UNIVERSIDADE CATÓLICA DO SALVADOR

JANAINA MARIA ALMEIDA CASTRO

DESAFIOS À EFETIVIDADE DOS DIREITOS À PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DO CREDIT SCORE.

Salvador

2020

JANAINA MARIA ALMEIDA CASTRO

DESAFIOS À EFETIVIDADE DOS DIREITOS À PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DO CREDIT SCORE.

Artigo apresentado na Graduação em Direito da Universidade Católica do Salvador, como requisito parcial para a obtenção do Título de Graduado em Direito.

Orientador:
Profª. Msc. Eurípedes B. Cunha Junior

Salvador

2020

DESAFIOS À EFETIVIDADE DOS DIREITOS À PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DO *CREDIT SCORE*.

Janaina Maria Almeida Castro[1]

Profª. Msc. Eurípedes B. Cunha Junior[2]

RESUMO: O avanço da tecnologia, em particular da internet e das decisões automatizadas, colocou a proteção de dados pessoais em posição de protagonismo. Neste mesmo compasso, os bancos de dados de proteção ao crédito e seus algoritmos para análise de risco e pontuação de crédito crescem em importância e sofisticação, exercendo um enorme poder sobre a vida dos consumidores. Este trabalho se propõe a analisar, através de pesquisa bibliográfica, os desafios à efetividade dos direitos à proteção de dados, em especial o direito à transparência e de autodeterminação informacional, no contexto do processo de *credit score* realizado pelos gestores de banco de dados de proteção ao crédito e apontar possíveis soluções.

Palavras-chave: Privacidade. Proteção de dados pessoais. Cadastro positivo. Pontuação de crédito. Bancos de dados de proteção ao crédito. LGPD. Direitos dos consumidores.

ABSTRACT: The advancement of technology, in particular the internet and automated decisions, has placed the protection of personal data in a leading position. In the pace speed, credit protection databases and their algorithms for risk analysis and credit scores are growing in relevance and sophistication, exercising enormous power over consumers' lives. This work aims to analyze, through bibliographic research, the challenges to the effectiveness of data protection rights, in particular right to transparency and to informational self-determination, within the scope of “the positive credit record” and to point out possible solutions.

Keywords: Privacy. Personal data protection. Positive credit records. Credit score. Credit protection database. LGPD. Consumer’s rights.

[1] Bacharel em Comunicação Social pela UCSAL em 1999. MBA em *Project Management* pela George Washington University e graduanda do Curso de Bacharel em Direito pela UCSAL.

[2] Mestre em Família na Sociedade Contemporânea, Professor de Direito Digital e de Ética na Universidade Católica do Salvador, Advogado

SUMÁRIO: 1 INTRODUÇÃO. 2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO 2.1 Evolução histórica do conceito de privacidade 2.2 Conceito de dados pessoais 2.3. Sociedade da informação e dados pessoais **3 ASPECTOS JURÍDICOS E REGULATÓRIOS DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS** 3.1 Da tutela da privacidade à proteção dos dados pessoais 3.2 as gerações das leis de proteção de dados 3.3 O direito à proteção de dados pessoais a luz da constituição federal do brasil de 1988 3.4 O direito à proteção dos dados pessoais na legislação infraconstitucional **4 O CREDIT SCORE E DIREITO À PROTEÇÃO DE DADOS** 1.1 Origem, finalidade e importância dos bancos de dados de proteção ao crédito 4.2 Desafios à efetividade dos direitos à proteção de dados **5 CONSIDERAÇÕES FINAIS. REFERÊNCIAS BIBLIOGRÁFICAS.**

1 INTRODUÇÃO

Testemunhamos hoje uma revolução tecnológica sem precedentes. Surge o *big data* a partir de bancos de dados com alta capacidade de armazenamento e com poder de processar um enorme volume de informações em uma velocidade incalculável. Algoritmos, altamente sofisticados, combinam as mais variadas informações pessoais e, através das suas fórmulas estatísticas, são capazes de formar perfis e predizer comportamentos. A "democratização da internet" mudou a forma como as pessoas se comunicam, se relacionam, se divertem, se informam e compram. Nasce, o que se convencionou chamar, a Sociedade da Informação.

Para esta "nova" sociedade a exposição é a regra, é condição de inclusão, de aceitação social. Como consequência, as pessoas passam a viver em um estado permanente de vigilância. Informações pessoais, hábitos, comportamentos, crenças, relacionamentos, passam a circular "livremente", sendo utilizados a todo tempo para nutrir a fome de poder de grandes empresas do setor privado e também do setor público. Afinal, quanto mais se conhece o "mercado", maiores as chances de dominá-lo e influenciá-lo.

Para o segmento de concessão de crédito, quanto mais informações se tem sobre o potencial tomador de crédito, mais preciso e confiável se torna o cálculo do seu risco de inadimplência. A partir de modelos estatísticos sofisticados, os algoritmos combinam informações pessoais, de forma a atribuir uma pontuação de crédito para uma determinada pessoa, ou seja, calcula seu nível de confiabilidade.

O fato é que o mercado de bancos de dados de proteção ao crédito (com seus algoritmos de *credit score*) está em franco crescimento e movimenta cifras estratosféricas. E, se por um lado, os benefícios para economia e também para a sociedade são inquestionáveis,

por outro lado, os riscos de lesão a princípios legais e direitos do titular de dados também o são. Desta forma, faz-se necessária a compatibilidade dos interesses comerciais e econômicos, que justifiquem o tratamento de dados pessoais nos processos de *credit score,* com os direitos e garantias conferidos aos indivíduos.

Nas últimas duas décadas, a matéria proteção de dados foi objeto de regulamentação na constituição (como uma dimensão da privacidade) e em diversas leis setoriais, inclusive a Lei de Cadastro Positivo - LCP, porém, dada a sua relevância, em 2018 foi aprovada a Lei Geral de Proteção de Dados - LGPD. Com a LGPD, o Brasil deu um passo importante no sentido de regulamentar o tratamento de dados pessoais pelas empresas e de proteger os direitos do cidadão.

O presente estudo tem como objetivo analisar, a partir de pesquisa bibliográfica qualitativa e debates virtuais, como o tratamento de informações pessoais no processo de *credit score* se conforma aos direitos de proteção de dados pessoais, apontar quais são os desafios encontrados à efetividade destes direitos e possíveis soluções.

Para estabelecer um caminho rumo a discussão central deste estudo serão abordados temas de suma importância para o entendimento do objeto de pesquisa, a saber: o impacto da tecnologia na vida em sociedade, evolução histórica do conceito de privacidade até a proteção de dados pessoais, como se deu o processo evolutivo das regulamentações envolvendo proteção de dados pessoais no direito comparado e no Brasil, por fim, se chegar a uma análise do processo de *credit score* no Brasil e sua relação com os direitos de proteção de dados pessoais.

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

Com o avanço expressivo da tecnologia, em especial da internet e dos bancos de dados, o paradigma da privacidade ganha novos contornos. Na sociedade da informação o eixo de preocupação extrapola o espaço íntimo, volta-se para a proteção daquilo que se expõe, independente de local e conteúdo, através do exercício da autodeterminação informacional por parte do titular de dados.

2.1 Evolução histórica do conceito de privacidade

Na antiguidade clássica, o privado estava relacionado com a família, a propriedade e a casa (*oikos*[3]). A esfera privada determinava o status social do individuo e era condicionante de acesso a esfera pública (*pólis*[4]), sendo por esta determinada. Percebe-se que a noção de privado tem uma estreita relação com bens materiais e pouca relação com a necessidade íntima do indivíduo (CANCELIER, 2017, p. 214).

Já na Idade Média, a esfera privada passou a ter uma conotação de preservação da esfera íntima, uma necessidade do indivíduo de ter o seu espaço particular dissociado da esfera pública e devendo ser por esta respeitada. O poder se desloca da esfera comum para esfera privada, passando a ser um espaço de discussão de pautas relevantes. No entanto, ainda neste período, ter acesso a uma vida privada, continuava sendo determinado pela situação econômica do indivíduo, tendo ainda um forte viés político (CANCELIER, 2017, p. 215).

Somente a partir da ascensão da burguesia que a privacidade passa a ter uma conotação mais próxima daquela dos dias atuais. Há um rompimento da relação com a política e com a necessidade de status social, e passa a ser expressão da necessidade do indivíduo de ter uma vida íntima, dissociada do que é público, um movimento de emancipação do indivíduo. A partir deste momento, começa a surgir a necessidade de uma atuação jurídica no sentido de garantir este "novo" direito individual que começa a ser formatado (CANCELIER, 2017, p. 216).

O caso paradigma realizado por *Warren* e *Brandeis* foi um marco para o tratamento do direito à privacidade como um instituto jurídico autônomo. Foi a partir deste trabalho que a tutela do direito à privacidade passa a ser conduzida a partir de um prisma de respeito à personalidade humana e não mais como uma proteção à propriedade. O direito de estar só inclui a proteção à expressão individual de qualquer natureza (pensamentos, palavras, sentimentos etc.), independente do meio utilizado para tanto (CANCELIER, 2017, p. 217 e 218).

Com a democratização da esfera pública, a partir da evolução tecnológica, resguardar a intimidade individual se tornou pré-requisito para o exercício da liberdade. Liberdade esta, que passa a assumir dois prismas: o de exercer a liberalidade de estar só, ou seja, exercer o direito de preservar aspectos íntimos, de não ser julgado, de "poder ser"; e o de autodeterminação, no que tange informações inerentes a sua pessoa, poder determinar o limite

[3] A palavra do grego antigo *oikos* refere-se a família, a propriedade da família e a casa.
[4] *Polis* era o modelo das antigas cidades gregas, desde o período arcaico até o período clássico.

de acesso e exercer o direito de concessão (CANCELIER, 2017, p. 220). Sendo assim, ser livre é ter o controle sobre o que expor, como expor e o quanto expor:

> No atual mundo digitalizado, como já ressaltado, o exercício do direito à privacidade será assegurado mesmo "em público", não sendo mais limitado ao que não é exposto. A privacidade está presente mesmo quando há exposição, mesmo quando há compartilhamento da informação, sendo que o "[...] que mais importa é a natureza da exposição e o que é feito posteriormente com essa informação [...] (CANCELIER, p. 229, 2017).

A mudança do paradigma é notória nos tempos atuais, onde a exposição é a regra, é condição de "pertencimento", de status. Este novo paradigma, traz um desafio ainda mais complexo no que tange à tutela do direito à privacidade, inclusive, no sentido de delimitar os seus limites e alcance. O fato de o indivíduo estar indo a público, expondo a sua privacidade, não significa que o mesmo está consentindo que esta seja invadida, ou multiplicada, ou utilizada para finalidades não autorizadas. Com isso, o objeto central da tutela deixou de ser um espaço ou mesmo o conteúdo em si, e passou a ser a expectativa de privacidade do titular, ou seja, até onde ele pretende consentir em relação ao que está sendo exposto. (CANCELIER, 2017, p. 367).

2.2 Conceito de dados pessoais

Inicialmente, importante ressaltar que o conceito de dados pessoais adotado por determinada lei é elemento crucial para delimitar o alcance da proteção abrangida por ela. Existem dois tipos de orientação conceitual possíveis: a reducionista e a expansionista. O que diferencia estas duas linhas, é o vínculo entre o dado pessoal e seu respectivo titular. Se este se dá de forma direta e imediata (conceito reducionista), ou, de forma mediata e indireta (conceito expansionista). Àquela, considera apenas a pessoa identificada e específica, ao passo que esta, inclui também, a pessoa identificável e indeterminada (BIONI, 2015).

As informações pessoais são aquelas que guardam um vínculo objetivo com a própria pessoa. Podem expressar suas características biológicas e biográficas, a exemplo do nome civil, estado civil, endereço, ou ainda, seus hábitos comportamentais (Ex.: dados referentes ao seu consumo, suas manifestações e opiniões). Considera-se a informação pessoal como um atributo da personalidade da pessoa. As principais legislações que versam sobre a matéria "proteção de dados pessoais", ao definir dados pessoais, coadunam com esta lógica conceitual, como será demonstrado a seguir (DONEDA, 2011).

A Convenção de Strasbourg, de 1981, define informação pessoal como “qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação” (DONEDA, 2011, p. 94). De forma muito similar, o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), aprovado em 2016 (EUROPA, 2016), define dado pessoal como “informação relativa a uma pessoa singular identificada ou identificável” (PINHEIRO, 2018).

A Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) segmenta dados pessoais em três categorias: 1) dados pessoais, toda informação relativa a uma pessoa identificada ou identificável; 2) dados pessoais sensíveis, relacionados a características da personalidade do indivíduo, assim como, suas escolhas pessoais, e; 3) dados anonimizados, dados que passam por um processo técnico para ocultação, de forma que não seja possível a sua associação com o seu titular, não sendo possível identificar o indivíduo, direta ou indiretamente, a partir da análise destes dados (PINHEIRO, 2018).

Consoante à classificação adotada pela LGPD, são exemplos de dados pessoais: nome civil, idade, endereço residencial ou e-mail, além de placas de automóvel, perfis de compra, número do *Internet Protocol* (IP). Por outro lado, questões de raça ou etnia, orientação sexual, religião, crenças e posições político-partidárias, saúde, dado genético ou biométrico, são consideradas dados sensíveis. Estes recebem uma tutela ainda mais rígida, uma vez que, podem ensejar comportamentos discriminatórios por parte de quem os detêm (PINHEIRO, 2018).

2.3 Sociedade da informação e dados pessoais

Ao analisar o processo histórico de formação das organizações sociais, é possível identificar um fator (socioeconômico) dominante que as determinava: na sociedade agrícola, a posse da terra; na sociedade industrial, a posse do capital, que movia a indústria de produção fabril; na sociedade pós-industrial, surgida pós 2ª Guerra Mundial, a prestação de serviços assumiu posição de destaque; e hoje, na dita sociedade atual, a informação é o novo elemento estruturante, fonte de poder e riqueza, que move a economia e a sociedade (BIONI, 2020).

A sociedade da informação é produto de uma rápida evolução tecnológica marcada pelo surgimento de máquinas capazes de processar, trafegar e armazenar dados, em volumes e velocidade inimagináveis (BIONI, 2020). Os bancos de dados cada vez mais robustos são as ferramentas responsáveis por executar tais atividades:

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações [...] (DONEDA, p.92, 2011).

No mundo atual, mais do que em qualquer outro período, deter informação é sinônimo de poder. Em um cenário de globalização e competição intensa, em que a tecnologia derrubou barreiras geográficas e agregou uma capacidade incalculável para combinar dados e transformar informação em inteligência, deter o domínio das informações de milhares de indivíduos é sinônimo de hegemonia de mercado e lucros estratosféricos (NAVARRO, 2011).

O apetite desenfreado pelo consumismo é outra marca da sociedade da informação, invertendo a hierarquia das motivações, fazendo com que o "ter" passe a valer mais que o "ser". De forma que, para empresas que transacionam na rede (as lojas virtuais), os dados pessoais dos consumidores são a mina de ouro para o sucesso dos seus negócios (PODESTÁ, 2000).

O avanço da tecnologia, por um lado, traz uma série de facilidades para humanidade, por outro, se não utilizado a serviço do homem, mas ocupando o seu espaço e vigiando-o, pode representar potencial ameaça de violação aos direitos da personalidade (PODESTÁ, 2000).

Para que tamanha democratização assuma um papel pró-sociedade, faz-se necessária a atuação do Estado para assegurar o exercício desta liberdade, sem que esta seja objeto de invasão ou discriminação, e que as informações sejam utilizadas em favor do interesse público, preservando-se o interesse particular do titular dos dados (NAVARRO, 2011).

Foi exatamente neste cenário de desenvolvimento da economia digital que, a partir de 1990, as regulamentações orientadas para proteção dos dados pessoais emergiram e ganharam força ao redor do mundo conforme será demonstrado a seguir.

õe

3 ASPECTOS JURÍDICOS E REGULATÓRIOS DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS

No contexto da sociedade da informação e da economia digital, a tutela dos dados pessoais dos indivíduos como forma de garantir o livre desenvolvimento da personalidade e a própria dignidade da pessoa humana ganha relevância jurídica. Com isso, evidencia-se no

âmbito mundial, o surgimento e o fortalecimento de um sistema normativo orientado à proteção dos dados pessoais.

3.1 Da tutela da privacidade à proteção dos dados pessoais

Como já mencionado, a normatização do direito à privacidade transitou entre os limites do que é público e privado, delimitando um espaço "particular", propício ao desenvolvimento da subjetividade individual, protegido da interferência de "terceiros", compreendido como um direito de ser deixado só (BIONI, 2020). No aspecto da proteção de dados, o exercício da liberdade negativa implica a proibição ou recusa ao acesso e utilização das informações sobre determinada pessoa (MACHADO, 2014).

No progresso tecnológico, existe uma alteração da sequência que há muito se prestou a definir a privacidade, deixando de ser "pessoa-informação-sigilo" e passando a ser "pessoa-informação-circulação-controle" (RODOTÁ, 2008, p. 93). Com isso, a proteção das informações pessoais, ganhou enorme relevância, demandando uma ampliação dos limites do direito à privacidade, que passou a incluir uma dimensão positiva de liberdade (RODOTÁ, 2008), de caráter dinâmico: positiva, já que cabe ao indivíduo exercer o controle sobre a forma de utilização dos seus dados pessoas e finalidade; dinâmica, uma vez que a proteção surge a partir do momento que existe a circulação destas informações, ou seja, no âmbito da esfera pública (BIONI, 2020).

Para além dos aspectos ora citados, existem outros assuntos que demonstram que a esfera de proteção dos dados pessoais é muito mais ampla que aquela da privacidade. Primeiramente, a proteção de dados pessoais demanda uma tutela jurídica coletiva, uma vez que, os danos causados pelo processamento inadequado de dados pessoais são, em regra, difusos. A contrário senso, os danos à privacidade normalmente alcançam o indivíduo (MENDES, 2008).

Outra questão relevante a ser considerada dentro do espectro de proteção dos dados pessoais, normalmente não considerada dentro dos limites da privacidade, é a igualdade. Tal disciplina se justifica, uma vez que, as informações pessoais podem ser utilizadas pelas entidades que as detém de forma discriminatória (MENDES, 2008), em particular os dados sensíveis:

> Insta destacar uma categoria específica de dados, chamados sensíveis, que significam determinados tipos de informação, que, caso sejam conhecidos ou divulgados, poderiam se prestar a uma potencial utilização discriminatória, como

> aqueles que dizem respeito a opções políticas, religiosas, filosóficas, sexuais, raciais e outros (MACHADO, 2014, p. 350).

Os dados pessoais, quando combinados, são capazes de construir uma representação do indivíduo (uma espécie de *avatar*[5]), mapeando gostos, hábitos, crenças, comportamentos, ou seja, traços significativos da sua personalidade (DONEDA, 2006). Vive-se em uma era de total vigilância, onde todos os passos dados na web são monitorados, construindo-se verdadeiros perfis pessoais, à total revelia do indivíduo (PODESTÁ, 2000).

O que determina o viés positivo ou negativo da utilização destes dados é a forma e a sua finalidade de uso. Sendo assim, um sistema que regulamente o tratamento destes dados, garantindo um efetivo controle (apesar da sua complexidade) pelo seu legítimo titular, tornou-se mandatório (DONEDA, 2006).

Resta claro, que o direito à proteção de dados pessoais, pela sua importância e alcance, se descola da sua original ligação com a privacidade, ganhando conotações próprias. Para além da privacidade, abrange a proteção da pessoa contra o controle indevido e a discriminação, garantindo a sua dignidade, igualdade e liberdade, elementos fundamentais ao desenvolvimento da personalidade humana (DONEDA, 2006).

Por fim, cumpre destacar, que a discussão não visa diferenciar estes dois direitos, até porque, o direito à proteção de dados pessoais também visa garantir a privacidade do indivíduo como um dos seus pilares, mas demonstrar que a dimensão do seu âmbito de proteção alcança outros direitos, o que justifica que ele seja considerado como um direito autônomo, merecedor de regulamentação própria (BIONI, 2020).

3.2 As gerações das leis de proteção de dados

O avanço acelerado da tecnologia, que trouxe no seu bojo a democratização do acesso à internet e potencialização da capacidade dos processadores de banco de dados, colocou ainda mais em evidência a temática envolvendo a proteção dos dados pessoais e sua respectiva regulamentação.

Se, inicialmente, o ordenamento jurídico envolvendo a matéria visava apenas regulamentar o aspecto da tecnologia em si e de forma esparsa, hoje, o tratamento autônomo da proteção de dados, em legislações específicas, é uma tendência e está construindo a base para o seu reconhecimento como um direito fundamental. Analisando-se o processo evolutivo

[5] O termo significa a representação de uma pessoa na internet

do sistema normativo, pode-se dividir, historicamente, a disciplina da matéria em quatro gerações de leis (DONEDA, 2011).

A primeira geração surge em um contexto de grande preocupação dos cidadãos com a coleta e processamento eletrônico de banco de dados pela Administração Pública e empresas privadas na Europa. O enfoque central das normas era o controle da tecnologia (MENDES, 2008).

> São exemplos de normas da primeira geração as seguintes: as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração pela sua estrutura e linguagem (MENDES, 2008, p. 33 e 34).

O conteúdo destas leis, de teor predominante técnico, era voltado para o controle (prévio) da atividade de processamento de banco de dados, através de um processo rígido de autorização para seu funcionamento. Buscava-se, também, disciplinar a forma de atuação dos seus agentes e a utilização dos dados pessoais pelo Estado, o foco era no banco de dados e não na privacidade (DONEDA, 2011).

Com a multiplicação dos centros de processamento de dados, o exercício do controle a partir de um rígido sistema de autorizações mostrou-se inviável, dando lugar à segunda geração de leis, ao final da década de 70. Destacam-se como marcos regulatórios deste período: a Lei da República Federativa da Alemanha sobre Proteção de Dados Pessoais (1977) e a Lei Francesa de Proteção de Dados Pessoais (1978) (DONEDA, 2011).

O enfoque deste sistema normativo desloca-se do fenômeno computacional para a privacidade e à proteção de dados pessoais, considerando-os como uma liberdade negativa, cabendo ao próprio indivíduo o controle do uso das suas informações, assim como reivindicar a sua tutela, em caso de uso indevido (DONEDA, 2011). Com isso, confere-se ao indivíduo, um poder maior de participação no processo de tratamento das suas informações e, de decisão, quanto ao grau de interferência no âmbito da sua privacidade informacional (MENDES, 2008)

administrativas responsáveis pela proteção de dados, como forma de garantir o direito à privacidade. Estas instituições atuavam tanto na fiscalização quanto no apoio aos cidadãos quando seus direitos eram violados (MENDES, 2008).

4 ASPECTOS JURÍDICOS E REGULATÓRIOS DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS

A terceira geração de leis nasce na década de 1980 a partir de uma mudança de paradigma em que o fornecimento de informações pelos indivíduos passa ser condição *sine qua non* para sua inserção na vida social (DONEDA, 2011). Nesse contexto de intensa socialização, focar na proteção de dados enquanto liberdade individual pode custar ao indivíduo a sua exclusão da sociedade e do mercado (MENDES, 2008).

A tutela promovida por esta nova geração de leis passa a incluir a autodeterminação informativa, que consiste no direito de consentimento atribuído ao titular dos dados e na sua participação ativa em todo processo de tratamento dessas informações, ou seja, exercendo uma liberdade positiva (DONEDA, 2011).

> São exemplos desta fase as leis dos Estados alemães após a decisão do Tribunal Constitucional, a emenda à lei federal de proteção de dados pessoais alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda (MENDES, 2008, p. 37 e 38).

Nesta participação mais intensa do indivíduo na gestão de todas as etapas de processamento dos seus dados, reside a maior diferença desta nova geração de leis. No entanto, a exemplo do que ocorreu com a segunda geração de leis, este propósito de participação e controle por parte do cidadão mostrou-se pouco factível, em razão do alto custo financeiro e social a ser pago pelo titular. Com o intuito de enfrentar este dilema surge a quarta geração de leis (MENDES, 2008).

A partir da análise das características da segunda e terceira gerações de leis depreende-se que seu enfoque de proteção era orientado para o indivíduo. Já a quarta geração de leis, vigentes hoje na maioria dos países, preocupa-se com a tutela da informação por uma perspectiva da coletividade. Este sistema normativo busca, por um lado, reduzir a assimetria existente entre o indivíduo e as entidades detentoras dos seus dados pessoais, fortalecendo a sua posição, mas, por outro, reduzir o seu poder de autotutela em situações que demandam proteção mais rígidas, a exemplo do tratamento dos dados sensíveis (DONEDA, 2011).

Ulterior aspecto dessa geração normativa é o surgimento de leis setoriais acerca da matéria, visando oferecer uma proteção orientada para cada contexto específico envolvendo o processamento e tratamento dos dados (MENDES, 2008). Notou-se que a disciplina da proteção de dados pessoais nas últimas três décadas passou por um intenso processo evolutivo

fortemente influenciado pelos avanços tecnológicos e que trouxeram no seu bojo a proteção da liberdade, a partir da autodeterminação informativa e da igualdade, através de estruturas rígidas de proteção aos dados sensíveis. Ademais, esta dinâmica evolutiva tende a ser contínua com vistas a acompanhar as novas realidades sociais (MENDES, 2008).

4.1 O direito à proteção de dados pessoais a luz da Constituição Federal do Brasil de 1988

Exaustivamente explorado, o avanço acelerado da informática que levou a um aumento expressivo no volume de informações (pessoais) circulando, fez com que os dados pessoais se transformassem em um fenômeno jurídico a ser regulado, inclusive pelo seu potencial de influência, positiva ou negativa, sobre diversos direitos fundamentais, a exemplo do direito à igualdade, à liberdade, honra, atingindo, pois, a própria dignidade da pessoa humana (MENDES, 2014).

Na Constituição Federal de 1988 (BRASIL,1988), ela se releva a partir do direito fundamental à liberdade de expressão e do direito de acesso à informação, da garantia de acesso e retificação dos dados pessoais através da ação de *habeas data* (art 5º, LXXII), da vedação à interceptação telefônicas, telegráficas ou de dados (art. 5º, XII) e do direito à inviolabilidade da vida privada e intimidade (art. 5º, X) (DONEDA, 2011).

Antes de enfrentar detalhadamente os principais incisos que versam acerca do tema na CF88, importante trazer uma visão geral do direito fundamental à liberdade. Não por acaso, ele é abordado no *caput* do artigo 5º do texto constitucional, por "tratar-se da própria essência dos direitos fundamentais de primeira geração" (PAULO e ALEXANDRINO, 2014, p. 122).

Este direito se impõe como um limitador à atuação do Estado perante o indivíduo e alcança, para além da liberdade física e de locomoção, as crenças, expressão de pensamento, dentre outros aspectos fundamentais ao desenvolvimento livre da personalidade humana e de sua dignidade (PAULO e ALEXANDRINO, 2014).

Partindo para uma análise mais detida desses direitos, a liberdade de expressão vem tratada nos incisos IV, V, e IX do artigo 5º da CF/88. Consoante o inciso IV, "é livre a manifestação do pensamento, sendo vedado o anonimato" (BRASIL,1988), por este comando, qualquer pessoa pode se expressar oralmente ou por escrito de forma livre, assim como pode escolher livremente o que ler, assistir ou ouvir.

Já os incisos XIV e XXXIII abordam o direito de acesso à informação. Sendo, no primeiro, informações de interesse público e, no segundo, informações que estão sob domínio dos órgãos públicos, devendo ser por estes providas, podendo ser de interesse particular ou coletivo. Ambos têm forte relação com os princípios da transparência e o exercício de controle popular. No sentido de garantir o exercício deste direito de acesso, em caso lhe seja negado, o cidadão tem a seu dispor a ação de *habeas data* (ALEXANDRINO e PAULO, 2014).

Os incisos XI (inviolabilidade do domicílio) e XII (inviolabilidade das correspondências e das comunicações) são igualmente dignos de nota como desmembramentos da proteção do direito à vida privada. Importante ressaltar que "domicílio" deve ser interpretado de forma ampla e abrange qualquer estabelecimento privado e não somente à residência (ALEXANDRINO e PAULO, 2014).

Cumpre salientar que o direito à proteção de dados, no contexto da Constituição Federal, deriva do direito à privacidade (art. 5º, X), mas ainda que seja reconhecido como direito fundamental de forma indireta, os mecanismos de proteção disponíveis se mostram insuficientes frente aos atuais efeitos que o processamento e a utilização de informações podem causar aos indivíduos (MENDES, 2014).

Exatamente por restar claro que somente um direito fundamental à proteção de dados pessoais seria capaz de resguardar os indivíduos face os atuais riscos, que se encontra em tramitação o projeto de emenda a constituição no. 17/2019 que acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

4.2 O direito à proteção dos dados pessoais na legislação infraconstitucional

Em relação à disciplina da proteção dos dados pessoais na legislação brasileira, quatro leis são protagonistas: o Código de Defesa do Consumidor (BRASIL, 1990), o Marco Civil da Internet (BRASIL, 2014), Lei do Cadastro Positivo (BRASIL, 2011) e a Lei Geral de Proteção de Dados (BRASIL, 2018), conforme sublinha Bruno Bioni (2020).

O Código de Defesa do Consumir (CDC) surgiu com o objetivo de promover a proteção dos consumidores diante da sua patente vulnerabilidade frente aos fornecedores e com isso buscar reestabelecer uma relação mais equilibrada entre eles. Por este mesmo viés,

o código consumerista pautou a disciplina do tema de proteção aos dados pessoais dos consumidores, com o intuito de evitar que suas informações fossem utilizadas, pelos seus detentores, de maneira discriminatória, afetando "expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais" (MENDES, 2008, p. 129).

> Nesse contexto, é fundamental levar-se em conta a vulnerabilidade do consumidor, tanto técnica, por possuir menos informações que o fornecedor a respeito do fluxo de seus dados, como fática, por possuir menos recursos intelectuais e econômicos para a reparação de prejuízos advindos do tratamento de dados (MENDES, 2008, p. 129 e 130).

Os bancos de dados e cadastro de consumidores estão disciplinados nos artigos 43 e 44 do CDC. Conforme restará demonstrado a seguir, é possível identificar que o sistema de proteção foi fortemente pautado em garantir ao consumidor o direito de exercer controle sobre seus dados pessoais (BIONI, 2020; MENDES, 2014).

No "*caput*" do artigo 43 é possível identificar o direito de acesso aos dados e suas fontes; o §1º trata do princípio da transparência e qualidade dos dados, determinando que devem ser objetivos, claros e de fácil compreensão, além de definir um lapso temporal para seu arquivamento (5 anos); o §2º versa sobre o dever de comunicação quando da inclusão em banco de dados se a mesma ocorrer sem consentimento; já o §3º garante o direito de retificação e exclusão dos dados pelo consumidor; o §4º determina o caráter público desses bancos de dados, isto implica que os mesmos se submetem ao crivo da legalidade e que cabe *habeas data* como instrumento de acesso às informações (MENDES, 2014).

Importante salientar que o sistema de proteção aos dados pessoais dos consumidores oferecidos pelo código consumerista representou um importante avanço legislativo, no entanto, a complexidade do tema exige uma estrutura jurídica muito mais robusta para garantir de fato uma tutela efetiva aos direitos fundamentais à privacidade, igualdade e liberdade dos cidadãos, no contexto da sociedade da informação, de forma que sua normatização seguiu evoluindo (MENDES, 2008).

A lei do Marco Civil da Internet (MCI) foi aprovada em 2014, em regime de urgência, devido ao escândalo de espionagem revelado pelo ex-analista *Edward Snowden*. O diploma legal foi editado com o objetivo de regular as relações dos cidadãos no ambiente eletrônico atribuindo-lhes direitos e obrigações. Dentre os pilares da MCI encontra-se o direito à proteção dos dados pessoais e da privacidade, coexistindo com a liberdade de expressão e neutralidade da rede (BIONI, 2020).

Repetindo a abordagem de outras legislações, o MCI também se pautou no princípio do consentimento, que consoante o texto da lei, deve ser "livre, expresso e informado" (BIONI, 2020, p. 126). Também determina que o controle exercido pelo titular deve ser amplo, contemplando todas as etapas do processo de tratamento de dados, desde a sua captação, compartilhamento e exclusão (BIONI, 2020).

Por fim, existem dois diplomas legais que são centrais para o propósito do presente estudo: a Lei de Cadastro Positivo (LCP) e a Lei Geral de Proteção de Dados (LGPD). A LCP foi regulamentada pela Lei 12.414/2011, tratando de questões envolvendo banco de dados e processamento de informações relacionadas às operações financeiras e comportamento de pagamento, com a finalidade de decidir acerca da concessão de crédito. Essa análise não se esgota no aspecto do inadimplemento, mas também observa aspectos positivos, como a capacidade financeira do cidadão (BIONI, 2020; MENDES, 2014).

Dentre os principais aspectos da LCP, no que tange à disciplina da proteção à privacidade e dados pessoais, pode-se destacar: o princípio da qualidade, exatidão das informações (art. 3º, § 1º); a vedação ao tratamento de informações excessivas e sensíveis (art. 3º, § 3º); o direito de informação, acesso, retificação e cancelamento dos dados pelos seus titulares, além do direito ao pedido de revisão de decisões baseadas por meios automatizados (art. 5º, I a VI e 6º); o princípio da finalidade específica envolvendo a coleta e uso dos dados (arts. 2º, I; 5º, VII e 7º); o limite temporal de 15 anos para armazenamento de informações de adimplemento (BRASIL, 2011).

O texto original da LCP sofreu alterações a partir da lei complementar n° 166/2019, sendo a mais relevante e polêmica, a mudança do modelo de inclusão dos dados no cadastro positivo, que antes só ocorria com o consentimento do consumidor (*opt-in*[6]), e passou a se dá de maneira automática, cabendo ao titular pedir a sua exclusão (*opt-out*[7]), se esta for a sua vontade, para tanto o mesmo deve ser comunicado no prazo de até 30 (trinta) dias (BESSA, 2019).

É possível concluir, a partir dos aspectos aqui discutidos, que a LCP, a exemplo dos diplomas anteriores, se pauta na autodeterminação informacional como base para a confecção dos seus comandos legais (BIONI, 2020; MENDES, 2014).

---

[6] O termo *opt-in* refere-se à expressão da vontade de um usuário de ser incluído em um banco de dados ou cadastro, afastando-se sua presunção de aceite pelo silêncio

[7] *Opt-out* é a expressão de vontade do titular de dados de não permanecer em um dado banco de dados ou cadastro.

Por fim, após quase uma década de debates públicos, foi editada e aprovada a tão esperada Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD foi eminentemente baseada no sistema europeu de proteção de dados, em particular na GDPR[8], o que pode ser evidenciado a partir de subsídios fundantes do seu texto: a exigência de base legal para tratamento de dados, a adoção de princípios gerais, nas regras para tratar dados sensíveis, assim como por contemplar a criação de uma autoridade de proteção de dados (DONEDA e MENDES, 2019). Segundo Doneda e Mendes (2019), o texto da LGPD é divido em cinco eixos principais:

> i) unidade e generalização da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes (DONEDA e MENDES, 2019, p. 312)

O âmbito de aplicação material da Lei consiste na proteção dos dados dos cidadãos, independente de quem realiza o tratamento do dado, incluindo os setores público e privado. Dentre as hipóteses que autorizam o tratamento de dados previstas na Lei estão: o consentimento (livre, informado, inequívoco e com finalidade específica), o legítimo interesse e a proteção ao crédito (DONEDA;MENDES, 2019).

No aspecto principiológico, a LGPD se baseou no *Fair Information Practice Principles* (FIPPs), uma espécie de tronco comum de todo sistema de proteção de dados, além de agregar outros princípios mais contemporâneos. Configuram o rol de princípios expressos na Lei: o livre acesso, segurança, transparência, qualidade, não discriminação e o da prevenção (DONEDA;MENDES, 2019).

O quarto eixo estabelece as obrigações e limites aos agentes responsáveis pelo tratamento de dados, além de prever procedimentos que visem proporcionar maior segurança ao titular dos dados. Em relação à responsabilização dos agentes, objeto do quinto eixo, cumpre destacar que o regime adotado foi o da "responsabilidade objetiva" em caso de danos materiais e morais causados aos titulares de dados (DONEDA;MENDES, 2019).

A partir do panorama traçado ao longo deste capítulo, é possível verificar que houve uma intensa atividade legislativa em torno da proteção de dados pessoais. Com exceção do CDC, todas as principais leis entraram em vigor ao longo dos últimos dez anos, inclusive a

[8] *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados 2016/679) é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu que foi criado em 2018.

LGPD, que “inaugurou um regime geral de proteção de dados pessoais” (DONEDA; MENDES, 2019, p. 310).

No entanto, apesar do notório avanço normativo, ainda são muitos os entraves à efetividade dos direitos e princípios por elas garantidos, alguns dos quais serão objeto de análise no contexto específico dos sistemas de pontuação de crédito.

5 O *CREDIT SCORE* E DIREITO À PROTEÇÃO DE DADOS

A massificação do consumo, em grande parte motivada pelas novas tecnologias, intensificou o movimento de oferta e demanda por crédito. Com isso, o processo de *credit score* utilizados pelos bancos de dados de proteção ao crédito ganharam enorme relevância, ao atribuir mais credibilidade e segurança às relações de concessão de crédito. No entanto, se por um lado, a pontuação de crédito traz impactos econômicos positivos, por outro, pode trazer sérios riscos a direitos fundamentais dos titulares dos dados pessoais, se as informações forem utilizadas de maneira excessiva e discriminatória.

5.1 Origem, finalidade e importância dos bancos de dados de proteção ao crédito

Os bancos de proteção ao crédito no Brasil surgiram na década de 50 em razão do aumento das vendas a crédito. Nesta ocasião, a análise era feita pelos próprios lojistas, de forma manual e lenta. Com a massificação do consumo, os bancos de dados de proteção ao crédito ganharam relevância e passaram a ser geridos por terceiros. A partir de 1955 começaram a surgir as Câmaras de Dirigentes Logistas (CDL), em Portal Alegre e São Paulo inicialmente. Hoje são mais de 2.000 CDLs interconectadas formando o SPC-Brasil (BESSA, 2019).

A partir da década de 60, o setor de crédito passou a ser explorado economicamente por empresas como a Serasa Experian (1968), detentora da maior base de dados da América Latina, a Boa Vista, criada há mais de 60 anos como o SCPC (Serviço Central de Proteção ao Crédito), que em 2010 virou a Boa Vista SCPC, a partir da junção da Associação Comercial de São Paulo, da Associação Comercial do Paraná, do CDL do Rio de Janeiro, além da TMG

Capital. Mais recentemente, em 2016, grandes bancos se uniram e criaram a Quod[9] (BESSA, 2019).

No âmbito das transações envolvendo concessão de crédito quanto mais se conhece sobre a pessoa do contratante através de informações que permitam avaliar com maior precisão a sua capacidade de adimplemento, maior o nível de confiabilidade e segurança para os credores. Aqui reside o papel dos gestores de bancos de dados de crédito (GDBs[10]), tratando e compartilhando com terceiros (consulentes[11]) informações relevantes acerca dos potenciais tomadores de crédito, a fim de reduzir a assimetria de informação e conferir mais segurança às transações (BESSA, 2019).

Com isso, teoricamente, existem ganhos para ambos: os consumidores podem ter mais facilidade de acesso ao crédito, com "custos" menores de aquisição (juros mais baixos); as empresas, com menor risco de inadimplência, podem ter o seu lucro empresarial satisfeito (BESSA, 2019). Do ponto de vista socioeconômico, o crédito exerce outras duas funções essenciais:

> Função Econômica, financiando o consumo e ampliando o acesso dos consumidores aos produtos e serviços, ampliando assim o seu poder de compra. Função Social, incentivando o aumento da produção em geral, gerando assim empregos e crescimento econômico (ZANATTA, 2017, p. 14, grifos nossos).

Jappelli e Pagano (2000) identificam outros potenciais efeitos gerados a partir da atividade realizada pelos bancos de dados de proteção ao crédito: cálculo mais preciso do preço do crédito a partir da redução da seleção adversa; potencial para disciplinar o consumidor a adimplir os créditos contratados, de forma a evitar que uma eventual reputação negativa imponha barreiras de acesso a novos créditos; inibe a aquisição de credito em múltiplos fornecedores, uma vez que estes terão visibilidade dos créditos ativos, contribuindo para evitar o superendividamento (JAPPELLI e PAGANO, 2000).

Mas afinal, como os GDBs atuam? Eles se valem de métodos estatísticos de avaliação para indicar a "confiabilidade" do possível tomador do crédito e determinar a probabilidade de inadimplência, atribuindo-lhes uma pontuação de crédito (*credit score*). O

---

[9] Quod: Gestora de Inteligência de Crédito S.A., formada pelo Banco do Brasil, Bradesco, Caixa Econômica Federal, Itaú-Unibanco e Santander.

[10] Gestor de Banco de Dados: pessoa jurídica que atenda aos requisitos mínimos de funcionamento previstos nesta Lei e em regulamentação complementar, responsável pela administração de banco de dados, bem como pela coleta, pelo armazenamento, pela análise e pelo acesso de terceiros aos dados armazenados.

[11] Consulente: pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida por Lei.

cálculo é realizado de forma automatizada, por meio de algoritmos[12], que em geral vai de 0 a 1000, sendo que quanto maior a nota menor o risco de inadimplência. Para realizar este processo utilizam como fonte de dados registros públicos (protestos formais e ações de execução) e bases de dados privadas (ZANATTA, 2017).

> Algoritmos preditivos extraem informações pessoais para fazer suposições sobre as prováveis ações e riscos dos indivíduos. As atividades *online* e *offline* de uma pessoa são transformadas em pontuações que as classificam acima ou abaixo de outras. Entidades privadas e públicas contam com avaliações algorítmicas preditivas para tomar decisões importantes sobre indivíduos (CITRON e PASQUALE, 2014, p. 3, tradução nossa).

Com o objetivo de realizar avaliações mais precisas, os GDBs passaram a munir suas bases de dados com maior quantidade de informações e das mais variadas. Houve uma expansão dos tipos de dados considerados relevantes, para além de informações de ordem econômica, informações comportamentais (a exemplo de perfis de mídias sociais, hábitos de navegação na internet e etc.) foram agregadas ao processo de pontuação de crédito (DIAS e NATUSCH, 2017).

No entanto, este processo de sofisticação crescente dos processos de pontuação de crédito, nutridos a partir de mais e mais informações pessoais dos consumidores, pode implicar em ofensa grave a direitos e garantias fundamentais dos titulares de dados pessoais, se realizados de maneira abusiva e com desvio de finalidade, colocando em risco à privacidade, à honra e dignidade do consumidor. Se de um lado não existem controvérsias acerca da relevância econômica do *score* de crédito, por outro, o debate em torno da sua conformidade aos direitos à proteção de dados é bastante polêmico.

Sendo assim, analisar os sistemas de pontuação de crédito para além do interesse comercial e econômico, levando em consideração também o interesse público, em particular no que tange os direitos à proteção de dados pessoais, faz-se necessário.

5.2 Desafios à efetividade dos direitos à proteção de dados

Com a mudança no modelo de adesão dos cadastrados causada pela lei complementar n° 166/2019, de opt-in para opt-out, toda população economicamente ativa poderá ser inserida no cadastro positivo sem consentimento prévio, devendo apenas ser

[12] De uma maneira simplificada, um algoritmo é um programa de computador que recebe e segue instruções especificas programadas previamente para atingir um certo fim.

comunicada, nos termos da LCP13, optando posteriormente por cancelar seu cadastro positivo. Importante salientar que a mudança foi pautada em interesse meramente econômico, sem que o aspecto do interesse do consumidor fosse considerado. A expectativa é que a adesão alcance em torno de 120 milhões de cadastrados, ou seja, um salto dantesco em relação aos 15 milhões aderentes antes da mudança na lei (MORIBE e SILVA, 2020).

Este aumento expressivo no número de pessoas que terão seus dados tratados, combinado com a sofisticação dos modelos estatísticos preditivos realizados pelos algoritmos, que se utilizam de informações "infinitas" (cadastrais, financeiras e comportamentais) para determinar o quanto um consumidor é ou não "confiável", reforça a importância do debate em torno de práticas capazes de conferir efetividade aos direitos à proteção de dados pessoais, amplamente garantidos na CF/88, na própria Lei de Cadastro Positivo, no CDC (e outras lei setoriais) e de maneira especial, na LGPD.

Em síntese, especificamente consoante a Lei de Cadastro Positivo, o cadastrado tem o direito: 1) de saber quais os dados e critérios utilizados para compor o *score* de crédito; 2) de corrigir informações erradas e imprecisas; 3) de revisar decisões automatizadas que gerem consequências negativas; 4) de ter seus dados negativos e positivos armazenados por um período determinado de tempo e; 5) de impedir a análise de informações sensíveis[14] e/ou excessivas[15] sob pena de responsabilização por danos morais *in re ipsa* (ZANATTA, 2017).

Neste mesmo sentido, o STJ, no paradigmático Recurso Especial 1.419.697/RS, firmou importante tese baseada em cinco pilares: 1) o *credit score* não é banco de dados, mas uma metodologia de avaliação de risco baseada em fórmulas matemáticas e a utilização destes algoritmos consiste em uma prática comercial legal; 2) o processo de avaliação de risco deve seguir as normas do sistema de proteção do consumidor no que tange à privacidade e transparência; 3) o consumidor possui direitos de privacidade quanto aos seus dados pessoais e de transparência com respeito à utilização do sistema de "credit score" e o seu funcionamento, de acordo com o Código de Defesa do Consumidor e com a Lei 12.414/2011; 4) que são deveres daqueles que se utilizam de tal metodologia, por exemplo, utilizar informações objetivas, claras e não excessivas (DONEDA e ZANATTA, 2017)

[13] O art. 4º, § 4º, I e III da LCP, determina o prazo de comunicação em até 30 dias e que o cadastrado deve ser informado de maneira clara e objetiva acerca dos canais para cancelamento do seu cadastro.
[14] dados sensíveis: contém aspectos mais íntimos da vida de um indivíduo, na LCP como aquelas "pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".
[15] dados excessivos: que excedem a finalidade para o qual estão sendo coletadas.

No entanto, apesar da ampla legislação e jurisprudência acerca da matéria, a real discussão gira em torno dos seguintes pontos: esses direitos são conhecidos e efetivamente exercidos pelos consumidores? A realidade mostra que não. Segundo o IBDC[16], até 2018 foram registradas mais de 90 mil reclamações contra Serasa, SPC Boa Vista e outros birôs de crédito, em grande parte relacionadas com a não observância do direito à transparência e uso indevido de informações pessoais (ZANATTA, 2018).

Cintro e Pasquale (2014) relatam alguns problemas básicos envolvendo os sistemas de *credit score*, dos quais, dois são dignos de nota por reforçarem o quanto afirmado: a obscuridade dos resultados e a disparidade de impactos.

Como existe um desconhecimento acerca dos critérios utilizados para atribuir uma pontuação de crédito, torna-se difícil para o indivíduo questionar sua pontuação, assim como a sua auditoria por parte dos órgãos encarregados de garantir a sua proteção. Corriqueiramente os gestores dos bancos de dados de proteção ao crédito negam acesso aos detalhes do seu sistema de crédito e não permitem que pessoas externas auditem seus algoritmos (CITRO e PASQUALE, 2014).

Existe uma total falta de transparência nestes sistemas que deixam os consumidores confusos em relação à pontuação que lhes é atribuída. Com isso, os consumidores não são capazes de determinar o comportamento de crédito ideal ou mesmo o que fazer para evitar uma redução em suas pontuações (CITRO e PASQUALE, 2014).

Já a disparidade de resultados relaciona-se com a ausência de isenção de preconceitos que certamente envolvem o sistema de pontuação de crédito. Os engenheiros de software constroem os conjuntos de dados extraídos pelos sistemas de pontuação, definem os parâmetros das análises de mineração de dados, criam os *clusters*, *links* e árvores de decisão aplicados, geram os modelos preditivos. Destarte, os preconceitos e valores dos desenvolvedores de sistema e programadores de software estão introduzidos em cada etapa do desenvolvimento, podendo causar potenciais discriminações no processo de avaliação (CITRO e PASQUALE, 2014).

Adicionalmente, consoante assevera Zanatta (2018), outros entraves se colocam frente à efetivação destes direitos no contexto do *credit score*, dos quais vale destacar: 1) a falta de conhecimento e consciência jurídica por parte dos consumidores acerca dos seus direitos; 2) a insuficiência de instrumentos e meios para que os consumidores exerçam o direito de acesso e controle sobre suas informações; 3) a ausência de um sistema de

[16] Instituto Brasileiro de Defesa do Consumidor.

governança e responsabilização que assegure parâmetros de funcionamento para estes *credits scorings* de forma a atingir a suas finalidades; 4) inexistência de um órgão regulador e fiscalizador que atue neste mercado (ZANATTA, 2018).

Em suma, se é possível condensar tudo o quanto exposto no que tange aos desafios postos à efetivação dos direitos à proteção de dados pessoais nos seguintes pilares: conscientização (dos consumidores), transparência, fiscalização e *accountability*[17].

Para que os titulares possam exercer os direitos sobre suas informações pessoais que lhes são garantidos por lei (autodeterminação informativa), eles precisam conhecer e saber como buscar a efetividade destes direitos. Uma vez conscientes dos seus direitos, faz-se mister que exista transparência em relação aos critérios utilizados para cálculo da pontuação de crédito, e não se trata de acesso aos algoritmos em si (ininteligíveis), mas quais e como as informações são consideradas. Somente a partir deste acesso que o cidadão vai poder "controlar" o uso dos seus dados e verificar se os limites legais estão sendo respeitados.

Já a fiscalização está relacionada com a necessidade de atuação (efetiva e preventiva) por parte do Estado, através de órgãos reguladores, com autonomia para auditar à conformidade das práticas de *credit score* com as normas de proteção de dados pessoais e com poder de punir as irregularidades identificadas. O aspecto do *accountability* inclui o comprometimento dos agentes com a ética, a boa-fé, as leis e, principalmente, com a responsabilidade social.

Por fim, o enfrentamento destes desafios é árduo, mas inteiramente possível, e perpassa pelo esforço conjunto do Poder Público (regulando, fiscalizando e informando), da sociedade civil organizada, das empresas envolvidas nas relações comerciais e dos próprios consumidores (enquanto agentes de controle).

6 CONSIDERAÇÕES FINAIS

Indiscutivelmente, a tecnologia transformou de maneira abrupta e irreversível toda sociedade. "Universalizou" os continentes, mudou a forma como as pessoas se expressam, se relacionam e consomem. Transformou o paradigma de privacidade e de liberdade. Para a sociedade da informação ser livre é ter o controle sobre o que expor, como expor e o quanto expor.

[17] Termo da língua inglesa que pode ser traduzido como responsabilidade com ética e remete à obrigação, à transparência.

Neste “novo” mundo sem barreiras, a “propriedade” da informação é sinônimo de poder, quanto mais se sabe sobre algo ou alguém, maior a capacidade de exercer controle, de manipular e de competir. A atuação dos Estados no sentido de proteger a “propriedade informacional” dos indivíduos garantindo-lhes um conjunto de direitos e impondo limites de acesso e utilização aos agentes públicos e privados, se tornou mandatório. Neste sentido, a pauta “proteção de dados pessoais”, especialmente a partir da aprovação da LGPD, tem sido objeto de profundos debates nas mais diversas “arenas”, tanto pública, quanto privada.

O *credit score* também é fruto desta nova sociedade do consumo, até por ser uma poderosa ferramenta de acesso ao “ter”. Inegavelmente, são instrumentos contemporâneos que trazem benefícios para a economia e para sociedade, como já amplamente demonstrado ao longo deste trabalho. Porém, tamanha a sua relevância social, que o seu monitoramento deve ser tratado como uma questão de interesse público.

A utilização de informações pessoais no processo de *score* de crédito tem efeitos de grande extensão na vida dos consumidores. O acesso ao crédito exerce um papel importante de inclusão dos indivíduos na sociedade, ele tem o condão de permitir acesso a produtos e serviços que são basilares para o livre desenvolvimento da personalidade e para a própria dignidade da pessoa humana (Ex.: acesso a habitação, saúde particular, eletrodomésticos ou ainda, meios que facilitam a inserção no “mercado” de trabalho e etc.).

A utilização inadequada, excessiva e com desvio de finalidade das informações cadastrais, no processo de pontuação de crédito tem um alto poder de afronta a direitos fundamentais do indivíduo. Portanto, é essencial a atuação do Poder Público e de entidades privadas, no sentido de fiscalizar e coibir práticas discriminatórias, garantindo a uso responsável das informações pessoais pelos birôs de crédito.

Sendo assim, para que os sistemas de *score* de crédito realizem de maneira sustentável a sua função econômica e social, ou seja, que exista um equilíbrio entre o atendimento aos interesses do mercado e da população, é patente que se promovam ações capazes de dar real efetividade aos princípios e direitos a proteção de dados pessoais expressos em nosso ordenamento jurídico.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRINO, Marcelo; PAULO, Vicente. **Direito Constitucional Descomplicado**. 12ª ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO: 2014.

BESSA, Leonardo Roscoe. **Nova Lei do Cadastro Positivo**: comentários à Lei 12.414, com as alterações da lei complementar n. 166/2019 e de acordo com a LGPD. 2019. São Paulo: Revista dos Tribunais, 2019.

BIONI, Bruno Ricardo. **O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores**: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo 'Lulu'. Revista Direito do Consumidor – v. 94 – p. 283-326 – jul.- ago. / 2014

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. – Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo. **Xeque-Mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo (SP): GROPAI USP; 2015.

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

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil. Brasília**, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2020.

BRASIL. Lei nº. 12.414, de 09 de junho de 2011. **Lei de Cadastro Positivo**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 20 de out. 2020.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 20 out. 2020.

BRASIL. Supremo Tribunal Federal. STF, **Ação Direta de Inconstitucionalidade** no. 1790/DF, Relator: Ministro Sepúlveda Pertence. DJ 08/09/2000.1998. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=347269. Acesso em: 22 out. 2020.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje**: perspectiva histórica e o cenário brasileiro. Sequência, Florianópolis, n. 76, p. 213-239, maio 2017.

Citron, D. K., & Pasquale, F. A. (2014). **The scored society**: due process for automated predictions. Washington Law Review, 89.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo; Zanata, Rafael. **O que há de novo no debate "credit score" no Brasil?**. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017. Acesso em: 26 de out. 2020.

DIAS, Tatiana; NATUSCH, Igor. **Como empresas financeiras stalkeiam suas informações online**. 2017. Disponível em: https://www.vice.com/pt/article/bjd883/como-empresas-financeiras-stalkeiam-suas-informacoes-online. Acesso em: 25 out. 2020.

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

DONEDA, Danilo; MENDES, Laura Schertel Ferreira. **Um perfil da nova Lei Geral de Proteção de Dados brasileira**. In: BELLI, Luca; CAVALLI, Olga (org.). Governança e regulações da internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 325-343.

JAPPELLI, Tullio; PAGANO, Marco. *Information Sharing in Credit Markets: A Survey*. 2000. *Centro Studi in Economia e Finanza*. *Working paper* n. 36. Disponível em: http://www.csef.it/WP/wp36.pdf. Acesso em: 28 out. 2020.

MACHADO, Joana de Moraes Souza. **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados**. Revista da AJURIS – v. 41 – n. 134 – Junho 2014.

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

MENDES, Laura Schertel. **Transparência e Privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de Brasília, Brasília, 2008.

MORIBE, Gabriela;SILVA,Gustavo Henrique Luz. **O que ainda não te contaram sobre a "nova" Lei do Cadastro Positivo?**. 2020. Disponível em:https://baptistaluz.com.br/institucional/lei-do-cadastro-positivo/. Acesso em: 26/10/2020.

NAVARRO, Ana Maria Neves de Paiva. **O Direito fundamental à autodeterminação informativa. Publica Direito**. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c>. Acesso em: 8 de abril de 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). – São Paulo: Saraiva Educação, 2018.

PODESTÁ, Fábio Henrique. **Direito à intimidade em ambiente da internet**. In: Lucca, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & internet – aspectos jurídicos relevantes. Bauru, SP: EDIPRO, 1ª reimp., 2001. p. 155-176.

RODOTÁ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008.

ZANATTA, Rafael. **Pontuação de crédito e direitos dos consumidores**: o desafio brasileiro. 2017. São Paulo, 2017. Disponível em: https://idec.org.br/ferramenta/estudo-pontuacao-de-credito-e-direitos-dos-consumidores. Acesso em: 27 de out. 2020.

ZANATTA, Rafael (Org.). **Por trás da pontuação de crédito**: conheça seus direitos. / Instituto Brasileiro de Defesa do Consumidor. São Paulo: Idec, 2017. Disponível em: https://idec.org.br/ferramenta/por-tras-da-pontuacao-de-credito-conheca-seus-direitos. Acesso em: 28 de out. de 2020.