Revista de
Direito Econômico e
Socioambiental

ISSN 2179-8214

REVISTA DE DIREITO ECONÔMICO E SOCIOAMBIENTAL

vol. 12 | n. 2 | maio/agosto 2021 | ISSN 2179-8214

Periodicidade quadrimestral | www.pucpr.br/direitoeconomico

Curitiba | Programa de Pós-Graduação em Direito da PUCPR

Revista de
Direito Econômico e Socioambiental

doi: 10.7213/rev.dir.econ.soc.v12i2.27156

ISSN 2179-8214

Impactos da Lei Geral de Proteção de Dados nas Instituições Financeiras Bancárias

Impacts of the General Data Protection Law on Brazilian Financial Institutions

Bianca Cavalli Almeida[*]
Centro Universitário das Faculdades Metropolitanas Unidas (Brasil)
biancacavallialmeida@gmail.com

Jorge Shiguemitsu Fujita[**]
Universidade de São Paulo (Brasil)
jorge.fujita@fmu.br

Como citar este artigo/*How to cite this article*: ALMEIDA, Bianca Cavalli; FUJITA, Jorge Shiguemitsu. Impactos da Lei Geral de Proteção de Dados nas Instituições Financeiras Brasileiras. **Revista de Direito Econômico e Socioambiental**, Curitiba, v. 12, n. 2, p. 281-303, maio/ago. 2021. doi: 10.7213/rev.dir.econ.soc.v12i2.27156

* Mestre em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (São Paulo – SP, Brasil). Especialista em Direito Empresarial e Econômico pela Faculdade Paulista de Pesquisa e Ensino Superior (São Paulo – SP, Brasil), em Direito Tributário pela Faculdade Damasio de Jesus (São Paulo – SP, Brasil), e em Finanças e Gestão Pública pela Faculdade São Braz (Curitiba – PR, Brasil). Pós-graduanda em Direito Público Avançado pelo IBMEC (São Paulo – SP, Brasil). Membro da Comissão de Direito Digital da OAB SP Seccional Tatuapé. E-mail: biancacavallialmeida@gmail.com.

** Professor Emérito e Titular de Direito Civil na Graduação, na Pós-Graduação "lato sensu" do Centro Universitário das Faculdades Metropolitanas Unidas (São Paulo – SP, Brasil); do Curso de Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas (São Paulo – SP, Brasil); do Curso de Pós-Graduação "stricto sensu" da Faculdade de Direito da Universidade de São Paulo (São Paulo – SP, Brasil); do Curso de Pós-Graduação "lato sensu" da Escola Superior de Advocacia da Ordem dos Advogados do Brasil, Seção de São Paulo – SP (São Paulo – SP, Brasil); e do Curso de Pós-Graduação da Faculdade de Direito da Universidade Estadual de Londrina (Londrina – PR, Brasil). Doutor em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (São Paulo – SP, Brasil). Coordenador do Curso de Pós-Graduação "lato sensu" em Direito de Família e das Sucessões da Faculdades Metropolitanas Unidas (São Paulo – SP, Brasil). Consultor jurídico do Comitê de Bioética do Hospital do Coração - HCor. Editor Resp. da FMU Direito Revista Eletrônica. Associado do Instituto dos Advogados de São Paulo, da Associação dos Advogados de São Paulo e da Associação dos Antigos Alunos da Faculdade de Direito da USP. E-mail: jorge.fujita@fmu.br.

Recebido: 21/06/2020 Aprovado: 01/09/2021
Received: 06/21/2020 *Approved: 09/01/2021*

Resumo

O presente artigo versa sobre a adaptação pelas instituições financeiras brasileiras à Lei Geral de Proteção de Dados (nº 13.709/2018), analisando os principais desafios à sua implementação no segmento. Ainda, o estudo possui o escopo de identificar os riscos legais apontados pela doutrina e pelos relatórios técnicos em segurança da informação à proteção dos dados pessoais, principalmente com o advento das novas tecnologias utilizadas pelo setor, como também verificar possível relação conflituosa entre a proteção de dados ora normatizada e a legislação regulatória atinente aos bancos. Por fim, será investigada a dicotomia entre o desenvolvimento da economia de dados e a necessidade de proteção aos dados pessoais do consumidor bancário.

Palavras-chave: direito bancário; proteção de dados pessoais; o*pen banking*; segurança cibernética; consumidor bancário.

Abstract

This article deals with the adaptation by Brazilian financial institutions to the General Data Protection Law (nº 13,709/2018), analyzing the main challenges to its implementation in the segment. Also, the study has the scope of identifying the legal risks pointed out by the doctrine and technical reports on information security to the protection of personal data, especially with the advent of new technologies used by the sector, as well as to verify possible conflicting relationship between the data protection now standardized and the regulatory legislation related to banks. Finally, the dichotomy between the development of data economy and the need to protect the personal data of the banking consumer will be investigated.

Keywords: *banking law; protection of personal data; open banking; cybersecurity; banking costumer.*

Sumário

1. Introdução

Dados pessoais são o novo (petr)óleo da internet e a nova moeda do mundo digital[1] (EUROPEAN COMISSION EU, 2009). Com tal afirmação da Comissão União Européia do Consumidor em palestra apresentada em 2009, pode-se afirmar a primordial a necessidade de identificar e destacar quais são os direitos e deveres relacionados aos usos de dados pessoais dos cidadãos, de forma a garantir tal proteção ao direito do consumidor.

Decerto, o fenômeno da globalização econômica guiou o aumento das relações à distância, potenciadas pelos avanços na tecnologia, e pela melhoria nas transações eletrônicas, bem como pelo forte fluxo de capitais, pessoas e bens, realizado à escala internacional. Contudo, o consumidor que se utiliza das benéfices de soluções, serviços e produtos ancorados em novas tecnologias, por vezes desconhecem a destinação de seus dados pessoais concedidos para realização de determinado negócio, ou ao menos não desconfiam da amplitude do uso destes dados na prática.

Como bem pontua Victor Drummond (2003, p.05), "a tecnologia deixa o cidadão comum à mercê das corporações e dos governos no que diz respeito à manutenção, ou ainda, à manipulação dos dados e informações a si referentes".

Importante ressaltar que o ecossistema financeiro está à frente de outros mercados quando se trata de implementar o plano de ação para a implementação da Lei Geral de Proteção de Dados, nº 13.709/2018, norma que corrobora a transformação dos negócios no setor[2]. Além de ser o setor que mais investe em tecnologia e segurança da informação, tradicionalmente atende uma série de regulamentações, haja vista sua eficácia em autorregulamentação (FEBRABAN, 2019).

Como rol exemplificativo, podem-se destacar legislações vigentes que devem ser observadas pelas instituições financeiras em seus negócios

[1] Tradução livre de: "Personal data is the new oil of the internet and the new currency of the digital world". Meglena Kuneva - European Consumer Commissioner - Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling. Discurso proferido por Meglena Kuneva, European Consumer Commissioner, na mesa redonda sobre coleta de dados online, direcionamento e perfilação. Bruxelas, 31 mar. 2009. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156. Acesso em: 12 jun.2020.

[2] Plataforma NOOMIS CIAB FEBRABAN. Bancos se preparam para cumprir Lei de proteção de dados. Edileuza Soares, publicação de 30/05/2019. Disponível em: https://noomis.febraban.org.br/temas/regulacao/bancos-se-preparam-para-cumprir-lei-de-protecao-de-dados. Acesso em: 05 abr. 2020.

hodiernamente: Constituição Federal de 1988 (Direito à Privacidade – artigo 5º, X), a Lei de Sociedades Anônimas (Lei nº 6.404/1976); Lei de Valores Mobiliários (Lei nº 6.385/1976); Código de Defesa do Consumidor (Lei nº 8.078/1990); Crime de Lavagem de Dinheiro (Lei nº 9.613/1998, atualizada em 2003 e 2012); Lei de Sigilo Bancário (Lei Complementar nº 105/2001); Código Civil (Lei nº 10.406/2002); Banco de Dados para histórico de Crédito (Lei nº 12.414/2011); Lei de Acesso à informação (Lei nº 12.527/2011) e Crimes Cibernéticos (Lei nº 12.737/2012).

Assim, cumpre questionar neste artigo o conflito entre o cumprimento de tais exigências amparadas no arcabouço legal acima descrito e a observação de preceitos dispostos na LGPD, considerando que a nova lei estabelece como coletar, armazenar e compartilhar os dados pessoais e sensíveis de clientes e consumidores, tanto por meios físicos quanto digitais.

Importante destacar que estão sujeitas às normas da LGPD empresas públicas e privadas, independentemente de dimensão e segmento da economia, que atuam no país e usam dados pessoais em suas operações. O objetivo precípuo é proteger os direitos fundamentais de liberdade e privacidade das pessoas naturais.

Certamente, a promulgação da Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018) brasileira propiciou um espectro diferente para o cenário regulatório. Antes desta, o Brasil contava com o Marco Civil da Internet (nº 12.965/2014) e leis esparsas para regular a proteção de dados, embora o setor financeiro já dispusesse de ambiente de proteção de dados robusto, em virtude da necessidade de atender à sua autorregulação oriunda da Federação Brasileira de Bancos (FEBRABAN), conforme supramencionado, como também à regulação do Conselho Monetário Nacional (CMN) e ao Banco Central do Brasil (BCB) (BRASIL,2014;2018).

Como organizações que de forma basilar se preocupam pela adequação à LGPD, os bancos brasileiros se organizam desde a promulgação da referida lei para garantir a conformidade das operações financeiras e assim assegurar os direitos de privacidade dos consumidores bancários, como também usuários do sistema, considerando que a norma disciplina o tratamento de dados pessoais dos cidadãos pelas organizações que ofertam produtos e serviços no país.

Há que se mencionar que a LGPD é um divisor de águas na relação entre os clientes e as instituições financeiras, por deixar claro que o

cidadão é o proprietário de seus dados, adquirindo direitos até então sem proteção. É o caso do direito de exclusão (ou direito ao esquecimento), pelo qual o cliente pode solicitar que seus dados sejam excluídos da base de dados da instituição pela qual manteve relacionamento.

A problemática que se pretende abordar neste artigo, ainda, está voltada para a necessidade de enquadrar o tratamento dos dados pessoais do consumidor bancário, dados estes que já estão sob a posse dos bancos, em uma das previsões legais existentes na norma em questão, o inciso IX do artigo 7º da referida lei, que versa sobre o interesse legítimo do controlador no uso do dado pessoal[3].

Abordar-se-ão, ainda, os princípios elencados na norma objeto central desta pesquisa, e em quais deles o setor financeiro precisa ater especial relevância.

Neste contexto, busca-se também verificar os desafios para a proteção de dados frente à disponibilização do *Open Banking*[4] no Brasil e possível incompatibilidade de tal proteção legal com a lei de cadastro positivo (Lei nº 12.414/2011), outrora mencionada, além da preocupação do setor por medidas de segurança efetivas em ambiente virtual (BRASIL, 2011).

Outrossim, a lei exigirá que os negócios dessa área modifiquem todas as suas regras de segurança e privacidade digital para se alinharem com o novo cenário, considerando que os consumidores deverão contar com um uso de dados mais transparente, objetivo e eficaz, caso contrário, os negócios estarão sujeitos a multas, perdas de clientes e eventual dano reputacional à marca.

A metodologia do artigo fundamenta-se na técnica analítica, na qual são avaliados os aspectos formalistas da sistematização das regras e normas jurídicas, com foco no ordenamento jurídico e suas relações internas, associado ao enfoque hermenêutico interpretativo.

[3] O artigo 7º, inciso IX traz expresso que o tratamento do dado pessoal poderá ser realizado "quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

[4] O Comunicado nº 33.455, de 24 de abril de 2019, expedido pelo Banco Central do Brasil - BACEN, estabeleceu os requisitos fundamentais para a implementação do Sistema Financeiro Aberto no Brasil, conhecido como *Open Banking* e o definiu como compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação.

2. Lei Geral de Proteção de Dados e os diplomas legais relativos às atividades financeiras

Inicialmente, faz-se relevante destacar que a lei brasileira é inspirada na *General Data Protection Regulation* (GDPR), a Regulamentação Geral de Proteção de Dados, criada pela União Europeia (UE) e vigente desde maio de 2018. Ressalte-se que, atualmente, todos os países que formam o bloco econômico europeu são obrigados a cumprir a GDPR (COMISSÃO EUROPEIA, 2020).

Imperioso ainda mencionar que a norma foi criada como uma espécie de diretriz geral para toda a sociedade, sem tratar de detalhes relativos às diferentes indústrias. No entanto, as iniciativas pelo setor financeiro, que têm por objetivo facilitar o exercício dos direitos dos titulares (as pessoas de quem se coletam os dados), o controle dos tratamentos de dados e a demonstração de sua efetividade são indiscutivelmente necessárias.

Danilo Doneda, ao examinar a questão de uma regulamentação geral em detrimento a regulamentações setoriais referentes à proteção de dados, afirma que:

> Algumas normativas específicas de proteção da pessoa surgem então em torno de necessidades - específicas (...). Este é, aliás, um paradoxo com o qual deparamos: a unidade do ordenamento e do valor da pessoa humana coexiste com uma multiplicação sem precedentes nos quais é realizada a tutela. Sem menosprezarmos o perigo fragmental do próprio conteúdo da tutela em diversas peculiaridades setoriais, esta situação justifica um apego aos direitos fundamentais e seus instrumentos de legitimação, tanto mais forte quanto justificado por esta finalidade específica, que ao unificarem a tutela da pessoa, exercem igualmente outra função: ordenar um sistema que tende ao caos. (DONEDA, 2006, p. 100).

Visto que a área de serviços financeiros lida com vários dados sensíveis, que dizem respeito a hábitos muito íntimos dos consumidores, e também que seu tratamento pode impactar questões de igualdade e isonomia da população brasileira por meio de um potencial impacto positivo na inclusão ou em decisões por parte das instituições financeiras que gerem ou reforcem a exclusão financeira, reforça-se a necessidade de

uma regulamentação setorial acerca do uso de dados pessoais na prestação de serviços financeiros.

Outrossim, a LGPD visa a diminuir a assimetria informativa entre os titulares e os controladores da coleta de dados, no que diz respeito às finalidades de uso das informações coletadas. Assim, a lei define direitos das pessoas referentes ao acesso aos seus dados em poder do controlador, a possibilidade de retificá-los em caso de erros, a portabilidade para outra organização, além da revogação do termo de consentimento, relevante tema para o segmento.

Conforme publicação da Escola Nacional de Defesa do Consumidor - ENDC acerca da proteção de dados de caráter pessoal:

> A abundância da informação passível de ser obtida sobre o consumidor pode caracterizar uma nova vulnerabilidade do consumidor em relação àqueles que detêm a informação pessoal. O acesso do fornecedor a estas informações é capaz de desequilibrar a relação de consumo em várias de suas fases, ao consolidar uma nova modalidade de assimetria informacional. Esta nova assimetria informacional não se revela somente no poder a que o fornecedor pode ascender em relação ao consumidor ao tratar suas informações pessoais, porém também em uma nova modalidade de modelo de negócio na qual a própria informação pessoal se objetiva como *commodity*, como um ativo que pode chegar a ser o eixo de um determinado modelo de negócios. (ENDC, 2010, p. 09).

De fato, o setor financeiro lida com dados pessoais extremamente importantes, tais como nome, CPF, perfil de crédito, ativos e dívidas do consumidor, os quais necessitam de uma proteção específica por parte do Estado, pois são questões que interferem diretamente na economia e na vida do cidadão.

No entanto, os contornos jurídicos do tratamento de dados pessoais pelas instituições financeiras são delineados a partir de diálogo das fontes entre vários diplomas legais, a seguir expostos.

Ponto relevante na LGPD diz respeito à privacidade de dados pessoais, sendo esta, em ordem primária, direito fundamental previsto na Constituição Federal Brasileira de 1988 no artigo 5º, X[5] (BRASIL, 1988).

Exemplo usual relacionado ao tema, é o julgamento do repetitivo realizado pelo Superior Tribunal de Justiça (STJ) sobre "*credit scoring*", ou mais precisamente, a atividade de tratamento de dados com escopo de gerar uma pontuação que será utilizada na atividade bancária ou de crédito para avaliar a possibilidade de liberação de um valor a um determinado cliente.

Do acórdão, que reconheceu legítima a atividade de geração de *score* e reforçou a ausência de necessidade de autorização prévia do consumidor para sua criação, destaca-se o seguinte:

> 1) O sistema "*credit scoring*" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). 2) essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n.12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da **tutela da privacidade e da máxima transparência nas relações negociais**, conforme previsão do CDC e da Lei nº 12.414/2011." (BRASIL, 2014. Grifos nossos).[6]

Diante da fundamentação acima do relator do acórdão, faz-se necessário clarificar que as instituições financeiras estão sujeitas, desde 2001, a uma lei específica no tratamento de dados de seus clientes, que versa sobre o dever de manter o sigilo das relações financeiras confiadas a cada uma das Instituições. A Lei Complementar 105 de 10 de janeiro de 2001 (Lei do Sigilo Bancário), é a normativa principal sobre o tema de privacidade para os bancos e demais empresas listadas em seu artigo 1º, e

[5] Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: 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

[6] Julgamento do Recurso Especial 1457199/RS, tendo como relator o Ministro Paulo de Tarso Sanseverino. Decisão publicada em 17 de dezembro de 2014.

provocou ao longo dos últimos anos mudanças consideráveis no que tange à segurança da informação ou segurança cibernética no segmento.

A Lei do Sigilo Bancário propiciou vantagem para as instituições financeiras no cenário LGPD, já que a nova lei brasileira também traz em seu texto exigências quanto a quesitos mínimos de segurança, pontos estes que os bancos já têm atendidos, não apenas em função da mencionada lei complementar de 2001, mas também pelas regulamentações do Banco Central do Brasil, órgão regulador do setor a respeito do tema.

No que se refere ao sigilo bancário, supracitado, a regra geral do sistema financeiro prima pela manutenção do sigilo dos dados pessoais e bancários do cliente. Todavia, existem regras que caminham desde a necessária divulgação até o sigilo, como informações que possam afetar o mercado que não possam ficar sob proteção desta norma, ou, até mesmo em função de fatos relacionados à prática de crime de lavagem de dinheiro, por exemplo.

Ainda com relação à fundamentação do acórdão, há que se mencionar a Lei do Cadastro Positivo, nº 12.414/2011, alterada recentemente pela Lei nº 166/2019. Na respectiva lei, fora adotado o modelo *opt in*, ou seja, o consumidor deveria fazer a opção para integrar o cadastro. A nova Lei do Cadastro Positivo altera o modelo para *opt out*, ou seja, todos estão incluídos no cadastro positivo até a manifestação de vontade em sentido contrário (cancelamento do cadastro) (BRASIL, 2019).

Em verdade, quando se editou a Lei nº 12.414/2011, as entidades de proteção ao crédito já estavam em processo de ampliação do número e espécies de informações pessoais que são coletadas, armazenadas e divulgadas para o mercado. O argumento preponderante refere-se ao volume e a variedade dessas informações, quanto maior melhor será a avaliação do risco da concessão de crédito, destacando-se a possibilidade de redução do *spread* bancário e concessão de taxa de juros menor para consumidores com um bom histórico de crédito (BRASIL, 2011).

Em favor do tomador do empréstimo (consumidor), o principal argumento é a possibilidade de redução de juros em face de um bom histórico de crédito, considerando que um maior número de informações (entre estas profissão, rendimentos pessoais, hábitos de consumo, patrimônio, comprometimento do orçamento mensal em razão de outros empréstimos) possui importantes efeitos nas atividades vinculadas ao crédito, destacando-se: (1) melhora da avaliação dos riscos de eventual

inadimplência do tomador do empréstimo; (2) possibilidade de se estabelecer uma taxa de juros menor para o consumidor com um bom histórico creditício; (3) constituição de "dispositivo" de disciplina do consumidor; (4) educação do comportamento do consumidor, evitando situações de superendividamento (JAPPELLI; PAGANO, 2003, p. 17-18).

Neste contexto, se o titular de dados não desejar a abertura do cadastro positivo, basta manifestar sua vontade assim que for comunicado (art. 4º, § 4º). Realizada a abertura do cadastro, deve o gestor, no prazo de 30 dias, comunicar ao consumidor a referida abertura.

Na mesma comunicação, o titular dos dados deve ser informado "de maneira clara e objetiva os canais disponíveis para o cancelamento do cadastro no banco de dados" (art. 4º, § 4º, III). Esclarece a lei que a comunicação deve ser sem custo e que pode ser realizada diretamente pelo gestor ou por intermédio de determinada fonte (credor).

A coleta das informações, todavia, deve ser legítima, sob pena de macular a nota atribuída ao consumidor. Em outros termos, deve observar os pressupostos indicados pela LGPD, entre os quais cabe destacar o princípio da boa-fé objetiva, finalidade, adequação e necessidade. Ademais, "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" (art. 7º, § 3º, da LGPD) (BRASIL, 2018).

Um dos grandes desafios da implementação da Lei do Cadastro Positivo é conciliar o segredo empresarial com a necessidade de transparência ao consumidor sobre os critérios utilizados para pontuação do titular de dados. A política, exigida pelo dispositivo, deve indicar as informações e como são coletadas, além de elementos que são considerados para compor a nota do consumidor. É direito do consumidor saber quais comportamentos e dados pessoais elevam ou reduzem sua pontuação.

A salutar necessidade de transparência, exigida pelo art. 7º-A, deve sugerir atos e condutas financeiramente saudáveis que, ao final, elevam a pontuação do consumidor, ensejam a obtenção de taxa de juros mais reduzida. O consumidor deve ser informado sobre em que medida seu histórico de crédito (cadastro positivo) pode afetar a sua nota (BRASIL, 2019).

De fato, esta lei contraria os dispositivos do Código de Defesa do Consumidor, da Lei de Sigilo Bancário e, principalmente, a Lei Geral de

Proteção de Dados, em um dos seus aspectos mais importantes, que é a autodeterminação informativa do cidadão, pois permite a abertura de cadastro e compartilhar informações cadastrais com outros bancos de dados.

No que tange à segurança cibernética de dados bancários, a Resolução 4.658, de 26 de abril de 2018, refere-se exclusivamente à atividade de tratamento ou processamento de dados e computação em nuvem[7]. Tal regulação trouxe às instituições a necessidade da criação de uma Política de Segurança Cibernética específica, bem como a obrigação de prever nos contratos que possuem como objeto esses serviços, desde que considerados relevantes, cláusulas-padrão que visam a garantir a segurança dos dados bancários, como também permitir uma maior visibilidade pelo Banco Central do Brasil quanto ao processamento de informações em ambiente externo a cada um dos bancos.

Por fim, vale ressaltar que na economia moderna baseada em dados é importante que os bancos estejam atentos à LGPD, preocupando-se com o que deve ser adotado para a proteção de dados do consumidor bancário, em consonância com toda legislação supra apresentada, com o fim de padronização a todos os agentes do setor econômico, aumentando a transparência e a segurança em relação a coleta, uso e tratamento de dados pessoais.

No capítulo a seguir serão analisados os principais princípios que norteiam o tratamento, uso e coleta de dados pessoais do consumidor no âmbito das instituições financeiras.

3. Questões principiológicas da LGPD atinentes às Instituições Financeiras

Conforme já exposto, os desafios para as instituições financeiras na implantação da LGPD são muitos, mas é relevante destacar a necessária mudança cultural que deverá ocorrer em todas as estruturas que trabalham com o processamento de dados, pois a LGPD trouxe 10 princípios dispostos

[7] Computação em nuvem ou cloud é uma forma de processamento em larga escala, utilizando servidores com alta capacidade de armazenamento e que podem estar hospedados em diversos locais do mundo, sendo utilizados de acordo com a demanda.

em seu artigo 6º, como o da necessidade[8] e o da transparência[9] que não deverão mais ser considerados como opcionais na atividade (BRASIL, 2018).

De fato, as decisões automatizadas, utilizadas nas análises de crédito e também em modelos de prevenção à fraude, deverão respeitar a lei supra e todo o uso que se dá ao legado de informações adquiridas, não apenas na relação com os clientes já existentes, mas também nos contratos de fornecedores de dados existentes no mercado, deverão ser revistos e enquadrados nas possibilidades de tratamento que a lei determina.

O referido princípio da transparência precisa permear toda a atividade bancária com a vigência da LGPD. Se antes não havia necessidade de esclarecimento ao cliente bancário sobre o que era feito com os seus dados pessoais, esta não será mais uma opção, pois a transparência passa a ser a forma de continuidade no uso das informações.

Nesse sentido, a questão não é impedir que o banco realize a análise dos dados ou limitar ao máximo as informações que são acessadas pelos agentes financeiros para que acessem apenas o estrito necessário, mas sim mostrar ao cliente que os seus direitos são garantidos ainda que no tratamento de seus dados financeiros, e que os princípios da Lei estão garantidos ainda que neste segmento.

É importante destacar também que os dados que os Bancos vão trabalhar não são necessariamente os dados capturados no ambiente digital ou remoto, mas também informações coletadas em meios físicos, ações realizadas pelo cliente nas suas interações com aquele Banco determinado. Um exemplo interessante é utilizar o dado de quantas vezes aquele cliente efetuou pagamentos ou transações em agências físicas, assim entendendo o quanto aquele indivíduo pode ser considerado com um perfil digital ou não, ou ainda, qual o tipo de serviço deve ser priorizado nesses locais.

Pelo princípio da finalidade, os dados devem ser tratados para determinados propósitos, que devem ser informados ao titular de dados previamente, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação.

[8] Previsto no art. 6º, III da Lei 13.709 de 2018, o princípio da Necessidade destaca que apenas devem ser utilizados os dados minimamente necessários para se obter o resultado pretendido.

[9] Previsto no art. 6º, III da Lei 13.709 de 2018, o princípio da Transparência destaca que os titulares dos dados têm o direito a ter informações exatas, claras e acessíveis sobre o tratamento de seus dados.

> Para Doneda, "este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)". (DONEDA, 2005, p. 216).

Ainda com base no princípio da finalidade, Maria Celina Bodin de Moraes, em apresentação à obra de Stefano Rodotà, preconiza que o tratamento de dados e especialmente a sua coleta "não pode ser tomada como uma "rede jogada ao mar para pescar qualquer peixe". Ao contrário, as razões de coleta, principalmente quando se tratarem de "dados sensíveis", devem ser objetivas e limitadas" (MORAES, 2008, p. 9).

A medida dessa objetividade e limitação será determinada justamente pela finalidade legítima do tratamento, que fica condicionada "à comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada" (RODOTÀ, 2008, p. 87).

De início, a LGPD adota uma forte fundamentação no consentimento do titular de dados para admitir o tratamento dos dados pessoais. Significa dizer que será permitido o tratamento de dados pessoais em havendo manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII).

Em complementação, a LGPD estabelece restrições importantes quando diante do tratamento de dados sensíveis, e em relação ao consentimento, estabelece a necessidade de que ele seja realizado de forma específica e destacada, para finalidades singulares também (artigo 11, I, LGPD) (BRASIL, 2018).

Assim, e de acordo com Rodotà, reconhece-se que o consentimento do titular de dados sensíveis deve ser qualificado, na medida em que estamos diante de um "contratante vulnerável", caracterizado justamente pela ausência de liberdade substancial no momento da determinação da vontade (RODOTÀ, 2008, p. 90). No entanto, a LGPD permite que haja tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, quando for indispensável para o

tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (artigo 11, II, b, LGPD), além de outras hipóteses que se referem, em grande medida, a interesses públicos.

O legítimo interesse, por sua vez, é uma das formas previstas no artigo 7º da LGPD de tratamento dos dados pessoais. O autor do livro "Proteção de Dados Pessoais – A função e os limites do consentimento", Bruno Ricardo Bioni, destaca:

> Como já adiantado, essa base legal ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados (...). Tal como o consentimento no início do progresso geracional das leis de proteção de dados pessoais (...), o legítimo interesse ganhou o status de uma nova 'carta coringa regulatória' para abraçar uma miríade de possíveis usos dos dados (BIONI, 2019, p. 249).

Ademais, cabe ressaltar que a transferência de dados pessoais a terceiros apenas é permitida mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. Preceitua-se, também, o consentimento expresso, destacado das demais cláusulas contratuais, para que os dados possam ser coletados, armazenados e tratados, bem como a exclusão, a requerimento do consumidor, dos dados pessoais logo após o término da relação contratual, salvo disposição contrária na lei.

A coleta, uso, armazenamento e tratamento de dados pessoais só poderá ocorrer se a finalidade justifique sua coleta, não haja vedação legal e conste de cláusula contratual.

Ora, se as instituições financeiras estão sujeitas ao cumprimento de políticas, procedimentos e controles internos previstas na Circular BACEN nº 3.978 de 23 de janeiro de 2020[10] visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, encontra-se aqui a plena justificativa à aplicação do princípio do legítimo interesse na legislação nacional (CMN, 2020).

[10] CIRCULAR N° 3.978, DE 23 DE JANEIRO DE 2020. Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

Os artigos 16 e 17 da Circular acima informada dispõem sobre coleta e manutenção de dados pessoais dos clientes e até mesmo eventual confrontação destes dados com os disponíveis em bancos de dados de caráter público ou privado.

Diante disto, muito embora a LGPD permita que todas as pessoas tenham direito à privacidade dos seus dados, autorizando os usuários a solicitarem a remoção dos seus dados pessoais de bancos de informação, as instituições financeiras ainda assim poderão manter os dados nos casos em que houver necessidade de garantir conformidade com outras leis, segundo acima exposto. Entretanto, não havendo justificativa válida, deve-se excluir as informações do indivíduo, se assim o cliente desejar[11].

A seguir, serão analisados os desafios da LGPD nas instituições financeiras, frente à implementação do *Open Banking* no setor.

4. *Open Banking* como desafio à aplicação da LGPD nos bancos

Quando se trata de inovações tecnológicas ligadas às instituições financeiras, é salutar relatar a preocupação do segmento no que tange aos crimes cibernéticos, que deve-se ao fato do aumento significativo das realizações de transações bancárias por meio de canais digitais nos últimos anos, em pesquisa realizada pela Federação Brasileira de Bancos. Hodiernamente, as operações realizadas via internet banking ou mobile banking, representam um terço das transações bancárias (FEBRABAN, 2018).

O avanço das tecnologias e do compartilhamento de informações que modificaram a atual forma de desenvolvimento econômico e financeiro proporcionou o desenvolvimento e mudanças nos serviços oferecidos pelas instituições financeiras, permitindo a criação de novos modelos de mercado, produtos e serviços.

A prática de *Open Banking* é um exemplo de negócio bancário impulsionado por este novo cenário. Partindo de tais considerações, será analisado o conceito de *Open Banking* adotado pelo Banco Central do Brasil, a partir da expedição do Comunicado nº 33.455, de 24 de abril de

[11] Lei nº 13.709 de 14 de agosto de 2018. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei.

2019 e a sua possível implicação perante a proteção de dados pessoais dos consumidores (BCB, 2019).

A implementação do *Open Banking* tem como objetivo precípuo elevar a eficiência no mercado de crédito e de pagamentos, mediante a promoção de um cenário de maior inclusão e competitividade, de forma a preservar o equilíbrio do sistema financeiro e, sobretudo, a proteção dos consumidores.

Dessa forma, o Banco Central do Brasil definiu o conceito de *Open Banking* como: "compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação" (BRASIL, 2019).

De acordo com o Comunicado, os titulares das contas correntes poderão escolher com quem desejam compartilhar informações como dados pessoais, saldo da conta corrente e investimento. Tal situação ocorrerá por meio de parcerias entres *startups, fintechs* e empresas de tecnologias, por meio do uso de interfaces de aplicação de programação. (*Application Programming Interface – API*).

Dentre as informações e serviços que poderão ser compartilhados estão produtos e serviços oferecidos pelas instituições participantes (localização de pontos de atendimento, características de produtos, termos e condições contratuais e custos financeiros, entre outros); dados cadastrais dos clientes (nome, número de inscrição no Cadastro de Pessoas Físicas - CPF, filiação, endereço, entre outros); dados transacionais dos clientes (dados relativos a contas de depósito, a operações de crédito, a demais produtos e serviços contratados pelos clientes, entre outros); e serviços de pagamento (inicialização de pagamento, transferências de fundos, pagamentos de produtos e serviços, entre outros), devendo se aplicar às instituições financeiras, instituições de pagamento e demais instituições autorizadas (BRASIL, 2019).

No mesmo sentido, em 28 de março de 2018, o Banco Central expediu a Resolução nº 4.649 que expõe, indiretamente, um dos principais fundamentos do conceito de *Open Banking*: a possibilidade do cliente, a partir do princípio da autodeterminação informativa, escolher quais serviços financeiros que poderão ser transacionados por meio de sua conta corrente (ou mesmo de pagamento):

> Art. 1º É vedado aos bancos comerciais, aos bancos múltiplos com carteira comercial e às caixas econômicas limitar ou impedir, de qualquer forma, o acesso de instituições de pagamento e de outras instituições autorizadas a funcionar pelo Banco Central do Brasil aos seguintes produtos e serviços: I - débitos autorizados pelo titular de conta de depósitos ou de conta de pagamento mantidas nas instituições mencionadas no caput, inclusive débitos comandados pelo titular da conta por meio de instituições de pagamento ou de outras instituições autorizadas a funcionar pelo Banco Central do Brasil; II - emissão de boletos de pagamento; III - transferências entre contas no âmbito da mesma instituição; IV - Transferência Eletrônica Disponível (TED); e V - Documento de Crédito (DOC) (BRASIL, 2018).

Bruno Bioni destaca que o modelo de decisão compartilhada permite que a autorregulação não atenda a interesses apenas de um determinado setor da sociedade ou mesmo do governo, possibilitando a instauração de um diálogo participativo necessário para tratar de questões complexas próprias da sociedade contemporânea, de maneira a proporcionar o desenvolvimento de um ambiente regulatório mais técnico, de acordo com verticalização e concretização das normas e princípios gerais delineados pela legislação interna, como também das diretrizes delineadas pelos demais autores (BIONI, 2019, p.05-33)

Hodiernamente o setor financeiro demanda mecanismos de regulação mais ágeis e eficazes, sob pena da verificação de insegurança jurídica, riscos de violação a direitos e simultaneamente redução na inovação de negócios. Dessa forma, é necessário que o sistema jurídico desenvolva instrumentos que garantam estabilidade e segurança jurídica. Nesse diapasão, é necessário que a regulação busque o equilíbrio entre o livre fluxo de informações e a privacidade das pessoas que têm seus dados em trânsito (BIONI, 2019, p.252).

O *Open Banking*, ao reger-se pela LGPD e pelo CDC, parte do princípio que para que haja o compartilhamento das informações cadastrais contidas nos bancos de dados, deve haver o consentimento escrito do titular dos dados. Nota-se que para a LGPD, consentimento é manifestação livre, informada e inequívoca pela qual o titular concorda

com o tratamento de seus dados pessoais para uma finalidade determinada (BRASIL, 2018).

Logo, ao permitir o compartilhamento as informações cadastrais e de adimplemento armazenadas com outros bancos de dados sem o consentimento do titular de dados, a Lei Complementar nº 166/2019 poderá trazer fragilidade jurídica quanto à exigência de consentimento também para prática de *Open Banking* (BRASIL, 2019).

5. Considerações Finais

Diante de todo o exposto, tornam-se evidentes as oportunidades que a LGPD trouxe ao cenário bancário, possibilitando que o processamento de dados ocorra de forma segura, legítima e organizada. A lei, no entanto, não deve ser considerada como uma forma de punição agressiva, mas sim como uma norma que traz um marco de mudança ao Direito Brasileiro e vem para reforçar um universo que já é predominante nas relações entre indivíduos e empresas, a relação digital.

Um rol de direitos e obrigações que reflete em muito o status atual da sociedade contemporânea e o rumo que os negócios, sejam eles quais forem, estão seguindo. Uma norma que possibilita que os indivíduos escolham o serviço que mais lhes traga garantia de transparência, que não necessariamente está ligada ao ato de autorizar, mas certamente está conectada ao conceito de informar de forma clara e objetiva aos consumidores bancários sobre o uso, coleta e tratamento de seus dados pessoais.

Além disso, a nova forma que o banco tem de se relacionar com o seu cliente, tendo em vista a necessidade de se adequar à LGPD, traz a preocupação em mostrar valor no serviço prestado, tende a trazer mais transparência para tudo que se constrói com base no processamento de dados pessoais, e também pela forma como se constrói, pois, o tratamento de informações é sempre o meio e não o fim.

A exigência para que o tratamento do dado pessoal seja realizado de forma adequada, de acordo com as expectativas daquele consumidor pode ser muito vantajoso e trazer benefícios atrelados ao que cada um espera individualmente daquela atividade empresarial, e tende a se transformar no conceito hodierno de relacionamento entre indivíduos na economia mundial.

O novo modo de atuação nas relações consumeristas bancárias pode propiciar que cada vez mais o cliente, bancário ou não, apenas opte por fornecer seus dados pessoais e consumir um determinado produto ou serviço, se estiver ciente da clareza das informações concedidas pela instituição, com a devida necessidade e legitimidade de seu uso e tratamento.

A realidade do mundo do consumo mudou, e os bancos precisam acompanhar essa mudança de forma a mostrar que conhecer o seu cliente é sim muito vantajoso, e isso não tem nada a ver com o seu interesse econômico primariamente.

O legítimo interesse se torna opção muito relevante de tratamento do dado pessoal quando possibilita que as empresas utilizem raciocínio lógico, jurídico e operacional sobre um volume de dados que até então eram trabalhados de forma automática, ainda que com a devida segurança, respeitados os limites do sigilo e da privacidade.

Ainda, é necessário considerar os dados pessoais, no contexto da prática do *Open Banking*, sob dois aspectos: na qualidade de um insumo econômico e também como bem jurídico a ser tutelado. Logo, é impossível desvincular o *Open Banking* de uma política de proteção e privacidade de dados, uma vez que a proteção desses dados está exposta aos diversos riscos.

Assim, a identificação desses riscos permite reflexão sobre o papel do direito para regulação da abertura e, consequentemente, da proteção dos dados bancários pessoais, considerando harmonicamente os princípios de livre mercado, controle informacional e proteção da privacidade. Por fim, é preciso compreender que a capacidade e velocidade de inovação do cenário financeiro demandam do ordenamento jurídico nacional mecanismos de regulação ágeis e eficazes. Caso isso não ocorra, poderá surgir imensa insegurança jurídica no país, com riscos a violações aos direitos e ao mesmo tempo uma diminuição no potencial de inovação de negócios.

Referências

BCB. **Resolução nº 4658 de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF, 2018.

BIONI, Bruno Ricardo. **Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet.** Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo. São Paulo, 2016.

BIONI. **Compreendendo o conceito de anonimização e dado anonimizado** *in* Revista do Advogado São Paulo: AASP, 2019.

BIONI. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. 1. Ed. São Paulo: Almedina, 2018.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, DF: Senado, 1988.

BRASIL. **Decreto nº 8.771 de 11 de maio de 2016.** Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF, 2016.

BRASIL. Banco Central do Brasil. **Comunicado n. 33.455, de 24 de abril de 2019.** Divulga os requisitos fundamentais para a implementação, no Brasil, do Sistema Financeiro Aberto (*Open Banking*).

BRASIL. Banco Central do Brasil. **Resolução n. 3.401, de 06 de outubro de 2006.** Dispõe sobre a quitação antecipada de operações de crédito e de arrendamento mercantil, a cobrança de tarifas nessas operações, bem como sobre a obrigatoriedade de fornecimento de informações cadastrais.

BRASIL. Banco Central do Brasil. **Resolução n. 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

BRASIL. **Decreto n. 7.962 de 15 de março de 2013.** Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.

BRASIL. **Lei Complementar n. 105 de 10 de janeiro de 2001**. Brasília: Distrito Federal. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF, 2001.

BRASIL. **Lei Complementar n. 166 de 08 de abril de 2019.** Brasília: Distrito Federal. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF, 2019.

BRASIL**. Lei nº 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 1990.

BRASIL. **Lei nº 12.414 de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF, 2011.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF, 2018.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1457199/RS.** Relator Ministro Paulo de Tarso Sanseverino. Decisão publicada em 17 de dezembro de 2014.

CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 7ª ed. São Paulo: Atlas, 2007.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (coord.). **Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014**). São Paulo: Quarter Latin, 2014.

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. **Revista Espaço Jurídico**, vol. 12. n. 2. Joaçaba: Unoesc, 2011.

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

DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Editora Lumen Juris. 2003.

ESCOLA NACIONAL DE DEFESA DO CONSUMIDOR. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Caderno de Investigações Científicas, vol. 2. Brasília: SDE/DPDC, 2010. Disponível em: https://www.defesadoconsumidor.gov.br/images/manuais/vol_2_protecao_de_dados_pessoais.pdf. Acesso em: 10 jun. 2020.

EUROPEAN COMISSION. EU. **Discurso proferido por Meglena Kuneva, European Consumer Commissioner, na mesa redonda sobre coleta de dados online, direcionamento e perfilação**. Bruxelas, 31 mar. 2009. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156. Acesso em: 10 abr. 2020.

GENERAL DATA PROTECTION REGULATION. **GDPR.** Disponível em: https://gdpr-info.eu/. Acesso em: 10 abr. 2020.

GONÇALVES, Andrey Felipe Lacerda; BERTOTTI, Monique; MUNIZ, Veryzon Campos. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. **Doutrinas Essenciais de Direito Constitucional**, v. 8/2015, p. 597 - 614, ago. de 2015.

JAPPELLI, Túlio; PAGANO, Marco. Information sharing in credit markets: a survey. **Working paper**, Universidade de Salerno, Itália, n. 36, mar. 2003.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. **Panorama brasileiro sobre proteção de dados pessoais: discussão e análise comparada. Novas práticas em informação e conhecimento**. Curitiba: v. 2, n. 1, p. 6076, jan./jun. de 2013.

MACEDO JR., Ronaldo Porto. **Contratos relacionais e defesa do consumidor**. 2. ed. São Paulo: Revista dos Tribunais, 2006.

MARQUES, Claudia Lima; MIRAGEM, Bruno (Org.). **Coleção doutrinas essenciais: direito do consumidor – proteção da confiança e práticas comerciais**. São Paulo: Revista dos Tribunais, 2011.

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.

MORAES, Maria Celina Bodin de. Apresentação. In: RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil**. 7. edição. São Paulo: Editora Atlas, 2014.

PINHEIRO, Patrícia Peck. **Direito digital**. 6ª edição. São Paulo: Editora Saraiva, 2015.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais – Comentários à Lei n. 13709/2018 LGPD**. São Paulo: Editora Saraiva, 2018.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.