brasileiro, a operação interpretativa se deu pela mesma via, ou seja, pela expansão do direito fundamental à proteção da vida íntima e privada em direção aos direitos da personalidade e à proteção de dados pessoais. Todavia, no Brasil, essa expansão não encontrou amparo

5. MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, v. 20, n. 79, jul.-set. 2011. p. 45-82.

em disposições legislativas ou constitucionais diretas. Em suma, a diferença do Brasil em relação ao quadro jurídico europeu é a existência, no Direito Comunitário, da Carta dos Direitos Fundamentais, que contém um dispositivo específico para a proteção de dados pessoais, o artigo 8º[6], que vale ser visualizado:

> Artigo 8º Proteção de dados pessoais
>
> 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
>
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
>
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

No Brasil, a primeira fonte, ou origem, da proteção de dados pessoais está relacionada às informações pessoais armazenadas nos sistemas de registro estatal e ao direito dos cidadãos de conhecerem quais de seus dados estão arquivados junto ao Estado, bem como a exatidão deles. Portanto, a proteção de dados pessoais no Brasil remonta à Lei Federal 8.159/1991, legislação mais antiga, ainda em vigor, sobre arquivos. A segunda fonte de proteção de dados pessoais é uma evolução do direito à privacidade e dos direitos civis de personalidade com base em leituras constitucionais[7]. Da projeção dos direitos da personalidade – previstos no Código Civil de 1916 (Lei Federal 3.071/1916) e, depois, no Código Civil de 2002 (Lei Federal 10.406/2002) – constrói-se uma frágil proteção de dados pessoais.

O desafio contemporâneo, no Brasil, é aprovar uma legislação que seja aplicável tanto ao Poder Público quanto às relações privadas[8]. Essa pretensão está afirmada no Projeto de Lei 5.276/2016, da Câmara dos Deputados, pendente de aprovação. Isso porque, embora se verifique uma evolução, o Brasil está atrasado na regulação da proteção de dados pessoais se comparado a outros ordenamentos jurídicos. A União Europeia, por exemplo, acaba de aprovar um novo Regulamento (2016/679)

6. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 23-27.

7. TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v. 419, jan.-jun. 2014. p. 77-96.

8. Este é indicado como o ponto forte do Projeto de Lei 5.276/2016: MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, v. 9, ano 3, São Paulo, out.-dez. 2016. p. 38.

específico sobre o tema, que revogou a antiga Diretiva (94/46 CE) aplicável. O Chile e a Argentina também dispõem de leis específicas sobre o tema (Lei chilena 19.628/1999 e Lei argentina 25.326/2000)[9].

A literatura brasileira de direito da Internet, de uma forma geral, ignora que tanto a lei chilena quanto a lei argentina possuem origens similares com a Lei Federal 8.159/1991, do Brasil. Todas visam regular a gestão e a guarda de arquivos. A diferença central é que a legislação brasileira ignora expressamente a regulação dos arquivos privados, mencionando apenas que o Poder Público pode comprá-los, caso haja interesse público em sua manutenção. A legislação argentina, ao contrário, prevê a possibilidade de impetração de uma ação judicial de *habeas data* contra o gestor de arquivo privado (artigos 33 e ss.), o que no Brasil – pela Lei de arquivos – só é possível contra gestores de arquivos públicos. A lei chilena, igualmente, prevê direitos às pessoas privadas em face dos arquivos privados (artigo 12). Em suma, ausente a previsão de normas similares, o regramento da matéria dos arquivos privados no Brasil ficou, num primeiro momento, relegado aos direitos da personalidade e ao Código Civil. O centro do debate brasileiro estava dirigido às informações públicas. Tal panorama somente foi alterado com o advento do Código de Defesa do Consumidor (Lei Federal 8.078/1990). Todavia, com a expansão do uso de dados pessoais por empresas privadas, as prescrições do Código Civil e do Código de Defesa do Consumidor se mostravam insuficientes para lidar com o mundo contemporâneo, no qual o processamento maciço de dados apresenta (ou representa/constitui) um risco real e evidente aos cidadãos[10]. Em face da ausência de previsão de uma legislação específica no Brasil, autoras como Cláudia Lima Marques[11] e Laura Schertel Mendes[12] se esforçaram para, doutrinariamente, atualizar

9. Há debate na Argentina sobre a possibilidade de alteração na sua legislação por motivos vários, dentre os quais está o advento do Regulamento 2016/679: DIRECIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES. *Ley de protección de los datos personales en Argentina*: sugerencias y aportes recibidos em el proceso de reflexión sobre la necesidad de su reforma. Buenos Aires: Ministerio de la Justicia y Derechos Humanos, ago.-dez. 2016.
10. ZOLYNSKI, Célia. Big data et données personnelles: pour une meilleure gestion du risque informationnel. In: BEHAR-TOUCHAIS, Martine (Dir.). *L'effectivité du droit face à la puissance des géants de l'Internet*. Paris: IRJS Éditions, 2015. v. 1. p. 117-127; CARDON, Dominique. *À quoi rêvent les algoritmes*: nos vies à l'heure des big data. Paris: Éditions du Seuil/La République des idées, 2015.
11. MARQUES, Cláudia Lima; MENDES, Laura Schertel. O direito europeu muda nos contratos à distância e a domicílio: a nova Diretiva 2011/83 relativa aos direitos dos consumidores, das cláusulas abusivas, do crédito acessório ao consumo, da informação em geral e do comércio eletrônico. *Revista de Direito do Consumidor*, São Paulo, ano 21, n. 81, jan.-mar. 2012. p. 339-401.
12. MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, ano 24, v. 102, nov.-dez. 2015. p. 19-43.

a interpretação do Código de Defesa do Consumidor com atenção ao marco da proteção dos dados pessoais. Porém, isso não é suficiente, apesar da conclusão contrária de Ellen Carina Matias Sartori[13]. Uma legislação própria e um sistema administrativo de proteção específico, nos moldes do modelo europeu, continuam absolutamente necessários.

Feitas essas considerações, cabe ressaltar que o debate sobre a natureza e o conceito de "dados pessoais" ainda não é uma discussão fechada, como pode parecer pela leitura do Projeto de Lei 5.276/2016, que o define – seguindo a antiga Diretiva e o novo Regulamento – como "dado relacionado à pessoa natural identificada ou identificável" (art. 5º, I, do Projeto). Há necessidade de precisar melhor tal conceito, como bem coloca Marie-Anne Frisson-Roche sobre o conceito original, da norma europeia:

> No entanto, não podemos deixar de estar desconcertados por tal solução, que é pleonástica: é pessoal uma informação que concerne a uma pessoa... O pleonasmo parece ser a maldição que marca o dado e caracteriza a dificuldade de lhe definir. Passamos de pleonasmo em pleonasmo: o "banco de dados" é "definido" como um espaço no qual figuram os "dados diversos" tanto quanto o "dado pessoal" é "uma informação concernente a uma pessoa física identificável" [...]. Assim, do mesmo modo que Marcel Duchamp definia a obra artística como aquela que estava instalada no museu, o "dado pessoal médico" é definido como aquele que está inserido no prontuário médico. [...] Portanto, se não dispomos de uma verdadeira definição, logo deveremos nos resignar a aceitar que as conceituações somente valerão para um caso específico. É por isso que precisamos efetivamente nos reportar à prática decisória do Regulador, por natureza uma fonte de direito casuística, a qual produziu muitos detalhes, para evidenciar os pontos comuns fornecidos ao analista para os contornos de uma definição.[14]

A conclusão da autora é a mesma que é seguida aqui: há de se debater a regulação e a ação dos reguladores, pois dela se extrairá uma definição melhor para o conceito do objeto da proteção. O debate sobre a proteção de dados pessoais está diretamente relacionado à regulação. No caso brasileiro, todavia, o tema é mais complexo, pois a regulação da Internet precisa ser incluída em conjunto com os demais direitos relativos às atividades de comunicação. Assim, o maior problema do Brasil é a fragmentação regulatória e a desconcatenação de esforços em produzir

13. SARTORI, Ellen Carina Matias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na Internet. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, ano 3, out.-dez. 2016. p. 48-104.

14. FRISSON-ROCHE, Marie-Anne (Dir.). Penser le monde à partir de la notion de *donnée*. In: FRISSON-ROCHE, Marie-Anne. *Internet, espace d'interrégulation*. Paris: Dalloz, 2016. p. 8.

cooperação entre diferentes atores sociais para firmar padrões de comportamento, inclusive no campo da proteção de dados pessoais. Na próxima parte do texto serão descritas as normas de direito público, que marcaram o debate sobre a proteção de dados pessoais até o presente momento. Depois, serão analisadas as normas referentes ao direito privado, culminando com a Lei 12.965/2014 (Marco Civil da Internet)[15]. Por fim, será descrito o atual Projeto de Lei 5.276/2016 para que seja realizada a sua comparação com o modelo do Regulamento Geral de Proteção de Dados Pessoais.

2. O direito público brasileiro e a regulação do acesso à informação privada em bancos de dados do Estado

Ao longo das últimas décadas, várias prescrições relacionadas à proteção da vida privada e, por extensão, às informações de caráter pessoal foram incorporadas na Constituição Federal. Não obstante, deve-se destacar que não se objetivava a proteção de dados pessoais, ao contrário do que ocorreu em outros países, em especial na União Europeia. Também, cabe ressaltar que as prescrições constitucionais não estavam dirigidas às empresas; elas visavam proteger, primariamente, os indivíduos em face de outros indivíduos. Igualmente, as prescrições constitucionais não tinham por objetivo proteger os cidadãos do uso de seus dados pessoais pelos órgãos públicos. Em suma, o debate era restrito à proteção dos direitos da personalidade, em especial, da vida privada e da intimidade, conforme consta no art. 5º, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Um bom exemplo do caráter público da proteção de dados pessoais no Brasil está relacionado à regulação da utilização dos dados bancários. Estes possuem um regramento diverso, uma vez que existe um sistema unificado com informações dos correntistas, denominado Sistema de Informações de Crédito – SCR, que é mantido sob o controle do Banco Central do Brasil (BACEN). Esse sistema está baseado numa resolução administrativa do Conselho Monetário Nacional (Resolução 3.658/2008), que considera ser de responsabilidade do BACEN a manutenção do cadastro, o que não implica dizer que ele possa efetuar alterações no sistema. Tal competência é outorgada aos bancos, sendo o BACEN mero depositário das informações cadastradas.

Diante desse cenário, era muito comum que os cidadãos não conseguissem informações do seu próprio banco em relação às anotações feitas no SCR. Essa realidade

15. Todavia, será indicada adiante a dificuldade de inserir o Marco Civil da Internet como uma lei do ramo de direito civil.

começou a ser alterada pela jurisprudência do Superior Tribunal de Justiça (STJ), que, ao analisar alguns *habeas data* impetrados sobre a matéria, determinou ao presidente do BACEN que fornecesse os detalhes das informações previstas no SCR (HD 160, julgado em 2008; e HD 265, julgado em 2014). De fato, o *habeas data* é o remédio judicial para obtenção de informações públicas e para retificação de dados em sistemas, nos termos do art. 5º, LXXII, da Constituição Federal do Brasil. Verifica-se, assim, que nem a Constituição Federal brasileira traçou uma proteção administrativa de dados pessoais dos cidadãos em face do Estado. Uma proteção de dados pessoais arquivados, em registros públicos, só veio a ser normalizada com a promulgação da Lei 8.159/1991:

> Art. 4º Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Todavia, essa norma jurídica era bastante genérica e incapaz de regulamentar a complexidade da gestão das informações. O conceito de segurança da sociedade e do Estado é muito amplo e, por si mesmo, dificulta a construção de graduação de sigilos. Ainda, a própria gestão dos direitos da personalidade nos arquivos públicos era controvertida, não tendo sido resolvida pelo singelo dispositivo supratranscrito. Por fim, a referida legislação, ao contrário da lei argentina e da lei chilena, ignorou os arquivos privados como objeto de uma regulação protetiva. Diferentemente do caso chileno, no Brasil, a ação judicial de *habeas data* somente poderia ser impetrada contra um órgão estatal (Lei Federal 9.507/1997)[16].

Somente 20 anos depois é que o tema da gestão das informações pessoais nos sistemas públicos de arquivos veio a ser detalhada com a aprovação da Lei de Acesso à Informação (Lei Federal 12.527/2011). Esta apresentou, entre outras, as definições jurídicas de "informação" ("dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato": art. 4º, I) e de "informação pessoal" ("aquela relacionada à pessoa natural identificada ou identificável": art. 4º, IV) inexistentes antes

16. "Art. 7º Conceder-se-á *habeas data*: I – para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II – para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III – para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável".

no ordenamento jurídico brasileiro. A Lei também determinou aos órgãos públicos a necessidade de proteção das informações sigilosas e pessoais (art. 6º, III). Ainda, ela igualmente previu detalhes sobre a forma de gestão dessas informações pessoais. No art. 31, prevê-se a necessidade de proteção aos direitos da personalidade, e é mencionada a possibilidade do uso de informações pessoais por terceiros, desde que autorizados pelo titular dos dados (art. 31, § 1º, II e § 2º):

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

O mesmo artigo 31 prevê casos de exceção, nos quais não haveria a necessidade de um termo de consentimento: uso médico, uso estatístico e científico (com anonimato), determinação judicial, defesa dos direitos humanos e proteção do interesse público:

> Art. 31. [...]
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> III – ao cumprimento de ordem judicial;
>
> IV – à defesa de direitos humanos; ou
>
> V – à proteção do interesse público e geral preponderante.

O uso de informações pessoais – relacionadas à vida privada, à honra e à imagem – também é autorizado nas investigações de irregularidades e para estudos históricos:

> Art. 31. [...]
>
> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Por fim, a Lei de Acesso à Informação prevê a punição de condutas ilícitas dos agentes públicos de arquivos que divulguem dados sigilosos ou pessoais (art. 32, IV) e indica a responsabilidade objetiva dos órgãos e entidades públicas, bem como de entes privados que gerenciem dados estatais, quando for verificado dano por uso indevido de dados sigilosos ou informações pessoais (art. 34 e parágrafo único). A base de um sistema de proteção legal aos dados pessoais está, portanto, inicialmente desenhada na Lei de Acesso à Informação, ainda que esta esteja relacionada com um contexto diverso: a transparência nas ações estatais e a definição clara do sigilo que pode ser imposto aos documentos públicos, com base na razão de Estado.

É possível intuir, seguindo Laura Schertel Mendes, que o quadro jurídico brasileiro está a caminhar na direção do reconhecimento da proteção dos dados pessoais, em consonância com o modelo europeu[17]. Não obstante, existem algumas diferenças importantes. Não há no modelo brasileiro uma previsão sobre o "direito ao esquecimento", ainda que este tenha sido objeto de ações judiciais, com base nos direitos da personalidade[18]. Não há regras previstas sobre a proteção de dados pessoais na seara criminal. As regras aplicáveis às empresas deveriam ser mais claras. E, principalmente, inexiste uma autoridade independente, como está previsto no art. 8º (3) da Carta dos Direito Fundamentais da União Europeia.

3. O direito privado brasileiro e a ausência de normas específicas para a proteção de dados pessoais

Não existe legislação específica sobre a proteção de dados pessoais no Brasil. Todavia, tanto o Código Civil de 2002 (Lei Federal 10.406/2002) quanto o Código de Defesa do Consumidor (Lei Federal 8.078/1990) trazem prescrições referentes à vida íntima e à proteção da vida privada. O Código Civil contém uma previsão genérica de proteção que pode ser acionada entre pessoas privadas, em caso de violação da vida privada. Nesse sentido, o artigo 21 do Código Civil dispõe que

17. MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 160.

18. STJ, REsp 1.334.097/RJ (Globo Comunicações e Participações S.A. *versus* Jurandir Gomes de França), rel. Min. Luis Felipe Salomão, *DJe* 10.09.2013; BRASIL: STJ, REsp 1.335.153/RJ (Nelson Curi e outros *versus* Globo Comunicações e Participações S.A.), rel. Min. Luis Felipe Salomão, *DJe* 10.09.2013.

"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". Cabe ressaltar que esse artigo é o último dispositivo do capítulo do Código Civil dedicado aos direitos da personalidade. Podemos então concluir que as prescrições do Código Civil de 2002 estão adstritas ao conceito de intimidade (vida privada) e não estão relacionadas, diretamente, com as questões comerciais e com as bases de dados, sejam estas públicas ou privadas.

No Brasil, as questões comerciais referentes aos dados pessoais só foram previstas com a promulgação do Código de Defesa do Consumidor, que consagrou, em seu art. 43, o direito dos consumidores ao acesso de suas próprias informações registradas nos cadastros das empresas:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
>
> § 6º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Deve-se ressaltar que, diante da peculiaridade do regime do "*habeas data* brasileiro", que só pode ser utilizado contra órgãos e entidades estatais, o Código de Defesa do Consumidor, no § 4º do artigo 43, acabou consagrando uma interpretação extensiva da natureza "pública" dos bancos de dados e órgãos congêneres para possibilitar o uso do *habeas data* contra gestores privados. De fato, as regras brasileiras, como indicado ao longo do texto, estavam excessivamente focalizadas no direito público. Assim, não havia outra opção para proteger o consumidor.

Além da legislação civil, existem vários outros diplomas normativos que possuem disposições específicas que tratam do tema da privacidade, como a Lei de Informática (artigo 2º, VIII, da Lei 7.232/1984) e o Estatuto da Criança e do Adolescente (art. 100, V, da Lei 8.069/1990). Todavia, essas Leis não tratam especialmente dos dados pessoais. Elas tratam da necessidade de que a política nacional de informática crie meios técnicos e legais para a promoção da privacidade dos cidadãos – no caso da primeira lei – e que o desenvolvimento das crianças e dos adolescentes deve ser consentâneo com a proteção de sua intimidade e vida privada – no caso da última.

Em síntese, é evidente que a legislação brasileira não veio a tratar de uma forma mais específica a proteção de dados pessoais. Mesmo no caso das empresas fornecedoras de bens e serviços, inexistem normas referentes ao "*profiling*"[19] e ao direito ao esquecimento. Um bom exemplo de problema pode ser visualizado no estudo de Jorge Machado e Bruno Ricardo Bioni. Os autores avaliaram vários programas estaduais de incentivo à dedução de impostos de consumo. Tais sistemas são mantidos pelos Estados brasileiros e alimentados com dados das empresas e dos órgãos de fiscalização tributária. Na avaliação dos autores, inexiste a previsão de direitos relevantes, como a possibilidade de não se submeter ao programa, por parte do contribuinte e de apagamento dos dados. Cabe notar que os bancos de dados mantidos pela administração tributária são capazes de processar e analisar todas as compras de produtos feitas por consumidores brasileiros, sem que sequer haja qualquer pedido de consentimento e qualquer direito à informação, expressamente previsto[20]. Em outros setores empresariais, o quadro jurídico também não é claro. No caso dos bancos, foi longa a sua luta judicial em prol de não haver submissão deles ao Código de Defesa do Consumidor, o que afastaria a incidência da proteção ao cidadão prevista em seu art. 43. Todavia, a submissão dos bancos ao regime jurídico de proteção ao consumidor acabou por ocorrer após decisão do Supremo Tribunal Federal, nos autos da Ação Direta de Inconstitucionalidade (ADI) 2.591/DF, em 2006.

19. Trata-se da utilização de dispersos dados pessoais para a identificação de vários tipos de potenciais comportamentos de usuários, cujo uso mais típico é o *consumer profiling*, que visa direcionar ações de *marketing* (cf. GUNTER, Barrie. *The psychology of consumer profiling in a digital age*. London: Routledge, 2016). Uma visão crítica sobre a gestão dos dados pessoais na economia digital pode ser acessada em: ZOLYNSKI, Célia. Big data et données personnelles: pour une meilleure gestion du risque informationnel. In: BÉHAR-TOUCHAIS, Martine. *L'effectivité du droit face à la puissance des géants de l'Internet*. Paris: IRJS Édtions, 2015. p. 117-127.

20. MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal Paulista". *LIINC em Revista*, Rio de Janeiro, v. 12, n. 2, nov. 2016. p. 350-364.

4. Uma lei específica para a Internet brasileira: o Marco Civil (Lei 12.965/2014) e a proteção de dados pessoais

Após vários anos de debate, a Lei 12.965/2014 foi sancionada. É difícil restringir a aplicação da referida legislação somente ao campo do direito privado, apesar de ela ser denominada "Marco Civil". Como bem indicam José Augusto Fontoura e Marcos Wachowicz, o Marco Civil da Internet postula regular o uso da Internet no Brasil e acaba por ser uma legislação eclética[21]. Não obstante, o fato é que a regulação da Internet é marcada pela existência de contratos entre os prestadores de serviços de conexão e de conteúdo e os consumidores, e havia necessidade premente de estabelecer as balizas mínimas para essas relações jurídicas. Mesmo quando os consumidores não pagam, de forma direta, aos provedores de conteúdo, sabe-se que a sua visitação e exposição à publicidade configura fonte de receita para os sítios eletrônicos[22]. Logo, é possível inferir que há, portanto, uma relação de consumo. Todavia, o Código de Defesa do Consumidor não é suficiente para regrar a complexa teia de relações que se desdobram na navegação na Internet. O Marco Civil da Internet, portanto, é uma norma de direito privado, em muito assemelhada ao Código de Defesa do Consumidor. Ele prevê direitos padronizados para as partes, fixa elementos de princípios para políticas públicas e, também, prevê a formação de órgãos administrativos para imposição de sanções ao descumprimento de condutas legalmente previstas.

A Lei do Marco Civil da Internet previu que a proteção aos dados pessoais seria objeto de uma lei específica, a ser editada no futuro. De fato, quando da sua aprovação, em 2014, já havia um projeto de lei em tramitação sobre o tema, que acabou sendo substituído pelo Projeto de Lei 5.276/2016. A proteção aos dados pessoais figura como um dos princípios jurídicos do Marco Civil da Internet:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> [...]
>
> III – proteção dos dados pessoais, na forma da lei;
>
> [...]

21. FONTOURA COSTA, José Augusto; WACHOWICZ, Marcos. Cláusulas contratuais nulas no Marco Civil da Internet. *Revista da Faculdade de Direito da UFMG*, Belo Horizonte, n. 68, jan.-jun. 2016. p. 484.

22. BENABOU, Valérie-Laure; ROCHFELD, Judith. *À qui profite le clic? La partage de la valeur à l'ère numérique*. Paris: Odile Jacob, 2015; FARCHY, Joëlle; MÉADEL, Cécile; SIRE, Guillaume. *La gratuité à quell prix? Circulation et échange de biens culturels sur Internet*. Paris: Presses des Mines, 2015.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> [...]
>
> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> *a)* justifiquem sua coleta;
>
> *b)* não sejam vedadas pela legislação; e
>
> *c)* estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

O Marco Civil da Internet já traz algumas prescrições que são unanimemente aceitas como necessárias à proteção: obrigação de informação ao usuário sobre a coleta e seus limites; guarda responsável dos dados pelos provedores; necessidade de consentimento expresso do usuário para coleta; e possibilidade de exclusão dos dados, mediante pedido. Como bem observa Antônia Espíndola Longoni Klee, apesar de a referida Lei ser insuficiente enquanto quadro jurídico apto a fornecer plena proteção aos dados pessoais e equacionar os problemas relacionados às relações de consumo na Internet, ela é um passo importante por indicar a necessidade de uma legislação futura, além de firmar bases mais sólidas para o que se espera de uma efetiva legislação de proteção aos dados pessoais[23]. O novo Projeto de Lei de Proteção aos Dados Pessoais tramita em regime especial no Congresso Nacional do Brasil, em prol de sua celeridade para aprovação. Contudo, o processo legislativo no Brasil apresenta muita complexidade para que seja estimado o seu término em prazo razoável. O Projeto de Lei atual é evidentemente inspirado no Regulamento 2016/679 EU e é possível estabelecer uma comparação crítica entre a legislação europeia e o texto em tramitação.

23. KLEE, Antonia Espíndola Longoni. A regulamentação do uso da Internet no Brasil pela Lei 12.965/2014 e a proteção dos dados e dos registros pessoais. *Direito & Justiça*, Porto Alegre, v. 41, n. 2, jul.-dez. 2015. p. 126-153.

5. O atual Projeto de Lei de Proteção de Dados Pessoais no Brasil

O capítulo V do Regulamento 2016/679 UE estabelece – em seus artigos 44º a 50º – os padrões mínimos necessários para que haja o compartilhamento de dados entre os países europeus e países terceiros, como o Brasil. Ainda, o artigo 35º fixa condições que podem ser sumariadas da seguinte maneira: efetiva e completa predominância do Estado de Direito em vários níveis (art. 45º, 2, *a*); existência de uma autoridade de controle independente, com sujeição aos organismos internacionais (art. 45º, 2, *b*); e participação nos tratados internacionais sobre a proteção de dados pessoais (art. 45º, 2, *c*). Cabe notar que o Regulamento também é aplicável às relações comerciais, conforme se depreende da redação do art. 47º, com diversas regras vinculativas às empresas e aos grupos empresariais que se submetem à avaliação das autoridades de controle. De forma simplificada, o quadro comparativo a seguir evidencia como a elaboração do Projeto de Lei brasileiro foi inspirada na norma europeia:

	Projeto de Lei 5.276/2016	**Regulamento 2016/679 UE**
Objetivos da norma jurídica	Artigo 1º	Artigo 1º
Âmbito de aplicação material	Não há	Artigo 2º
Âmbito de aplicação territorial	Artigo 3º	Artigo 3º
Espaço de não incidência do Regulamento para tratamentos	–	Artigo 2º
Possibilidade de tratamento sem consentimento com base em interesse legítimo	Artigo 10	Não existe
Definições	Artigo 5º	Artigo 4º
Princípios relativos ao tratamento	Artigo 6º	Artigo 5º
Licitude do tratamento	Artigo 7º	Artigo 6º
Consentimento, em geral	Artigo 9º	Artigo 7º
Consentimento, no caso de menores – maiores de 16 anos; e tutela legal destes, no caso brasileiro	Artigo 14	Artigo 8º
Dados pessoais sensíveis	Artigos 11 e 12	Artigo 9º
Dados criminais	Não existe	Artigo 10º
Dados que não exigem identificação	Artigo 13	Artigo 11º

	Projeto de Lei 5.276/2016	Regulamento 2016/679 UE
Transparência aos titulares dos dados (direitos)	Artigo 8º	Artigo 12º
Dever de informar ao titular	Artigo 8º	Artigo 13º
Dever de informar de terceiro que detenha dados de titulares	Não existe	Artigo 14º
Direitos de acesso do titular aos dados	Artigo 8º	Artigo 15º
Direito de retificação	Art. 8º, VII, *a*	Artigo 16º
Direito de apagamento	Art. 18, VI	Artigo 17º
Direito de postular a limitação do tratamento	Não existe	Artigo 18º
Direito de obter resposta sobre a retificação, apagamento ou limitação de tratamento	Não existe	Artigo 19º
Direito à portabilidade dos dados	Artigo 18, V	Artigo 20º
Direito à oposição ao tratamento	Artigo 18, § 1º	Artigo 21º
Direito à oposição da participação na formação de perfil	Artigo 20 e parágrafo único	Artigo 22º
Limitações ou exclusão de incidência	Artigo 4º	Artigo 23º
Definição e função de responsável do tratamento	Artigos 36 e 37	Artigo 24º
Obrigação de técnicas mais avançadas, desenho do tratamento e certificação	Artigos 45 e 49	Artigo 25º
Responsabilidade solidária pelo tratamento	Artigo 44	Artigo 26º
Indicação de representante junto à UE	Não aplicável	Artigo 27º
Definição e função de operador/subcontratado	Artigos 36 e 37	Artigos 28º e 29º
Regras de registro das atividades	Artigo 37	Artigo 30º
Dever de cooperar com a autoridade de controle	Não existe	Artigo 31º
Deveres de segurança das informações	Artigos 45, 46 e 48	Artigo 32º

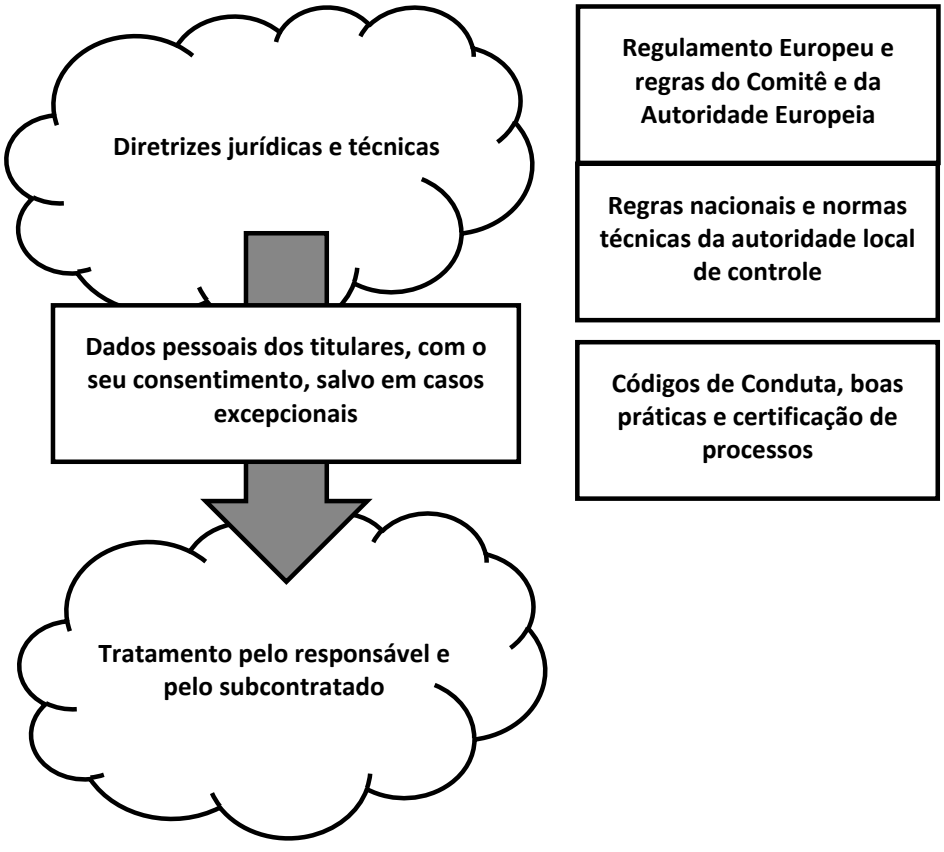
	Projeto de Lei 5.276/2016	**Regulamento 2016/679 UE**
Dever de notificar violação à autoridade	Artigo 47	Artigo 33º
Dever de notificar o titular dos dados	Artigo 48	Artigo 34º
Regras específicas para o poder público	Artigos 23 a 30	Artigo 35º
Avaliação prévia de impacto	Artigo 10, § 4º, artigo 12 e artigo 39	Artigo 35º
Dever de consulta prévia à autoridade	Não existe	Artigo 36º
Indicação de encarregado	Artigo 40 e artigo 24, § 1º (Poder Público)	Artigos 37º ao 39º
Códigos de conduta/boas práticas	Artigo 50	Artigos 40º e 41º
Certificação	Artigo 51	Artigos 42º e 43º
Intercâmbio de dados entre países	Artigos 33 a 35 e artigo 33, IV	Artigos 44º ao 50º
Regras obrigatórias e gerais às empresas e grupos	Artigo 34, §§ 1º e 2º	Artigo 47º
Previsão de regras globais das empresas e grupos para permitir intercâmbio	Artigo 34, §§ 2º e 3º	Artigo 47º
Restrição da cooperação internacional aos casos previstos em tratados	Artigo 33, II	Artigo 48º
Exceções possíveis para facultar intercâmbio	Artigo 33, III e VI	Artigo 49º
Determinação à ampliação da cooperação internacional	Não existe	Artigo 50º
Organização administrativa	Artigos 53 a 55	Artigo 51º a 76º
Direito de reclamação administrativa / direito de petição	Não existe	Artigo 77º
Direito de ação judicial	Não existe	Artigos 78º e 79º
Direito de associação coletiva dos titulares de dados	Não existe	Artigo 80º
Suspensão judicial de processos em prol da coerência de decisões na UE	Não aplicável	Artigo 82º
Regra geral de responsabilidade	Artigos 42 e 43	Artigo 82º

	Projeto de Lei 5.276/2016	Regulamento 2016/679 UE
Sanções administrativas	Artigo 52	Artigos 83º e 84º
Regras gerais de liberdade de expressão e informação	Não existe	Artigo 85º
Regras sobre documentos públicos	Não existe	Artigo 86º
Regras sobre identificação nacional	Não existe	Artigo 87º
Regras específicas para relações de trabalho	Não existe	Artigo 88º
Regras específicas para pesquisas científicas históricas e estatísticas	Artigo 11, II, *c*	Artigo 89º
Regras específicas sobre associações religiosas	Não existe	Artigo 90º
Dever de harmonizar regras de sigilo na UE	Não aplicável	Artigo 91º
Delegação de poderes ao Comitê	Vários trechos	Artigos 92º e 93º

Fonte: autoria própria

O projeto brasileiro segue a modelagem europeia. Todavia, ele utiliza uma terminologia menos clara e está redigido de uma forma ainda um pouco confusa, em comparação com a norma europeia. No sistema europeu, há um titular de dados pessoais, um responsável pelo tratamento dos dados e um subcontratado, além de um encarregado. Esse modelo é simples de ser visualizado: em síntese, o responsável define quais e como os dados serão processados. Ele pode assumir a responsabilidade e, também, efetuar o tratamento. O subcontratado realiza o processamento, do ponto de vista técnico, caso haja tal fato, sob as diretrizes do responsável. A norma europeia possui, ainda, a figura do representante, que pode ser indicado pelo responsável para lhe representar perante a autoridade europeia. A figura a seguir sintetiza – de modo simplificado – a partição de funções no modelo europeu.

Figura 2. Modelo gráfico para o tratamento de dados com proteção jurídica



Fonte: autoria própria

Após visualizar, panoramicamente, o Projeto brasileiro em cotejo com a legislação europeia, cabe destacar alguns pontos para comparação crítica. Em primeiro lugar, será criticada a definição frágil e vaga dada à autoridade brasileira de proteção aos dados pessoais. Em seguida será feita uma análise crítica da especificidade do regime de utilização de dados pessoais pelo Estado e da ausência de prescrições diretas às empresas.

5.1. As deficiências de proteção institucional no modelo do projeto brasileiro

O Projeto de Lei em discussão no Brasil possui um tamanho menor do que o Regulamento europeu. De plano, é possível notar que a norma projetada no Brasil não prevê detalhes sobre o futuro funcionamento do denominado órgão competente e do Conselho Nacional de Proteção de Dados e Privacidade, aludidos nos artigos 53 a 55 do Projeto. Assim, ou será necessária a ampliação da norma, para detalhar o

futuro órgão, ou será necessária outra legislação para definir sua estrutura administrativa. A norma europeia, por sua vez, prevê as diretrizes para as autoridades nacionais, para o Comitê Europeu e para uma Comissão[24]. O mesmo ocorre com várias disposições relacionadas à coerência no funcionamento coordenado das autoridades nacionais, com eventual suspensão de processos judiciais – em prol da coerência (artigo 82º do Regulamento) – e a previsão da harmonização de regras de sigilo (artigo 91º do Regulamento). Tais normas não são aplicáveis ao sistema brasileiro, a não ser que se estivesse propondo a realização de um tratado no âmbito do Mercosul.

Ainda sobre o futuro órgão, é bastante criticável que ele tenha sido desenhado de forma genérica e não como uma entidade estatal nos moldes de uma agência reguladora. Cabe anotar que, do conceito de órgão, não se deduz uma entidade autônoma. Há o risco de que esse órgão vire apenas um conselho na estrutura de um Ministério, o que colocaria em potencial risco a sua necessária independência. A criação de um comitê consultivo, existente no Projeto, tende a confundir mais do que auxiliar. Da forma como está previsto, o futuro órgão competente não terá uma estrutura administrativa própria que possa caracterizá-lo como uma "autoridade administrativa independente", conforme previsto no modelo europeu com base no artigo 8º da Carta dos Direitos Fundamentais da União Europeia. Dessa forma, corre-se o risco de reduzir-se o futuro órgão a um frágil conselho consultivo, dotado de poucos recursos, em razão da dificuldade do funcionamento da administração sem a definição de uma estrutura clara. A opção destoa da recomendação feita por Danilo Doneda, em 2006, ou seja, dez anos antes da submissão do presente Projeto de Lei:

> O que está em questão não é a emulação de um outro modelo estrangeiro, porém a devida consideração das características da matéria – e as balizas para tal operação serão a consideração da pessoa no ordenamento jurídico, em primeiro lugar, cotejadas com as possibilidades e especificidades do estado da tecnologia e da dimensão jurídica internacional da matéria [...]. A ação de uma autoridade para a proteção dos dados pessoais representa, portanto, a verdadeira realização de uma garantia institucional. [...]. Assim, o perfil de uma autoridade independente, baseada nos moldes de uma agência, parece o mais adequado[25].

Anote-se que a questão também se afigurava com problemática, no momento do debate sobre a proposta legislativa que deu ensejo ao Regulamento 2016/679,

24. Artigos 51º a 59º – autoridades nacionais. Artigos 60º a 62º – meios de cooperação. Artigos 68º a 76º – Comitê Europeu. Artigos 64º a 67º – Comissão e coerência.

25. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 400-402.

da União Europeia. Em volume coordenado por Nathalie Martial-Braz, o relatório de Céline Bloud-Rey é claro ao elucidar a necessidade de garantir que as diversas autoridades dos Estados-membros da União tenham recursos e pessoal em níveis adequados para que possam desempenhar suas funções de forma independente[26]. Em síntese, é necessário clarificar o futuro órgão, no Projeto de Lei, ao menos para indicar qual será o seu formato e seu corpo diretor.

5.2. Exígua previsão de sujeição das empresas ao sistema de proteção de dados pessoais e o curioso estatuto específico para o Estado

O artigo 3º do Projeto de Lei deixa claro que ele é aplicável ao Poder Público e às empresas. Todavia, parece claro que o Projeto brasileiro é menos detalhado do que o Regulamento Europeu no que tange às obrigações para as empresas. Talvez a menor quantidade de detalhes sobre as obrigações jurídicas de proteção de dados pessoais oponíveis às empresas pudesse revelar a ausência de vontade política de promover uma proteção mais radical no Brasil. Por essa hipótese que se compreenderia o fato de o Projeto de Lei possuir um leque de disposições vinculativas aplicáveis às empresas em menor quantidade, na comparação com o artigo 47º do Regulamento Europeu. Todavia, é importante transcrever a crítica de Josseline de Clausade ao projeto europeu no que concerne ao tratamento dado às empresas:

> Sobre a diversidade das empresas: das *startup* ao gigante mundial. [...] É de fato extremamente difícil legislar ao mesmo tempo para o Google e para a *startup* no setor digital, até porque todos os gigantes de hoje, como, por exemplo o Facebook, se desenvolveram a partir de *startup* as quais, no fim, dentre do ecossistema californiano e americano, encontraram poucos entraves de ordem fiscal, legal ou regulamentar e nenhuma restrição pelas autoridades da concorrência apesar de terem uma posição ultra dominante. Se os processos pesados, como todos os procedimentos prévios de conformidade previstos pelo projeto de regulamento poderão ser facilmente assimilados pelas enormes empresas – que podem lhes alocar todos os meios necessários –, eles serão inadequados ou muito pesados para as pequenas e médias empresas, cujos meios são limitados, já que suas estratégias são concentradas no seu crescimento[27].

26. BLOUD-REY, Céline. Quelle place pour l'action de l'autorité de contrôle? In: MARTIAL-BRAZ, Nathalie. *La proposition de règlement européen relatif aux données à caractère personnel*: propositions du réseau Trans Europe Experts. Paris: Société de Légilation Comparé, 2014. p. 305.

27. CLAUSADE, Josseline. Exposé sur le projet de règlement européen sur la protection des données personnelles. In : FAUVARQUE-COSSON, Bénédicte; ZOLYNSKI, Célia (Dir.). *Le cloud computing* – l'informatique en nuage. Paris: Société de Législation Comparée, 2014. p. 68.

A crítica anterior evidencia o risco de construir um excesso de obrigações que pode acabar por construir um ambiente prejudicial às empresas nascentes e inovadoras. Neste aspecto, o Projeto brasileiro acabou por não incorrer no excesso de obrigações, o que parece acertado, por um lado. Por outro, acaba por gerar certa indeterminação de futuras obrigações. Uma hipótese capaz de explicar essa disparidade remete ao costume jurídico de "legislar por decretos" ou simplesmente deixar certas questões em aberto para que estas sejam resolvidas em um momento futuro, muitas vezes com a necessidade de aprovação de uma nova lei. Cabe notar que alguns pontos cruciais da norma europeia não existem no Projeto de Lei brasileiro, tal como o dever dos responsáveis – Estado ou empresas – de informarem previamente sobre o tratamento de dados (artigo 36º do Regulamento), bem como a ausência de uma previsão de obrigação em cooperar com a autoridade independente (art. 31º do Regulamento). Essas omissões são graves, pois a ausência de colaboração prévia amplia a assimetria informacional entre a autoridade e os regulados, sejam eles públicos ou privados.

Ainda, a previsão de um capítulo específico ao tratamento de dados pessoais pelo serviço público é muito curiosa (artigos 23 a 30 do Projeto de Lei). O Regulamento europeu não previu um trecho da norma dedicado somente ao serviço público. Ele previu alguns casos, em razão de matérias ou áreas, nas quais haveria necessidade de tratamento de dados pessoais. Todavia, a generalidade da inclusão do serviço público não ocorre no Regulamento europeu. Uma explicação possível seria a complexidade administrativa do nosso País. O Brasil possui uma estrutura administrativa muito grande em razão do seu caráter federativo. Os Estados e o Distrito Federal são autônomos em relação à União, assim como os municípios são autônomos em relação aos Estados, ao Distrito Federal e à União. Outro tema peculiar e relacionado com o Estado é a possibilidade de tratamento de dados pessoais sem consentimento prévio com base no conceito de "interesse legítimo", tal como está previsto nos artigos 7º, II, e 10 do Projeto de Lei brasileiro:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> [...]
>
> IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.
>
> [...]
>
> Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular.

O grande problema reside no fato de que o conceito de "interesse legítimo" é indeterminado. Quem definirá o que é um interesse legítimo, se não existe um órgão forte e autônomo de controle? É certo que, para esses casos, o Projeto de Lei prevê diversas salvaguardas: a necessária simetria entre a expectativa do titular dos dados e o interesse do responsável (§ 1º do artigo 10); a oferta de possibilidade de oposição (§ 2º do artigo 10); a anonimização dos dados e a restrição do tratamento (§ 3º do artigo 10); e a possibilidade do pedido de uma análise de impacto prévio pelo órgão competente (§ 4º do artigo 10). Todavia, é sempre arriscado imaginar que um interesse legítimo e vago de uma empresa, ou de um ente estatal, possa fundamentar o tratamento de dados pessoais sem que haja a necessidade prévia de consentimento, além das hipóteses específicas listadas no artigo 11, II, do Projeto de Lei. Tal problema seria sanável com uma definição clara de autoridade independente, conforme antecipado anteriormente, já que o conteúdo efetivo das normas protetivas seria definido caso a caso[28]. Uma autoridade independente dotada de capacidade técnica e de meios administrativos poderia produzir previamente normas regulamentares que detalhassem o conceito de "interesse legítimo" e, autorizando, ou não, cada ação, poderia fiscalizar previamente os tratamentos baseados nesse conceito. Essa seria a melhor solução.

5.3. Vácuos normativos em comparação: áreas específicas de tratamento de dados, dados criminais e meios de proteção pelos cidadãos

Não parece que seria necessário ao Brasil incluir regras de incidência para o tratamento de dados de áreas específicas, como ocorreu no Regulamento europeu, tais como: documentos públicos (artigo 86º do Regulamento); identificação nacional (artigo 87º); relações de trabalho (artigo 88º) e atividades religiosas (artigo 90º). Não obstante, a ausência de uma norma específica para o âmbito criminal é criticável. A União Europeia fixou a Diretiva 2016/680 UE, ao passo que o Brasil não iniciou o debate do tratamento de dados pessoais em questões criminais, que é uma área muito delicada das políticas públicas atuais.

Por fim, a previsão de um direito de petição contra a autoridade ou contra o responsável pelo tratamento de dados não parece ser necessária no caso brasileiro (artigos 77º a 80º do Regulamento). Poderia ser feito, pois há uma tradição brasileira de repetir previsões constitucionais em normas legais e, afinal, o texto da Constituição Federal de 1988 prevê tal possibilidade. O mesmo ocorre com o direito de ação judicial individual e o direito de associação coletiva. Existem normas

28. Reitere-se a menção ao texto já citado: FRISSON-ROCHE, Marie-Anne (Dir). Penser le monde à partir de la notion de *donnée*. In: FRISSON-ROCHE, Marie-Anne. *Internet, espace d'interrégulation*. Paris: Dalloz, 2016. p. 7-16.

específicas no direito brasileiro que regulam a matéria. O modelo processual brasileiro aclimatou o conceito de *class actions* em um modelo de ação civil pública, que pode ser ajuizada por associações e por vários órgãos de representação pública, como a Defensoria Pública e o Ministério Público (Lei Federal 7.347/1985).

6. Conclusão

Ainda que o Projeto de Lei brasileiro possua alguns pontos que mereçam ser aprimorados, a sua finalidade parece clara e está bem alinhada com o Regulamento europeu, que lhe serviu de inspiração. É crucial reiterar a necessidade de que o Brasil construa um marco normativo para proteção de dados pessoais, já que a ação estatal em tal sentido vem sendo desenvolvida sem bases jurídicas adequadas, como bem indicou Laura Schertel Mendes:

> Entende-se que no âmbito da segurança de redes e da informação, o Brasil está diante de um desafio de construir um marco jurídico vinculante, que possa orientar normativamente os atores do setor público e privado sobre as medidas necessárias para garantir a segurança no processamento e no fluxo de informações. Se por um lado, há no país uma estrutura institucional que busca tratar da segurança da informação por meio do controle externo ou de protocolo de tratamento a incidentes de segurança, por outro, parece faltar exatamente a base normativa para apoiar a atuação desses órgãos.[29]

A necessidade de criação de bases jurídicas adequadas à proteção de dados pessoais em sintonia com o marco normativo europeu é evidenciada pelos recentes debates sobre a possível reforma da Lei de Proteção de Dados Pessoais na Argentina. Embora esta já fosse dotada de uma legislação compatível com o paradigma europeu, dispondo inclusive de uma autoridade administrativa especializada para a tarefa, o advento do Regulamento 2016/679 EU foi considerado um elemento importante a ser levado em conta para a adaptação da lei em vigor. Isso possibilitaria a Argentina obter vantagens competitivas em comparação com países atrasados na regulamentação de tais padrões de proteção de dados:

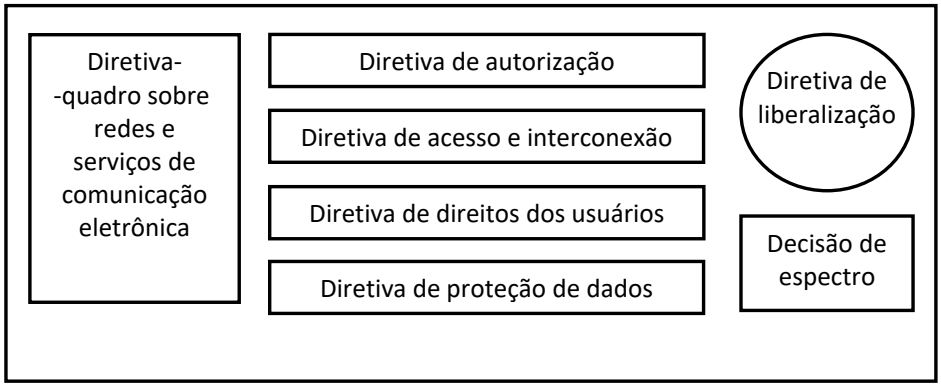
> Los participantes de las reuniones coincidieron en la necesidad de que la Ley 25.326 se adecuara al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante "Reglamento

29. MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. *Revista de Direito do Consumidor*, São Paulo, ano 22, v. 90, nov.-dez. 2013. p. 258.

> (UE) 2016/679"), para que Argentina siguiese siendo un país con nivel de protección adecuado conforme los lineamientos europeos y, por ende, continuara teniendo una ventaja comparativa en el mercado en relación a otros países con un nivel de protección no adecuado[30].

É visível a necessidade de debater o Regulamento Europeu e a aprovação de uma lei específica para proteção de dados pessoais no Brasil. Nesse sentido, o Projeto de Lei em tramitação possui méritos evidentes. Todavia, ele possui três grandes problemas. O maior problema da norma em questão é a ausência de diálogo desta com a esfera criminal. Como falar em proteção de dados pessoais sem pensar no seu uso em processos e investigações criminais? O segundo grande problema é a falta de um diálogo mais apurado acerca da regulação de tecnologias da informação e da comunicação no Brasil. Segundo Martin Fransman, o exemplo do Regulamento europeu demonstra que a proteção dos dados pessoais é parte de um quadro regulatório mais amplo composto pela Diretiva 2002/21/EC, que é a "diretiva-quadro" para redes e serviços de comunicações eletrônicas, bem como por discussões acerca de alterações normativas. A imagem a seguir sistematiza essa ideia:

Figura 3. O novo pacote regulatório para redes e serviços[31]



Fonte: autoria própria

É evidente que um quadro regulatório completo exige o diálogo com as normas que regem as atividades do setor de telecomunicações, de comunicação social e das

30. DIRECIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES. *Ley de protección de los datos personales en Argentina: sugerencias y aportes recibidos em el processo de reflexión sobre la necessidad de su reforma*. Buenos Aires: Ministerio de la Justicia y Derechos Humanos, ago.-dez. 2016. p. 11.

31. FRANSMAN, Martin. *The new ICT ecosystem*: implications for policy and regulation. Cambridge: Cambridge University Press, 2010. p. 146.

tecnologias da informação. Qualquer quadro normativo que não produza diálogo com esses segmentos da vida social será incompleto. Este elemento é central para a segurança da informação em vários setores empresariais do país, com destaque para os bancos, bem como para o setor público, como a informatização do Poder Judiciário e as demais ações de governo. Da mesma forma, órgãos estatais deveriam estar mais envolvidos nesse debate, em prol da construção de uma legislação viável e alinhada com o paradigma europeu. É certo, ainda, que deveria haver mais discussão no sentido de acoplar a norma projetada aos ditames de regras mais amplas, que regem as telecomunicações e a informática no Brasil. Ainda, o terceiro problema é a ausência de uma previsão de órgão administrativo específico para a realização da tarefa, cuja lacuna, na prática, complicaria sobremaneira a efetivação dos direitos previstos na futura. Não obstante, está claro que o Brasil deve seguir o caminho de firmar uma lei federal, de alcance nacional, para regular o tratamento dos dados pessoais, já que existem questões bastante graves de caráter social e de cunho comercial, tal como mencionado na introdução. Por fim, é importante destacar que a agenda brasileira de cooperação internacional nesse tema possui uma baixa expressão. Esse quadro precisa ser alterado, aumentando o diálogo em especial com a experiência europeia, para que uma eventual lei seja bem aplicada.

7. Referências bibliográficas

ARDON, Dominique. *À quoi rêvent les algoritmes*: nos vies à l'heure des big data. Paris: Éditions du Seuil/La République des idées, 2015.

ARTIGO 19. *Proteção de dados pessoais no Brasil*: análise dos projetos de lei em tramitação no Congresso Nacional. São Paulo: Artigo 19/Fundação Ford, nov. 2016.

BLOUD-REY, Céline. Quelle place pour l'action de l'autorité de controle? In: MARTIAL-BRAZ, Nathalie. *La proposition de règlement européen relatif aux données à caractère personnel*: propositions du réseau Trans Europe Experts. Paris: Société de Légilation Comparé, 2014.

CLAUSADE, Josseline. Exposé sur le projet de règlement européen sur la protection des données personnelles. In: FAUVARQUE-COSSON, Bénédicte; ZOLYNSKI, Célia (Dir.). *Le cloud computing* – l'informatique en nuage. Paris: Société de Législation Comparée, 2014.

DIRECIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES. *Ley de protección de los datos personales en Argentina*: sugerencias y aportes recibidos em el processo de reflexión sobre la necessidad de su reforma. Buenos Aires: Ministerio de la Justicia y Derechos Humanos, ago.-dez. 2016.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FARCHY, Joëlle; MÉADEL, Cécile; SIRE, Guillaume. *La gratuité à quell prix? Circulation et échange de biens culturels sur Internet*. Paris: Presses des Mines, 2015.

FONTOURA COSTA, José Augusto; WACHOWICZ, Marcos. Cláusulas contratuais nulas no Marco Civil da Internet. *Revista da Faculdade de Direito da UFMG*, Belo Horizonte, n. 68, p. 477-496, jan.-jun. 2016.

FRANSMAN, Martin. *The new ICT ecosystem*: implications for policy and regulation. Cambridge: Cambridge University Press, 2010.

FRISSON-ROCHE, Marie-Anne (Dir.). Penser le monde à partir de la notion de *donnée*. In: FRISSON-ROCHE, Marie-Anne. *Internet, espace d'interrégulation*. Paris: Dalloz, 2016.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. *Revista da Faculdade de Direito da Universidade Federal do Paraná*, Curitiba, v. 47, p. 141-153, 2008.

GUNTER, Barrie. *The psychology of consumer profiling in a digital age*. London: Routledge, 2016.

KLEE, Antonia Espíndola Longoni. A regulamentação do uso da Internet no Brasil pela Lei 12.965/2014 e a proteção dos dados e dos registros pessoais. *Direito & Justiça*, Porto Alegre, v. 41, n. 2, p. 126-153, jul.-dez. 2015.

MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal Paulista". *LIINC em Revista*, Rio de Janeiro, v. 12, n. 2, p. 350-364, nov. 2016.

MARQUES, Cláudia Lima; MENDES, Laura Schertel. O direito europeu muda nos contratos à distância e a domicílio: a nova Diretiva 2011/83 relativa aos direitos dos consumidores, das cláusulas abusivas, do crédito acessório ao consumo, da informação em geral e do comércio eletrônico. *Revista de Direito do Consumidor*, São Paulo, ano 21, n. 81, p. 339-401, jan.-mar. 2012.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, ano 24, v. 102, p. 19-43, nov.-dez. 2015.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, ano 20, v. 79, p. 45-82, jul.-set. 2011.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. *Revista de Direito do Consumidor*, São Paulo, ano 22, v. 90, p. 245-261, nov.-dez. 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, ano 3, p. 35-48, out.-dez. 2016.

ROCHFELD, Judith. *Les grands notions du droit privé*. 2. ed. Paris: Presses Universitaires de France, 2013.

SARTORI, Ellen Carina Matias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na Internet. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, ano 3, p. 48-104, out.-dez. 2016.

TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v. 419, p. 77-96, jan.-jun. 2014.

ZOLYNSKI, Célia. Big data et données personelles: pour une meullieure gestion du risque informationnel. In: BEHAR-TOUCHAIS, Martine (Dir.). *L'effectivité du droit face à la puissance des géants de l'Internet*. Paris: IRJS Éditions, 2015. v. 1.

Pesquisas do Editorial

Veja também Doutrina

- Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016, de Laura Schertel Mendes e Danilo Doneda – *RDCC* 9/35-48 (DTR\2016\24540);
- Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet, de Ellen Carina Mattias Sartori – *RDCC* 9/49-104 (DTR\2016\24542); e
- Proteção de dados, de Rafael Pinheiro Rotundo – *RDPriv* 74/133-158 (DTR\2017\80).