ÚRSULA BRANDÃO FARIA VALDETARO

Utilização de dados pessoais em serviços financeiros

Brasília
2017

Utilização de dados pessoais em serviços financeiros

Autora: Úrsula Brandão Faria Valdetaro

Orientador: Prof. Dr. Antônio de Moura Borges

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

Brasília, ____ de _____ de _____.

FOLHA DE APROVAÇÃO

ÚRSULA BRANDÃO FARIA VALDETARO

Utilização de dados pessoais em serviços financeiros.

Monografia apresentada como requisito parcial à obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília – UnB

BANCA EXAMINADORA

_____

Prof. Doutor Antônio de Moura Borges
(Orientador – Presidente)

_____

Mestre Adriana Teixeira de Toledo
(Membro)

_____

Mestre Paulo Alexandre Batista de Castro
(Membro)

_____

Doutora Marusa Vasconcelos Freire
(Suplente)

AGRADECIMENTOS

Agradeço a Deus, por ter me dado uma família maravilhosa, que me estimula a ter determinação, foco e perseverança. A meu filho lindo e muito amado, Alexandre, que tão pequenino já me ensinou o que é ser guerreiro, que com apenas um sorriso me dá a força necessária para continuar. A meu marido amado, querido, companheiro de longos anos, Rodrigo, que está sempre ao meu lado, que me apoia, me dá forças e não me deixa desistir. Aos meus pais, que agora durante a redação da monografia, estão sempre por perto e me auxiliam nos cuidados com meu pequeno.

Agradeço ao meu orientador, Prof. Antônio de Moura Borges, e aos membros da banca Adriana Toledo e Paulo Alexandre Castro, pela disponibilidade. Meus agradecimentos à Marusa Vasconcelos Freire, que não somente é suplente da banca, mas também grande incentivadora para que eu redigisse minha monografia e concluísse meu curso de Direito, e ao amigo Wilson Oliveira, pelas dicas.

Muito obrigada a todos!

RESUMO

O presente estudo tem por objetivo analisar a utilização de dados pessoais e seus impactos no direito do consumidor de serviços financeiros, especialmente no que tange ao direito à privacidade, ao potencial uso desses dados para fins discriminatórios, e à segurança e à confiabilidade dos bancos de dados. Destaca-se a importância do tema, dada a crescente utilização de fontes de dados pessoais até então não convencionais, como o uso de dados alternativos ou *Big Data.* Pretende-se também avaliar o quadro regulatório atual no Brasil, e traçar perspectivas regulatórias e de políticas públicas adequadas à proteção aos direitos dos consumidores de serviços financeiros titulares de dados pessoais, a partir da análise da legislação nacional já vigente, de Projeto de Lei acerca da matéria em tramitação no Congresso Nacional e da regulamentação setorial. Para subsidiar a análise o estudo contemplará breve relato acerca da regulação internacional da matéria, especialmente da regulação da União Europeia. Conclui-se necessária a aprovação de lei e de regulamentação setorial que promovam a proteção de uso de dados pessoais no Brasil, bem como a implementação de políticas públicas de incentivo às boas práticas na posse e manipulação de dados pessoais.

Palavras-chave: Dados pessoais, direito do consumidor, serviços financeiros, direito à privacidade, dados alternativos, *Big Data.*

ABSTRACT

This study aims to analyze the use of personal data and its impacts on the rights of the financial services consumer, particularly with respect to the right to privacy, the potencial use of these data for discriminatory ends and the safety and reliability of data banks. The importance of this subject should be highlighted, given the increasing use of hitherto unconventional sources of personal data, such as the use of alternative data or Big Data. One other aim is to assess the current Brazilian regulatory framework and outline regulatory and public policy perspectives suited for the protection of the rights of consumers of financial services that hold personal data, based on national legislation already in place, draft bill currently in Congress and sector regulation. In order to subsidize this analysis, the study shall contemplate a brief report surrounding international regulation on the issue, especially the European Union's. The conclusion is that it is necessary to put in place laws and sector regulation which will promote the protection of personal data usage in Brazil, as well as the implementation of public policies that would stimulate best practices in the holding and handling of personal data.

Keywords: personal data, consumer rights, financial services, right to privacy, alternative data, Big Data.

SUMÁRIO

INTRODUÇÃO

Cada vez mais tudo o que fazemos, inclusive pesquisas na internet, tem sido objeto de registro por sistemas especializados de tecnologia de informação e comunicação. Assim, temos, no mundo digital, uma enorme massa de dados compostas por dados já tradicionalmente utilizados bem como por outros que até pouco tempo atrás não eram considerados – ou porque não eram gerados e guardados ou por falta de capacidade de processá-los e analisá-los. Esse grande conjunto de dados foi denominado de *Big Data.*

Andre Petry[1], colunista da Veja, descreve um curioso caso que se tornou clássico no que se refere ao uso de *Big Data*:

> Há uma década, a Target, a gigantesca loja de departamentos com 1800 pontos de venda nos Estados Unidos, atribuiu um número a cada um dos seus milhões de clientes e passou a rastrear e armazenar todas as pegadas digitais deixadas por eles: produtos preferidos, hábitos de consumo, média de gastos, uso de cupons, cartão de fidelidade. Somou a isso dados demográficos de cada um deles, adquiridos em empresas do ramo, sexo, idade, profissão, local de moradia, estimativa de renda. Contratou estatísticos para analisar estatísticas e montou um retrato preciso do padrão de consumo de cada cliente. Um dia aconteceu um incidente.
> Um senhor entrou esbravejando numa loja da Target em Minnesota. Trazia nas mãos cupons de produtos para bebês. "Minha filha recebeu isto aqui pelo correio", reclama o senhor para o gerente. "Ela é uma adolescente. Vocês estão querendo estimulá-la a engravidar?". O gerente conferiu a remessa de cupons e, constrangido, pediu desculpas. Dias depois, com receio de perder o cliente, telefonou a fim de desculpar-se outra vez. O pai da adolescente estava desconcertado do outro lado da linha: "Tive uma conversa com a minha filha. Fiquei sabendo de algumas coisas que estavam acontecendo dentro da minha casa". Respirou fundo e completou: " Ela vai dar à luz em agosto".

Conhecer e entender, a partir de uma multiplicidade gigantesca de dados, os padrões de comportamento dos consumidores passou a ser um dos maiores desafios das grandes empresas e indústrias mundiais. Conforme destaca Andrade[2] (2014. p.11), a compreensão desses padrões, obtidos a partir da análise de dados pessoais, pode oferecer informações valiosas às empresas sobre seu público-alvo, uma vez que podem explicar como os consumidores decidem acerca de um serviço ou produto.

---

[1] PETRY, Andre. Vida Digital: O Berço do Big Data. **Revista Veja**, São Paulo. 2013, p.71-81.

[2] JUNIOR, Valter Lacerda de Andrade. **Utilização de técnicas de dados não estruturados para desenvolvimento de modelos aplicados ao ciclo de crédito**. 2014. 70p. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo. 2014. Disponível em: <https://sapientia.pucsp.br/bitstream/handle/18150/1/Valter%20Lacerda%20de%20Andrade%20Junior.pdf> Acesso em: 07 jun. 2017.

A indústria de serviços financeiros também é impactada por essa mudança de paradigma no gerenciamento de dados. Informações pessoais sobre os clientes, que até então estavam disponíveis apenas de forma desestruturada, agora são passíveis de tratamento e interpretação, podendo gerar informações valiosas para os fornecedores desses serviços, permitindo antever comportamentos previsíveis desses consumidores.

Não obstante o grande potencial do uso de *Big Data* ou de dados alternativos em possibilitar o fornecimento de serviços mais alinhados à necessidade do público e também em gerar informações sobre consumidores até então à margem dos grandes bancos de dados e cadastros estruturados com propósitos específicos, questões fundamentais são postas, como a necessidade de proteção do uso de dados pessoais, o direito à intimidade e à privacidade, à segurança de informações e os possíveis usos discriminatórios a partir da análise dos dados.

Assim, o presente estudo pretende: i) analisar a utilização de dados não convencionais nos serviços financeiros e sua relação com o sigilo, a segurança e a confiabilidade das informações; ii) examinar o quadro regulatório atual no Brasil, e iii) traçar perspectivas regulatórias e de políticas públicas adequadas à proteção aos direitos dos consumidores.

Para contemplar essa análise, o estudo compreenderá cinco capítulos. O primeiro capítulo abordará conceitos importantes como *Big Data*, dados tradicionais e dados alternativos, descreverá a utilização de dados não convencionais em serviços financeiros, dissertará sobre a relação dos dados alternativos e as *fintechs*[3], bem como pontuará potenciais benefícios do uso de dados alternativos ou de *Big Data* para os serviços financeiros.

No segundo capítulo será feita análise de aspectos legais do uso desses dados com base no Direito do Consumidor, especialmente no que tange ao direito à privacidade, ao potencial uso dos dados pessoais para fins discriminatórios, e à segurança e à confiabilidade dos bancos de dados.

O terceiro capítulo contemplará breve relato acerca da regulação internacional da matéria, sendo dada especial atenção à regulação dada pela União Europeia, seguido do

[3] Fintech é o termo utilizado para inovações financeiras que utilizam technologias de informação e comunicação a partir da expressão em inglês “financial technology” como sera visto mais adiante neste estudo.

quarto capítulo que tratará da regulamentação do uso de dados pessoais no território nacional.

Por fim, o quinto capítulo fará uma análise da regulamentação nacional frente à internacional e traçará perspectivas de regulamentação, geral e setorial, e sugestões de políticas públicas a serem implementadas.

1. BIG DATA E DADOS ALTERNATIVOS

1.1 Definição *de Big Data*, Dados Tradicionais e Dados Alternativos

A economia tem como um dos seus principais conceitos a escassez. É a escassez de recursos que faz com que os indivíduos tenham que optar, fazer escolhas; os famosos *trade-offs*. Entretanto, no mundo contemporâneo, com relação à disponibilidade de informações, vivemos uma nova realidade, a da superabundância de dados:

> Com a quantidade de informação disponível – hoje, fala-se em **superabundância de informação** em vez de escassez – deu-se o surgimento de inúmeras empresas, ou braços de empresas tradicionais, que tentam capturar essa quantidade absurda de dados e utilizá-los de várias formas: políticas de governo, seleção de investimento, gestão de empresas etc. A IBM, por exemplo, chegou a criar a Big Data University, um centro para fornecer conhecimento sobre o *Big Data*.[4]

Não há uma definição única de *Big Data* (ou megadados, em português) na literatura. Tendo em vista sua acelerada, desordenada e bem sucedida evolução, *Big Data* compreende diversas nuances de significados, as quais, como bem pontuam Mauro, Greco e Grimaldi, são todas igualmente válidas (2014, p.1 e p.5)[5].

Laney[6] propôs, em 2001, que as três dimensões para o gerenciamento de dados seriam os "3 Vs": Volume, Variedade, e Velocidade. Posteriormente, essas três dimensões foram incorporadas à definição de *Big Data.*

Mauro, Greco e Grimaldi (2014, p.6) dividem a evolução do conceito *Big Data* em três grandes grupos:

a) O primeiro grupo, surgido entre os anos de 2011 e 2013, tinha como principal objeto as características de *Big Data*. Assim, citam autores como Beyer & Laney, Eaton, Zaslavsky, que estabeleceram como condição de um banco de dados ser considerado como *Big Data* a compreensão dos já citados "3 Vs": volume, velocidade e variedade. Essas características foram posteriormente expandidas,

---

[4] NOVAIS, Leandro. **Big Data e o consumidor bancário**. 25 mai 2015. Disponível em: <http://educandoseubolso.blog.br/2015/05/25/big-data-e-o-consumidor-bancario/>. Acesso em: 02 jun. 2017.

[5] De MAURO, Andrea; GREGO, Marco; GRIMALDI, Michele. **What is Big Data? A consensual definition and a review of key research topics**. In: AIP Conference Proccedings, vol. 1644, n. 1, 2014. Disponível em: < https://www.researchgate.net/publication/265775800_What_is_Big_Data_A_Consensual_Definition_and_a_Review_of_Key_Research_Topics> Acesso em: 04 jun. 2017.

[6] LANEY, Doug. **Data management - controlling data volume, velocity and variety**. Meta Group. Publicado em: 06 fev. 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> Acesso em: 02 jun. 2017.

incluindo valor, veracidade e complexidade (características incluídas por Dijcks, Schoek e Suthaharan). Mauro, Greco e Grimaldi (2014, p.6).

b) O segundo grupo, por sua vez, centrou-se na necessidade de soluções tecnológicas para o processamento desse grande número de informações.
c) O terceiro grupo teve como foco o impacto que a *Big Data* tem na sociedade.

A partir de 1.437 resumos de artigos referentes a *Big Data* na plataforma *Elsevier's Scopus*, Mauro, Greco e Grimaldi (2014, p. 2) analisaram as mais frequentes palavras chaves utilizadas e encontraram que os temas mais estudados pela literatura com relação ao tema eram: informação, tecnologia, metodologia e impacto.

Ao realizar uma revisão dos conceitos de *Big Data*, Chen *et al* (2014 p.173)[7] destacam o conceito proposto no relatório da *International Data Corporation* – IDC, uma das empresas líderes na área de *Big Data*, descrevendo-a como:

> Uma nova geração de tecnologias e arquiteturas desenhadas para extrair valor de grandes volumes e variedade de banco de dados de forma eficiente, garantido descobertas, capturas e análises em alta velocidade. Os autores pontuam que esse contexto aborda o grande aspecto crítico da *Big Data*, explorar uma série de valores até então escondidos.

No presente estudo, a característica de *Big Data* que mais nos interessa é o da variedade. A quantidade gigantesca disponível para análise inclui dados que até há pouco tempo não eram considerados, como descritos na seção seguinte.

Chen *et al* (2014, p.173) pontuam bem que um ponto essencial para um bem sucedido gerenciamento de dados é como transformar o que eles denominam de "montes de dados" em uma *Big Data*.

O que seriam então esse "montes de dados"? Com o desenvolvimento de novas tecnologias, a capacidade de surgimento, de armazenamento e de análise de dados cresceu de forma exponencial. Assim, dados que anteriormente não existiam, não possuíam registro ou que não eram passíveis de processamento nos dias atuais podem fornecer informações importantes para o setor público e para iniciativa privada.

Para categorizar essa enorme base de dados surgidos na contemporaneidade, o mercado utiliza o termo dados alternativos. O *Consumer Financial Protector Bureau* –

[7] CHEN, Min; MAO, Shiwen; LIU, Yunhao. Big Data: a survey. **Mobile Networks and Applications**, vol. 19, p. 171-209, 2014. Disponível em: <http://www2.egr.uh.edu/~zhan2/ECE6111/class/BigDataSurvey2014.pdf > Acesso em: 04 jun. 2017.

CFPB (2017, p.5)[8] define dados alternativos como todos os aqueles que se diferem dos tradicionais, encontrados em bancos de dados relacionados à prestação de serviços financeiros. Por ser um conceito tão genérico, e por ser difícil traçar uma linha absoluta diferenciando dados tradicionais dos alternativos, o CFPB utiliza tal discriminação apenas em um sentido descritivo, e não normativo.

1.2 Utilização de *Big Data* e Dados Alternativos em Serviços Financeiros

O conceito de dados alternativos varia a depender do campo de conhecimento ou da aplicação a que ele se refere. No sistema financeiro, uma das áreas que mais se apropria desses dados não convencionais é a área de crédito, especialmente na gestão ou gerenciamento financeiro, na avaliação de riscos e na formulação dos escores de crédito.

Ao diferenciar dados tradicionais dos dados alternativos, o CFPB (2017, p.4 e 5)[9] explica que os dados tradicionais dizem respeito a dados coletados e geridos nos principais arquivos de serviços de proteção ao crédito[10],

> o que abrange informações de comércio (incluindo certas informações de empréstimo ou limite de crédito, história de negociações de dívida e status da conta)", bem como informações de registros públicos relativos a sentenças civis, penhoras e falências. Refere-se também aos dados habitualmente fornecidos pelos consumidores como parte dos pedidos de crédito, como o rendimento ou a residência. (tradução minha)

Por sua vez, dados alternativos referem-se a quaisquer dados que não são historicamente utilizados para análise e fornecimento de crédito, conforme rol exemplificativo (CFPB, 2017, p. 9 e 10):

> a) Dados que demonstram tendências em renegociação de dívidas.
> b) Dados relativos a outros pagamentos regulares que não de empréstimo (tipicamente mensais), tais como telecomunicações, aluguel, seguros ou utilitários.
> c) Dados referentes a fluxo de caixa e ativos do consumidor, que podem incluir a regularidade a entradas e saídas de conta corrente, informações sobre o rendimento prévio ou picos de gastos.
> d) Dados considerados relacionados à estabilidade do consumidor, que podem incluir informações sobre a frequência de mudanças de residência, de emprego, de números de telefone ou endereços de *e-mail*.

---

[8] CONSUMER FINANCIAL PROTECTION BUREAU. **Request for information regarding use of alternative data and modeling techniques in the credit process.** [Docket No. CFPB-2017-0005], 2017. Disponível em: <http://files.consumerfinance.gov/f/documents/20170214_cfpb_Alt-Data-RFI.pdf> Acesso em: 4 de jun. 2017.
[9] Idem, pp 4 e 5.
[10] Tais bancos possuem natureza pública.

> e) Dados sobre a escolaridade e ocupação do consumidor, incluindo informações sobre escolas frequentadas, graus obtidos e cargos ocupados.
> f) Dados referentes aos comportamentos e hábitos do consumidor, como sua forma de interação com a *interface web* ou responder determinadas questões, sobre como eles compram, navegam na rede, ou utilizam dispositivos em suas vidas diárias.
> g) Dados relativos à rede de relacionamento e de amizade dos consumidores, incluindo dados sobre conexões em mídias sociais. (tradução minha)

Uma pesquisa desenvolvida pelo *Factor Trust*[11], o *Bureau* Alternativo de Crédito[12], investigou as principais razões pelas quais os provedores de serviços financeiros e de crédito pretendiam utilizar dados alternativos para tomada de decisões em seus negócios no ano de 2017. As principais razões elencadas foram: i) mitigação de perda e expansão do número de consumidores que poderiam ter escore de crédito (63%); ii) permitir uma segunda chance aos consumidores que tiveram sua proposta de crédito originalmente rejeitada (55%); e iii) melhorar a precificação dos serviços baseada no risco.

Outros usos de dados alternativos ou *Big Data* por fornecedores de serviço financeiros[13] são: i) utilizar o banco de reclamações contra instituições financeiras nos Procons, Banco Central do Brasil, e nos SACs e Ouvidorias das próprias instituições financeiras para aprimorar o serviço prestado para os clientes; e ii) utilização no mercado de capitais, utilizando tecnologia de algoritmos para estabelecer qual tipo de aplicação é mais adequado para cada consumidor, a depender de seu perfil e desejos.

Bholat[14] (2015, p. 5) pondera que, até o momento, o uso de *Big Data* e outras tecnologias tiveram impactos menos expressivos na área de fornecimento de serviços financeiros quando em comparação a outras áreas. Entretanto ele pontua, ao citar Davenport, que os grandes bancos começam a perceber o valor de dados transacionais de seus consumidores como forma de fornecer serviços mais adequados para seus clientes e também de evitar fraudes.

---

[11] RICHARD, Dan. **Top 3 uses for alternative credit data in 2017 decisioning**. 06 fev. 2017. Disponível em: <https://ws.factortrust.com/2017/02/06/top-3-uses-for-alternative-credit-data-in-2017-decisioning/> Acesso em: 02 jun. 2017. A pesquisa contou com a participação de 130 particiapantes, entre eles gerentes, consultores legais, diretores de marketing e outros profissionais do segmento de serviços financeiros e de tecnologia.

[12] O Factor Trust é considerada um *bureau* alternativo de crédito porque se dedica à analise de dados e informacões não disponíveis nas três maiores empresas de informações de crédito do mundo (Experian, Equifax e TransUnion) para a previsão de riscos de concessão de crédito e da capacidade de pagamento de consumidores financeiros.

[13] NOVAIS, Leandro. **Big Data e o consumidor bancário**. 25 mai 2015. Disponível em: <http://educandoseubolso.blog.br/2015/05/25/big-data-e-o-consumidor-bancario/>. Acesso em: 02 jun. 2017.

[14] BHOLAT, David. Big Data and central banks. **Bank of England Quarterly Bulletin**, vol. 55, n. 1, pp. 1-6. Disponível em: <http://journals.sagepub.com/doi/pdf/10.1177/2053951715579469> Acesso em: 04 jun. 2017.

Nesse estudo, então, serão trabalhados e discutidos os dados de caráter pessoal utilizados na contratação e fornecimento de serviços financeiros, sejam eles alternativos ou constantes de *Big Data*. Preocupa-se aqui com as possíveis repercussões de seu uso no direito à privacidade, à segurança, e com possíveis discriminações advindas da sua má utilização.

1.3 Advento das *Fintechs* e o Uso de Dados Alternativos

Outra mudança de paradigma advinda da evolução tecnológica no contexto da prestação de serviços financeiros é o surgimento das chamadas *fintechs*. O termo *fintech* vem da junção dos termos *"Financial"* e "*Tecnology",* ou seja, essas "*empresas são, em geral,* startups *que desenvolvem inovações tecnológicas voltadas para o mercado financeiro"*[15].

O Banco Central do Brasil – BCB relaciona vários tipos de serviços oferecidos pelas *fintechs*, em seu Relatório de Estabilidade Financeira de Setembro de 2016[16]: tecnologias como o *distributed ledger*, por exemplo, *blockchain*; soluções para o comércio eletrônico; desenvolvimento de infraestruturas e surgimento de carteiras eletrônicas; *peer-to-peer lending*; *robo-advisor*; e novos modelos de negócio para realização de operações de remessas internacionais. O Relatório explicita, ainda, que:

> Tais empresas aplicam as mais recentes tecnologias na adaptação de produtos e de serviços oferecidos no mercado financeiro, no lançamento de novas soluções e na provisão de serviços de mitigação e de gerenciamento de riscos de *compliance* para as instituições reguladas.[17]

Apesar de no Brasil ainda ser pequeno o montante financeiro movimentado pelas *fintechs*, o número de clientes por elas já abarcados é bem expressivo. A Simplic, empresa de crédito, já possui um milhão de clientes e estima-se que o Nubank, empresa de cartões de crédito, possua aproximadamente 800 mil cartões ativos. [18]

---

[15] PRADO, José. **O que é Fintech?** 14 dez. 2016. Disponível em: <http://conexaofintech.com.br/fintech/o-que-e-fintech/>Acesso em: 02 jun. 2017.
[16] BANCO CENTRAL DO BRASIL. **Relatório de estabilidade financeira**, vol. 15, n. 2. Brasília, 2016. Disponível em: <http://www.bcb.gov.br/htms/estabilidade/2016_09/refPub.pdf> Acesso em: 02 jun. 2017.
[17] Idem, p. 50.
[18] ALVES, Aluísio. Fintechs se multiplicam com BC e CVM atentos e regulação precária. **Exame**, 03 mar. 2017. Disponível em: <http://exame.abril.com.br/pme/fintechs-se-multiplicam-com-bc-e-cvm-atentos-e-regulacao-precaria/> Acesso em: 04 jun. 2017.

Outra *fintech* com um número muito expressivo é o Guia Bolso, ferramenta de assessoria em controle financeiro, já possuindo mais de 3 milhões de usuários no Brasil[19], tratando-se de um dos aplicativo mais baixados do segmento financeiro, ultrapassando até mesmo *apps* de bancos. Agora o novo desafio do Guia Bolso é atuar na área de crédito pessoal, e tal decisão baseou-se no fato de no Brasil não existirem muitas opções de crédito pessoal de custo baixo e de longo prazo. Assim, criaram o *Just*, "*um serviço de prestação de crédito pessoal focado na consolidação de dívidas"*[20]. Para tanto, estabeleceram parecerias com bancos de pequeno e médio porte e desenvolveram um escore de crédito próprio.

A Simplic, *fintech* citada anteriormente, é um dos braços da Enova, empresa que atua em 5 diferentes países. Como forma de possibilitar sua atuação no Brasil, vinculou-se à Sorocred, instituição financeira já autorizada a funcionar pelo Banco Central do Brasil. Para oferecer os serviços financeiros,

> conforme explica Rafael Pereira, diretor da Enova no País, a plataforma proprietária da empresa usa mais de duzentas variáveis de diversas fontes de dados e processá-las a tempo de responder à solicitação do cliente em segundos.
> "Passamos este tempo refinando a ferramenta, alimentando-a com dados já utilizados comumente no sistema financeiro local, assim como outros cadastros e dados não estruturados, construindo isso sobre a base que trouxemos do exterior", explicou Pereira.
> Conforme aponta o diretor, o modelo da Enova considera dados não convencionais, como o comportamento do cliente no *site* ao efetuar seu pedido de empréstimo e redes sociais. Segundo ele, isso permite emprestar a um grupo de clientes que nem sempre tem acesso a crédito.[21]

Até o momento, essa associação entre *fintechs* e instituições autorizadas a funcionar pelo Banco Central do Brasil tem se realizado com fundamento em norma que dispõe sobre a contratação de correspondentes no País visando à prestação de serviços, pelo contratado, de atividades de atendimento a clientes e usuários da instituição contratante (Resolução 3.594, de 24 de fevereiro de 2011). Percebe-se, entretanto, que com o surgimento e potencial aumento de mercado das *fintechs*, a tendência de crescimento de utilização de dados alternativos, adquiridos das mais diversas fontes, se torna ainda mais expressivo, tornado esses novos atores importantes focos da regulação financeira e especialmente da regulação do uso de dados pessoais.

---

[19] LAZAROW, Alexandre**. Investidor explica por que apostou no GuiaBolso**. 05 mai 2017. Disponível em: <https://blog.guiabolso.com.br/2017/05/05/por-que-investimos-no-guiabolso/ > Acesso em: 05 jun. 2017.
[20] Idem.
[21] SOUZA, Leandro. **Enova entra no cenário das fintechs**. 04 set. 2015. Disponível em: <https://www.baguete.com.br/noticias/04/09/2015/enova-entra-no-cenario-das-fintechs> Acesso em: 05 jun. 2017.

1.4 Potenciais Benefícios e Riscos do Uso de Dados Alternativos ou *Big Data* em Serviços Financeiros

Antes de falar sobre as possíveis consequências nocivas que o mau uso de *Big Data* ou dados alternativos podem causar ao consumidor de serviços financeiros, é importante verificar também as potencialidades de sua utilização.

O CFPB elenca as diversas vantagens na utilização de dados alternativos ou *Big Data*, tendo em vista um contexto em que grande parte da população é excluída do mercado de crédito. Assim, explica que nos Estados Unidos, até os dias atuais, a maior parte das instituições financeiras decide sobre a concessão de crédito baseada em dados tradicionais[22]. Estima-se que 45 milhões de norte-americanos estejam à margem desse mercado, 26 milhões por não possuírem registro algum nos principais *bureaus* de crédito[23] (o que eles caracterizam como *"credit invisible"*), e outros 19 milhões não são passíveis de produzir escores, devido ao escasso histórico de crédito (CFPB, pp 6 e 7).

Assim, os benefícios elencados pelo CFPB são:

a) *"Ampliação do acesso de crédito"*: tendo em vista a possibilidade de coleta e análise de um número maior de dados, de diversas fontes e naturezas, as pessoas até então não abrangidas por informações tradicionais ("*credit invisible*") poderiam ter seus escores de crédito calculados com base nesses dados alternativos.

b) *"Aprimoramento da análise de crédito":* Mesmo com relação a clientes que já possuem escore de crédito, a utilização de dados alternativos pode fornecer informações adicionais que permitam predizer melhor sua capacidade de pagamento. Com essas informações, potencialmente esses clientes poderão acessar melhores condições de crédito.

c) *"Informações mais tempestivas":* Na análise de dados tradicionais, muitas informações atuais ainda não estão disponíveis quando do momento da análise de

[22] O CFPB descreve as principais fontes de dados tradicionais até então utilizadas para análise de crédito por instituições financeiras norte-americanas : *Many lenders base their decisions, in whole or in part, on scores using traditional data as inputs and generated from commercially-available, third-party models such as one of the many developed by FICO or VantageScore Solutions. Other lenders may base their decisions, in whole or in part, on proprietary scoring algorithms that use traditional data, and perhaps scores from these third-party models, as well as consumer-supplied information, as inputs.* (p.6)

[23] Entidades equivalentes às instituições brasileiras de Serviço de Proteção ao Crédito.

crédito. De tal maneira, a utilização de dados alternativos pode adicionar informações relevantes sobre a situação presente do consumidor.

d) *"Menores custos":* a automatização de obtenção e análise dos dados alternativos pode possibilitar uma diminuição dos custos operacionais das instituições financeiras, que poderão repassar aos consumidores como queda nos preços de seus produtos e serviços.

e) *"Melhores serviços e conveniência":* o uso de dados alternativos e também de novas técnicas de análises de dados podem gerar melhorias operacionais que garantiriam o aprimoramento na prestação dos serviços financeiros em geral.

Apesar de todos esses efeitos benéficos potenciais relativos ao uso de *Big Data* e dados alternativos, o próprio CFPB lista uma série de riscos associados. Citam a preocupação com a invasão da privacidade, aspectos de segurança, e potencial utilização para fins de discriminação, três aspectos que serão melhores examinados posteriormente. Destacam ainda o difícil controle da qualidade e de correção desses dados, a perda de transparência e a maior dificuldade em educar os consumidores sobre os fatores e as técnicas utilizados na análise dos bancos de dados.

2. UTILIZAÇÃO DE DADOS PESSOAIS E DIREITO DO CONSUMIDOR

"Dados pessoais são o novo (petr)óleo da internet e a nova moeda do mundo digital. (Tradução minha).[24] Diante dessa realidade, é importante identificar e destacar quais são os direitos que estão relacionados aos usos desses dados, de forma a garantir a proteção ao direito do consumidor e, assim, evitar que a internet e o mundo digital se tornem uma "terra sem lei".

Como bem pontua Drummond (2003,p.5)[25], *"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."*

---

[24] No original: "*Personal data is the new oil of the Internet and the new currency of the digital world*". 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: < http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> Acesso em: 12 jun. 2017.

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

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.[26]

Mas como podem ser definidos os dados pessoais? Conceito já consolidado em documentos internacionais estabelece dado pessoal como "qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação (titular dos dados)".[27]

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, complementa:

> Uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, em particular pela referência a um número de identificação ou a um ou mais fatores específicos de sua identidade física, fisiológica, mental, econômica, cultural ou social.[28] (tradução minha)

Depreende-se do conceito de dados pessoais que a origem dos dados não é relevante. Assim, não importa se o indivíduo é autor daquelas informações ou se a coleta dessas informações se deu por terceiros. O que importa é que esses dados sejam referentes ao indivíduo. Esses dados podem ser tanto referentes a dados legais, como nome, estado

---

[26] 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. 122 p. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf > Acesso em: 10 jun. 2017.

[27] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD guidelines governing the protection of privacy and transborder flows of personal data.** 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>;

PARLAMENTO EUROPEU - CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Luxembourg: Jornal Oficial das Comunidades Europeias, 24 out. 1995. p. 281/31-281/39. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML> Acesso em 09 jun. 2017;

CONSELHO DA EUROPA. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. European Treaty Series n. 108, Estrasburgo, 28 jan. 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm> Acesso em: 09 jun. 2017.

[28] Diretiva 95/46/Ce do Parlamento Europeu e do Conselho da UE, de 24 de outubro de 1995. Texto original*: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*.

civil, ou podem dizer respeitos a seus hábitos, como por exemplo comportamentos relacionados ao consumo.[29]

Ademais, evidentemente dados anônimos não são abarcados pela definição de dados pessoais. A questão, todavia, não é tão simples quanto parece. Na realidade, é praticamente impossível assegurar que, após diversas análises e criações de algoritmos, os dados dos consumidores sejam realmente anônimos. Muitas vezes é possível reidentificar dados pessoais em um banco de dados em tese aleatório.[30]

Kuneva (2009)[31] destaca, mesmo que ninguém saiba o nome de um determinado consumidor, que se eliminem dados que possibilitem a identificação de um indivíduo, como seu nome e endereço do IP, e existe ainda um perfil sobre ele o qual possibilita empresas conhecerem seus hábitos e gostos e, então, disponibilizarem produtos e serviços a partir desse perfil gerado.

Daí a importância de se conhecer e analisar todos os direitos relacionados à disseminação das informações de natureza pessoal no mundo digital e, a partir disso, pensar qual a melhor forma de o Estado proteger e regular tais práticas e direitos.

O direito que está mais relacionado à utilização de dados pessoais é o direito à privacidade e à intimidade. A partir desse direito, como forma de protegê-lo e garanti-lo, torna-se relevante a proteção a outros direitos: a segurança, a confiabilidade e a transparência no armazenamento e uso dos bancos de dados com informações de natureza pessoal.

---

[29] 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. 122 p. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf > Acesso em: 10 jun. 2017.

[30] BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS. **A comprehensive approach on personal data protection in the European Union.** European Commission's Communication. BEUC, The European Consumers' Organisation's response. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf> Acesso em: 12 jun. 2017.

[31] Trecho do 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: < http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> Acesso em: 12 jun. 2017.

2.1 Uso de Dados Pessoais e o Direito à Privacidade

Conforme pontua Maceira (2015, p.15)[32], *"a personalidade é o gênero do qual a privacidade é a espécie".* O direito à intimidade ou à privacidade integra um dos cinco grandes agrupamentos dos direitos da personalidade, quais sejam: vida e/ou integridade física, honra, imagem, nome e intimidade/privacidade.[33]

Destaca-se que, conforme art. 11 do Código Civil, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária, excetuando-se apenas os casos previstos em leis.[34]

Quanto à problemática relacionada à conceituação de privacidade, Danilo Doneda (2006, p 101)[35] destaca que:

> Ao se tratar de privacidade, há de se fazer antes de tudo um esclarecimento inicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representá-la, propriamente ou não, é considerável; além da de "privacidade" propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados como "privatividade" e "privaticidade", por exemplo. O fato de a doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas.

O autor defende que é importante a consolidação de uma terminologia âncora, tal qual está estabelecido nos Estados Unidos com referência ao direito à *privacy*.[36] Ocorre, no entanto, que todos os termos listados pertencem a um conjunto de mesmo campo semântico e, dessa forma, essa multiplicidade de terminologias não causa grande prejuízo à fruição do direito. O que importa sim é definir de forma clara quais aspectos da privacidade serão realmente protegidos e, não menos importante, de que forma.

Ao continuar a análise sobre a conceituação da privacidade, o próprio autor afirma que "*o problema reside menos na definição em si do que em se determinar o que se espera*

---

[32] MACEIRA, Irma Pereira. **A proteção do direito à privacidade familiar na internet**. Rio de Janeiro: Editora Lumen Juris. 2015.

[33] SPAGLIARI, Italo. **Direitos da personalidade**. 26 abr. 2014. Disponível em: <https://italospagliari.jusbrasil.com.br/artigos/117634705/direitos-da-personalidade> Acesso em: 07 jun. 2017.

[34] DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro 1. Teoria Geral do Direito Civil**. 30ª ed. São Paulo: Saraiva. 2013, p. 137. Maria Helena Diniz, destaca, no entanto, o enunciado n. 139 do Conselho de Justiça Federal, aprovado na III Jornada de Direito Civil de 2004, que dispõe que "os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas em lei, não podendo ser exercidos com abuso de direito de seu titular, contrariamente à boa-fé objetiva e aos bons costumes"

[35] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 101.

[36] Idem, p. 102.

desta definição"[37] e ainda complementa "*que esta definição deve ser tomada mais como uma característica intrínseca da matéria do que como um defeito ou obstáculo"*[38].

O ordenamento jurídico pátrio, na Constituição Federal, escolheu os seguintes termos: intimidade e vida privada (conforme inc. X do art. 5º). Prestigiou também (no mesmo inciso) outros dois direitos correlatos como fundamentais: honra e imagem.

Apesar da escolha dos legisladores em fazer referência a dois termos nas disposições constitucionais, estes não devem ser entendidos como diferentes ou se referindo a aspectos divergentes; decidiu-se, provavelmente, pecar pelo excesso, tendo em vista o ineditismo da matéria com *status* constitucional.[39]

Questão que se coloca na contemporaneidade é como deve se dar a proteção do direito à privacidade em um contexto em que os próprios indivíduos escolhem expor suas informações pessoais, seja por meio de redes sociais como Facebook, Twitter e Instagram, seja em diversos *reality shows* como o Big Brother.

Uma forma de lidar com o conceito de *privacidade* tendo em vista essa grande exposição, muitas vezes voluntária dos indivíduos, é por meio de uma compreensão dialética. Como bem dispõe Thibes (2013, p.94)[40], a privacidade compreende dois aspectos: a existência pública e a privada de cada indivíduo. Esses dois aspectos variam de magnitude e características no decorrer da existência da humanidade, ou seja, nesse momento há uma maior abertura, uma preponderância do que é visto como existência pública quando em comparação a tempos passados.

Drummond (2003, p.18) refere-se ao direito de intimidade como *"a distância confortável que uma pessoa mantém, espontaneamente, desde a sua mais profunda individualidade até o mundo exterior."* Entende, dessa forma, a privacidade como um direito subjetivo.

---

[37] Idem, p. 104.
[38] Idem, p. 106.
[39] Idem, p. 110.
[40] THIBES, Maria Zanata. **O Público, o privado e o íntimo na era digital**. São Paulo: Biblioteca 24 horas, 2013.

Nessa mesma linha, Mendes[41] acredita que cada indivíduo possui autonomia para determinar qual o limite de exposição e o quanto de informações ele quer preservar distante da vida pública. Trata-se de não negar o direito à autodeterminação individual e respeitar a visão de uma sociedade pluralista com diferentes opiniões. Ela pontua que, caso assim não fosse, a privacidade não mais seria um direito, passando a constituir-se um dever.

É interessante, no entanto, a visão do autor Doneda[42] (2006), que traz uma reflexão sob um diferente prisma ao defender que o direito à privacidade muda de perspectiva e ganha um caráter coletivo, passando a ser entendido com um direito difuso.

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania da própria atividade política em sentido amplo e dos direitos da liberdade de uma forma geral.

Essa abordagem é de grande relevância ao se pensar a utilização em imensa escala de dados pessoais. A má utilização dessas informações pode potencialmente lesar não apenas um indivíduo, mas sim todo um grupo, classe ou os consumidores difusos. Essa ideia se tornará mais clara ao se tratar de dados sensíveis, assunto que será posteriormente tratado na seção acerca do uso de dados pessoais e discriminação.

Diante dessa análise da importância da privacidade frente ao incremento da utilização de dados pessoais no mundo digital, a proteção jurídica a esse direito da personalidade se torna indispensável para a garantia de fruição aos indivíduos de um espaço interno, livre de censuras e com possibilidade do exercício de sua liberdade e do livre pensar, e também para que os consumidores possam encontrar na internet e outros meios eletrônicos a confiança de que seus dados não serão comercializados ou impropriamente utilizados.[43]

Espera-se, da mesma maneira, que a proteção desse direito tão caro à dignidade da pessoa humana possa consolidar o exercício da privacidade como um direito coletivo, não no sentido de limitar a autonomia dos consumidores quanto aos dados que eles realmente desejem disponibilizar em suas redes sociais ou por instrumentos eletrônicos, mas, sim, de forma que eles possuam a certeza de que esses dados não serão usados de forma injusta,

---

[41] MENDES, Laura Schertel. **Transparência e privacidade: violação da informação pessoal na sociedade de consumo**. 156 p. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília. 2006, p. 22 e 23.
[42] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.146.
[43] MACEIRA, Irma Pereira. **A proteção do direito à privacidade familiar na internet**. Rio de Janeiro: Editora Lumen Juris. 2015, p.23.

incerta, em canais por eles desconhecidos e não autorizados. Enfim, que o mundo digital seja um mundo em que se potencializem as trocas de informações voluntárias e que estas contribuam para a formulação e a disponibilização de serviços mais adequados a cada cliente.

2.2 Uso de Dados Pessoais e a Potencial Utilização Discriminatória

Dentre os dados pessoais, criou-se uma categoria especial que consiste nos dados sensíveis. São todos aqueles cuja utilização pode gerar algum tipo de discriminação.

> Seriam tipos de informação que, caso sejam conhecidas ou processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva que apresentaria maiores riscos potenciais que a média para a pessoa e não raro para uma coletividade. Alguns desses dados seriam as informações sobre raça, credo político ou religioso, opções sexuais, o histórico médico ou dados genéticos de um indivíduo.[44]

Entretanto, uma questão que se coloca é se os dados, em si próprios, tem o potencial de causar questões discriminatórias e de preconceito. *"Um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo."*[45]

Realmente, todo e qualquer dado, dependendo da forma que for manipulado, pode trazer à tona tratamentos antiéticos que ensejam práticas discriminatórias. Todavia, há certos tipos de dados que possuem um potencial ainda maior para isso. Um exemplo clássico são as informações de histórico médico e genético de um indivíduo. Até tempos atrás, por exemplo, pessoas eram deixadas de ser contratadas para um trabalho por serem portadoras do vírus HIV.

Sobre tal prisma, Rodotá adverte para o perigo do uso de dados genéticos tanto pra questões trabalhistas quanto para questões relacionadas a serviços financeiros, como na contratação de crédito e de seguros. [46]

---

[44] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 146.

[45] 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. 122 p. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf > Acesso em: 10 jun. 2017. O Caderno da ENDC faz referência ao trecho muito elucidativo de Colin Bennett (1992, p.35): "*There are no harmless data, there are no harmful data. A datum is a datum – it is that which is given. It is what data you string together and what you do with them … which may or may not do harm"*

No contexto de serviços financeiros, quais dados podem ser considerados como sensíveis? Além dos já acima dispostos (referentes à raça, à religião, à ideologia política, à opção sexual, à saúde e à genética) haveria outras classes de dados que também deveriam estar compreendidas nessa categoria.

Como já relatamos anteriormente, uma das principais utilizações de dados alternativos e de *Big Data* é para o escore de crédito. Essa utilização tem como possível consequência benéfica a inclusão de consumidores que até então estavam excluídos do mercado de crédito por não possuírem informações suficientes em seus cadastros "tradicionais". Assim, a utilização de dados pessoais seria bem-vinda para a inclusão financeira.

Todavia, se as informações advindas dos processos de mineração de dados alternativos e de *Big Data,* referentes a dados de consumo e de capacidade de pagamento de suas contas periódicas, por exemplo, permitissem que os consumidores até então excluídos fizessem agora parte do sistema, mas a custos altíssimos de juros? Esses dados pessoais estariam sendo usados com potencial de aumentar ainda mais a desigualdade já existente?

A resposta é afirmativa. No entanto, não seria razoável impedir práticas dessa natureza. A evolução tecnológica fornece grandes possibilidades de avanços em diversas áreas do saber, ao fornecer informações valiosas sobre os consumidores, possibilitando grandes oportunidades para aprimoramento da prestação de serviços. Também pode sim auxiliar na formulação de políticas públicas que estimulem e promovam a inclusão financeira de forma estruturada e adequada aos diversos perfis de consumidores e que atendam a demanda de grupos vulneráveis.

Assim, o que se busca é a implementação de instrumentos regulatórios para garantir que a utilização de dados alternativos e *Big Data* não produza efeitos nocivos ou, quando esses forem inevitáveis, que sejam disponibilizados meios para efetiva reparação. No Capítulo 5, serão discutidos possíveis rumos regulatórios e de políticas públicas.

---

[46] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008, p. 250. Ainda com relação à preocupação da coleta e utilização de dados genéticos, Rodotá alerta para o grande perigo de programas de disponibilização de testes genéticos pela internet.

2.3 Uso de Dados Pessoais e o Direito à Segurança e Confiabilidade dos Bancos de Dados

No contexto digital, condição indispensável para garantir o pleno gozo ao direito à privacidade é a segurança e a confiabilidade no armazenamento, gerenciamento e análise dos bancos de dados. Alguma falha em determinada etapa do processamento dos dados pessoais pode causar sérias lesões a consumidores individuais ou, pior ainda, a toda uma coletividade.

Dessa forma, deve-se buscar entender quais as principais formas de ataques à segurança de banco de dados de forma a melhor buscar caminhos legais para coibi-las.

Bernstein et al (1997, pp.29 e 30) elencam as principais classes de ameaças de sistemas informatizados:[47]

a) Espionagem – a qual consiste na observação de troca de informações confidenciais pela rede;

b) Disfarce – quando um indivíduo assume secretamente o lugar de outro, passando então a ter privilégios de acesso;

c) *Replay* – trata-se da observância de sequências de eventos para posterior reprodução, de forma a possibilitar, por exemplo, esquemas de autenticação;

d) Manipulação de dados - refere-se ao comprometimento indetectável da integridade de dados;

e) Roteamento incorreto – diz respeito a interceptações de mensagens;

f) Armadilha ou cavalo de Troia – está relacionado à substituição de um programa ou sistema com seção alterada tendo por finalidade a execução de atividade má intencionada;

g) Vírus – referem-se a códigos de programa que, ao se associarem a um arquivo ou programa, se autorreproduzem e os modificam;

h) Repúdio – quando um indivíduo ou grupo nega participação em uma comunicação eletrônica, tais quais transações financeiras ou contratos eletrônicos. Decorrem de falta de controles na origem, destino, tempo ou prova de entrega; e

[47] BERNSTEIN, Terry; BHIMANI, Anish B.; SCHULTZ, Eugene; SIEGEL, Carol A. **Segurança na internet**. Rio de Janeiro: Campus, 1997.

i) Negação de serviço – Quando não é possível acesso a um sistema ou aplicação por, por exemplo, esgotamento da capacidade da rede ou do próprio sistema.

Observa-se que qualquer uma dessas ameaças, individualmente ou em conjunto, possui o potencial de prejudicar o exercício da privacidade dos consumidores: por um lado, uma vez que atuam contrariamente à fidedignidade e à não publicação não autorizada de dados pessoais, além de dificultar o direito de acesso, de pedido de exclusão e de correção do titular dos dados; por outro, prejudicam as empresas e entidades que manuseiam de forma legítima e ética os dados obtidos legalmente de seus consumidores e que desejam, por meio do manejo desses, fornecer serviços mais adequados.

Uma das formas de se proteger as informações pessoais em bancos de dados pessoais é a materialização de preceitos como a "minimização de dados" e o "legítimo interesse", decorrentes do princípio da necessidade de coleta de dados pessoais. Segundo esses preceitos, devem ficar registrados nos bancos de dados apenas aquelas informações pessoais realmente necessárias ao desenvolvimento da atividade de determinada organização. Isso se demonstra necessário uma vez que, quanto maior o número de dados registrados, mais eles podem se tornar alvos de ataque de *hackers*[48].

Outra medida apontada é a utilização de plataformas abertas:

> Padrões abertos e tecnologias de código aberto (*open source*) possuem impacto positivo na segurança, pois possibilitam o controle por inúmeros pares e desenvolvedores, permitindo, além disso, o aprendizado conjunto e o estímulo a um maior número de competidores – o que possui o potencial efeito de redução de oligopólios, aumento da competição e benefícios aos consumidores finais.[49]

Weber (2010)[50] aponta quatro requisitos de segurança e privacidade: i) "*resiliência aos ataques*", " *autenticação de dados*", "*controle de acesso*", e "*privacidade do cliente*". Destaca que para conquista desses requisitos foram desenvolvidas as "*tecnologias de*

---

[48] ZANATTA, Rafael A. F. **Internet das Coisas: privacidade e segurança na perspectiva dos consumidores**. Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017, Instituto Brasileiro de Defesa do Consumidor, p.5. Disponível em: <http://www.idec.org.br/ckfinder/userfiles/files/Contribuic%CC%A7a%CC%83o%20Pu%CC%81blica_%20Idec_%2006022017.pdf>. Acesso em: 10 jun. 2017.

[49] Idem.

[50] WEBER, Rolf H. Internet of things – new security and privacy challenges. **Computer Law & Security Review** v. 26, n. 1, p. 23–30, 2010. Disponível em: <https://www.researchgate.net/file.PostFileLoader.html?id=55c4147460614b25168b45a3&assetKey=AS%3A273981783904256%401442333755312> Acesso em: 11 jun. 2017.

melhoria da privacidade", que consitem em: *"Virtual Private Networks (VPN)*", "*Transport Layer Security (TLS)*", "*DNS Security Extensions (DNSSEC)*", "*Onion Routing encrypts*", "*Private Information Retrieval (PIR)*", e "*Peerto-Peer (P2P) systems*".

É de grande relevância a regulação de requisitos mínimos de segurança como forma de salvaguardar os direitos dos consumidores titulares de informações constantes de bancos de dados e também a confiança nas instituições financeiras, tão relevante para o regular funcionamento de todo o sistema financeiro.

3. REGULAMENTAÇÃO DE USO DE DADOS PESSOAIS NO CONTEXTO INTERNACIONAL

A utilização de dados pessoais passou a ser uma preocupação mundial. Assim, o tema vem sendo tratado e regulado por organismos internacionais e diversos países. Conhecer a experiência internacional, a fim de trazer subsídios para a análise de melhor forma de regular a matéria, é fundamental.

Acerca da regulação de dados no mundo, uma publicação muito interessante é disponibilizada por DLA Piper, uma firma de advocacia global.[51] Eles realizam um estudo periódico sobre o estado da arte da regulação de dados em vários países (ao todo, no momento, eles possuem informações sobre 93 países).[52] Por meio dessa análise, eles disponibilizam um mapa mundial demonstrando quão fortemente a matéria é regulada em cada região estudada[53] (nesse mapa, também é possível realizar a comparação entre dois países).

[51] Está localizada em mais de 40 países, nas Américas, Europa, Oriente Médio, África e Ásia.
[52] DLA PIPER GLOBAL LAW FIRM. **Data protection laws of the world: full handbook**. 2017. Disponível em: <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all> Acesso em: 14 jun. 2017.
[53] Disponível no sítio eletrônico: <https://www.dlapiperdataprotection.com/index.html>

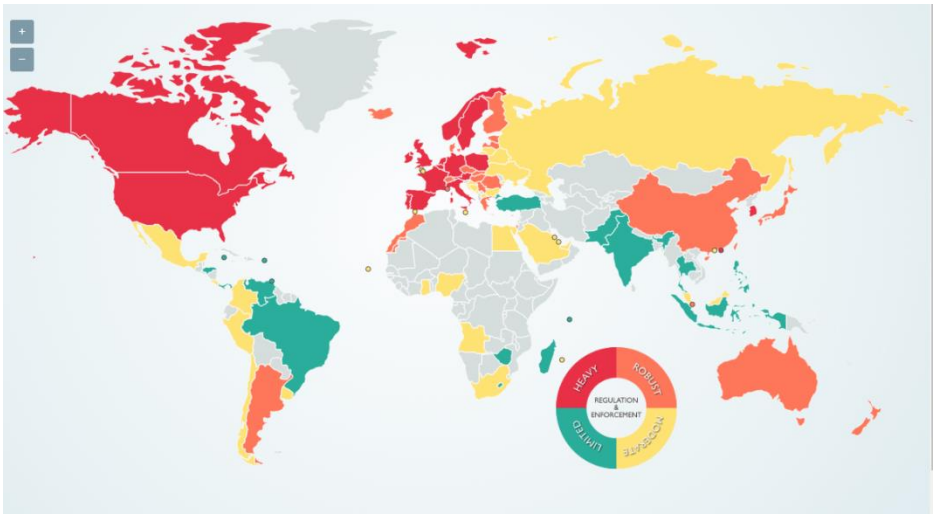

Figura 1. Classificação de regulação de uso de dados pessoais no mundo. Em vermelho, os países em que uso de dados pessoais são mais fortemente regulados. Extraído de https://www.dlapiperdataprotection.com/index.html (DLA Piper, 2017).

Conforme pode ser observado, entre as regiões com regulações mais bem estabelecidas concernentes à proteção dos direitos relacionados ao uso de dados pessoais estão a América do Norte e a Europa. Assim, a partir de documentos de organismos internacionais e legislações transnacionais, faremos uma breve análise da situação da regulamentação e regulação do uso de dados no contexto internacional e na União Europeia. Para efeito de comparação com a legislação brasileira, escolhemos focar na regulação da União Europeia (UE), tendo em vista esta última possuir um grande histórico sobre a matéria, bem como o fato de que a Regulação Geral de Proteção de Dados ou *General Data Protection Regulation* – GPDR[54], legislação mais recente da UE que entrará em vigor no ano de 2018, vinculará empresas mundialmente, pois alcançará qualquer empresa que trate dados de consumidores europeus, conforme será visto adiante.

3.1 A Proteção de Dados em Organismos Internacionais

A proteção à intimidade remonta ao ano de 1948, conforme disposição da Declaração Universal dos Direitos Humanos, em seu art. 12, que estabeleceu que

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[54] Disponível em: <http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf> Acesso em: 18 jun. 2017.

Em 1950, tendo como base os dispositivos trazidos pela Declaração Universal, a Convenção Europeia de Direito Humanos, em seu art. 8º dispôs, além do respeito à vida privada e familiar e ao lar, fez menção expressa à defesa das correspondências[55]. Essa proteção é oponível aos Estados e a particulares e só pode ser mitigado nos casos previstos na própria convenção.

Também dispuseram sobre a inviolabilidade da vida privada e da correspondência o Pacto Internacional sobre Direitos Civis e Políticos, de 1966, em seu art. 17, e a Convenção Americana de Direitos Humanos ("Pacto São Jose de Costa Rica"), de 1969, em seu art. 11.

Em 1990, a Organização das Nações Unidas – ONU publicou as *Guidelines for the Regulation of Computerized Personal Data Files*[56], que estabeleceram uma série de princípios sobre a manipulação de dados pessoais que deveriam embasar as legislações nacionais sobre o tema:

> a) *Princípio da legalidade e justiça*: Discorre que não podem ser coletadas ou processadas informações pessoais de forma injusta ou ilegal, ou ainda contrariamente aos princípios contidos na Carta das Nações Unidas.
> b) *Princípio da precisão:* Dispõe sobre a obrigação dos processadores dos bancos de dados de realizar checagens para assegurar a acurácia dos dados armazenados e também que estes estejam completos e atualizados.
> c) *Princípio da especificação de propósitos*: Estabelece a obrigação de se determinar o propósito de determinado banco de dados, bem como informar ao titular de dados sobre esse propósito, garantindo que as informações pessoais só sejam utilizadas para esse propósito especificado e somente pelo tempo necessário ao seu alcance.
> d) *Princípio de acesso pela pessoa interessada:* Determina a obrigatoriedade de acesso do titular – tempestiva, gratuita e de forma compreensível – a suas informações.

---

[55] CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (Convenção Europeia de Direitos Humanos)**, adotada em 4 de novembro de 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf> Acesso em: 12 de jun. 2017.
[56] ASSEMBLEIA GERAL DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Resolução nº 45/95. Guidelines for the regulation of computerized personal data files.** Disponível em: <http://www.refworld.org/pdfid/3ddcafaac.pdf> Acesso em: 10 jun. 2017.

e) *Princípio da não discriminação:* Proíbe a coleta de qualquer tipo de dados que possam ensejar discriminação arbitrária e ilegal, a não ser nos casos expostos no princípio de exceção.

f) *Princípio da exceção*: Admite o estabelecimento de exceções à aplicação de um ou mais princípios em casos relacionados à segurança nacional, ordem pública, saúde pública ou moralidade, e razões humanitárias.

g) *Princípio da segurança:* Estabelece a necessidade do desenvolvimento de medidas de segurança que garantam segurança aos dados pessoais e os protejam contra acidentes e fraudes.

h) *Princípio da supervisão e da sanção:* Determina a designação autoridade para supervisionar a aderência dos controladores e possuidores dos bancos de dados às regras estabelecidas, bem como aplicar sanções quando do seu descumprimento.

i) *Princípio do fluxo de dados internacionais:* Indica que se deve garantir o livre fluxo de informações entre países que possuam o mesmo nível de proteção a dados pessoais.

j) *Princípio do campo de aplicação*: Recomenda que os princípios acima estipulados sejam aplicados a todos os bancos de dados computadorizados públicos e privados, podendo-se estender também, em certos casos, a bancos de dados manuais.

A Organização para a Cooperação e Desenvolvimento Econômico – OCDE publicou, em 1980, *as Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[57], as quais foram atualizadas em 2013. Como consta nas definições gerais em seu anexo inicial, essas diretrizes "se aplicam a dados pessoais, seja no setor público ou privado, que, devido ao modo como são processados, ou por causa de sua natureza ou do contexto em que são usados, representam perigo para privacidade e liberdades individuais".

As diretrizes da OCDE listam oito princípios base de aplicação, a saber: limitação de coleta, qualidade dos dados, especificação de propósitos, limitação de uso, medidas de proteção, participação do indivíduo, responsabilização e princípio da abertura. Embora com nomenclatura um pouco diferente da utilizada nos princípios das diretrizes da ONU, listados

[57] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD guidelines governing the protection of privacy and transborder flows of personal data.** 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>Acesso em: 24 jun.2017

anteriormente, quase todos aqueles princípios são abarcados de uma maneira ou de outra nas diretrizes da OCDE. À exceção do último mencionado, o princípio de abertura, que preceitua que deve haver uma política geral nos países com vistas à abertura para implementação de políticas que garantam o conhecimento sobre a existência de bancos de dados, se eles possuem dados de natureza pessoal, quais são os propósitos de sua utilização e aonde eles estão armazenados.

Kuschewsky (2013)[58] destaca os novos conceitos introduzidos com a atualização das *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* feita em 2013, que se referem à implementação de programas de gerenciamento de privacidade (processos de avaliação, auditoria, treinamento e políticas educativas), ao estabelecimento de estratégias nacionais de privacidade nos países membros (e autoridades responsáveis por sua aplicação e cumprimento), à obrigatoriedade da notificação de quebras de segurança (tanto aos indivíduos afetados quanto à autoridade responsável) e ao aprimoramento da interoperabilidade (visando a dimensão global da privacidade em acordos internacionais). Ademais, o princípio da responsabilização foi reforçado, lembrando que, independentemente da localização dos dados, o controlador dos dados é responsável por eles e deve protegê-los continuamente com várias medidas técnicas e organizacionais.

3.2 A Proteção de Dados na União Europeia

3.2.1 Convenção 108

Em razão do contexto de incremento de uso de dados pessoais na União Europeia, e com o intuito de conciliar o livre trânsito de informações com o direito à privacidade, em 1981 foi assinada a Convenção para a proteção de indivíduos com relação a processamentos automáticos de dados pessoais (Convenção 108, também conhecida como Convenção de

[58] KUSCHEWSKI, Monika. **Revised OECD Privacy Guidelines Strengthen Accountability Principle**. 23 set. 2013. Disponível em: < https://www.insideprivacy.com/international/revised-oecd-privacy-guidelines-strengthen-accountability-principle/> Acesso em: 24 jun. 2017.

Estrasburgo) [59]. As obrigações nela contidas alcançam tanto o Estado quanto particulares (art. 3º da Convenção).

> É possível considerar a Convenção de Strasbourg como o ponto de referência inicial do modelo europeu de proteção de dados pessoais, mesmo porque ela é fruto de reflexões e debates sobre os rumos da matéria no espaço europeu.[60]

Essa convenção estabelece, em seu art. 5º, uma série de obrigações referentes ao processamento automático de dados: a obtenção e o processamento devem ser feitos de forma legal e justa; o armazenamento deve ser adequado, relevante e proporcional aos seus propósitos legítimos, não devendo exceder a estes; os dados devem ser corretos e atualizados quando necessários; devem ser inidentificáveis com relação aos sujeitos a que se referem; e não devem ser armazenados por tempo superior ao necessário.

Verificamos, dessa forma, que já estavam contidos na Convenção 108 princípios caros à segurança dos dados pessoais, tais como: a minimização de dados e o legítimo interesse, e a necessidade de coleta de dados pessoais.

Sobre os direitos dos indivíduos e seus dados armazenados, o art. 8º determina que deve ser garantido o acesso aos seus dados armazenados, em tempo razoável, bem como a possibilidade de correção dos dados incorretos ou até mesmo a exclusão dos dados.

Outro ponto importante estabelecido refere-se à categorização dos dados sensíveis, denominados pela Convenção, em seu art. 6º, como categoria especial de dados pessoais. No documento, constam como dados sensíveis: origem racial, opiniões políticas, crenças religiosas, referentes à saúde ou vida sexual, e relacionados ao histórico criminal. Tais informações só podem ser automaticamente processadas caso haja garantias nas leis nacionais para proteção desses dados.

Com relação à segurança na manipulação de dados pessoais, o art. 7º estabelece que devem ser tomadas medidas que assegurem a proteção de dados para que eles não sejam perdidos ou sofram ataques de terceiros não autorizados. Entretanto, não há maior detalhamento sobre a forma de proteção.

---

[59] CONSELHO DA EUROPA. Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. European Treaty Series n. 108, Estrasburgo, 28 jan. 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm> Acesso em 09 jun. 2017.

[60] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 235.

As obrigações previstas na Convenção não podem ser afastadas a não ser quando justificadas pela segurança, por interesses monetários do Estado, na supressão de infrações penais, para proteger os direitos e a liberdade do possuidor dos dados ou de terceiros. Também não são alcançados pela Convenção dados utilizados para estatística ou pesquisas científicas, desde que não haja claro risco de violação da privacidade de a quem os dados se referem (art. 9º).

O art. 4º determina que os países signatários devem implementar as mudanças legais em seus ordenamentos jurídicos a fim de garantir a consecução dos princípios básicos de proteção de dados. Assim, a Convenção 108 possui efeito vinculante com relação a seus membros. Até o determinado momento é o único instrumento internacional com tal efeito.[61]

Podem ser aceitas adesões à Convenção 108 de outros países que não fazem parte do Conselho da Europa. Até o presente momento dois países nessa condição aderiram à Convenção: Uruguai[62] e República de Maurício[63].

3.2.2 Diretiva 95/46/EC

O Parlamento Europeu e o Conselho da União Europeia editou, em 1995, Diretiva relacionada à proteção de dados pessoais e à livre circulação desses dados. A Diretiva teve como objetivo, dentre vários outros, proteger os direitos humanos e a liberdade, especialmente no tocante à privacidade, e garantir padrões mínimos para tratamento de dados pessoais entre todos os seus Estados membros, com a finalidade de evitar barreiras ao fluxo de informações. Dessa forma, em seu art. 1º, a Diretiva proíbe a restrição de fluxos de informações entre os Estados membros da União Europeia.

Em seu art. 2º, são compreendidas as definições básicas para a Diretiva. O conceito de dados pessoais já foi exposto anteriormente neste trabalho, na seção relativa à utilização de dados pessoais e Direito do Consumidor (Capítulo 2), se referindo a qualquer informação referente a pessoa singular que possibilite a identificação de seu titular. Com relação ao

---

[61] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Handbook on European data protection law**. 2014, p.16. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> Acesso em: 17 jun. 2017.
[62] Idem, p.17.
[63] CONSELHO DA EUROPA. **Newsroom – Mauritius joins "Convention 108".** 2016**.** Diponível em: shttps://www.coe.int/en/web/human-rights-rule-of-law/-/international-data-protection-conference-mauritius-joins-convention-108-. Acesso em: 25 de jun. de 2017.

processamento de dados pessoais, a Diretiva inclui tanto o processamento automático quanto o manual, diferentemente da Convenção 108, que se focou apenas no primeiro. No entanto, estabeleceu também exclusões ao seu alcance, como segurança pública e estatal, e também excluiu aqueles produzidos e guardados por um indivíduo no seu cotidiano exclusivamente pessoal ou familiar.

Outros conceitos interessantes inseridos é o de controlador e processador, estabelecendo a distinção entre os dois. O controlador diz respeito à pessoa física ou jurídica que estabelece qual é o propósito e significado para o processamento de determinado banco de dados. Já o processador é de fato quem manuseia os dados, de acordo com os propósitos estabelecidos pelo controlador.

Definição muito relevante compreendida na Diretiva é o consentimento do titular dos dados, que refere-se à indicação de vontade livre e específica de permissão do tratamento de seus dados.

Tendo em vista o disposto na Diretiva e, respeitando seus limites, cada Estado membro teve que especificar as condições legais para o tratamento de dados pessoais.

A Diretiva estabeleceu uma série de princípios fundamentais para o arquivamento e processamento de dados: i) *Processamento de dados justo e legal*; ii*) limitação e especificação de propósito*; iii) *armazenamento mínimo*, iv) *transparência*, v) *qualidade*, vi) *segurança*, vii) *categoria especial de dados* e viii) *minimização de dados*, e foi adotada pelos 28 Estados membros da União Europeia; entretanto, com significativas diferenças em suas legislações domésticas.[64]

3.2.3 Carta dos Direitos Fundamentais da União Europeia

Em 2000 foi proclamada a Carta dos Direitos Fundamentais da União Europeia, que está dividida em seis capítulos: *dignidade*, *liberdade*, *igualdade*, *solidariedade*, *direito dos cidadãos e justiça*.[65]

---

[64] DLA PIPER GLOBAL LAW FIRM. **Data protection laws of the world: full handbook**. 2017. Disponível em: <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all> Acesso em: 14 jun. 2017, p. 6.

[65] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Handbook on European data protection law**. 2014, p.20. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> Acesso em: 17 jun. 2017.

É um documento importante para proteção de dados pois reitera e fortalece no território da Europa os direitos de respeito à família e à vida privada (art. 7°) e, especificamente, a proteção de dados (art. 8º). Nota-se que, a partir desse momento na Europa, a proteção de dados ganha status de direito fundamental. [66]

3.2.4 Regulação Geral de Proteção de Dados

A Regulação Geral de Dados ou *General Data Protection Regulation* - GDPR teve seu texto finalizado em 2016, e começará a vigorar em de 2018, em todos os Países membros da União Europeia, sem a necessidade de edição de norma nacional nas legislações de cada país. Vincula-se, dessa maneira, várias empresas e vários países a se ajustarem aos seus dispositivos e inovações.[67]

Logo em suas definições iniciais, no seu artigo 4º, o GDPR conceitua dados pessoais de forma mais ampla, abrangendo explicitamente fatores identificadores como nome, dados de localização e identificadores *online*, que não constavam da Diretiva anterior. Ademais, ainda acrescenta um fator específico para se identificar uma pessoa natural antes não contemplado: o fator genético.

Outras definições inéditas em relação ao marco regulatório anterior foram os conceitos apresentados de *profiling* e o de *pseudonymisation*. Importante definição para os propósitos deste trabalho, o art. 4º (4) explicita que *profiling* significa qualquer forma de processamento de dados pessoais para avaliar certos aspectos a uma pessoa de forma a analisar ou prever comportamentos relativos a trabalho, situação econômica, saúde, preferências, etc. *Pseudonymisation* (5), por sua vez, seria o processamento de dados pessoais de forma a estes não poderem ser mais atribuídos a um sujeito específico sem uso de informações adicionais, mantidas separadamente e submetidas a medidas técnico-organizacionais que as garantam não serem atribuídas a uma pessoa identificada ou identificável, como um pseudônimo de uma pessoa mesmo.

---

[66] Idem, p. 20.
[67] DLA PIPER GLOBAL LAW FIRM. **Data protection laws of the world: full handbook**. 2017. Disponível em: <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all> Acesso em: 14 jun. 2017, p.6.

Outra adição conceitual concernente à segurança foi a explicitação da definição de *personal data breach*. Além de outros, mais conceitos que mereceram definições no art. 4º deste regramento foram os de (13) dados genéticos, (14) dados biométricos e (15) dados referentes à saúde, todos dados sensíveis e relevantes de serem explicitamente apresentados.

Em seu Capítulo II, artigo 6º, o GDPR elenca os princípios relativos ao processamento de dados pessoais, postulando que estes devem ser:

> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (princípios da licitude, lealdade e transparência);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais (...)(princípio da limitação das finalidades);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados);
> d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (exatidão);
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (...), sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (limitação da conservação);
> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizacionais adequadas (integridade e confidencialidade)[68];

Visando proteger os dados pessoais de todos os cidadãos europeus sob sua influência, o GDPR na verdade alcançará empresas globalmente, visto que em suas diretrizes é estabelecida bem sua jurisdição: se aplica a controladores e processadores na União Europeia, mesmo que o processamento em si não se dê dentro da UE, e se aplica também a controladores e processadores não estabelecidos na UE quando oferecem bens ou serviços a cidadãos europeus ou quando o monitoramento se dê em algum lugar dentro da Europa (Portal da EUGDPR)[69]. Ponto esse que, de acordo com Reis (2016)[70,] está sendo

---

[68] Disponível em: <http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf> Acesso em: 18 jun. 2017.

[69] EUGDPR.ORG. **Key changes with the general data protection regulation**. Disponível em: <http://www.eugdpr.org/key-changes.html> Acesso em: 17 jun. 2017.

[70] REIS, Daniel. Preparados para as novas regras sobre dados pessoais? **Público**, 12 mai 2016. Disponível em: <https://www.publico.pt/2016/05/12/economia/noticia/preparados-para-as-novas-regras-sobre-dados-pessoais-1731660>. Acesso em: 17 jun. 2017.

contestado por muitas grandes empresas norte-americanas, tais como Google, Facebook e Microsoft.

O Regulamento fortalece o direito dos cidadãos ao definir claramente o que seria o consentimento: uma ação positiva, manifestação de vontade livre e explícita, impedindo que omissão ou consentimento tácito sejam aceitos. Ainda esclarece que os termos do consentimento devem vir em linguagem clara e direta, corolário do princípio da transparência, e garante ao titular dos dados a possibilidade de recusar ou retirar o consentimento sem ser prejudicado.

Outros direitos e obrigações listados no GDPR e considerados mudanças chave (Saias, M.A.)[71] envolvem:

a) *"A portabilidade dos dados"*, em que o titular dos dados tem o direito a receber e transmitir esses dados que lhe sejam relacionados. Para tanto, o titular dos dados também tem seu direito ao acesso garantido, sendo obrigação do controlador confirmar se há dados seus sendo tratados, onde e para qual propósito, devendo até mesmo enviar-lhe uma cópia destes, aumentando sobremaneira a transparência do processo;
b) *"O direito ao apagamento dos dados (ou direito de esquecimento*[72]*)*", em que o titular dos dados pode solicitar o apagamento de seus dados pessoais e a cessação de sua propagação e disseminação, num prazo razoável, sem demoras injustificadas. Tais requerimentos devem, é claro, levar em consideração também o interesse público na disponibilidade de tais dados como ponderação de sua aplicabilidade, conforme pontuado no próprio Regulamento;
c) "*A proteção dos dados desde a concepção (privacy by design)"*, um conceito já existente há alguns anos mas que agora ganha respaldo legal, em que o responsável pelo tratamento dos dados é obrigado a incluir medidas técnicas e organizacionais desde sua implementação, ativamente e não apenas reativamente, visando a proteção dos dados pessoais, aplicando os princípios da minimização

[71] SAIAS, Marco Alexandre. **O novo regulamento geral de proteção de dados pessoais, em 3 minutos!**. Disponível em: <https://www.pra.pt/pt/communication/news/o-novo-regulamento-geral-de-protec-o-de-dados-pessoais-em-3-minutos/>. Acesso em: 17 jun. 2017.
[72] Em inglês: *right to be forgotten.*

dos dados, limitação, e também o conceito da pseudonimização de dados pessoais e encorajando a encriptação destes (Hawthorne, N.)[73];

d) *"Obrigatoriedade de notificação de violação de segurança, ou breach notification".* Segundo o art. 33 da norma, aquelas violações que possam resultar num risco para os direitos e liberdades fundamentais dos indivíduos titulares dos dados devem mandatoriamente ser reportadas às autoridades de controle, dentro de 72 horas depois de terem sido percebidas as violações ou "quebras" de segurança. Conforme esclarece artigo da Comissão Nacional de Protecção de Dados de 2017[74], todas as violações devem ser documentadas, mesmo as que não forem notificadas ao titular.

4. REGULAMENTAÇÃO DE USO DE DADOS PESSOAIS NO BRASIL

Ainda não há no Brasil uma norma específica para a regulamentação do armazenamento, processamento e transferência de dados pessoais. No entanto, existem várias disposições legais que se referem ao direito à privacidade, tendo tal direito inclusive *status* constitucional.

Conforme já ressaltado anteriormente, a Carta Magna reconhece a vida privada e a intimidade, bem como a imagem e a honra, direitos fundamentais, conforme disposto em seu art. 5º, inc. X[75].

Atualmente, tramitam no congresso três projetos de lei que pretendem regulamentar a matéria relativa à utilização de dados pessoais no território nacional: PL nº 4.060/2012, PLS nº 330/2013, e o PL nº 5.276/2016.

Além disso, a Carta Magna estabelece ação constitucional que tem por objetivo garantir o direito de acesso do cidadão a suas informações constantes de bancos de dados, denominada *habeas data*, prevista no art. 5º, inc. LXXII e regulada pela Lei nº 9.507, de 12 de novembro de 1997.

---

[73] HAWTHORNE, Nigel. **9 important changes in the new EU GDPR likely to become law in 2016**. Disponível em: <https://www.skyhighnetworks.com/cloud-security-blog/9-important-changes-in-the-new-eu-gdpr-likely-to-become-law-in-2016/>. Acesso em: 17 jun. 2017.

[74] COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS. **10 medidas para preparar a aplicação do regulamento europeu de proteção de dados**. 28 jan. 2017.
Disponível em: <https://www.cnpd.pt/bin/rgpd/10_medidas_para_preparar_rgpd_cnpd.pdf>. Acesso em: 17 jun. 2017.

[75] BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988.

Ademais, a legislação nacional abarca ordenamento jurídico de proteção ao consumidor avançada, estabelecido pelo Código de Defesa do Consumidor, que inclusive compreende regras sobre a inscrição de informações do consumidor em bancos de dados e cadastro[76].

Com relação à regulação de serviços financeiros, ainda que não haja até o momento nenhuma norma específica para o uso de dados, já existem diversas normas setoriais que impactam na forma que os dados pessoais podem ser processados por instituições financeiras.

4.1 Código de Defesa do Consumidor

A Constituição Federal estabeleceu, em seu art 5º, inc. XXXII, que *"o Estado promoverá, na forma da lei, a defesa do consumidor*". Além disso, em seu art. 170, que trata da ordem econômica, estabeleceu, entre outros princípios, o direito do consumidor (inc. V).

O Código de Defesa do Consumidor – CDC foi editado em 11 de setembro de 1990, constituindo-se em:

> Norma de ordem pública e interesse social que se originou de modo especial e diferente de outras leis vigentes no País. Isto porque o CDC foi elaborado em decorrência de um comando contido no Ato das Disposições Constitucionais Transitórias (ADCT), parte da Constituição Federal de 1988 que, em seu artigo 48, assim determinou: "O Congresso Nacional, dentro de cento e vinte dias da promulgação da Constituição, elaborará Código de Defesa do Consumidor".[77]

Marques (2007) ressalta o duplo dever do Estado advindo das normas constitucionais: este deve por um lado exercer uma tutela protetiva, evitando qualquer lesão ao Direito do Consumidor. Por outro lado, deve atuar positivamente, implementando políticas públicas que permitam a materialização desse direito constitucional.[78]

---

[76] BRASIL. Código de Defesa do Consumidor, de 11 de setembro de 2015.

[77] SECRETARIA NACIONAL DO CONSUMIDOR. **Manual de direito do consumidor**. 4. ed. Brasília: Escola Nacional de Defesa do Consumidor. 2014, p.28. Disponível em: <http://www.defesadoconsumidor.gov.br/images/manuais/manual-do-direito-do-consumidor.pdf> Acesso em: 04 jun. 2017.

[78] MARQUES, Claudia Lima. Introdução ao Direito do Consumidor. In: **Manual do Direito do Consumidor**, São Paulo: Editora Revista dos Tribunais. 2007, p.25.

Efing[79] (2002) elenca os princípios trazidos pelo CDC: da vulnerabilidade, da informação, da garantia de adequação, do dever governamental, do acesso à justiça e da boa-fé. Todos esses têm como objetivo garantir a defesa dos direitos dos consumidores, inclusive com relação aos cadastros e bancos de dados de consumidores.

O CDC traz uma seção exclusiva para os bancos de dados e cadastro de consumidores, composta dos arts. 43 e 44. O *caput* do art. 43 preceitua que é garantido ao consumidor acesso a suas informações mantidas nesses bancos. Os parágrafos desse artigo ditam as condições para o armazenamento desses dados: i) devem ser claros e verídicos; ii) a abertura está condicionada a pedido ou comunicação por escrito ao consumidor; iii) sendo verificada a inexatidão, é garantida sua correção e comunicação aos destinatários da informação, e vi) disponibilização das informações (conforme *caput* do artigo).

Ademais, estabelece caráter público aos bancos de dados e cadastros relativos a consumidores e veda qualquer fornecimento de informações de consumidores já prescritas que dificultem acesso a novos serviços de crédito.

As disposições do CDC sobre bancos de dados e cadastro revelam a importância do cuidado com relação a informações creditícias dos consumidores.

> Somente as informações relevantes para o mercado de consumo podem ser selecionadas e registradas, franqueando-se ao consumidor completo acesso aos bancos de dados a fim de que possa exigir as correções e supressões necessárias, bem como demandar por eventuais prejuízos sofridos em virtude da inexatidão dos cadastros.[80]

É importante salientar que as informações referentes ao histórico de crédito dos consumidores podem ser consideradas como dados sensíveis, uma vez que podem gerar atos de discriminação contra sua pessoa e seus direitos. Justifica-se, portanto, tratamento especial dispensado por nosso ordenamento pátrio a esse tipo de dado.

Silva e Brum (2013)[81] destacam a importância do controle sobre os bancos de dados e cadastro, tendo em vista o potencial lesivo do uso inadequado ou ilegal das informações inseridas aos consumidores:

---

[79] EFING, Antônio Carlos. **Bancos de dados e cadastro de consumidores**. São Paulo: Editora Revista dos Tribunais. 2002, pp. 88 e 89.

[80] OLIVEIRA, James Eduardo. **Código de Defesa do Consumidor anotado e comentado – doutrina e jurisprudência**. 5ª Ed. São Paulo: Atlas. 2011.

[81] SILVA, Kelyana Ribeiro; BRUM, Amanda Netto. Cadastro de inadimplentes e direito do consumidor sob a ótica do STJ. *In*: **Âmbito Jurídico**, Rio Grande, XVI, n. 113, jun 2013. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13296>. Acesso em: 14 jun. 2017.

> Importa considerar a indiscutível licitude desta atividade, porém, se por um lado a inserção desses dados promove a ampliação da circulação de bens e serviços, na medida em que agiliza a concessão de créditos, de outra banda o mau uso do sistema pode causar danos irreparáveis ao consumidor.[82]

4.2 *Habeas Data*

A Carta Magna determina que será concedida *habeas data* para garantir o acesso ao cidadão das informações a ele pertinentes que constem de registros ou banco de dados públicos ou de caráter público, ou ainda para assegurar o direito de retificação dos dados (art. 5º LXXII). Também confere a gratuidade de tal ação (art. 5º, LXXVII).

> Assim, o *habeas data* é o instrumento processual apto a garantir à pessoa, brasileira ou estrangeira, física ou jurídica, os direitos fundamentais aviltados pela prática dos cadastros e banco de dados pessoais, possibilitando o acesso às informações neles constantes e, se necessária, a retificação das informações inverídicas.[83]

O parágrafo único do art.1º da lei do *habeas data* (Lei nº 9.507, de 12 de novembro de 1997) esclarece o que é entendido como bancos de dados de caráter público. São aqueles que não são privativos do produtor ou armazenador do banco de dados e, dessa forma, possuam informações que podem ser transmitidas a terceiros[84].

Sobre esse assunto, o STJ entende, em sua jurisprudência, que os bancos com informações dos clientes constantes das instituições financeiras não se enquadram como bancos de dados públicos, e, dessa feita, as instituições financeiras, como regra geral, não têm legitimidade passiva em ação de *habeas data*, conforme as seguintes ementas:

> O Tribunal conheceu e deu provimento a recurso extraordinário para indeferir *habeas data* impetrado por ex-empregada do Banco do Brasil que, tendo seu pedido de readmissão negado, pretendia obter informações sobre sua ficha funcional. Considerou-se que o Banco do Brasil não tem legitimidade passiva *ad causam* para responder ao *habeas data* uma vez que não figura como entidade governamental - mas sim como explorador de atividade econômica -, nem se enquadra no conceito de registros de caráter público a que se refere o art. 5º, LXXII, a, da CF, porquanto a ficha funcional de empregado não é utilizável por terceiros (CF, art. 5º, LXXII: "conceder-se-á *habeas data*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;"). **RE 165.304-MG, rel. Min. Octavio Gallotti, 19.10.2000. (RE-165304)**

---

[82] Idem.
[83] EFING, Antônio Carlos. **Bancos de Dados e Cadastro de Consumidores**. São Paulo: Editora Revista dos Tribunais. 2002, pp. 64 e 65.
[84] BRASIL. Lei nº 9.507, de 12 de novembro de 1997.

> PROCESSUAL CIVIL. HABEAS DATA. FGTS. CAIXA ECONÔMICA FEDERAL. EXTRATOS. CABIMENTO.
> 1. A empresa recorrente impetrou *habeas data* sob a alegação de que a Caixa Econômica Federal deixou de conferir andamento ao pedido de informações deduzido em janeiro de 2001 com o escopo de obter os extratos relativos aos depósitos efetuados em seu nome – mas vinculados individualmente a seus empregados –, os quais eram resgatados pela pessoa jurídica quando da dispensa de funcionário não-optante do FGTS, após o recebimento da indenização devida.
> **2. É inadmissível o cabimento do *habeas data* para o simples fornecimento pela CEF de extratos bancários, os quais podem se enquadrar, a título de exemplo, como obrigação derivada de relação de consumo entre a empresa e a instituição financeira, mas não como informações relativas a dados do impetrante que se encontram armazenados em banco de dados de entidade governamental.**
> **3. Para uma hipotética conta bancária regular junto à CEF, os eventuais dados não pertenceriam a uma entidade governamental no desempenho de suas funções públicas, tampouco possuiriam caráter público, pois não são franqueados a terceiros; na verdade, essas informações diriam respeito única e exclusivamente a um contrato bancário de nítido cunho privado firmado entre a CEF a determinada pessoa, física ou jurídica. (grifo nosso)**
> 4. O caso concreto guarda uma singularidade que conduz à admissão do *habeas data*: não se trata de conta bancária comum, mas de conta bancária titularizada pela empresa com o escopo de cumprir o mandamento legal constante no art. 2º da Lei nº 5.107/66, diploma legal que, após introduzir a opção pelo FGTS, determinou aos empregadores que fosse depositada certa quantia mensalmente em benefício de cada trabalhador, inclusive para aqueles que não houvessem optado pelo fundo.
> 5. De acordo com o art. 18 da Lei nº 5.107/66 – reproduzido, em essência, pela vigente Lei nº 8.036/90 –, quando da dispensa do empregado não optante, a empresa poderia levantar a quantia depositada – caso não houvesse direito à indenização ou se operasse a prescrição – ou fazer uso do montante até o limite da verba a ser paga ao empregado, resgatando o restante do valor.
> **6. Por conseguinte, as informações pertinentes a essas contas vinculadas constituem dados acerca da pessoa do recorrente – em seu aspecto econômico-financeiro – que um ente governamental detém em razão do exercício de função estatal de gerência e centralização expressamente estipulada em norma cogente, inexistindo liberdade da empresa em deixar de efetuar os depósitos acerca dos quais, agora, deseja de maneira legítima obter notícia. (grifo nosso)**
> 7. Recurso especial provido.
> STJ - RECURSO ESPECIAL : REsp 1128739 RJ 2009/0049436-2, rel. Min. Castro Meira, 17.02.2010 (RE-165304)

No último caso da jurisprudência extrai-se que o Recurso Especial só foi provido por tratar-se de informações referentes a contas de FGTS e, portanto, de caráter público, ao contrário do que se entende dos dados de conta-corrente de um consumidor.

A Lei nº 9.507/1997, ainda, no art. 7º, amplia o escopo desse remédio constitucional, incluindo no inc. III a possibilidade de impetrar *habeas data* para *a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável*[85].

[85] BRASIL. Lei nº 9.507, de 12 de novembro de 1997 .

4.3 Lei do Cadastro Positivo

Em 9 de junho de 2011 foi editada a Lei nº 12.414. Trata-se de uma norma que autoriza a formulação e consulta a bancos de dados contendo informações de adimplemento, para formação de histórico de crédito de uma pessoa natural ou jurídica. Apesar dessa autorização de acesso de informações dessa natureza, a norma estabelece vários limites e também direito aos consumidores com relação a seus dados.

Isso se demonstra claramente, por exemplo, no fato de se tratar de norma com direito de *opt-in,* ou seja, as informações na norma referidas só serão disponibilizadas se o consumidor assim optar; é imprescindível uma concordância ativa do sujeito de direito, conforme se aduz do texto do art. 4º:

> A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada[86].

Também se determinou a finalidade exclusiva dos bancos de dados. Assim, conforme o art. 7º, as únicas finalidades autorizadas para o Cadastro Positivo são a realização de análise de risco de crédito e dar subsídios ao processo de concessão ou extensão de crédito, de venda a prazo ou transações que gerem risco de crédito ao consulente das informações. O texto traduz o princípio da necessidade de coleta de dados pessoais, que dita que devem ser mantidos em bancos de dados apenas as informações realmente relevantes à consecução do objeto determinado em sua coleta. Tal medida, como já posteriormente ressaltado, constitui-se em importante medida de segurança.

As informações armazenadas devem ser objetivas, claras e de fácil compreensão (art. 3º, § 1º). Veda-se a utilização de informações excessivas, ou seja, todas aquelas não úteis para a análise de risco de crédito ao consumidor (art. 3º, § 3º, inciso I). Depreende-se outro princípio caro à segurança de dados, o de minimização de dados. É proibido também o uso de qualquer dado sensível à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (art. 3º, § 3º, inciso II).

O art. 5º estabelece os direitos dos titulares dos dados:

> I - obter o cancelamento do cadastro quando solicitado;
> II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone

[86] BRASIL. Lei nº 12.414, de 9 de junho de 2011.

> ou por meio eletrônico, de consulta para informar as informações de adimplemento;
> III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação;
> IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;
> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

Como discorremos na seção 1.2 dessa monografia, um dos exemplos de dados alternativos fornecido pelo CFPB - *Consumer Financial Protector Bureau* é a utilização de informação advinda do histórico de pagamento de contas regulares de natureza não creditícia. A lei sobre Cadastro Positivo disciplina o uso desse tipo de dado, incluindo a faculdade de seu titular autorizar o acesso de informações provenientes de prestadores de serviços continuados de água, esgoto, eletricidade, gás e telecomunicações, dentre outros, para compor os bancos de dados (art. 11).

No tocante às instituições financeiras, a Lei fixa que estas devem fornecer as informações ao banco de dados quando solicitadas pelo consumidor, abrangendo apenas o histórico das operações de empréstimo e de financiamento realizadas pelo cliente (art. 12, § 1º). Veda-se que essas instituições, mediante solicitação do titular dos dados, dificultem ou impeçam a sua transmissão.

O Banco Central do Brasil reconhece a importância do Cadastro Positivo

> permitindo uma melhor avaliação do risco envolvido na operação. Essa melhora na avaliação do risco, por sua vez, poderá resultar na oferta de condições mais vantajosas para o interessado.[87]

4.4 Marco Civil da Internet

Outra lei que aborda a questão da utilização de dados pessoais no Brasil é a Lei nº 12.965, de 23 de abril de 2014, e refere-se ao marco civil da internet. Em seu art. 2º o dispositivo legal reconhece *a escala mundial da rede de internet* (inc. I); *os direitos*

[87] BANCO CENTRAL DO BRASIL. **FAQ – Cadastro Positivo**. Disponível em: <http://www.bcb.gov.br/pre/bc_atende/port/faqcadpositivo.asp> Acesso em: 18 jun. 2017.

humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais (inc. II); *a pluralidade e a diversidade* (inc. III); *a abertura e a colaboração* (inc. IV); *a livre iniciativa, a livre concorrência e a defesa do consumidor* (inc. V); *e a finalidade social da rede (inc. VI)*[88].

Entre os diversos princípios incorporados (art. 3º) estão: proteção da privacidade (inc. II); proteção dos dados pessoais (inc. III); e preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas (inc. V).

O art. 7º postula diversos direitos no acesso à internet relacionados à proteção dos dados pessoais. De tal modo, são protegidas a vida privada e intimidade, o sigilo das informações trocadas na rede e armazenadas em comunicações privadas. Ademais, é vedada a transferência de dados pessoais a terceiros (tanto de conexão quanto de casos na internet), só sendo 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 ou em termos de uso de prestação de serviço de internet. Vê-se aqui clara aplicação do princípio do legítimo interesse na legislação nacional.

A norma analisada preceitua, em seu art. 10, que

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

Assim, o conteúdo das comunicações privadas só será disponibilizado por meio de ordem judicial. (art. 10, § 2º). Faculta-se requerer em juízo, com a finalidade de subsidiar conjunto probatório, requerimento à justiça de acesso a registros de conexão ou de registros de acesso a aplicações de internet. (art. 22). O juiz deverá analisar, entre outros requisitos de admissibilidade, se há indícios da ocorrência de um ilícito, e, caso autorize o fornecimento

[88] BRASIL. Lei nº 12.965, de 23 de abril de 2014 Marco Civil Internet.

das informações, deve adotar medidas para respeito à intimidade e vida privada das partes, como a determinação de sigilo de justiça (art. 23).

Também se determinou a transparência quanto a procedimentos de segurança e sigilo, ressalvados os segredos empresariais, e também a adesão de padrões de segurança e sigilos ditados pela norma (art. 10, § 4º).

Com relação ao alcance dessa legislação, aplica-se o disposto a qualquer operação que resulte de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, desde que alguma destas ações tenha ocorrido no Brasil. (art. 11). Aplica-se, também, à pessoa jurídica com sede no exterior, mas que oferte serviço a consumidores brasileiros ou que tenha algum integrante com estabelecimento no País.

Apesar de importantes disposições relevantes ao direito de proteção de dados no Brasil, o marco civil não se constitui ou pretende ser uma norma geral sobre proteção de dados pessoais; dessa forma, não protege a privacidade de maneira abrangente e estruturada.[89]

4.5 Regulação Setorial de Serviços Financeiros

O Conselho Monetário Nacional (CMN), instituído pela Lei nº 4.595, de 31 de dezembro de 1964, composto pelo Ministro da Fazenda (Presidente), o Ministro do Planejamento, Orçamento e Gestão e o Presidente do Banco Central do Brasil, é o órgão responsável por emitir diretrizes gerais que visam o funcionamento adequado do Sistema Financeiro Nacional. Dessa forma, estipula várias normas que regem o funcionamento das instituições financeiras, por meio de resoluções. Algumas das quais dizem respeito a dados e ao tratamento de informacões dos consumidores de serviços financeiros, sendo, portanto, relevantes no que se refere à disciplina da matéria.

4.5.1 Resolução CMN nº 3.694/2009

[89] DONEDA, Danilo. Privacidade e proteção aos dados pessoais. In: **Apresentação ao Ministério da Transparência, Fiscalização e Controladoria-Geral da União.** Brasília, 2017. Disponível em: <http://www.cgu.gov.br/sobre/institucional/eventos/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf> Acesso em: 20 jun. 2017.

A Resolução CMN nº 3.694, de 26 de março de 2009, estabeleceu regras gerais acerca da prevenção de riscos na contratação de operações e na prestação de serviços por parte de instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Foram impostas, entre outras, as seguintes obrigações às instituições financeiras com relação à contratação e à prestação de serviços financeiros (conforme redação dada pela Resolução nº 4.283, de 4 de novembro de 2013.):

> II - a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas, bem como a legitimidade das operações contratadas e dos serviços prestados; (Redação dada pela Resolução nº 4.283, de 4/11/2013.).
> IV - o fornecimento tempestivo ao cliente ou usuário de contratos, recibos, extratos, comprovantes e outros documentos relativos a operações e a serviços.

Apesar de tratar-se de norma genérica sobre a contratação e prestação de serviços financeiros, a Resolução estabelece diversas regras que devem ser seguidas pelas instituições financeiras ao longo de todo seu relacionamento com o cliente e, portanto, mesmo quando da análise e tratamento de dados pessoais de seus clientes.

Portanto, as instituições financeiras têm por obrigação o sigilo e a exatidão de dados referentes a seus consumidores, bem como garantir ao consumidor o acesso a documentos e informações referentes a extratos, comprovantes e outros documentos relacionados aos serviços financeiros.

A norma também dita dever se assegurar a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas, assim como a legitimidade dos serviços também em serviços realizados em meios alternativos aos convencionais, como operações em caixas eletrônicos ou pela internet.

4.5.2 Resolução CMN nº 3.401/2006

A Resolução nº 3.401, de 6 de setembro de 2006, dispõe, entre outras matérias, sobre a obrigatoriedade de fornecimento de informações cadastrais referentes a seus clientes. Ela determina às instituições financeiras o fornecimento a terceiros das informações cadastrais de seus clientes, quando formalmente solicitados e autorizados por estes, em um prazo máximo de 15 dias, com informações referentes aos, no mínimo, 12 meses anteriores.

Devem ser incluídas todas as operações referentes ao cliente a contar do dia útil anterior à solicitação.

Entre as informações repassadas, devem estar ainda compreendidas (art. 3º):

> a) os dados do cliente (...);
> b) o saldo médio mensal mantido em conta-corrente;
> c) o histórico das operações de empréstimo, de financiamento e de arrendamento mercantil, contendo a data da contratação, o valor transacionado e as datas de vencimentos e dos respectivos pagamentos;
> d) o saldo médio mensal das aplicações financeiras e das demais modalidades de investimento mantidas na instituição ou por ela administradas.

Conforme informação destacada no sítio do Banco Central do Brasil[90], quando da solicitação do cliente, não pode a instituição financeira recusar o fornecimento de dados. Essas informações podem ser úteis para os clientes buscarem melhores condições na contratação de serviços financeiros dado seu histórico de relacionamento com um banco ou outra instituição financeira.

4.6 Projetos de Lei de Proteção de Dados Pessoais

Estão em análise no Congresso Nacional três projetos de lei que têm por finalidade a proteção de dados pessoais no Brasil: PL nº 4.060/2012, PLS nº 330/2013, e o PL nº 5.276/2016. O estudo *Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso* Nacional, publicado pela organizacão não governamental Artigo *19*[91] contém um compilado com informações relevantes comparando os textos dos três projetos de lei, em referência a diversos aspectos relevantes, como a proteção de dados sensíveis, os graus de consentimento, a proteção para transferência internacional de dados e adoção de medidas de segurança e manuseio dos dados pessoais. Segue quadro sintético com as principais conclusões de tal estudo comparativo:

---

[90] BANCO CENTRAL DO BRASIL. Portabilidade. **Série I - Relacionamento com o Sistema Financeiro Nacional**. Disponível em: <https://www.bcb.gov.br/pre/pef/port/folder_serie_I_portabilidade.pdf> Acesso em: 17 jun. 2017.

[91] ARTIGO 19. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional,** 2016. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 02 jun. 2017.

ASPECTOS DA LEI	PL 5276/2016	PLS 330/2013	PL 4060/2012
Menção expressa à proteção da liberdade de expressão			
Exceção à atividade jornalística e outras formas de expressão			
Menção expressa à Lei de Acesso à Informação (LAI)			
Evita interpretações que possam ensejar reivindicações do direito ao esquecimento			
Órgão regulatório			
Mecanismo de participação e controle social			
Proteção aos dados sensíveis			
Graus de consentimento			
Consentimento do titular para compartilhamento a terceiros			
Proteção para transferência internacional de dados			
Proteção de dados em acesso público			
Adoção de medidas de segurança e de manuseio dos dados pessoais			
Aplicação ao setor público como um todo, incluindo forças de segurança			
Delimitação de pesquisa estatística			
PRAZO PARA A LEI ENTRAR EM VIGOR	180 dias	120 dias	90 dias

Figura 2. Quadro comparativo entre o Projeto de Lei nº 5.276/16, o PLS nº 330/13 e o PL nº 4.060/12, mostrando vários fatores importantes para a plena proteção do uso de dados pessoais e classificando-os em quatro níveis: *satisfatório*, *parcialmente satisfatório*, *insatisfatório* ou *ausente*.

Conforme se pode verificar de tal estudo comparativo entre as normas tratativas, o projeto de lei mais completo – também o mais recente – é o PL nº 5.276/2016, de autoria do Ministério da Justiça.

> O Anteprojeto de Lei de Proteção de Dados Pessoais foi elaborado pela **Senacon**, em conjunto com a **Secretaria de Assuntos Legislativos** do Ministério da Justiça, após a realização de dois debates públicos, realizados via internet. O primeiro em

> 2010 e o segundo no primeiro semestre de 2015. No total foram mais de **2.000 contribuições** dos setores público e privado, academia e organizações não-governamentais. Durante os últimos cinco anos também foram realizadas inúmeras reuniões técnicas, seminários e discussões por diversos órgãos e entidades.[92]

Percebe-se, dessa maneira, que houve um processo colaborativo de construção do texto que seria proposto, de forma a viabilizar a participação de diversos setores da sociedade na produção de um texto mais completo e que retrate as reais necessidades dos variados atores envolvidos nas trocas de informações promovidas no mundo digital.

O Projeto de Lei foi encaminhado para avaliação do Congresso Nacional em 12 de maio de 2016 com regime de urgência constitucional, o que visa lhe garantir um trâmite mais célere.[93] Entretanto, até hoje o projeto segue ainda em tramitação na Câmara dos Deputados.

O alcance do Projeto de Lei engloba pessoas naturais ou jurídicas, de direito público ou privado, e alcançam operações em que o tratamento se der no Brasil, tenha por objeto oferta de bens e serviços ou tratamento de dados no território nacional ou em que a coleta ocorra dentro do País. Independe, dessa forma, a localização da sede da pessoa jurídica ou ainda onde estão os dados (art. 3º).

Exclui-se de seu escopo dados processados com finalidade exclusivamente: pessoal por pessoa natural; jornalísticos, artísticos, literários ou acadêmicos; e de segurança pública ou do Estado, de defesa nacional, ou de atividades de investigação e repressão de ilícitos penais por pessoa de direito público ou sob sua tutela (art. 4º).

Com relação às definições básicas, a PL conceitua dado pessoal conforme a definição clássica referente à informação relacionada à pessoa natural identificada ou identificável, incluindo dados de localização ou identificadores eletrônicos (art. 5º, inc. I).

Também compreende outros conceitos importantes, como o de dados sensíveis (art. 5º, inc. III), dados anonimizados (art. 5º, inc. IV), consentimento (art. 5º, inc. VII), e anonimização (art. 5º, inc. XII).

---

[92] Conforme a notícia *Conheça a nova versão do anteprojeto de lei de proteção de dados pessoais,* publicada em 21 de outubro de 2015 e divulgada no sítio Pensando o Direito, do Ministério da Justiça, e disponível em: <http://pensando.mj.gov.br/dadospessoais/2015/10/conheca-a-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 19 jun. 2017.

[93] BIONI, Bruno Ricardo; MONTEIRO, Renato Leite. O Brasil caminha rumo a uma Lei Geral de Proteção de Dados Pessoais? **Carta Capital,** 25 mai 2016. Disponível em: <https://www.cartacapital.com.br/politica/o-brasil-caminha-rumo-a-uma-lei-geral-de-protecao-de-dados-pessoais > Acesso em 18 jun. 2017.

Princípios importantes foram incluídos na norma, em seu art. 6º, como se segue:

> I – finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informado ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;
> II – adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;
> III – necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV – livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;
> V – qualidade dos dados: pelo qual devem ser garantidas aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;
> VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
> VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII – prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX – não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

Segundo o Projeto de Lei, o tratamento de dados pessoais só poderá ocorrer de acordo com as hipóteses legais previstas no art. 7º entre os incisos II a IX, que compreendem, por exemplo, a necessidade para execução de políticas públicas pelo poder público e para pesquisas históricas, científicas ou estatísticas. Determina-se que, caso não se vincule à necessidade estabelecida em um desses incisos, o consentimento livre, informado e inequívoco do titular dos dados. (art 7º, inc I). Deve também ser escrito ou por outro meio que o certifique (art. 9º) e específico com relação à(s) sua(s) finalidade(s) (art.9º § 4º). O consentimento poderá ser revogado (art. 8º, VII, a e art.9º § 5º).

Garante-se o acesso a seus dados pelo titular e as informações relevantes pertinentes a esse, tais como finalidade, forma e duração do tratamento, a quem os dados podem ser comunicados. Assegura-se ainda, o direito à revogação dos dados (art. 8º).

Com relação aos dados sensíveis, a norma determina tratamento especial, só sendo admitido seu tratamento por meio de consentimento livre, informado e inequívoco, expresso e específico do titular dos dados, aparatado da manifestação referente a outros dados, que contenha alerta aos riscos da utilização de dados dessa natureza (art. 11, I), ou em outros casos relevantes, como na proteção à vida e à saúde (art. 11, II).

O Projeto de Lei assegura aos titulares dos dados direito à confirmação e ao acesso aos dados tratados; à retificação dos dados que estejam errados, incompletos ou desatualizados; ao bloqueio de dados necessários, ou sua anonimização; e à eliminação de qualquer dado, a qualquer momento (art, 18). Determina, ao mesmo tempo, o alcance das normas de proteção do Código de Defesa do Consumidor.

No que concerne à segurança e o sigilo de dados, o Projeto de Lei prevê a adoção de medidas que garantam a prevenção de ilícitos ou acidentes que possam gerar a perda ou alteração de dados, comunicações indevidas, ou outra operação ilegal (art.45). Também se determina que as medidas de segurança devem ser estabelecidas desde a fase de concepção do produto ou serviço que compreenda dados pessoais (art. 45, § 2º).

Os agentes ou outras pessoas envolvidas no armazenamento ou tratamento de dados pessoais devem guardar sigilo com relação a tais informações (art.46).

Um importante ator considerado pelo Projeto de Lei é o órgão competente para tratar das questões relativas ao uso de dados pessoais. A norma tratativa estabelece várias competências (que estão espalhadas no texto do PL e também dispostas no art. 53). No que se refere à segurança dos bancos de dados, caberá a este órgão estabelecer requisitos mínimos de segurança, bem como ser comunicado no caso de qualquer incidente relacionado à segurança (art. 45, § 2º e art. 47).

Outra importante competência do órgão a ser criado é a de garantir o cumprimento das normas estipuladas no Projeto de Lei e aplicar sanções quando da desobediência aos preceitos estabelecidos (art.52).

Merece destaque ainda o dispositivo constante do parágrafo único do art. 42, que prevê a possibilidade de inversão de ônus da prova em casos em que o juiz verificar que há verossimilhança na alegação do impetrante ou quando for excessivamente onerosa a produção de provas para o titular dos dados.

5. PERSPECTIVAS DE POLÍTICAS PÚBLICAS E REGULAÇÃO RELACIONADAS À PROTEÇÃO DE DADOS PESSOAIS

Uma vez examinadas o quadro normativo e proposta legislativa referente ao uso de dados no Brasil, é importante lembrar que, mesmo tendo em mente todos os potenciais riscos aos direitos fundamentais decorrentes do incremento da utilização de dados pessoais vindos de fontes até então não utilizadas pelos fornecedores de serviços financeiros, não é possível, e provavelmente nem desejável, frear tal processo de uso de dados no Pais.

O que se deve buscar é a criação pelo Estado de um sistema protetivo aos consumidores visando assegurar que seus dados só sejam utilizados da maneira como eles consentirem, de forma que eles possuam pleno e irrestrito conhecimento de onde seus dados estão localizados, como eles estão sendo tratados e/ou analisados, se eles estão sendo repassados para terceiros, e quais são as finalidades de seu uso.

Atingir tal objetivo, no entanto, é um grande desafio, especialmente em um contexto de mudanças tecnológicas tão velozes e de um incremento exponencial, e também pouco controlado, de troca de dados e informações.

É muito difícil para o Estado, por meio de seus poderes Executivo, Legislativo e Judiciário, acompanhar o ritmo acelerado dessas alterações. Como, então, assegurar os direitos individuais e coletivos de privacidade, vida privada, sigilo ou tratamento diferencial de dados sensíveis frente a essa conjuntura?

Saldanha (2015) destaca a grande dificuldade em regulamentar o uso de dados pessoais:

> Árdua é a conquista do equilíbrio nesse domínio. De um lado há de ser deixado aos atores econômicos uma margem para autorregulação para, afinal, permitir o dinamismo do mundo virtual. Mas, de outro, há de ser assegurada a atuação do sistema de justiça para garantir o respeito e a efetivação dos direitos fundamentais, domínio no qual a centralidade da vida privada é evidente.[94]

Antes de iniciar a análise sobre a legislação atual e perspectivas regulatórias e de políticas públicas, é interessante destacar análise desenvolvida por Boyd e Crawford (2012)[95] que discorrem sobre seis questões críticas atinentes ao uso de *Big Data*:

---

[94] SALDANHA, Jânia Maria Lopes**.** Qual direito para os dados pessoais em tempos de Big data? **Carta Capital**. 16 mar 2015. Disponível em: <http://justificando.cartacapital.com.br/2015/03/16/qual-direito-para-os-dados-pessoais-em-tempos-de-big-data/> Acesso em: 07 jun. 2017.

[95] BOYD, D.; CRAWFORD, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**,15, 662–679.

a) As autoras defendem que os *Big Data* mudam a definição do que é conhecimento, pois alteram amplamente o processo de pesquisa de informações. Preocupam-se com uma "matematização" do conhecimento, em que não importam as razões de os indivíduos se comportarem de determinada maneira, e sim a simples detecção dos padrões de comportamento.

b) A busca pela objetividade e acurácia seria falaciosa, vez que, apesar de as análises de dados transformarem as informações em dados quantificados, a interpretação ainda deve ser subjetiva. Assim, deve-se ter clareza de que mesmo que uma análise seja automatizada e quantitativa, há o viés subjetivo de quem a formulou. Ademais, mesmo que os *Big Data* possuam uma enorme quantidade de tipo de dados, não possui todos, e, portanto, é incompleta.

c) Elas ressaltam que nem sempre um banco de dados maior é melhor, e pontuam a importância de não se esquecer de aspectos importantes para determinação de amostras. Devem ser reconhecidas as limitações de um banco de dados, bem como quais questões podem ser a ele postas e por ele respondidas de maneira apropriada. Deve-se também valorizar os bancos de dados pequenos, por exemplo, referentes a um só indivíduo, que podem fornecer informações muito relevantes.

d) *Big Data* podem perder seu sentido quando retirados de contexto, o que é um problema, visto que muitas vezes para que sejam adequadas a um modelo matemático, as informações são utilizadas de forma descontextualizada.

e) Destacam que nem tudo que está acessível pode ser utilizado de forma ética. Ressaltam o problema de se usar fontes inicialmente públicas, mas utilizadas fora do contexto e para propósitos desconhecidos pelo autor dos dados. Isso é um problema ainda maior pois muitos de nós não temos conhecimento sobre a multiplicidade de atores e algoritmos que se utilizam ou podem se beneficiar da coleta de nossos dados públicos.

f) O acesso diferenciado a *Big Data* pode gerar divisões digitais. Ressalta-se que nem todos os atores têm o mesmo nível de acesso a informações. Assim, estabelece-se uma assimetria, sendo privilegiados os que possuem recursos financeiros ou quem está vinculado a uma companhia com recursos. Outra questão posta é que quem detém as informações determina quais serão os usos dos dados e endereçaram quais seriam as questões posta a esses dados.

5.1 Análise do estado da arte da legislação nacional

Como visto, são grandes os desafios postos. Conforme já verificado, a legislação pátria já abarca regulamentações legais e infralegais que tangenciam questões relacionadas ao uso de dados pessoais, legislações essas que já conferem ao consumidor certo grau de segurança quanto ao uso de suas informações. Instrumento importantíssimo, por exemplo, de garantia de respeito aos dados pessoais é o remédio constitucional *Habeas Data.*

Relevantes avanços foram inseridos pelo Marco Civil da Internet, como os princípios de proteção dos dados pessoais, de segurança e funcionalidade da rede compatíveis com os padrões internacionais, e a vedação de transferência de dados a terceiros sem o consentimento livre, expresso e informado do titular dos dados. A aprovação do dispositivo legal também inseriu os princípios da limitação da coleta e especificação de propósitos, conforme as *Guidelines* da ONU.

Entretanto, a legislação até então aprovada não é suficientemente robusta para lidar com utilização de dados pessoais em uma escala tão grande, até mesmo porque o alcance do Marco Civil da Internet limita-se aos dados coletados na internet, não abarcando outras fontes.

Por não possuir ainda um texto legal aprovado sobre a matéria que discorra sobre a proteção de uso de dados pessoais de forma ampla e específica, há muitas lacunas que precisam ser preenchidas, lacunas tais que podem fazer com que o consumidor não consiga plena proteção de seus direitos.

Um exemplo desse vácuo de proteção aos titulares dos dados pessoais é o direito ao acesso às suas informações que estão sob a guarda de instituições financeiras. Conforme já verificamos ao tratar do *habeas data*, via de regra, as informações relacionadas ao consumidor não são de caráter público e, por conseguinte, não podem ser protegidas pelo remédio constitucional. Assim, caso ele pretenda ver quais fatores e quais dados foram utilizados para que ele tivesse determinado escore de crédito, por exemplo, não há previsão legal que garanta o fornecimento dessas informações.[96]

[96] Sobre o acesso de informações do cliente a documentos a ele relativos, conforme já ressaltado, a Resolução CMN nº 3.694/2009 garante, em seu inc. I do art 1º o fornecimento tempestivo *de cópia de contratos, recibos, extratos, comprovantes e outros documentos relativos a operações e a serviços prestados.* Entretanto, apesar de fazer referência a outros documentos relativos a operações e a serviços prestados, o banco ou demais

Torna-se, dessa maneira, imprescindível a aprovação de diploma legal que legisle especificamente sobre o uso de dados pessoais. A aprovação do Projeto de Lei nº 5.276/2016, aqui examinado, materializará um grande avanço na defesa dos direitos referentes aos dados pessoais dos consumidores no solo pátrio, uma vez que garantirá explicitamente vários direitos aos titulares das informações.

> Uma lei sobre proteção de dados permite que o cidadão tenha controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Ela tem por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado para seu uso e outros, sempre garantindo ao cidadão protagonismo nas decisões fundamentais a este respeito. O impacto maior de uma lei sobre proteção de dados pessoais é o equilíbrio das assimetrias de poder sobre a informação pessoal existente entre o titular dos dados pessoais e aqueles que os usam e compartilham. (Ministério da Justiça)[97]

Por exemplo, o Projeto de Lei introduz na legislação pátria princípios importantes à salvaguarda dos dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação, em consonância com os estabelecidos pela ONU, OCDE e União Europeia.

Outro grande avanço a ser introduzido pela aprovação do Projeto de Lei é a criação de um órgão especializado no tratamento de questões vinculadas à utilização de dados pessoais. Esse órgão é importante por várias razões. Uma delas é que ele que terá a competência de fiscalizar e também estabelecer sanções aos que não estiverem respeitando as normas aprovadas.

Outra atuação muito relevante será na edição de normas infralegais sobre o tema. Conforme já aqui destacado, a velocidade das mudanças tecnológicas é altíssima, e, portanto, torna-se praticamente impossível que apenas por lei se consiga regular todos os aspectos relevantes que surjam para proteção aos titulares dos dados pessoais. Torna-se, logo, fundamental uma regulamentação por meio de resoluções e outras normas infralegais. O Projeto de Lei estabelece assim, ao longo de vários dispositivos de seu texto, aspectos que deverão ser regulamentados pelo órgão competente. Mais especificamente, em seu art. 53, estipula que este órgão deverá estabelecer diretrizes para uma Política Nacional de Proteção

---

instituições financeiras podem se recusar a prestar informações relativas a escore de crédito ou também relativas *a profling*, ou seja, dados que direcionem a oferta de produtos e serviços a depender do perfil do cliente, sob a justificativa de segredo do negócio. Por isso a importância da aprovação da lei sobre a matéria que disserte sobre esses aspectos e que também crie órgão competente para tratar de casos omissos ou de dúvidas.

[97] Disponível em: <http://pensando.mj.gov.br/dadospessoais/importancia-de-uma-lei-sobre-protecao-de-dados/>

de Dados e normas complementares concernentes à proteção de dados pessoais e privacidade, bem como sobre a comunicação desses dados (incisos II, X e XII).

Não obstante a grande relevância da previsão da criação de um órgão especializado, como ressaltado, um ponto negativo que se pode apontar é o Projeto de Lei não ter em seus dispositivos estabelecido desde já a criação do órgão, determinado qual seria sua natureza jurídica, a qual órgão estaria vinculado, qual seria sua composição, entre outros aspectos relevantes de sua natureza jurídica.

Portanto, ao nos referirmos a uso de *Big Data* ou dados não convencionais, não se pode pensar apenas em uma regulamentação setorial. Deve-se pensar em todo um sistema de regulamentações amplo e integrado. Em uma realidade em que as informações estão todas interligadas, um banco ou outra instituição financeira pode coletar dados de redes sociais de seus consumidores, a edição de uma lei geral acerca da proteção aos dados pessoais é fundamental e urgente, bem como regulamentações infralegais que tratem o tema permeando todos os setores da sociedade.

5.2 Regulação Setorial

Apesar de ser fundamental uma regulamentação ampla sobre o uso de dados pessoais, dadas as peculiaridades do Sistema Financeiro Nacional e da oferta de produtos e serviços financeiros, não se pode abrir mão de uma regulação setorial.

Doneda (2006, p. 100)[98], ao examinar a questão de uma regulamentação geral *versus* 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.

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

[98] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 100.

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.

Um relatório do *Federal Trade Commission – FTC*[99] (órgão responsável pela defesa do consumidor nos Estados Unidos) lista uma série de riscos na utilização de *Big Data* e dados alternativos, muitos dos quais atinentes à área de serviços financeiros. Entre eles destaca-se a categorização dos consumidores para predição de comportamentos e, então, decisões acerca da oferta de produtos e serviços financeiros. Assim, a decisão sobre a concessão de crédito pode basear-se na análise de pessoas com características similares a de quem está pretendendo a contratação desse serviço, e não se suas próprias informações. Essa análise pode englobar a capacidade de pagamento de pessoas residentes em uma mesma área residencial, de mesma escolaridade, com comportamentos similares de consumo e de uso das mídias sociais.

Esse tipo de análise pode gerar vários tipos de vieses que podem prejudicar um consumidor específico ou, pela sua natureza de categorização, uma classe inteira de consumidores. Um ponto criticado pelo próprio FTC em seu relatório é que, dessas análises, várias correlações podem ser estabelecidas, mas essas não pressupõem necessariamente causalidades. [100]

Como já ressaltado anteriormente, a acurácia do *Big Data* é questionável e, dessa forma, é sempre importante reconhecer os vieses incorporados por parte de quem realizou as análises. Faz-se necessário, deste modo, prever que as decisões baseadas em técnicas de processamento de dados totalmente automatizadas possam ser contestadas, dando a chance de o cliente comprovar, de outras formas, e baseado em seu histórico – e não a de um grupo no qual ele foi categorizado –, que ele possua capacidade de pagamento e, dessa forma, é elegível para o produto ou serviço que prende adquirir.

Outro ponto de regulamentação importante refere-se à vedação de uso de qualquer dado sensível que tenha potencial de gerar discriminação nas decisões referentes a serviços

---

[99] FEDERAL TRADE COMMISSION. Big Data: A tool for inclusion or exclusion? **FTC Report**, jan. 2016. Disponível em: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf > Acesso em: 21 jun. 2017.

[100] Idem.

financeiros, de forma que se iniba a utilização nas categorizações acima relatadas de dados como raça, religião, informações médicas e genéticas do consumidor etc.

Diante do exposto, deve-se editar uma regulamentação setorial que abranja os seguintes pontos:

a) Que determine que seja comunicado ao cliente quais são as fontes de dados que serão utilizadas para determinar se ele terá ou não acesso a determinado produto e serviço, e sob quais condições;
b) Que proíba o uso de informações sensíveis – tais como, raça, sexo, orientação sexual, crença, orientação política, informações genéticas ou de histórico médico – para basear decisões de oferta e prestação de serviços financeiros;
c) Que determine a possibilidade de revisão de qualquer decisão automatizada, especialmente as que se utilizem da categorização de consumidores.

Mesmo com uma regulamentação nesse sentido, outro ponto que merece atenção do regulador dos serviços e produtos financeiros é o surgimento das *fintechs.* As *fintechs*, por um lado, são muito bem-vindas, pois permitem novas soluções e diferentes produtos potencialmente mais adequados aos diversos públicos, além de muitas vezes poderem oferecer custos mais baixos que as tradicionais instituições financeiras, por possuírem uma estrutura administrativa mais enxuta, e assim, menor custo operacional. Ademais, por sua grande afinidade às novas tecnologias da informação, podem trazer soluções criativas que atendam às necessidades dos consumidores.

Entretanto, por se tratar de público ainda não tão bem conhecido do regulador, e não existir ainda regulação setorial específica para essas empresas, a utilização de dados pessoais por essas empresas pode ser uma ameaça ainda maior para o direito individual e coletivo dos consumidores.

5.3 Para além da regulação

Apenas soluções de regulamentação não são serão suficientemente capazes de endereçar todas as necessidades de salvaguarda do direito dos titulares de dados pessoais. É importante que o Estado promova políticas públicas com base a resguardar tais direitos.

Nesse contexto, são fundamentais ações e campanhas educacionais que busquem explicar aos cidadãos as utilizações potenciais advindas da coleta de seus dados pessoais das

mais diversas fontes: dados cadastrais, dados recolhidos por meio do acompanhamento de suas ações em mídias sociais, dados de adimplemento e inadimplemento de obrigações etc., bem como que expliquem quais são os cuidados necessários para que se evitem possíveis usos indesejados desses dados.

Dessa forma, são necessárias ações em conjunto entre os integrantes da Estratégia Nacional de Educação Financeira - ENEF[101] a fim de planejar e desenvolver projetos e programas com essa finalidade, tendo em vista o crescente impacto do uso de dados na oferta e serviços financeiros e a grande complexidade das análises de *Big Data* e dos dados alternativos, que tornam ainda mais difícil a compreensão por parte do cidadão comum dos fatores relativos à concessão de um produto ou prestação de um serviço financeiro.

Outra política pública importante é o fomento pelo Estado para que as instituições financeiras aproveitem os principais benefícios da *Big Data* e de uso de dados alternativos em prol da inclusão financeira, desenvolvendo produtos adequados para a população vulnerável e excluída do sistema. Importantes atores nesse fomento podem ser as *fintechs*, por esses já possuírem como um de seus objetivos atender especificidades de cada público.

Esse fomento pode ser conduzido por meio de diversos instrumentos: incentivos fiscais, concursos que premiem iniciativas de inclusão financeira, cooperação técnica de compartilhamento de *expertise*, entre outros.

[101] A Estratégia Nacional de Educação Financeira – ENEF – é uma mobilização multissetorial em torno da promoção de ações de educação financeira no Brasil. A estratégia foi criada através da articulação de sete órgãos e entidades governamentais e quatro organizações da sociedade civil, que juntos integram o Comitê Nacional de Educação Financeira – CONEF. O Banco Central do Brasil é um desses membros. Informação disponível em: http://www.vidaedinheiro.gov.br/pagina-29-quem_somos_e_o_que_fazemos.html. Acesso em 25 de jun. de 2017.

6. CONCLUSÃO

É nítida a importância da proteção dos dados pessoais à garantia da plena fruição dos direitos fundamentais dos indivíduos. Esse estudo pretendeu jogar luz e trazer pontos de reflexão relativos a questões protetivas caras aos diretos dos consumidores de serviços financeiros titulares de dados, bem como sugerir novos caminhos a partir das soluções já existentes em nosso ordenamento pátrio.

Assim, verificou-se que o uso de *Big Data* e de dados alternativos podem afetar a vida dos consumidores. A má utilização de dados pessoais pode trazer sérios riscos à fruição do direito à privacidade. Também constatou-se a necessidade de atenção a uso de dados sensíveis, os quais, quando do seu uso, podem ensejar impactos discriminatórios, e, portanto, merecem maior cuidado da legislação. Relevante, ainda, o estabelecimento de padrões mínimos de segurança na manipulação de bancos de dados, de forma a garantir que os dados pessoais não sejam apagados, comunicados ou alterados de forma ilícita ou acidentalmente.

Organismos internacionais, transnacionais e diversos Estados passaram a regulamentar o uso de dados pessoais, tendo em vista o grande crescimento na utilização de tais dados. Nesse contexto, a União Europeia editou diversos documentos estabelecendo os princípios e regras mínimas a que seus Estados membros deveriam atentar-se quando da redação de suas legislações próprias.

No contexto brasileiro, ainda não há lei que disponha especificamente sobre a proteção de dados pessoais no território nacional; todavia, existem no Congresso Nacional três projetos de lei a esse respeito. O mais recente deles, o PL nº 5.276/2016. Conforme verificado, sua aprovação implementará grandes avanços na proteção aos direitos dos titulares de dados.

São grandes os desafios regulatórios no Brasil, porém a solução não perpassa somente a implementação de soluções regulatória, sendo necessária a implementação de políticas públicas adicionais.

O potencial benéfico da utilização de *Big Data* e de dados alternativos pode ser grande, tendo potencial de gerar impactos positivos na inclusão financeira e até mesmo na redução de juros dos produtos ofertados.

Dessa forma, deve ser encorajada a formulação de vários estudos sobre o tema, de forma a auxiliar e embasar políticas públicas que estimulem as melhores práticas na utilização de dados pessoais pelas instituições financeiras.

A maior parte da produção científica referente a uso de *Big Data* e dados alternativos é internacional, sendo muito relevante o desenvolvimento de novos estudos e pesquisas no Brasil, pensando como incorporar da melhor forma as experiências exitosas internacionais às peculiaridades nacionais.

Por se tratar de matéria que merece contribuição de variados campos do saber, o estudo da proteção de dados pessoais é um grande desafio e merece diversos estudos com diferentes enfoques.

É importante, por exemplo, o desenvolvimento de estudos em parceria com a área de tecnologia da informação, com vistas a melhor subsidiar o regulador e o órgão responsável por cuidar dos direitos dos titulares de dados – hoje a Senacon[102], e, com a aprovação do Projeto de Lei, um órgão próprio – a estabelecer padrões mínimos de segurança e transparência.

Outra área que merece atenção, conforme ressaltado na seção anterior, é a formulação de políticas de educação tendo por objetivo disseminar aos consumidores seus direitos com relação à disseminação de suas informações pessoais. Portanto, é desejável parcerias com as áreas de pedagogia, como forma de desenhar as melhores metodologias e estratégias para alcançar esses objetivos.

Na área jurídica, é importante acompanhar como o advento dessa multiplicação de dados pessoais utilizados se traduzirá nas ações judiciais. Portanto, recomendam-se estudos de acompanhamento da jurisprudência sobre a matéria.

Outros estudos interessantes seriam pesquisas aplicadas à análise jurídica de contratos de prestação de serviço, verificando se as normas de direito à privacidade e ao uso de dados estão compatíveis com a legislação existente e quais seriam as modificações necessárias para compatibilização, se o Projeto de Lei de proteção dados pessoais for aprovado.

[102] Secretaria Nacional do Consumidor.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Aluísio. Fintechs se multiplicam com BC e CVM atentos e regulação precária. **Exame**, 03 mar. 2017. Disponível em: <http://exame.abril.com.br/pme/fintechs-se-multiplicam-com-bc-e-cvm-atentos-e-regulacao-precaria/> Acesso em: 04 jun. 2017.

ANDRADE JR, Valter Lacerda de. **Utilização de técnicas de dados não estruturados para desenvolvimento de modelos aplicados ao ciclo de crédito**. 2014. 70p. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo. 2014. Disponível em: <https://sapientia.pucsp.br/bitstream/handle/18150/1/Valter%20Lacerda%20de%20Andrade%20Junior.pdf> Acesso em: 07 jun. 2017.

ARTIGO 19. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional,** 2016. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 02 jun. 2017.

ASSEMBLEIA GERAL DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Resolução nº 45/95. Guidelines for the regulation of computerized personal data files.** Disponível em: <http://www.refworld.org/pdfid/3ddcafaac.pdf>. Acesso em: 10 jun. 2017.

BANCO CENTRAL DO BRASIL. FAQ – Cadastro Positivo. Disponível em: <http://www.bcb.gov.br/pre/bc_atende/port/faqcadpositivo.asp> Acesso em: 18 jun. 2017.

BANCO CENTRAL DO BRASIL. **Relatório de estabilidade financeira**, vol. 15, n. 2. Brasília, 2016. Disponível em: <http://www.bcb.gov.br/htms/estabilidade/2016_09/refPub.pdf> Acesso em: 02 jun. 2017.

BANCO CENTRAL DO BRASIL. Portabilidade. **Série I - Relacionamento com o Sistema Financeiro Nacional**. Disponível em: <https://www.bcb.gov.br/pre/pef/port/folder_serie_I_portabilidade.pdf> Acesso em: 17 jun. 2017.

BERNSTEIN, Terry; BHIMANI, Anish B.; SCHULTZ, Eugene; SIEGEL, Carol A. **Segurança na internet**. Rio de Janeiro: Campus, 1997.

BHOLAT, David. Big Data and central banks. **Bank of England Quarterly Bulletin**, vol. 55, n. 1, pp. 1-6. Disponível em: <http://journals.sagepub.com/doi/pdf/10.1177/2053951715579469> Acesso em: 04 jun. 2017.

BIONI, Bruno Ricardo; MONTEIRO, Renato Leite. O Brasil caminha rumo a uma Lei Geral de Proteção de Dados Pessoais? **Carta Capital,** 25 mai 2016. Disponível em: https://www.cartacapital.com.br/politica/o-brasil-caminha-rumo-a-uma-lei-geral-de-protecao-de-dados-pessoais > Acesso em 18 jun. 2017.

BOYD, D.; CRAWFORD, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**,15, 662–679.

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS. **A comprehensive approach on personal data protection in the European Union.** European Commission's Communication. BEUC, The European Consumers' Organisation's response. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf> Acesso em: 12 jun. 2017.

CHEN, Min; MAO, Shiwen; LIU, Yunhao. Big Data: a survey. **Mobile Networks and Applications**, vol. 19, p. 171-209, 2014. Disponível em: <http://www2.egr.uh.edu/~zhan2/ECE6111/class/BigDataSurvey2014.pdf > Acesso em: 04 jun. 2017.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS. **10 medidas para preparar a aplicação do regulamento europeu de proteção de dados**. 28 jan. 2017. Disponível em: <https://www.cnpd.pt/bin/rgpd/10_medidas_para_preparar_rgpd_cnpd.pdf>. Acesso em: 17 jun. 2017.

CONSELHO DA EUROPA. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. European Treaty Series n. 108, Estrasburgo, 28 jan. 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm> Acesso em: 09 jun. 2017.

CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (Convenção Europeia de Direitos Humanos)**, adotada em 4 de novembro de 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf> Acesso em: 12 de jun. 2017.

CONSUMER FINANCIAL PROTECTION BUREAU. **Request for information regarding use of alternative data and modeling techniques in the credit process.** [Docket No. CFPB-2017-0005], 2017. Disponível em: <http://files.consumerfinance.gov/f/documents/20170214_cfpb_Alt-Data-RFI.pdf> Acesso em: 4 de jun. 2017.

De MAURO, Andrea; GREGO, Marco; GRIMALDI, Michele. **What is Big Data? A consensual definition and a review of key research topics**. In: AIP Conference Proccedings, vol. 1644, n. 1, 2014. Disponível em: < https://www.researchgate.net/publication/265775800_What_is_Big_Data_A_Consensual_Definition_and_a_Review_of_Key_Research_Topics> Acesso em: 04 jun. 2017.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro 1. Teoria Geral do Direito Civil**. 30ª ed. São Paulo: Saraiva. 2013, p. 137.

DLA PIPER GLOBAL LAW FIRM. **Data protection laws of the world: full handbook**. 2017. Disponível em: <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all> Acesso em: 14 jun. 2017.

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

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 101.

EFING, Antônio Carlos. **Bancos de Dados e Cadastro de Consumidores**. São Paulo: Editora Revista dos Tribunais. 2002, pp. 64 e 65.

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. 122 p. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf > Acesso em: 10 jun. 2017

EUGDPR.ORG. **Key changes with the general data protection regulation**. Disponível em: <http://www.eugdpr.org/key-changes.html> Acesso em: 17 jun. 2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Handbook on European data protection law**. 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> Acesso em: 17 jun. 2017.

FEDERAL TRADE COMMISSION. Big Data: A tool for inclusion or exclusion? **FTC Report**, jan. 2016. Disponível em:

<https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf > Acesso em: 21 jun. 2017.

HAWTHORNE, Nigel. **9 important changes in the new EU GDPR likely to become law in 2016**. Disponível em: <https://www.skyhighnetworks.com/cloud-security-blog/9-important-changes-in-the-new-eu-gdpr-likely-to-become-law-in-2016/>. Acesso em: 17 jun. 2017.

KUSCHEWSKI, Monika. **Revised OECD Privacy Guidelines Strengthen Accountability Principle**. 23 set. 2013. Disponível em: < https://www.insideprivacy.com/international/revised-oecd-privacy-guidelines-strengthen-accountability-principle/> Acesso em: 24 jun. 2017.

LANEY, Doug. **Data management - controlling data volume, velocity and variety**. Meta Group. Publicado em: 06 fev. 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> Acesso em: 02 jun. 2017.

LAZAROW, Alexandre**. Investidor explica por que apostou no GuiaBolso**. 05 mai 2017. Disponível em: <https://blog.guiabolso.com.br/2017/05/05/por-que-investimos-no-guiabolso/ > Acesso em: 05 jun. 2017.

MACEIRA, Irma Pereira. **A proteção do direito à privacidade familiar na internet**. Rio de Janeiro: Editora Lumen Juris. 2015.

MARQUES, Claudia Lima. Introdução ao Direito do Consumidor. In: **Manual do Direito do Consumidor**, São Paulo: Editora Revista dos Tribunais. 2007.

MENDES, Laura Schertel. **Transparência e privacidade: violação da informação pessoal na sociedade de consumo**. 156 p. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília. 2006.

NOVAIS, Leandro. **Big Data e o consumidor bancário**. 25 mai 2015. Disponível em: <http://educandoseubolso.blog.br/2015/05/25/big-data-e-o-consumidor-bancario/>. Acesso em: 02 jun. 2017.

OLIVEIRA, James Eduardo. **Código de Defesa do Consumidor anotado e comentado – doutrina e jurisprudência**. 5ª Ed. São Paulo: Atlas. 2011

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD guidelines governing the protection of privacy and transborder flows of personal data.** 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> Acesso em: 24 jun.2017.

PARLAMENTO EUROPEU - CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Luxembourg: Jornal Oficial das Comunidades Europeias, 24 out. 1995. p. 281/31-281/39. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML> Acesso em 09 jun. 2017.

PETRY, Andre. Vida Digital: O Berço do Big Data. **Revista Veja**, São Paulo. 2013, p.71-81.

PRADO, José. **O que é Fintech?** 14 dez. 2016. Disponível em: <http://conexaofintech.com.br/fintech/o-que-e-fintech/>Acesso em: 02 jun. 2017.

RICHARD, Dan. **Top 3 Uses for Alternative Credit Data in 2017 Decisioning.** 06 fev. 2017. Disponível em: <https://ws.factortrust.com/2017/02/06/top-3-uses-for-alternative-credit-data-in-2017-decisioning/> Acesso em: 02 jun. 2017.

REIS, Daniel. Preparados para as novas regras sobre dados pessoais? **Público**, 12 mai 2016. Disponível em: <https://www.publico.pt/2016/05/12/economia/noticia/preparados-para-as-novas-regras-sobre-dados-pessoais-1731660>. Acesso em: 17 jun. 2017.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008, p. 250.

SAIAS, Marco Alexandre. **O novo regulamento geral de proteção de dados pessoais, em 3 minutos!**. Disponível em: <https://www.pra.pt/pt/communication/news/o-novo-regulamento-geral-de-protec-o-de-dados-pessoais-em-3-minutos/>. Acesso em: 17 jun. 2017.

SALDANHA, Jânia Maria Lopes**.** Qual direito para os dados pessoais em tempos de Big data? **Carta Capital**. 16 mar 2015. Disponível em: <http://justificando.cartacapital.com.br/2015/03/16/qual-direito-para-os-dados-pessoais-em-tempos-de-big-data/> Acesso em: 07 jun. 2017.

SECRETARIA NACIONAL DO CONSUMIDOR. **Manual de direito do consumidor**. 4. ed. Brasília: Escola Nacional de Defesa do Consumidor. 2014, p.28. Disponível em:

<http://www.defesadoconsumidor.gov.br/images/manuais/manual-do-direito-do-consumidor.pdf> Acesso em: 04 jun. 2017.

SILVA, Kelyana Ribeiro; BRUM, Amanda Netto. Cadastro de inadimplentes e direito do consumidor sob a ótica do STJ. *In*: **Âmbito Jurídico**, Rio Grande, XVI, n. 113, jun 2013. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13296>. Acesso em: 14 jun. 2017.

SOUZA, Leandro. **Enova entra no cenário das fintechs**. 04 set. 2015. Disponível em: <https://www.baguete.com.br/noticias/04/09/2015/enova-entra-no-cenario-das-fintechs> Acesso em: 05 jun. 2017.

SPAGLIARI, Italo. **Direitos da personalidade**. 26 abr. 2014. Disponível em: <https://italospagliari.jusbrasil.com.br/artigos/117634705/direitos-da-personalidade> Acesso em: 07 jun. 2017.

THIBES, Maria Zanata. **O Público, o privado e o íntimo na era digital**. São Paulo: Biblioteca 24 horas, 2013.

WEBER, Rolf H. Internet of things – new security and privacy challenges. **Computer Law & Security Review** v. 26, n. 1, p. 23–30, 2010. Disponível em: <https://www.researchgate.net/file.PostFileLoader.html?id=55c4147460614b25168b45a3&assetKey=AS%3A273981783904256%401442333755312> Acesso em: 11 jun. 2017.

ZANATTA, Rafael A. F. **Internet das Coisas: privacidade e segurança na perspectiva dos consumidores**. Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017, Instituto Brasileiro de Defesa do Consumidor, p.5. Disponível em: <http://www.idec.org.br/ckfinder/userfiles/files/Contribuic%CC%A7a%CC%83o%20Pu%CC%81blica_%20Idec_%2006022017.pdf>. Acesso em: 10 jun. 2017.