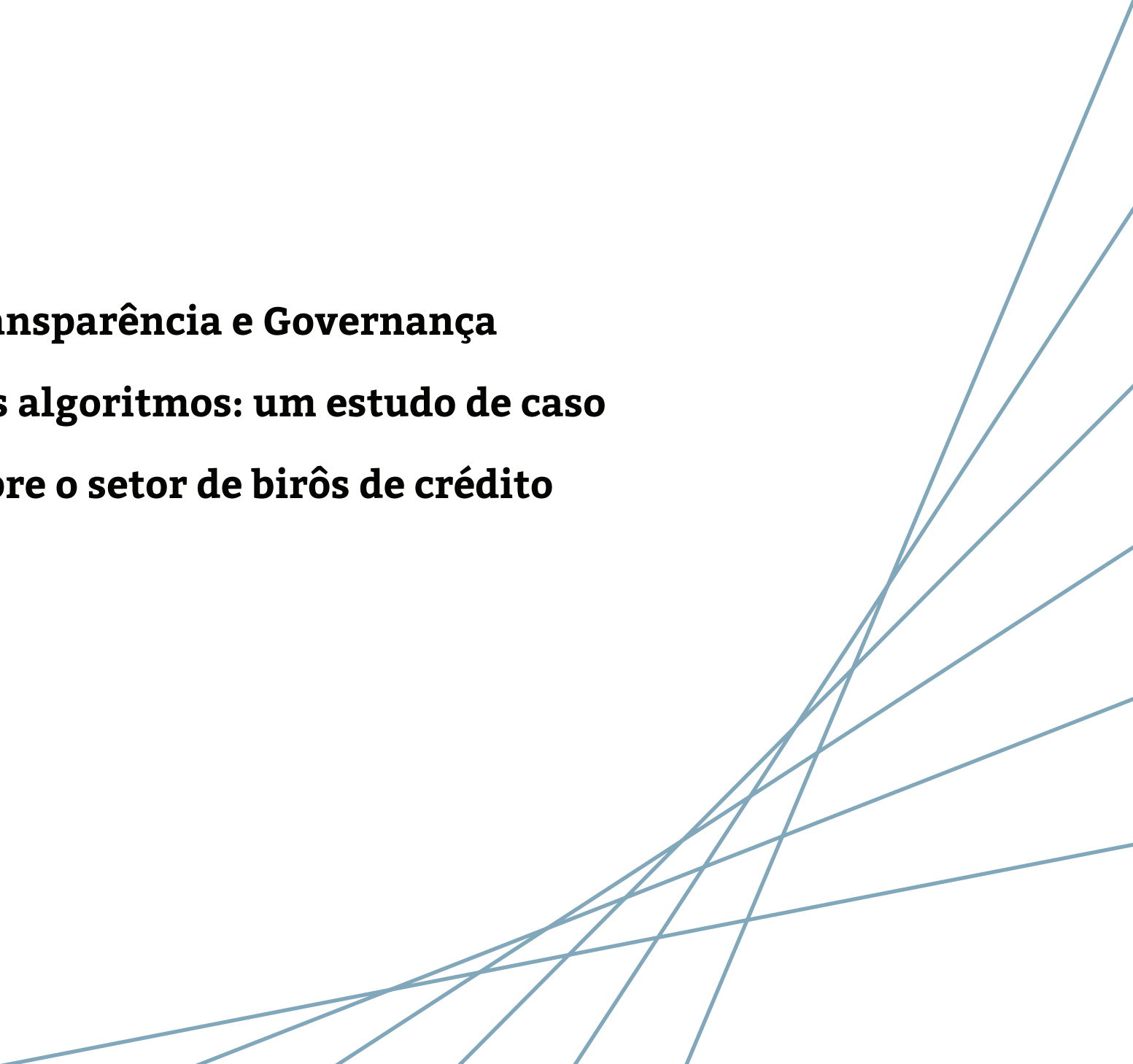


**Transparência e Governança  
nos algoritmos: um estudo de caso  
sobre o setor de birôs de crédito**



# Sumário Executivo

O objetivo deste estudo é analisar a utilização (coleta, tratamento e acesso) de dados pessoais por *bureaux* de crédito<sup>1</sup> (“BdC”), com foco nos eventuais impactos que tal uso têm para grupos vulneráveis, tendo por fim último identificar melhores práticas voltadas a tornar a relação entre BdC e titulares de dados pessoais mais transparente e informada.

Para alcançar esse objetivo o presente estudo se divide em três partes:

Na primeira, abordamos de que forma BdC lidam com conceitos como avaliação de risco e como o uso de dados pessoais podem acarretar condutas discriminatórias na concessão de crédito.

A seguir, apresentamos panorama legislativo brasileiro relativo à proteção de dados

pessoais. Considerando que o Brasil não conta com norma legal específica sobre o tema, o segundo capítulo deste estudo abrangerá normas como o Código de Defesa do Consumidor (“CDC”), a Lei do Cadastro Positivo, a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet, entre outras.

Finalmente, no terceiro e último capítulo, indicamos as conclusões a que chegamos a partir da análise de mecanismos de acesso de dados oferecidos por *bureaux* de informação. Foram examinados os termos de uso dos seguintes serviços: Serasa-Experian (em relação ao serviço *Mosaic*) e Boa Vista. Ainda neste capítulo final, tecemos considerações acerca de melhores práticas a serem adotadas por serviços ofertados por *bureaux* de informação no que diz respeito à coleta, ao tratamento e ao acesso de dados de terceiros.

A fim de obter o melhor resultado em nossa pesquisa, a metodologia utilizada consistiu em análise dos contratos de prestação de serviços desses BdC disponíveis tanto em suas páginas de internet quanto em páginas

---

<sup>1</sup> *Bureaux* (ou birô, no vernáculo) de crédito tradicionalmente é uma instituição privada, com ou sem fins lucrativos, que administra bases de dados sobre a situação dos tomadores de crédito do sistema financeiro (v. Simeon Djankova, Caralee McLiesha, Andrei Shleifer. Private credit in 129 countries. *Journal of Financial Economics* 84 [2007]. P. 305). Hoje, entretanto, essas entidades ampliaram seu escopo, atuando não apenas no setor financeiro, mas em diversos setores, inclusive provendo informações para o setor público, transformando-se em verdadeiros *bureaux* de informação, como explicaremos melhor no próximo tópico. As traduções constantes do texto foram realizadas pelos autores deste relatório.

de entes públicos com os quais mantém contrato e que disponibilizam tais informações por força da LAI. Também analisamos informações sobre os produtos disponibilizados e as informações tratadas por tais BdC encontradas em suas páginas de internet. A escolha desses 02 (dois) serviços se deu em razão de serem os maiores BdC em operação no Brasil e os únicos integrantes da Associação Nacional dos Birôs de Crédito<sup>2</sup>. Ademais, a terceira instituição considerada como BdC seria o SPC, entretanto este está ligado ao setor varejista, sendo, inclusive, vinculada diretamente às Câmaras de Dirigentes Lojistas, não fazendo parte Associação Nacional dos Birôs de Crédito. Em sua página de Facebook o SPC Brasil se descreve como “uma empresa de tecnologia vinculada à CNDL para processar e armazenar todas as operações de crédito realizadas pelas empresas”, não se enquadrando, portanto, no conceito de birô de crédito o que, somado ao fato de não integrar a Associação Nacional dos Birôs de Crédito, nos fez não considera-lo neste estudo<sup>3</sup>.

---

2 <http://www.anbc.org.br/#empresasparceiras>

3 <https://www.facebook.com/SPCBrasilCNDL/posts/945691855461435>. Acesso em 30.01.2017.

# 1. Crédito e discriminação

## 1 - Análise de risco, bureaux de crédito (“BdC”) e discriminação positiva/negativa

Os BdC baseiam suas atividades em um mecanismo de análise de risco<sup>4</sup>. Esse mecanismo costuma funcionar da seguinte maneira: em um primeiro momento, o BdC verifica a probabilidade que uma pessoa tem de não pagar uma dívida<sup>5</sup>. Depois disso, em um segundo momento, essa pessoa é alocada em uma certa categoria de risco de modo a fundamentar as decisões que dizem respeito ao crédito a ser concedido<sup>6</sup>, à taxa de juros<sup>7</sup> a ser estabelecida e até mesmo à eventual conclusão do contrato<sup>8</sup>.

---

4 LIEDTKE, Patrick M. What’s Insurance to a Modern Economy. *The Geneva Papers*, 2007, 32; p. 214.

5 JENTZSCH, Nicola. *Financial Privacy: An International Comparison of Credit Reporting Systems*. Springer: 2007; p. 274.

6 BAKER, Tom. *Containing the Promise of Insurance: Adverse Selection and Risk Classification*. University of Connecticut School of Law Articles Working Paper Series. 2001.

7 International Finance Corporation (IFC) - World Bank Group. *Credit bureau knowledge guide*. Disponível em <http://www.ifc.org/wps/wcm/connect/2867f3804958602ba222b719583b6d16/FI-CB-KnowledgeGuide-E.pdf?MOD=AJPERES&CACHEID=-2867f3804958602ba222b719583b6d16>. Acesso em 13.11.16.

8 VIOLA DE AZEVEDO CUNHA, Mario. *Privacidade e Seguro: a coleta e utilização de dados pessoais nos ramos de pessoas e de saúde*. *Cadernos de Seguro – Teses n. 33*. Funenseg: Rio de Janeiro, 2009; p. 22.

Para que essa análise possa ser realizada, esses atores procuram obter o máximo de informações possíveis sobre seus potenciais clientes<sup>9</sup>; informações concernentes aos seus hábitos, à sua condição econômica<sup>10</sup> e, eventualmente, sobre quesitos que possam não estar diretamente ligados à capacidade creditícia, como informações sobre a sua saúde, seus dados genéticos, dentre muitos outros<sup>11</sup>.

Os BdC surgiram para explorar uma nova atividade - que já era realizada, com variados graus de sofisticação, pelo comércio e por instituições financeiras antes do seu surgimento.

A necessidade crescente do comércio em ter informações a respeito de consumidores que demandam crédito para então tomarem decisões informadas a respeito da sua con-

---

9 MEYER, Roberta B. MEYER, Roberta B. The insurer perspective. In *Genetics and life insurance - Medical underwriting and social policy*. Mark. A. Rothstein. MIT Press: 2004; p. 29.

10 International Finance Corporation (IFC) - World Bank Group. Op. cit.; p. 12

11 International Finance Corporation (IFC) - World Bank Group. Op. cit.; p. 7.

cessão fez com que fossem criadas no Brasil as Câmaras dos Dirigentes Lojistas (“CDLs”). Essas Câmaras, juntamente com outras associações comerciais, criaram as primeiras bases de dados unificadas a respeito de informações sobre inadimplência, bases essas que eram alimentadas e podiam ser consultadas por seus associados. A partir da primeira CDL, criada em Porto Alegre em 1951, congêneres surgiram no Rio de Janeiro, São Paulo e em outras unidades da federação, dotando diversas cidades dos serviços de proteção ao crédito visando a uma maior segurança na concessão de crédito para o comércio.

Esses serviços tinham, no entanto, natureza marcadamente local. Para obter maior grau de cobertura e eficiência, estes serviços locais foram sendo paulatinamente substituídos por outros de abrangência nacional e com bases de dados unificadas, como praticado hoje por Serasa, Boa Vista e SPC Brasil. Tais serviços se valem de informações provenientes de fontes públicas (por exemplo, protestos ou ações de execução) e privadas (de seus próprios bancos de dados) para integrar o rol de serviços que oferecem a seus clientes.

Hoje a atividade desses BdC não se res-

tringe, muitas vezes, à mera análise de crédito. Alguns BdC passaram, com o tempo, a oferecer outros tipos de serviços que eram voltados a outras finalidades: *marketing*, prospecção de mercado e outros. Tornaram-se assim verdadeiros *bureaux* de informação, chegando até a atual figura dos *data brokers* - entidades que procuram extrair para os seus clientes conteúdo e utilidade da gama de informações às quais têm acesso, o que inclui, muitas vezes, transacionar a própria informação.

Os clientes desses *bureaux* são os seus consulentes. No caso da análise de crédito, esses consulentes podem ser comerciantes ou instituições financeiras que precisam tomar determinada decisão a respeito da concessão de crédito ou eventualmente algum outro serviço financeiro a uma pessoa. Uma vez realizada a operação de crédito, o cedente do crédito (que foi o consulente do bureau) torna-se credor do titular dos dados (que passa a ser o seu respectivo devedor).

Os dados que são levados em consideração pelos *bureaux* são de pessoas, naturais ou jurídicas. Essas pessoas serão, neste estudo, referenciadas como os titulares dos dados.

Estes titulares, dado o escopo do estudo, serão, salvo alguma referência específica, pessoas naturais, visto que as considerações e conclusões a serem tomadas dizem respeito àquelas que acometem as pessoas naturais.

Neste estudo utilizaremos “titular de dados”, “cliente em potencial”, “cliente” e “consumidor” para tratar da pessoa a respeito da qual se referem as informações que estão sendo coletadas e tratadas. Apenas optamos por utilizar essas nomenclaturas distintas para destacar o momento contratual em que se encontram, antes da tomada de crédito ou durante esta relação ou quando a lei que se analisa faz uso de uma nomenclatura específica, como no caso do Código de Proteção e Defesa do Consumidor (“CDC”), que utiliza “consumidor”, ou do projeto de lei geral de proteção de dados pessoais em tramitação na Câmara dos Deputados, que utiliza “titular de dados”.

## **2. Generalização e discriminação**

As técnicas de análise de perfis dos BdC funcionam com base em generalizações. A generalização ocorre quando um grupo inteiro é tratado do mesmo modo por conta do

comportamento de sua minoria<sup>12</sup>.

Os BdC baseiam boa parte de suas decisões em generalizações. Isso ocorre pois quando projetam um perfil de risco (analisando um grupo de clientes), ou até mesmo quando analisam riscos individuais (cliente a cliente), fazem-no com base em comportamentos anteriores de outras pessoas que tenham características semelhantes, levando-se em conta dados como idade, gênero, etnia ou até localização, como no uso do CEP da residência<sup>13</sup>.

Por um lado, essa generalização é necessária. Ante a assimetria de informações entre clientes e fornecedores de crédito, é necessário, a quem empresta, saber mais sobre quem pode vir a tomar empréstimo. Se assim não fosse, haveria um estímulo a mais clientes com alto risco de inadimplemento.

Esse tipo de generalização pode, contudo, criar distorções sobre indivíduos ou grupos de indivíduos, particularmente entre aqueles em situação vulnerável, ou entre aqueles que se comportam de maneira desviante.

---

<sup>12</sup> SCHAUER, Frederick. Profiles, Probabilities and Stereotypes. Cambridge, Massachusetts: Belknap Press of Harvard University Press, 2003. P. 3.

<sup>13</sup> Ibid; p. 4.

Por exemplo, “quando um adolescente tira a carteira de motorista, o valor do seguro de sua família vai aumentar drasticamente, mesmo que ele seja extremamente cuidadoso e que muito dificilmente acabe envolvido em um acidente, em comparação com outros adultos”<sup>14</sup>.

Ao generalizar o comportamento de jovens motoristas, pode-se definir de modo abstrato que jovens são mais associados a danos com veículos do que motoristas mais experientes. A partir desse exemplo, percebe-se que o grande problema da generalização é a discriminação que pode ocasionar, uma vez que indivíduos que fazem parte de um grupo alvo não possuem a oportunidade de demonstrar que as generalizações feitas sobre o grupo a que pertencem não se aplicam a eles e que isso pode lhes causar sérias consequências<sup>15</sup>.

Embora “todos os seres humanos - adolescentes que dirigem, ex-presidiários, vendedores de carros usados, escoceses, contadores, e todo mundo - mereçam ser tratados como indivíduos e não simplesmente como membros de um grupo”<sup>16</sup>, há que se ponderar

que, todavia, dependendo da sua utilização, generalizações são necessárias para análise de crédito. Se o preço do seguro for o mesmo para quem causa mais acidentes e para os que não causam, uma outra forma de desequilíbrio pode surgir: a subida de preço do seguro para todos. O mesmo raciocínio vale para a concessão de crédito.

### **3. Seleção adversa**

A coleta e tratamento de informações pessoais<sup>17</sup> têm como finalidade reduzir a assimetria de informações entre fornecedores e clientes. Na visão dos fornecedores, os consumidores conhecem sua própria situação financeira e, com isso, sabem o risco que representam. Já o fornecedor de crédito não. A coleta e tratamento de informações pessoais dos clientes/consumidores visa equilibrar essa assimetria.

Contudo, há um risco de novo desequilíbrio ao fazer essa operação. Quando as informações pessoais do cliente são por este fornecidas, de forma explícita, em teoria o fornecedor poderia atingir o mesmo grau de

---

14 Ibid. p. 4.

15 Op. cit.; p. 50.

16 SCHAUER, Frederick. Op. cit.; p. 19.

17 O inciso V do art. 4º da Lei nº 12.527/11 define como tratamento da informação o “conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação”.

conhecimento que o cliente. Contudo, existem situações em que o fornecedor pode buscar informações por si só (ou seja, situação em que o potencial cliente não disponibiliza a informação para o fornecedor), ou quando uma informação específica, mesmo que fornecida, não pode ser usada na análise de risco por conta de previsões legais, como no caso da Lei do Cadastro Positivo, que veda a utilização de informações sensíveis ou excessivas<sup>18</sup>.

Há, portanto, casos em que a assimetria de informação (de coleta ou tratamento) entre o titular dos dados e o fornecedor de crédito pode ser inevitável. Nessas situações, pode ocorrer o processo de seleção adversa<sup>19</sup>, e com isso os BdC desempenham papel fundamental, pois eles conseguem reunir informações de outras fontes que não exclusivamente o titular dos dados.

---

18 Lei n. 12.414, de 9 de junho de 2011.

Art. 3º (...)

(...)

§ 3º Ficam proibidas as anotações de:

I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e

II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

19 BAKER, Tom. Op. cit.; p. 2.

No caso da concessão de crédito, “a seleção adversa acontece quando o credor não tem ciência de algumas informações de desempenho do devedor”, ou seja, a seleção adversa é uma consequência indesejada da falta de conhecimento de informações a respeito do desempenho do futuro cliente com relação à sua habilidade de pagar dívidas. De fato, há casos em que a assimetria entre potencial cliente e fornecedor de crédito é uma realidade. Nesses casos, o BdC presta um serviço importante ao fornecedor de crédito, a fim de completar “a informação fornecida diretamente por quem está solicitando crédito - o que pode ou não refletir, de maneira fiel, o risco de crédito ou habilidade de pagar um empréstimo”<sup>20</sup>, reduzindo, portanto, a possibilidade de ocorrência do fenômeno da seleção adversa, que seria a entrada de um maior número de clientes com um potencial elevado de inadimplência.

A discussão sobre seleção adversa não é simples, uma vez que lida não só com aspectos econômicos, mas também com outras questões relevantes, como o potencial risco de que ocorra discriminação na concessão

---

20 Report of the Expert Group on Credit Histories. May 2009; p. 13.



de crédito. Um exemplo de seleção adversa aconteceu nos EUA, quando seguradoras decidiram se valer de informações relativas a vítimas de violência doméstica. Nesse caso, a busca por se evitar a seleção adversa acabou por ocasionar uma discriminação negativa, ao propor que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez, o que acabou por motivar a ação de diversos estados americanos no sentido de adotar leis que vedassem tal prática<sup>21</sup>:

(...) algumas seguradoras estavam se recusando a vender seguros de vida, saúde e invalidez para mulheres vítimas de violência, com base no argumento de que elas representavam um risco inaceitavelmente alto. (Hellman 1997) Em resposta a esse fato, alguns estados começaram a aprovar propostas legislativas que proibiam as seguradoras de exercer tal discriminação contra as mulheres vítimas de violência doméstica, e com o mesmo teor também foram apresentadas propostas no Congresso Nacional Americano. A defesa das seguradoras, apresentada com o intuito de barrar tais propostas, baseava-se no argumento de que a exclusão da mulher da compra de seguros era, na verdade, “justo”. Segundo eles, a probabilidade dessas mulheres reivindicarem seguros de vida, saúde e incapacidade no futuro era maior do que a de outras

21 BAKER, Tom. Op. cit.; p. 12.

pessoas, tendo em vista a existência de um histórico de abusos, que mulheres com similar perfil que não fossem vítimas de abuso doméstico não teriam. Esse risco inaceitável foi usado como justificativa para excluí-las da compra de seguros: assim como outros riscos inaceitáveis, elas foram excluídas, na medida em que representavam um.

Outro exemplo ocorrido nos EUA demonstra os riscos por trás do uso autorizado de informações sensíveis em transações comerciais<sup>22</sup>:

(...) no que se refere à privacidade médica, quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados. Há pouca ou nenhuma contribuição para o bem comum nessas intervenções, mas sim uma alta intromissão, uma das mais altas que se pode imaginar.

Por outro lado, a ausência de uma correta seleção dos riscos pode levar, por exemplo, a crises econômicas<sup>23</sup>:

Existem vários canais, como o aumento das taxas

---

22 ETZIONI, Amitai. A Communitarian Approach: A Viewpoint on the Study of the Legal and Ethical Policy Considerations Raised by DNA Tests and Databases. *Journal of Law, Medicine & Ethics*, V. 34 (2006): 217.

23 KIRABAEVA, Korlai. Adverse Selection and Financial Crises. *Bank of Canada Review*, Winter 2010–2011. Disponível em <http://www.bankofcanada.ca/wp-content/uploads/2011/02/kirabaeva.pdf>. Acesso em 13.11.16.

de juros, a deterioração do balanço das instituições financeiras e o desfasamento entre prazos de vencimentos que podem agravar os problemas causados pela seleção adversa e levar à instabilidade financeira. Na presença de informações assimétricas, um pequeno aumento na taxa de juros pode levar a uma grande redução nos empréstimos. Uma taxa de juros mais elevada aumenta a probabilidade de que os mutuários de alta qualidade se retirem do mercado, agravando o problema da seleção adversa. Como resultado, a qualidade média dos tomadores cai, o que por sua vez aumenta a taxa de juros ainda mais. Se a seleção adversa for suficientemente grave, o mercado de crédito pode entrar em colapso (Mishkin 1990).

Vê-se, portanto, que a coleta e utilização de informações pessoais é de fundamental importância para se evitar a seleção adversa e assegurar a saúde dos mercados financeiros. Porém, por outro lado, há limites para tal coleta e utilização, a fim de evitar que ela dê ensejo a hipóteses de discriminação negativa, como vimos nos exemplos ocorridos nos EUA. Nos próximos capítulos deste estudo tentamos identificar os limites trazidos tanto pela legislação quanto pela jurisprudência nacionais, notadamente do Superior Tribunal de Justiça, para a coleta e tratamento de dados por parte dos BdC.

#### 4. Grupos vulneráveis

Em primeiro lugar, é necessário defini-los. Trataremos como grupos vulneráveis o conjunto de pessoas que, por motivos distintos, não tem o mesmo acesso a bens e serviços ou ao pleno exercício de direitos civis como outros setores da sociedade. Exemplos de grupos vulneráveis são idosos, mulheres, deficientes e população de baixa renda<sup>24</sup>.

Conforme discutido no tópico anterior, generalizações podem gerar distorções que algumas vezes podem afetar de maneira desproporcional alguns grupos, em particular aqueles em situação de vulnerabilidade. Por exemplo, exigir que um homossexual pague mais por um seguro de saúde por pertencer a um grupo que “possui, estatisticamente, maior probabilidade de contrair o vírus do HIV”<sup>25</sup>, representaria, a nosso ver, um tipo de generalização que gera uma distorção desproporcional.

---

24 Centro Brasileiro de Análise e Planejamento-Cebrap, do Serviço Social do Comércio-SESC e da Secretaria Municipal de Assistência Social de São Paulo, SAS-PMSP. Mapa da Vulnerabilidade Social da População da Cidade de São Paulo. 2004. Disponível em [http://www.fflch.usp.br/centrodametropole/upload/arquivos/Mapa\\_da\\_Vulnerabilidade\\_social\\_da\\_pop\\_da\\_cidade\\_de\\_Sao\\_Paulo\\_2004.pdf](http://www.fflch.usp.br/centrodametropole/upload/arquivos/Mapa_da_Vulnerabilidade_social_da_pop_da_cidade_de_Sao_Paulo_2004.pdf). Acesso em 13.11.16. Vide, também, Fundo Monetário Internacional. O papel do FMI para ajudar a proteger os mais vulneráveis na crise mundial. Disponível em <https://www.imf.org/external/lang/portuguese/np/exr/facts/protectp.pdf>. Acesso em 13.11.16.

25 Ibid; p. 5.

Outro exemplo, dessa vez relacionado a gênero e etnia, é o de mulheres judias da Europa Oriental (Ashkenazi). Em termos médicos, esse grupo tem risco mais elevado de desenvolver câncer de mama ou ovário, tendo em vista que a mutação do gene BRCA, que aumenta o risco de câncer de mama, é mais frequente nesse grupo em comparação com os demais<sup>26</sup>. Se tal argumento fosse utilizado para fins de análise de risco, mulheres pertencentes a esse grupo provavelmente teriam dificuldade de conseguir empréstimos de longa duração<sup>27</sup> (p.ex. financiamentos de imóveis), ou teriam que contratar seguros de vida para garantir o pagamento dos empréstimos em caso de falecimento (e esses seguros provavelmente seriam muito caros diante do risco aumentado de óbito), o que acabaria por discriminar o grupo como um todo, diminuindo severamente a possibilidade de adquirirem um imóvel financiado.

É importante destacar que, com relação a informações sobre orientação sexual, dados genéticos, entre outros, a já citada lei do ca-

---

26 UK National Cancer Institute. BRCA1 and BRCA2: Cancer Risk and Genetic Testing. Disponível em <http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA>. Accessed 8 March 2010.

27 LENOX, Bryce A. Genetic Discrimination in Insurance and Employment: Spoiled Fruits of the Human Genome Project. *University of Dayton Law Review*. Vol. 23. 1997-1998; p. 194; 196-197.

astro positivo veda de forma expressa sua utilização para fins de formação e consulta a bancos de dados com informações de adimplemento. Tal vedação foi ampliada pelo Superior Tribunal de Justiça para outros bancos de dados relacionados a crédito, conforme analisaremos no próximo capítulo.

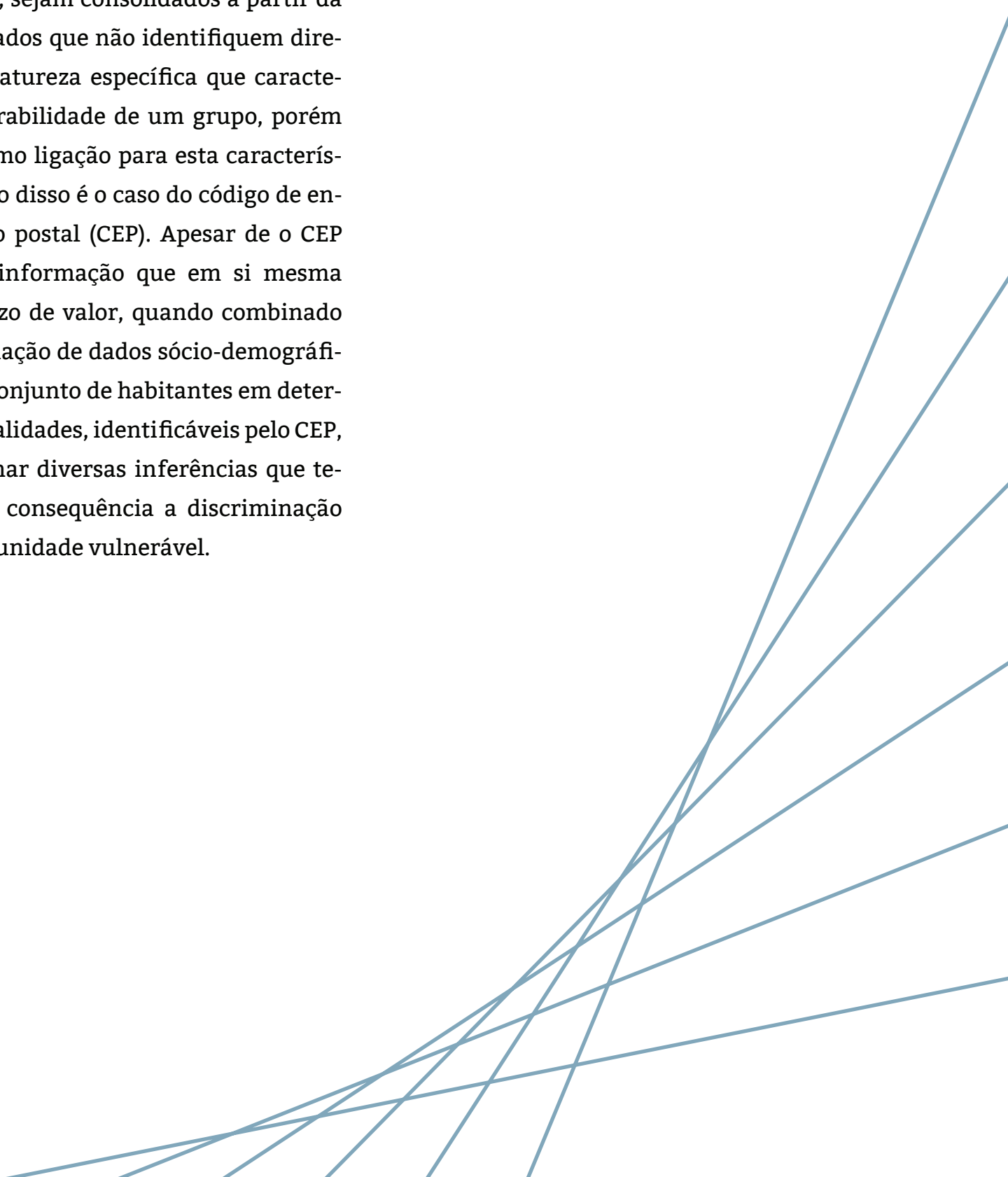
No Brasil, a discriminação para fins de concessão de crédito “com base em técnica estatística de análise discriminante para distinguir bons e maus empréstimos, atribuindo-se pesos diferentes para cada uma das variáveis escolhidas para execução de seu método” teve sua licitude reconhecida pelo Superior Tribunal de Justiça<sup>28</sup>. Entretanto, em momento algum referida decisão tratou de segmentação da sociedade ou de enquadramento de pessoas e nichos específicos da população, como aqueles apresentados pelo nosso estudo de caso.

A verificação da discriminação de grupos considerados vulneráveis demanda análise não meramente da amostragem dos dados utilizados em um sistema decisional, mas, também, dos seus critérios. É comum que

---

28 Resp nº 1.419.697 - RS. Rel. Min. Paulo de Tarso Sanseverino. 2ª Seção. Julg. em 12.11.2014.

determinados *outputs* que possam ser considerados negativamente discriminatórios, por exemplo, sejam consolidados a partir da análise de dados que não identifiquem diretamente a natureza específica que caracteriza a vulnerabilidade de um grupo, porém funcione como ligação para esta característica. Exemplo disso é o caso do código de endereçamento postal (CEP). Apesar de o CEP não conter informação que em si mesma implique juízo de valor, quando combinado com a apreciação de dados sócio-demográficos sobre o conjunto de habitantes em determinadas localidades, identificáveis pelo CEP, pode ocasionar diversas inferências que tenham como consequência a discriminação de uma comunidade vulnerável.



## 2. Limites ao tratamento de dados para concessão de crédito

### 1. Da normativa aplicável ao tratamento de dados pessoais

O Brasil, ao contrário de cerca de 110 outros países, não possui lei geral de proteção de dados pessoais. Em nosso ordenamento jurídico, o tema é disciplinado por dispositivos constitucionais gerais e algumas normas setoriais.

A Constituição Federal brasileira reconhece, em seu art. 5º, X, a vida privada, a intimidade, a honra e a imagem como direitos fundamentais. Esse mesmo artigo 5º garante a proteção de outros aspectos da vida privada (art. 5º, XI, XII, XIV). Além disso, o inciso LXXII criou uma nova ação constitucional, o *habeas data*.

O Código Civil brasileiro, por sua vez, adotou disciplina similar à da Constituição Federal, incluindo em seu artigo 21 a privacidade como um direito da personalidade e estendeu, no que couber, a proteção dos direi-

tos da personalidade às pessoas jurídicas<sup>29</sup>.

As únicas normas que tratam especificamente do tratamento de dados pessoais, além do *habeas data*, e que, por isso, merecerão atenção especial neste estudo, são o CDC<sup>30</sup>, a Lei do Cadastro Positivo<sup>31</sup>, a Lei de Acesso à Informação (LAI)<sup>32</sup> e o Marco Civil da Internet, este último com relação aos dados coletados *online*.

O CDC regula em seus artigos 43 e 44 a manutenção de bases de dados e arquivos de dados<sup>33</sup>, estabelecendo uma série de direitos para os consumidores, e, por isso, é de fundamental importância para o objeto deste estudo, já que tem aplicação direta à atividade desenvolvida pelos *bureaux* de crédito.

---

<sup>29</sup> Nesse sentido é o art. 52 do Código Civil.

<sup>30</sup> A Lei Complementar n.º 105/2001 regula a troca de informações negativas entre as instituições financeiras e o Banco Central do Brasil.

<sup>31</sup> Lei n.º 12.414, de 2011.

<sup>32</sup> Lei n.º 12.527, de 2011.

<sup>33</sup> O CDC não traz uma definição de dados pessoais, porém se aplica tanto a pessoas físicas quanto jurídicas. Vide artigo 2º.

O CDC reconhece, em primeiro lugar, o direito do consumidor de ser informado pelo responsável pelo banco de dados<sup>34</sup> de que seus dados estão sendo tratados<sup>35</sup>. Essa comunicação deve ser efetuada antes da informação ser disponibilizada para consulta<sup>36</sup>, para que o consumidor possa exercer seu direito de acesso e correção e os demais direitos assegurados pelo artigo 43<sup>37</sup>. Como consequência, caso o responsável pelo tratamento de dados não comunique ao consumidor num prazo razoável o registro de seus dados, o consumidor poderá pleitear indenização pelos danos causados.

O CDC também reconhece os direitos de acesso<sup>38</sup> e correção<sup>39</sup>, dando aos consumidores a possibilidade de acessar qualquer infor-

34 Apesar de o CDC estabelecer responsabilidade solidária para o gestor da base de dados e o fornecedor de bens ou serviços que incluiu os dados do consumidor nos cadastros de proteção ao crédito, o Superior Tribunal de Justiça pacificou entendimento de que a responsabilidade é apenas do fornecedor de produtos ou serviços (Súmula n.º 359 do STJ).

35 Art. 43, §2º.

36 Não há previsão legal do momento em que a comunicação deverá ser feita, porém é consenso tanto na doutrina quanto na jurisprudência no sentido de que essa comunicação deve ser feita de forma a possibilitar que o consumidor possa exercer seus direitos antes de o dado estar disponível para consulta. Vale salientar que existe uma lei do Estado do Rio de Janeiro que estabelece o prazo de dez dias como razoável (Lei n.º 3.244, 6 de setembro de 1999). Disponível em <http://www.alerj.rj.gov.br/processo2.htm>.

37 BENJAMIN, Antonio Herman Vasconcelos et al. Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto. 9.ed. Forense, São Paulo, 2007; p. 405.

38 Ibid; p. 413.

39 Ibid; p. 416.

mação armazenada e de corrigi-la caso haja inexatidão (art. 43, *caput* e §3º, do CDC)<sup>40</sup>. Tais direitos encontram-se nas principais leis de proteção de dados do mundo<sup>41</sup>. Nos casos em que o responsável pelo tratamento de dados não permitir que os consumidores exerçam os direitos estabelecidos neste Código, estes poderão pleitear a compensação de eventuais danos e poderão exercer seus direitos por meio das vias judiciais ordinárias (conforme art. 43, §4º, do CDC) ou se valer da ação de *habeas data*<sup>42</sup>. O artigo 43, em seus §§ 1º e 5º, do CDC, ainda estabelece limite temporal para a manutenção de qualquer informação negativa sobre o consumidor em seus cadastros, que não poderá ser armazenada por mais de cinco anos ou após a consumação da prescrição da ação de cobrança do respectivo débito. Esses direitos também se aplicam a outras hipóteses de tratamento de dados pessoais de consumidores e não apenas às que se referem a cadastros protetivos de crédito. Ne-se sentido são as palavras do Ministro Antônio

40 O direito de cancelamento do dado está implícito, visto que caso haja alguma informação incorreta ou quando o prazo de armazenamento tenha expirado, o consumidor poderá solicitar a exclusão de tal informação.

41 Vide, a título de exemplo, a lei francesa de proteção de dados pessoais, Loi n.º 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponível em <https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee>. Acesso em 13.11.16.

42 O procedimento do *Habeas data* foi regulado pela Lei Federal n.º 9.507, 12 de novembro de 1997. Disponível em [http://www.planalto.gov.br/ccivil\\_03/Leis/L9507.htm](http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm).

Herman de Vasconcelos Benjamin<sup>43</sup>:

(...) Ao consumidor é assegurado acesso às informações arquivadas, quaisquer que sejam elas ('dados pessoais e de consumo') e qualquer que seja o local onde se encontrem armazenadas ('cadastros, fichas, registros e dados'). É indiferente, sejam os dados arquivados pelo próprio fornecedor (nos termos do conceito do art. 3º) ou, diferentemente, por entidade prestadora de serviço a terceiros, como Serviços de Proteção ao Crédito – SPCs, SERASA e congêneres. Em outras palavras, a raison d'être da lei brasileira é, pois, conferir ao consumidor acesso amplo e irrestrito às informações a seu respeito, colhidas de outra fonte que não ele próprio, estejam elas onde estiverem: em organismos privados ou públicos, em cadastros internos das empresas ou em banco de dados prestador de serviços a terceiros (...). Ressalte-se que o caput do art. 43 não limita o direito de acesso aos SPCs. Ao revés, é até prolixo ao mencionar 'cadastros', 'fichas', 'registros', 'dados pessoais' e 'dados de consumo'. (Grifo nosso).

No mesmo sentido, sustenta Luiz Rizzato Nunes, afirmando que “muito embora a ênfase e a discussão em torno das regras instituídas no art. 43 recaiam nos chamados cadastros de inadimplentes dos serviços de proteção ao crédito, a norma incide em sis-

43 BENJAMIN, Antônio Herman de Vasconcelos et al. Código Brasileiro de Defesa do Consumidor: comentado. 7. ed. Rio de Janeiro: Forense Universitária, 2001; p. 405.

temas de informação mais ampla”<sup>44</sup>. Essa interpretação foi seguida recentemente pelo Superior Tribunal de Justiça, em voto da lavra do Ministro Paulo de Tarso Sanseverino<sup>45</sup>:

Ressalte-se que o CDC não restringiu sua regulamentação aos cadastros ou bancos de dados de informações negativas (arquivos negativos), embora tenham se tornado os mais comuns no mercado até poucos anos atrás (SPC, Serasa, etc).

Destaque-se ainda que o mesmo Superior Tribunal de Justiça consolidou entendimento no sentido de que “[r]estrições ao crédito derivadas de informações constantes em bancos de dados públicos, como os pertencentes a cartórios de protesto de títulos e de distribuição judicial, por serem de notoriedade pública, afastam o dever de notificação por parte do órgão de proteção ao crédito”<sup>46</sup>. Entretanto, nos bancos de dados de consulta restrita, como é o caso do cadastro de emitentes de cheques sem fundo mantido pelo Banco Central, permanece o dever de notificação por par-

44 Grifo nosso. NUNES, Luiz A. Rizzato. Comentários ao Código de Defesa do Consumidor: Direito Material (arts. 1 ao 54). São Paulo: Saraiva, 2000, p. 514.

45 Superior Tribunal de Justiça. Recurso Especial nº 1.419.697 – RJ. Rel. Min. Paulo de Tarso Sanseverino. Julg. em 12.11.2014.

46 Superior Tribunal de Justiça. 4ª Turma. RECURSO ESPECIAL Nº 1.033.274 – MS. Rel. Min. Luis Felipe Salomão. Julg. em 06.08.2013.

te do mantenedor da base de dados que incluir em seu banco de dados informação oriunda de banco de dados de consulta restrita, quando essa informação tiver caráter negativo <sup>47</sup>

Cabe salientar que o princípio da finalidade, um dos princípios basilares das legislações sobre a proteção de dados pessoais, mesmo antes de ser expressamente reconhecido pela legislação brasileira – com a Lei do Cadastro Positivo e, posteriormente, com o Marco Civil da Internet – foi aplicado em um célebre julgamento do Superior Tribunal de Justiça, relatado pelo então Ministro Ruy Rosado de Aguiar, como limite para o tratamento de dados realizado por cadastros de proteção ao crédito<sup>48</sup>:

2. O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento. É evidente o benefício que dele decorre em favor da agilidade e da segurança das operações comerciais, assim como não se pode negar ao vendedor

47 Superior Tribunal de Justiça. 4ª Turma. RECURSO ESPECIAL Nº 1.033.274 – MS. Rel. Min. Luis Felipe Salomão. Julg. em 06.08.2013.

48 Apud DONEDA, Danilo; VIOLA DE AZEVEDO CUNHA. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. Revista Brasileira de Risco e Seguro. v. 5, n. 10, p. 85-102, out. 2009/mar. 2010; p. 99.

o direito de informar-se sobre o crédito do seu cliente na praça, e de repartir com os demais os dados que sobre ele dispõe. Essa atividade, porém, em razão da sua própria importância social e dos graves efeitos dela decorrentes – pois até para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização de sua finalidade, não se transforme em causa e ocasião de dano social maior do que o bem visado. (Grifo nosso).

Por outro lado, de acordo com o CDC, a criação de uma base de dados que contenha dados pessoais (cuja definição não se encontra no CDC) não está sujeita a autorização, seja do consumidor ou de qualquer autoridade pública<sup>49</sup>.

Outra lei que trata da proteção de dados pessoais é a Lei do Cadastro Positivo (Lei 12.414/2011), que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Dentro das disposições sobre proteção de dados pessoais contidas nessa lei estão a definição de dados sensíveis e alguns direitos

49 Artigo 43, parágrafo 2º, do CDC.



dos titulares dos dados. Vale ressaltar que o Superior Tribunal de Justiça, em julgado recente, decidiu pela legalidade de serviço que “consiste em compilar dados cadastrais disponibilizados publicamente com cadastros de inadimplência para que o comerciante decida se concede ou não crédito ao consumidor”, o chamado *Credit Scoring*. Assim, deixou claro que, apesar de tal atividade não se enquadrar na definição de “cadastro positivo”, deveriam os fornecedores desse serviço observar as disposições contidas tanto no CDC quanto na Lei do Cadastro Positivo, “sob pena de caracterização de abuso de direito com eventual ocorrência de danos morais”, dispensado o dever de obtenção do consentimento do titular do dado nessas hipóteses, por não se tratar de cadastro positivo<sup>50</sup>. Destaque-se que neste mesmo julgamento o Superior Tribunal de Justiça decidiu que “[n]a avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei 12.414/2011”, reconhecendo aos consumidores o direito de obter

---

50 Superior Tribunal de Justiça. Recurso Especial nº 1.419.697 – RJ. Rel. Min. Paulo de Tarso Sanseverino. Julg. em 12.11.2014.

esclarecimentos “acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas”.

A Lei de Acesso à Informação - LAI (Lei 12.527/2011) tem como diretrizes a observância da publicidade como preceito geral e do sigilo como exceção; a divulgação de informações de interesse público, independentemente de solicitações; a utilização de meios de comunicação viabilizados pela tecnologia da informação; o fomento ao desenvolvimento da cultura de transparência na administração pública e o desenvolvimento do controle social da administração pública.<sup>51</sup> Esta lei reconhece a proteção de dados pessoais que estejam em mãos do poder público como uma possível barreira ao acesso a informações pessoais quando esse acesso puder representar risco para a intimidade, vida privada, honra, imagem ou outras liberdades e direitos individuais, na forma do que estabelece seu artigo 31. A LAI, em seu art. 4o, IV, define informação pessoal como “aquela relacionada à pessoa natural identificada ou identificável”.

---

51 O inciso III do art. 1o do Decreto no Decreto nº 8.777, de 12 de maio de 20016, que instituiu a política de dados abertos do Poder Executivo no âmbito federal, tem como um de seus objetivos “franquear aos cidadãos o acesso, de forma aberta, aos dados produzidos ou acumulados pelo Poder Executivo federal, sobre os quais não recaia vedação expressa de acesso”

Por fim, o Marco Civil da Internet (Lei 12.965/2014) estabelece a proteção da privacidade e dos dados pessoais como um dos princípios do uso da internet (Art. 3º, II e III), além de enumerar uma série de regras relacionadas ao tratamento de dados pessoais no ambiente virtual, sendo exemplos a exigência de consentimento para o tratamento de dados pessoais (art. 7º, IX), o dever de cancelamento dos dados por solicitação do seu titular ao término da relação com o responsável pelo tratamento (art. 7º, X) e a observância ao princípio da finalidade (art. 7º, VIII, a, b, e c). Em 2016, o Decreto nº 8.771, que regulamenta o Marco Civil da Internet, definiu dados cadastrais<sup>52</sup> e de dados pessoais<sup>53</sup>.

## **2. Fontes de Informação e seu uso para fins de concessão de crédito**

### **2.1. Informações detidas pelo Poder Público - Acesso à Informação v. Proteção de Dados**

---

<sup>52</sup> Art. 11 (...).

§ 2º São considerados dados cadastrais: I - a filiação; II - o endereço; e III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

<sup>53</sup> Art. 14. Para os fins do disposto neste Decreto, considera-se:

I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;

O art. 31 da Lei 12.527/11 (LAI) prevê que as informações pessoais relativas à intimidade, vida privada, honra e imagem “terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem” (grifo nosso).

Já o art. 4º, IV, da LAI, estabelece que informações pessoais “são aquelas relacionadas à pessoa natural identificada ou identificável”. Inferese, assim, que os dados relativos a pessoas jurídicas não estão sujeitos à restrição de acesso estabelecida no art. 31. Note-se, ainda, que mesmo informações pessoais com acesso restrito podem ser divulgadas ou acessadas por terceiros, mediante previsão legal ou consentimento expresso da pessoa a que elas se referirem, conforme admite o inciso II do mesmo §1º do art. 31.

A restrição ao fornecimento de informações pessoais apenas para aquelas relativas à intimidade, vida privada, honra e imagem parece ser a posição adotada pela Controladoria Geral da União, em seu Manual da Lei de Acesso à Informação para Estados e Mu-

nicípios, ao definir informação pessoal como “aquela relativa à intimidade, à vida privada, à honra e à imagem das pessoas”<sup>54</sup>, repetindo a redação do art. 3º, V, do Decreto 7.724/12, que regulamentou a LAI.<sup>55</sup>

Tércio Sampaio Ferraz Júnior, em artigo sobre o sigilo bancário, afirma que a intimidade se refere àqueles “dados que a pessoa guarda para si e que dão consistência à sua pessoalidade, dados de foro íntimo, expressões de autoestima, avaliações personalíssimas com respeito a outros, pudores, enfim, dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e confiança e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito”<sup>56</sup>.

O mesmo autor define informações pessoais relativas à vida privada como aquelas “referentes às opções da convivência, como a escolha de amigos, a frequência de luga-

54 Controladoria Geral da União. Manual da LAI para Estados e Municípios. 1ª edição Brasília, 2013; p. 29.

55 Art. 3º, V - informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

56 FERRAZ JÚNIOR, Tércio Sampaio. Sigilo Bancário. Revista de Direito Bancário, do Mercado de Capitais e da Arbitragem. V. 14, nº 14, out-dez 2001. RT: São Paulo; p. 18.

res, os relacionamentos familiares, ou seja, de dados que, embora digam respeito aos outros, não afetam (embora no interior da própria convivência, possam vir a afetar) direitos de terceiros (exclusividade da convivência)”<sup>57</sup>. Para ele, a proteção da imagem corresponde ao “direito de não vê-la mercantilizada, usada, sem o seu exclusivo consentimento, em proveito de outros interesses que não os próprios”<sup>58</sup>. Complementa o referido autor que “a privacidade, nesse caso, protege a informação de dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é, o modo como ele supõe e deseja ser visto pelos outros”<sup>59</sup>.

No mesmo sentido Alexandre de Moraes afirma que “intimidade relaciona-se às relações subjetivas e de trato íntimo da pessoa, suas relações familiares e de amizade, enquanto vida privada envolve todos os demais relacionamentos humanos, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo etc.”<sup>60</sup>.

57 Ibid; p. 18.

58 FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da USP. Disponível em <http://www.revistas.usp.br/rfdusp/article/viewFile/67231/69841>; p. 443.

59 Ibid; p. 450.

60 Apud VILLELA, Fábio Goulart. Manual de Direito do Trabalho: teoria e questões. Rio de Janeiro: Elsevier, 2010; p. 148.

Por fim, a honra tem sua definição como o “princípio que leva alguém a ter uma conduta proba, virtuosa, corajosa e que lhe permite gozar de bom conceito junto à sociedade”<sup>61</sup>. Nas palavras de Marcos Vinícius de Corrêa Bittencourt, “[d]ireito à honra significa a proteção das qualidades pessoais do cidadão, tanto no seu aspecto interno como em relação ao conceito de sua integridade moral na sociedade”<sup>62</sup>.

A grande questão trazida pelo processamento automatizado de dados pessoais, no entanto, é a incerteza quanto aos reais efeitos do tratamento de dados pessoais - o que inviabiliza, em última análise, uma associação inequívoca do tratamento de um dado pessoal a um determinado efeito - no caso, ao dano à imagem ou à honra, por exemplo.

Esta vinculação dos dados pessoais a determinados efeitos é algo cada vez mais difícil de ser aferida com clareza dada a enorme facilidade de coleta e as possibilidades trazidas pelo tratamento de dados pessoais com técnicas capazes de extrair significados e usos passíveis de influenciar diversas esfe-

ras da vida da pessoa. Neste sentido, torna-se anacrônica a mera referência a efeitos do tratamento de dados pessoais para os direitos da personalidade e torna-se praticamente impossível determinar quais os efeitos que o acesso a determinados dados pessoais, pela mera análise seccional de suas características, possa acarretar ao seu titular. Neste panorama, é necessário que o titular dos dados tenha direitos concretos sobre a sua utilização e ganha relevância uma visão objetiva do tratamento de dados pessoais que reconheça como princípio a sua proteção por si só.

A verificação da existência de interesse público relevante na divulgação de dados pessoais, cotejada com o interesse dos titulares à sua não divulgação, foi o caminho apontado pelo Supremo Tribunal Federal ao julgar o ARE 652777, onde se discutia a constitucionalidade da publicação, pelo Município de São Paulo, inclusive em website mantido por este ente federativo, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias e que possui a seguinte ementa<sup>63</sup>:

---

61 Grande Dicionário Houaiss da Língua Portuguesa. Versão Eletrônica. 2012. Disponível em <http://houaiss.uol.com.br>.

62 Apud GIRÃO, Ingrid Pequeno Sá. Op. cit.

---

EMENTA: CONSTITUCIONAL. PUBLICAÇÃO, EM

63

SÍTIO ELETRÔNICO MANTIDO PELO MUNICÍPIO DE SÃO PAULO, DO NOME DE SEUS SERVIDORES E DO VALOR DOS CORRESPONDENTES VENCIMENTOS. LEGITIMIDADE. 1. É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias. 2. Recurso extraordinário conhecido e provido.

O Supremo Tribunal Federal já tinha manifestado esse posicionamento de forma clara quando do julgamento do Agravo Regimental na Suspensão de Segurança 3.902, cujo relator foi o Ministro Ayres Britto, conforme se infere de forma clara da sua ementa:

Ementa: SUSPENSÃO DE SEGURANÇA. ACÓRDÃO QUE IMPEDIAM A DIVULGAÇÃO, EM SÍTIO ELETRÔNICO OFICIAL, DE INFORMAÇÕES FUNCIONAIS DE SERVIDORES PÚBLICOS, INCLUSIVE A RESPECTIVA REMUNERAÇÃO. DEFERIMENTO DA MEDIDA DE SUSPENSÃO PELO PRESIDENTE DO STF. AGRAVO REGIMENTAL. CONFLITO APARENTE DE NORMAS CONSTITUCIONAIS. DIREITO À INFORMAÇÃO DE ATOS ESTATAIS, NELES EMBUTIDA A FOLHA DE PAGAMENTO DE ÓRGÃOS E ENTIDADES PÚBLICAS. PRINCÍPIO DA PUBLICIDADE ADMINISTRATIVA. NÃO RECONHECIMENTO DE VIOLAÇÃO À PRIVACIDADE, INTIMIDADE E SEGURANÇA DE SERVIDOR PÚBLICO. AGRAVOS

DESPROVIDOS. 1. Caso em que a situação específica dos servidores públicos é regida pela 1ª parte do inciso XXXIII do art. 5º da Constituição. Sua remuneração bruta, cargos e funções por eles titularizados, órgãos de sua formal lotação, tudo é constitutivo de informação de interesse coletivo ou geral. Expondo-se, portanto, a divulgação oficial. Sem que a intimidade deles, vida privada e segurança pessoal e familiar se encaixem nas exceções de que trata a parte derradeira do mesmo dispositivo constitucional (inciso XXXIII do art. 5º), pois o fato é que não estão em jogo nem a segurança do Estado nem do conjunto da sociedade. 2. Não cabe, no caso, falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo “nessa qualidade” (§ 6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. 3. A prevalência do princípio da publicidade administrativa outra coisa não é senão um dos mais altaneiros modos de concretizar a República enquanto forma de governo. Se, por um lado, há

um necessário modo republicano de administrar o Estado brasileiro, de outra parte é a cidadania mesma que tem o direito de ver o seu Estado republicamente administrado. O “como” se administra a coisa pública a preponderar sobre o “quem” administra – falaria Norberto Bobbio -, e o fato é que esse modo público de gerir a máquina estatal é elemento conceitual da nossa República. O olho e a pálpebra da nossa fisionomia constitucional republicana. 4. A negativa de prevalência do princípio da publicidade administrativa implicaria, no caso, inadmissível situação de grave lesão à ordem pública. 5. Agravos Regimentais desprovidos. (Grifos nossos).

A consideração de que nome e vencimentos de servidores não estão sujeitos à restrição de acesso prevista no art. 31 da LAI seguiu-se à apreciação de que há interesse geral na sua divulgação. Desta forma, torna-se possível o controle social dos gastos públicos, de modo que o interesse público suplantara o interesse que os titulares dos dados têm na sua não divulgação.

No caso já citado, sobre Credit Scoring, no qual não se usava como base a LAI, o Superior Tribunal de Justiça estabeleceu a impossibilidade de tratamento de dados tantos sensíveis quanto excessivos<sup>64</sup>:

64 Superior Tribunal de Justiça. Recurso Especial nº 1.419.697

Devem ser prestadas também as informações pessoais do consumidor avaliado que foram consideradas para que ele possa exercer o seu direito de controle acerca das informações excessivas ou sensíveis, que foram expressamente vedadas pelo art. 3º, §3º, I e II da própria Lei nº 12.414/2011.

Não podem ser valoradas pelo fornecedor do serviço de ‘credit scoring’ informações sensíveis, como as relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, ou excessivas, como as referentes a gostos pessoais, clube de futebol etc. (Grifos no original)

Desta forma, considerando-se o conjunto de meios hoje disponíveis para o tratamento de dados pessoais<sup>65</sup> que impossibilitam uma avaliação apriorística dos efeitos de seu tratamento para a pessoa, conjuntamente com a cláusula geral de proteção da personalidade presente em nosso ordenamento jurídico,

---

– RJ. Rel. Min. Paulo de Tarso Sanseverino. Julg. em 12.11.2014

65 O já citado Decreto n. 8.771/16 trouxe, também, uma definição de tratamento de dados:

Art. 14. Para os fins do disposto neste Decreto, considera-se:

(...)

II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

reconhece-se a necessidade de uma interpretação que considere na máxima extensão a proteção aos dados pessoais em conjunto com uma aplicação do acesso à informação que atenda ao interesse público de transparência e controle.

É importante salientar, porém, que o fato de a informação pessoal pura e simples não estar abarcada pela restrição de acesso prevista no art. 31 da LAI não equivale de forma alguma a que se considere que há uma opção padrão da lei a permitir o acesso a dados pessoais quando não considerados relacionados à intimidade, à vida privada, à honra e à imagem da pessoa em questão. A mencionada dificuldade em reconhecer os efeitos derivados da utilização de uma determinada categoria de dados pessoais faz com que se nivele como padrão a consideração de que qualquer informação pessoal é, atualmente, capaz de acarretar consequências indesejadas a aspectos da personalidade, fazendo com que, na prática, o não fornecimento de dados pessoais seja padrão. Ainda, pode a administração pública lhe restringir o acesso em razão de entender que é imprescindível à segurança da sociedade ou do Estado, conforme lhe autoriza o art. 23 da LAI<sup>66</sup>.

66 Art. 23. São consideradas imprescindíveis à segurança da

Além disso, o fato de a informação não ter acesso restrito não importa dizer que nenhum procedimento deva ser observado para sua obtenção. Os arts. 10 a 14 da LAI e 11 a 14 do Decreto nº 7.724/12 estabelecem o procedimento para acesso a informações em poder da União, Estados, Distrito Federal e Municípios e das autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente por esses entes federativos.

Por fim, outro limite ao acesso à informação pessoal, seja ela de acesso restrito ou não, é o princípio da finalidade. A utilização secundária de informações pessoais, isto é, a sua utilização para finalidades diversas daquelas para as quais as informações foram obtidas, é questão de absoluta relevância em várias normativas relacionadas à proteção de dados pessoais.

---

sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam: I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; III - pôr em risco a vida, a segurança ou a saúde da população; IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País; V - prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas; VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

De acordo com o princípio da finalidade, o motivo da coleta ou fornecimento de uma informação pessoal deve ser compatível com o objetivo final do tratamento ao qual esta informação será submetida. Desta forma, seja quando a informação for coletada diretamente do seu titular ou quando houver a consulta a um repositório de dados, a sua utilização sempre estará vinculada ao motivo que fundamentou esta coleta. Cria-se, desta forma, uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, de modo que esta deva ser levada em consideração em qualquer tratamento ulterior.

Assim, o princípio da finalidade se coloca como um potencial limite à utilização das informações pessoais obtidas com base na LAI, já que seu tratamento inicial pela administração pública se deu para o atingimento de um fim de interesse público, como a realização de políticas públicas, apenas para citar um exemplo.

O princípio da finalidade é um corolário do pressuposto de que a informação pessoal, como expressão direta da personalidade, nunca perde o vínculo com seu titular. Antes de ser meramente abstrata e sujeita

à livre disposição, esta informação, à medida que identifica alguma característica de uma pessoa, estará sempre vinculada a ela. Um desvio da finalidade para a qual foi recolhida pode tornar inócua qualquer tentativa de proteção e controle desta informação por parte do seu titular.

Ainda que não exista no ordenamento jurídico brasileiro normativa genérica que trate do princípio da finalidade, as disposições contidas na Lei do Cadastro Positivo e no Marco Civil da Internet, lidas à luz da cláusula geral de proteção da personalidade e da consideração de que a informação pessoal é elemento integrante da personalidade, materializam esse princípio de forma transversal. Não obstante, nota-se que a ideia da afetação da informação pessoal à razão pela qual foi coletada vem prosperando em diversos documentos normativos mais recentes, como o Decreto 6.135/07, que trata da elaboração do Cadastro Único para programas sociais do Governo Federal e que, portanto, influencia a utilização dessas informações com base na LAI. Prevê referido decreto, em seu artigo 8º, que:

Art. 8º Os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utiliza-



dos para as seguintes finalidades:

I - formulação e gestão de políticas públicas; e

II - realização de estudos e pesquisas. (Grifo nosso).

Portanto, mesmo que essas informações venham a ser divulgadas publicamente pela administração pública, para fins de garantir transparência e o controle democrático das políticas públicas a elas relacionadas por parte da população em geral, elas têm a finalidade de seu tratamento restritivamente definida, o que importa dizer que sua utilização para finalidades distintas estaria vedada, sendo a finalidade nesse caso outro obstáculo ao acesso e utilização posterior dessas informações com base na LAI.

## **2.2. Informações coletadas diretamente do titular**

O CDC, conforme visto, não exige o consentimento do titular para a abertura de cadastro em seu nome - situação bem distinta da prevista no Marco Civil da Internet e na Lei do Cadastro Positivo.

Além disso, há entendimentos no sentido

de que em situações nas quais haja um tratamento diverso daquele para o qual os dados se destinavam deveria haver o consentimento do seu titular. Nesse sentido é o enunciado aprovado pelo 16º Congresso Nacional dos Magistrados da Justiça do Trabalho (16º Conamat), realizado em João Pessoa-PB entre dias 1º a 4 de maio de 2012, que estabelece a necessidade de consentimento do trabalhador para o tratamento de seus dados pessoais de uma forma geral, quando forem tratados para um fim diverso daquele ao que se destinam:

DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR. USO E TRATAMENTO. VEDAÇÃO. Os dados pessoais do trabalhador e aqueles sensíveis, referentes à opção religiosa, sexual, filosófica, partidária, entre outros, são protegidos constitucionalmente (arts. 5º, X e XII) e por lei (art. 43 do CDC e Lei 12.414/2011, aplicados analogicamente ao Direito do Trabalho). Por isso, em regra, não podem ser usados nem tratados, sem o consentimento do trabalhador, para fins diversos aos que se destinam.

Vale destacar, contudo, que o Superior Tribunal de Justiça editou – a partir do julgamento do caso sobre credit scoring – súmula que afasta a exigência de consentimento do consumidor nesses casos:

Súmula 550: “A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo”.

### **2.3. Informações obtidas de terceiro - privado**

O uso de informações pessoais para fins de concessão de crédito é tema bastante delicado. Desse modo, torna-se imperioso analisar os limites de sua coleta, seja com relação aos dados pessoais obtidos junto ao Poder Público - como discutido acima -, diretamente de seus titulares ou de outros agentes privados.

O CDC não proíbe a coleta de dados nem tampouco exige o consentimento do seu respectivo titular, como se verifica a partir da leitura do *caput* e do §2º de seu artigo 43:

Art. 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

(...)

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

Esses cadastros, contudo, devem ser “objetivos, claros, verdadeiros e em linguagem de fácil compreensão”, além de que não devem conter informações negativas que digam respeito a períodos superiores a cinco anos, como determina o parágrafo 1º do referido artigo.

Ainda no âmbito do CDC, os atos referentes à coleta de dados pessoais e de consumo, quando não solicitadas pelo consumidor, deverão ser comunicados a ele por escrito - percebe-se, assim, que o consentimento não é elemento fundamental, o que nos permite concluir que, com base no CDC, dados pessoais poderiam ser coletados sem a autorização de seu titular. É evidente que isso não autoriza que dados submetidos a sigilo ou a qualquer outro tipo de proteção legal possam ser obtidos por BdC e tratados para fins de avaliação do perfil de crédito de seus titulares. Além disso, qualquer eventual correção aos dados de cadastro deverá ser realizada imediatamente e comunicada ao titular no prazo de cinco dias úteis.

Entretanto, a tendência mais recente no ordenamento brasileiro é no sentido de se exigir o consentimento do titular dos dados para que eles possam vir a ser tratados em diversas situações. Nesse sentido é a Lei do Cadastro Positivo, que em seu art. 4º<sup>67</sup> condiciona a abertura do cadastro à prévia autorização do seu titular, ainda que também disponha que, uma vez autorizada a abertura do cadastro positivo, não se faz necessária nova autorização para comunicação de futuras informações de adimplemento.

Além disso, a Lei do Cadastro Positivo, em seu art. 5º, l<sup>68</sup>, estabelece uma série de direi-

67 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.

§ 1º Após a abertura do cadastro, a anotação de informação em banco de dados independe de autorização e de comunicação ao cadastrado.

§ 2º Atendido o disposto no *caput*, as fontes ficam autorizadas, nas condições estabelecidas nesta Lei, a fornecer aos bancos de dados as informações necessárias à formação do histórico das pessoas cadastradas.

68 Art. 5º São direitos do cadastrado: 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 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 - solici-

tos/deveres: (i) cancelar o cadastro quando solicitado; (ii) acessar gratuitamente as informações sobre ele existentes no banco de dados; (iii) impugnar qualquer informação errada sobre ele e ter, em até sete dias, sua correção ou cancelamento; (iv) conhecer os principais elementos e critérios considerados para a análise de risco; (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 a revisão de decisão realizada exclusivamente por meios automatizados; e (vii) ter seus dados pessoais utilizados somente de acordo com a finalidade para a qual foram coletados.

O art. 6º do mesmo diploma legal<sup>69</sup>, com

tar 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.

69 Art. 6º Ficam os gestores de bancos de dados obrigados, quando solicitados, a fornecer ao cadastrado: I - todas as informações sobre ele constantes de seus arquivos, no momento da solicitação; II - indicação das fontes relativas às informações de que trata o inciso I, incluindo endereço e telefone para contato; III - indicação dos gestores de bancos de dados com os quais as informações foram compartilhadas; IV - indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos 6 (seis) meses anteriores à solicitação; e V - cópia de texto contendo sumário dos seus direitos, definidos em lei ou em normas infralegais pertinentes à sua relação com bancos de dados, bem como a lista dos órgãos governamentais aos quais poderá ele recorrer, caso considere que esses direitos foram infringidos. § 1º É vedado aos gestores de bancos de dados estabelecerem políticas ou realizarem operações que impeçam, limitem ou dificultem o acesso do cadastrado previsto no inciso II do art. 5º. § 2º O prazo para atendimento das informações

o intuito de reforçar tais garantias, estabelece uma série de obrigações aos gestores dos bancos de dados no fornecimento de informações.

Esta lei, em seu art. 9º<sup>70</sup>, para estimular a disseminação e, conseqüentemente, a maior disponibilização de informações no conjunto de banco de dados, permite, desde que expressamente autorizado pelo cadastrado, o compartilhamento e a troca de informações. Mais uma vez o consentimento do titular do dado é fator determinante para a sua utilização. Não obstante, equipara o gestor que recebe informações ao gestor que as anotou originariamente, inclusive estabelecendo um regime de responsabilidade solidária por eventuais prejuízos causados, bem como o dever de

---

estabelecidas nos incisos II, III, IV e V deste artigo será de 7 (sete) dias.

70 Art. 9º O compartilhamento de informação de adimplemento só é permitido se autorizado expressamente pelo cadastrado, por meio de assinatura em instrumento específico ou em cláusula apartada. § 1º O gestor que receber informações por meio de compartilhamento equipara-se, para todos os efeitos desta Lei, ao gestor que anotou originariamente a informação, inclusive quanto à responsabilidade solidária por eventuais prejuízos causados e ao dever de receber e processar impugnação e realizar retificações. § 2º O gestor originário é responsável por manter atualizadas as informações cadastrais nos demais bancos de dados com os quais compartilhou informações, bem como por informar a solicitação de cancelamento do cadastro, sem quaisquer ônus para o cadastrado. § 3º O cancelamento do cadastro pelo gestor originário implica o cancelamento do cadastro em todos os bancos de dados que compartilharam informações, que ficam obrigados a proceder, individualmente, ao respectivo cancelamento nos termos desta Lei. § 4º O gestor deverá assegurar, sob pena de responsabilidade, a identificação da pessoa que promover qualquer inscrição ou atualização de dados relacionados com o cadastrado, registrando a data desta ocorrência, bem como a identificação exata da fonte, do nome do agente que a efetuou e do equipamento ou terminal a partir do qual foi processada tal ocorrência.

receber e processar impugnações e realizar retificações solicitadas por titulares dos dados.

Fica claro, portanto, que a Lei do Cadastro Positivo, ao contrário do CDC, exige o consentimento por parte do titular para que seus dados sejam coletados e tratados.

Ainda, o art. 3º da Lei de Cadastro Positivo estabelece limitações que podem ser sintetizadas em cinco deveres a serem cumpridos pelo fornecedor de serviços: (i) dever de veracidade; (ii) dever de clareza; (iii) dever de objetividade; (iv) vedação de informações excessivas; e (v) vedação de informações sensíveis<sup>71</sup>. Confira-se:

Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.

§ 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.

---

71 STJ, REsp n. 1.419.697 - RS (2013/0386285-0), Min. Rel. Paulo de Tarso Sanseverino, p. 32.

§ 2o Para os fins do disposto no § 1o, consideram-se informações:

I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;

II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;

III - verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e

IV - de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.

§ 3o Ficam proibidas as anotações de:

I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e

II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Esses são alguns limites para a coleta de dados pessoais e para sua utilização, visto que informações excessivas, ou seja, aquelas que não sejam necessárias à finalidade do tratamento, e informações sensíveis, isto é, aquelas relativas “à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”, não podem ser utilizadas para fins de análise de risco de crédito.

Para Leonardo Roscoe Bessa, “a primeira forma de limitar a qualidade da informação que circula em arquivos de consumo é exigir que ela esteja vinculada ao propósito específico do banco de dados. Os dados coletados devem ser visivelmente úteis para os objetivos específicos do arquivo. Se não atenderem a esse pressuposto, a coleta e o tratamento de dados da informação devem ser considerados ilegais, ilegítimos e ofensivos à privacidade (art. 5º, X, CF)”<sup>72</sup>.

O Superior Tribunal de Justiça, no julgamento do caso envolvendo o serviço chamado credit scoring, entendeu que “[n]a avaliação do risco de crédito, devem ser respeitados os

<sup>72</sup> BESSA, Leonardo Roscoe. Cadastro Positivo: comentários à lei 12.414/2011. São Paulo: Ed. Revista dos Tribunais, 2011. P. 93/94.

limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011”. Desta forma, em qualquer situação na qual se avalie risco de crédito devem ser observadas as regras trazidas tanto pelo CDC quanto pela Lei do Cadastro Positivo, o que importa dizer que os dados pessoais dos consumidores somente poderão ser coletados e tratados para este fim quando não forem excessivos, isto é, quando estiverem vinculados à análise de risco de crédito do consumidor, e quando não forem sensíveis. Com isso, já temos dois limites claros para a coleta e tratamento de dados pessoais para fins de avaliação de risco de crédito.

Reconheceu ainda o STJ que, apesar de o consentimento do titular do dado que está sendo avaliado quanto ao seu risco de crédito ser em grande parte dos casos desnecessário, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.

O Marco Civil da Internet, por sua vez, reforça a lógica do consentimento como forma

a legitimar determinado tratamento de dados, assim como para seu fornecimento para terceiros. Isso é o que se extrai dos incisos VII e IX de seu art. 7º:

Art. 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

(...)

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

(...)

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais.

Outro limite estabelecido pelo MCI é o direito do usuário de ter excluídos, definitivamente, dados pessoais fornecidos a determinada aplicação de internet ao término da relação contratual entre as partes.

O MCI também se vale dos princípios da finalidade e da transparência como norteadores dos tratamentos de dados pessoais no ambiente virtual, o que tem plena aplicação às análises de risco de crédito efetuadas por *bureaux* de informação, eis que muitas vezes essas entidades se valem de informações coletadas na Internet. Isso é o que se extrai das alíneas do inciso VIII do art. 7º do MCI:

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

- a) justifiquem sua coleta;
- b) não sejam vedadas pela legislação; e
- c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

Vale destacar que o princípio da transparência, conforme salientado pela Prof<sup>a</sup> Claudia Lima Marques, “significa informação clara e correta sobre o produto a ser vendido, sobre o contrato a ser firmado, significa lealdade a respeito das relações entre fornecedor e consumidor, mesmo na fase pré-negocial, isto é, na fase

negocial dos contratos de consumo”<sup>73</sup>.

Nessa linha é importante salientar que o bureau de informações está obrigado a informar as fontes das informações utilizadas aos titulares dos dados cujo risco de crédito é avaliado, o que consta, inclusive, do inciso IV do art. 5º da Lei do Cadastro Positivo, na linha do que foi decidido pelo Superior Tribunal de Justiça no julgamento sobre o credit scoring.

---

<sup>73</sup> Claudia Lima Marques. Contratos no Código de Defesa do Consumidor. São Paulo: Editora Revista dos Tribunais, 1999. p. 286.

# 3. Estudos de Casos

## 1. Análise de mecanismos de acesso de dados oferecidos por bureaux de informação

Como consequência do incremento inaudito do uso da informação pessoal por mecanismos de avaliação e estratificação social, esta atividade hoje está marcada por sua notável complexidade. Isto se deve tanto à sua utilização em diversas áreas e situações (para além da análise de risco), ao elevado volume de dados que é passível de tratamento por estes mecanismos de forma automatizada e, enfim, pela opacidade inerente a estes mecanismos de análise.

Tais mecanismos são usualmente identificados como algoritmos. Algoritmos são, basicamente, um conjunto de passos ou atividades necessárias para a realização de uma tarefa - seja um cálculo balístico, uma plataforma de comércio eletrônico e até mesmo tarefas como o reconhecimento de voz. Os algoritmos, à medida que se tornaram também passíveis de serem automatizados e executados por computadores, passaram a aumentar sobremaneira a sua capacidade e, conseqüentemente, o seu campo de aplicação.

O fato de um número cada vez maior de tarefas ser executado por algoritmos os torna ubíquos em nossa vida cotidiana. Em razão disso, é cada vez mais comum a delegação de tarefas que realizávamos pessoalmente (como encontrar a melhor rota de trânsito entre dois endereços), ou que habitualmente eram confiadas a terceiros (como a decisão sobre uma concessão de crédito). Neste novo cenário, ao lado da maior eficiência que pode se verificar ao se considerar vários parâmetros de novas modalidades de negócio transformadas ou possibilitadas por algoritmos, há de se levar em conta que eles também proporcionam alterações fundamentais no que se pode esperar das atividades a eles confiadas em termos de transparência, confiança, previsibilidade e outros fatores que interessam diretamente o indivíduo e a sociedade.

Muitas destas alterações são devidas a características intrínsecas aos algoritmos. Talvez a mais evidente diga respeito à transparência do seu funcionamento. Neste sentido, já é quase usual a referência a diversos algoritmos como sendo “caixas pre-



tas” (black boxes, em denominação tornada célebre por Frank Pasquale<sup>74</sup>). Esta analogia evoca a dificuldade intrínseca que possui o cidadão de compreender de fato de que forma seus dados serão utilizados e quais critérios serão utilizados para avaliação, sempre que estes forem executados por um algoritmo cuja complexidade seja tamanha (o que é geralmente o caso) de forma a que não possa ser passível de conhecimento ou compreensão por ele, titular dos dados.

Verifica-se, assim, que muitas vezes falta ao titular dos dados qualquer evidência sobre o que de fato ocorre entre a entrada da sua informação pessoal e o resultado final, justamente por conta da complexidade das operações realizadas. Além disso, esta situação é de tal natureza que torna difícil que possa ser solucionada por mecanismos convencionais de transparência.

Eventualmente, a transparência em relação ao funcionamento dos algoritmos pode ser afetada por ao menos dois fatores: o primeiro é uma tradicional alegação, por parte de utilizadores de algoritmos, de que

estes estariam sujeitos a regras de propriedade intelectual e que consistiriam em segredo comercial, dado que o conhecimento detalhado de seu funcionamento poderia lhes retirar vantagem competitiva em relação aos seus concorrentes.

Além deste fator de ordem concorrencial que, muitas vezes, é alegado para afastar a transparência sobre as características de um algoritmo, outro fator deve ser considerado de forma muito clara: ainda que houvesse ampla transparência sobre o funcionamento e estrutura de diversos dos algoritmos mais utilizados, sua operação é muitas vezes tão complexa que de pouca ou nenhuma valia seria para os titulares dos dados que, diretamente, pouco teriam a ganhar em relação ao seu poder de barganha. Um elemento usual em muitos algoritmos que vêm sendo utilizados dificulta ainda mais qualquer ganho objetivo em relação à transparência neste ponto: os algoritmos que “aprendem” a partir dos dados com que são alimentados e que, a partir destes, modificam-se a si próprios e ao seu funcionamento - através das chamadas técnicas de *Machine Learning* - geram produtos cujo funcionamento e cujo resultado final - seu output - não é a rigor

<sup>74</sup> Pasquale, Frank. *Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

passível de ser antecipado nem mesmo pelos seus idealizadores ou programadores, dada a sua natureza dinâmica.

Estas considerações, aliadas à enorme relevância que algoritmos vêm apresentando em nossa vida cotidiana, fazem com que haja cada vez maior necessidade de estabelecer parâmetros para que se possa acompanhar o funcionamento de algoritmos para, quando necessário, realizar eventual correção de seus resultados. Casos clássicos em que isso possa ser necessário ocorrem quando, por exemplo, algoritmos acabem favorecendo a discriminação ou o favorecimento de determinados indivíduos em situações que deveriam ser de igualdade<sup>75</sup>. De fato, a inovação e a automatização de diversas tarefas não se podem dar às expensas de parcelas da população ou da solidificação de preconceitos que, eventualmente, deixariam de ser originários de atos realizados por pessoas para passarem a estar incorporados numa lógica estatística condensada em um determinado algoritmo.

**Como forma de fazer frente a este problema, diversas linhas de ação vêm sendo**

<sup>75</sup> O tema foi abordado em detalhe em: Solon Barocas & Andrew Selbst. *Big Data's Disparate Impact*. In 104 California Law Review (2016).

avaliadas. Como eixo comum a várias delas está a constatação de que a transparência em relação aos algoritmos, ainda que fundamental, não é o suficiente para colocar o cidadão em condições de conhecer os efeitos destes em suas vidas e tomar escolhas informadas e legítimas em determinadas situações, para as quais pode ser necessário algum tipo de facilitação ou intermediação<sup>76</sup>.

Outras iniciativas que vêm sendo consideradas, e que podem não depender diretamente da existência de um órgão público ou um corpo técnico especializado, tendo a ver com a incorporação ao ordenamento jurídico de normas que estabeleçam requisitos para o funcionamento dos algoritmos e estabeleçam parâmetros de responsabilidade e *accountability* para os que deles fazem uso. Neste sentido, surgem igualmente propostas que procuram abarcar o conjunto de atores envolvidos na implementação e utilização de algoritmos de forma ampla para que sejam estruturados procedimentos de governança na sua utilização<sup>77</sup>.

<sup>76</sup> Neste sentido já se vislumbrou inclusive a criação de uma agência reguladora para trabalhar com algoritmos. Andrew Tutt. *A new agency. An FDA for algorithms*. in: [ssrn.com/abstract=2747994](https://ssrn.com/abstract=2747994).

<sup>77</sup> Doneda, Danilo; Almeida, Virgílio. *What is algorithm governance?* In: IEEE Internet Computing, julho-agosto 2016, pp. 60-62.

Outra possibilidade, que se torna especialmente relevante ante o estado ainda inicial de implementação de soluções que se apliquem diretamente aos algoritmos, é a de trabalhar diretamente com o controle dos dados que alimentam o algoritmo. A bem da verdade, normas referentes à proteção de dados pessoais vêm há anos apresentando regras que se aplicam diretamente a sistemas de avaliação realizados por algoritmos que se utilizam de dados pessoais. Neste sentido é usual, por exemplo, que normativas deste gênero apresentem regras que limitem ou estabeleçam direitos ao titular em caso de avaliações sobre sua pessoa serem feitas por meios automatizados, não raro disciplinando algo sobre a transparência desta atividade ou estabelecendo a necessidade de intervenção humana neste processo.

Note-se que, hoje, a situação não é tão diferente em outros países, ainda que existam marcos normativos com incidência direta sobre o tema. Nos Estados Unidos, por exemplo, pode-se recorrer ao FCRA (Fair Credit Reporting Act), de 1970, para que o cidadão acesse e controle seus dados utilizados em sistemas de score de crédito; já na União Europeia temos o que há talvez de mais re-

cente em relação à sua incidência direta sobre a matéria, que é o novo Regulamento Geral sobre Proteção de Dados, que entrará em vigor em 2018, mas que explicita e atualiza algumas regras já presentes na legislação atual sobre o direito de conhecer a motivação de decisões tomadas de forma automatizada por algoritmos e, eventualmente, de contestá-las.

## **2. Utilização de dados pessoais por bureaux e data brokers: apresentação e análise**

No Brasil, diversas empresas vêm oferecendo em seu portfólio serviços de análise de informações pessoais para fins diversos de avaliação. Alguns deles são limitados ou, ao menos, centrados na análise de crédito; outros possuem alçada mais ampla e podem ser utilizados para uma gama de objetivos que, a bem da verdade, variam conforme a demanda de cada cliente do serviço.

Como abordagem e estudo de caso, foram identificados serviços de 2 *bureaux* que desempenham atividades no Brasil para que seja feito um cotejo da transparência e natureza das informações pessoais que os alimentam. São estes: Serasa-Experian (em relação ao serviço *Mosaic*) e Boa Vista.

A partir da descrição dos serviços oferecidos pelos respectivos *bureaux*, verifica-se que estes afirmam obter uma série de informações pessoais que servem como input de seu mecanismo de geração de score de crédito. Ao final dessa análise apresentaremos uma tabela com os dados que Os dados que cada empresa declaradamente utiliza.

### **3. Análise do serviço Mosaic, da Serasa-Experian**

Serviços de dois *bureaux* de crédito foram analisados e submetidos a análise dos dados pessoais de que se utilizam e a um *accountability check*. Note-se que o serviço que é objeto do presente estudo, qual seja o *Mosaic*, da Serasa-Experian, foi avaliado em maior detalhe, tendo também em vista igualmente que o referido serviço permite maior detalhamento de como os seus resultados são oferecidos ao usuário final. A avaliação do outro bureau possui caráter complementar.

#### **3.1 A coleta do dado pessoal se deu diretamente do titular ou por intermediário?**

Os dados utilizados pelo sistema *Mosaic* são obtidos a partir de terceiros. Em determinadas e raras ocasiões os dados podem ter

sidos diretamente fornecidos pelo seu titular à gestora do banco de dados que administra o *Mosaic* (Serasa Experian), em casos em que este os forneça à empresa para alimentação de alguma base de dados que esta administre e que também seja utilizada pelo sistema (o que pode ser o caso do cadastro da Lei 12.414/2011).

As fontes dos dados são indicadas apenas genericamente - há menção à utilização de “*variadas fontes de informações sobre consumidores, empresas e households (integrantes de família pertencentes a um mesmo domicílio) em consonância com a legislação brasileira*”.

#### **a) caso a coleta tenha sido feita junto ao titular, esta foi consentida?**

O consentimento direto do titular somente poderá ser verificado nas situações nas quais o dado é coletado diretamente dele ou a partir de uma autorização sua, como na hipótese de coleta por via da inscrição no cadastro da Lei 12.414/2011, conforme mencionado.

#### **b) caso a coleta tenha sido feita de intermediário, este possui legitimidade para utilizar o dado e repassá-lo a terceiro?**

A legitimidade da coleta realizada por intermediário deve ser verificada caso a caso e, ainda, cumpre avaliar se não há eventual ruptura do princípio da finalidade resultante do repasse da informação. Para tal verificação, é fundamental conhecer qual a fonte específica de cada informação pessoal utilizada, o que não é uma informação disponibilizada pelo BdC - que, inclusive, afasta essa obrigação nos contratos de fornecimento de informações que celebra com seus clientes, medida esta que apresenta grande potencial para reduzir a transparência no processo bem como, conforme ressaltado, pode implicar na virtual impossibilidade de verificação do atendimento ao princípio da finalidade.

### **3.2 O dado em questão pode ser considerado como enquadrado em alguma hipótese legal ou regulamentar de uso permitido?**

Em determinadas hipóteses pode-se, a partir do dado em si e considerando a finalidade da sua utilização, vislumbrar a legitimidade do seu tratamento, por exemplo o caso de dados coletados inicialmente para a gestão de algum programa social ou política pública e que posteriormente foram utilizados para fins de crédito. Tais hipóteses foram

objeto de avaliação e comentário na seção denominada *accountability check*, abaixo.

### **3.3 O output do serviço permite a identificação pessoal de cidadãos ou apresenta como resultados informações em forma agregada e anônima?**

O serviço não contempla a identificação pessoal nem o fornecimento de dados pessoais de cidadão, ao menos em forma individualizada e específica. O serviço, por outro lado, realiza o enquadramento de um cidadão - a partir de seus dados pessoais - em determinadas categorias sócio-econômicas.

Ainda cumpre ressaltar que um dos serviços oferecidos é o fornecimento de listagens identificativas de cidadãos que se enquadram em determinados critérios de segmentação, o que implica diretamente na identificação de determinados indivíduos, ainda que associados a critérios de segmentação que não são individualizados. Não é claro quais dados pessoais são fornecidos conjuntamente com a identificação e mesmo se estes dados são objetivamente transferidos, ou o próprio bureau se encarrega de realizar o direcionamento de publicidade ou a comunicação pretendida para as pessoas identificadas.

Neste sentido, a utilização de dados pessoais pelo serviço se dá por duas vias: (i) pela coleta de dados para que seja realizada a estratificação; (ii) pelo tratamento de dados para que sejam definidos os critérios e variáveis para a estratificação.

### **3.4 Existe alguma modalidade de estratificação já implementada na apresentação dos dados?**

Sim, a estratificação é apresentada ao cliente em moldes pré-definidos e com destaque para indicativos potenciais de atributos atinentes àquele estrato (como, por exemplo, a chance potencial de insolvência, fator capaz de interessar a ampla gama de clientes do serviço). Há de se atentar para o fato, bastante discutido em literatura, referente aos efeitos do enquadramento de indivíduos em determinadas segmentações, fator que pode eventualmente gerar atrito e prejuízos decorrentes seja de falhas nesta segmentação como sua impossibilidade de abarcar corretamente as características de cada indivíduo, podendo sujeitá-lo, inclusive, a medidas discriminatórias.

#### **a) Em caso positivo, pode-se afirmar que os critérios de estratificação são direta ou potencialmente discriminatórios?**

A presença de qualquer tipo de estratificação tem um potencial, em si, discriminatório, ao ressaltar aspectos genéricos em detrimento de condições e atributos pessoais. Como generalização, no entanto, pode servir como ferramenta útil para diversas modalidades decisórias e de planejamento, contanto sejam evitados os desvios que induzem à manutenção e até acirramento de preconceitos e de escolhas discriminatórias. Neste sentido, verifica-se como questionável a existência de classificações que, já em sua titulação, induzem à exclusão ou ressaltam aspectos culturais associados à marginalização. Destaque nesta utilização de elementos que tendem a induzir posturas discriminatórias é a utilização de imagens de representantes de cada estratificação.

**3.5 O serviço e as suas características essenciais (em particular a informação sobre os dados pessoais tratados, o escopo do serviço e potenciais efeitos que a sua utilização pode ocasionar para o titular dos dados) são informações acessíveis publicamente?**

Tal qual as fontes dos dados não são disponibilizadas pelos administradores do serviço *Mosaic*, da mesma forma o escopo do tratamento e as potenciais utilizações que podem ser aplicadas aos dados coletados não são transparentes aos titulares de dados, que podem ter noção da destinação a ser dada às suas informações basicamente por inferências tomadas a partir das informações fornecidas a potenciais clientes do serviço por ocasião da oferta do serviço.

Neste particular, ganha relevância a ausência de um canal de comunicação da gestora dirigido aos titulares de dados, capaz de tornar o processo transparente e, eventualmente, de permitir ou facilitar a estes o exercício de direitos sobre seus próprios dados.

**a) em caso positivo, estas informações são facilmente acessíveis, claras, compreensíveis e completas?**

Não se aplica, dada a indisponibilidade da informação mencionada

**3.6 O titular de dados pessoais utilizados pelo bureau tem acesso aos dados e informações sobre o tratamento de seus dados e sobre critérios para a realização de avaliações a seu respeito?**

Como já mencionado, não há um canal ou outra estratégia de comunicação ou transparência destinada ao esclarecimento aos titulares de dados sobre a utilização de suas informações - em que pese a decisão do STJ no caso do credit scoring apontar para a necessidade de *bureaux* de crédito trabalharem no sentido de construírem tais instrumentos. A este respeito, estes vêm trabalhando basicamente em termos de acesso às informações sobre inclusão em cadastro negativo de crédito, no que diz respeito à própria negativação.

### 3.7. Accountability check

#### - Mosaic/Serasa-Experian<sup>78</sup>

#### 3.7.1. Adequação dos dados utilizados à normativa brasileira

Os dados considerados pelo bureau Serasa-Experian para alimentação de seu serviço de estratificação denominado *Mosaic* serão classificados de acordo com a sua origem, procurando identificar se se tratam de dados de acesso público ou se são passíveis de serem obtidos somente com alguma modalidade de privilégio de acesso (p.ex. mediante pagamento ou para pessoas ou agentes específicos).

Optou-se por associar o atributo de “pública” ou “privada” à informação coletada, referindo-se essa associação mais à expectativa do titular dos dados em relação à disponibilidade de sua informação do que a uma verificação estrita sobre a legitimidade de sua coleta. Isto se dá pelo fato de que (i) não há uma descrição concreta e exaustiva das fontes de dados utilizados; (ii) mesmo com esta lista de fontes em mãos, seria necessário

---

<sup>78</sup> Usamos aqui a expressão *accountability check* com a ideia de se efetuar uma análise de adequação das coletas e tratamentos de dados realizados pelos BdC analisados com os limites estabelecidos no capítulo 2 deste relatório.

levar-se em conta igualmente os procedimentos utilizados para o acesso aos dados para perquirir sobre a legitimidade de seu uso.

E, mais importante dentro de uma perspectiva de proteção de dados fundada na situação do titular dos dados: ao se levar em conta as expectativas deste, tendo em vista tanto o critério concreto da sua disposição em bases de dados e fontes de acesso geral, mas também o seu conhecimento sobre este fato, enfatiza-se o critério da legitimidade e boa-fé na utilização de dados pessoais. Esta ênfase no critério da boa-fé é, por um lado, necessária diante da inexistência, em um grande número de vezes, de critérios claros quanto à natureza pública ou privada de determinados dados pessoais, que tem raiz na escassa legislação e tratamento doutrinário dado ao tema, como pelo fato de que, em última análise, o objetivo do estudo gira em torno de recomendações sobre proteção de dados a serem dirigidas aos gestores de bancos de dados, para os quais se afigura de grande utilidade o emprego de critério geral que pode compensar a ausência de medidas normativas específicas. Ao final da análise com relação a todos os BdC objeto do presente relatório apresentaremos uma tabela contendo



do as informações compiladas de todos eles, com indicação da disponibilidade (se pública ou privada, conforme explicado acima) e com os nossos comentários a respeito.

### **3.7.2. Verificação da proporcionalidade dos dados utilizados em relação à sua finalidade e adequação dos dados utilizados aos princípios de proteção de dados pessoais**

Para a verificação da proporcionalidade da informação coletada com as finalidades almeçadas pelo bureau, os dados que alimentam o sistema serão considerados a partir de categorias gerais pré-definidas pela Serasa-Experian para que, dentro delas, seja realizada uma aferição qualitativa da sua pertinência em relação às finalidades almeçadas bem como para identificar eventual abusividade na sua utilização. Caso a informação ofereça algum risco específico, este será igualmente ressaltado.

Os dados coletados pelo bureau também serão examinados em relação à sua aderência aos princípios de proteção de dados pessoais, tais como presentes em diversas legislações e no ordenamento brasileiro em normativas, entre outras, como a Lei 12.414/2011, Lei 12.527/2011 e Lei 12.965/2014.

De início, cabe ressaltar que, a despeito de serem feitas observações em função de características específicas do uso de determinados tipos de informação pessoal e de grupos nos quais elas estão agrupadas, esta análise não é exaustiva em relação aos riscos potenciais de seu uso, dado que diversas técnicas podem realizar novas inferências e constatações a partir da análise de um determinado grupo de informações que exorbite a soma do que estas individualmente revelariam. Tal possibilidade, que foi aventada com pioneirismo pela pesquisadora Latanya Swenney em 2000<sup>79</sup> e hoje é fartamente ilustrada em estudos subsequentes, torna necessário que se considere igualmente as práticas referentes ao uso de dados pessoais e não somente à sua coleta para uma análise integrada de risco. Tal análise somente pode ser realizada caso elementos objetivos sobre os procedimentos utilizados pelo bureau para análise dos dados sejam transparentes, o que não ocorre na presente análise.

---

<sup>79</sup> Latanya Sweeney. Simple Demographics Often Identify People Uniquely. In Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh, 2000, disponível em: <http://dataprivacylab.org/projects/identifiability/paper1.pdf>.

### **(a) Informações pessoais**

As informações consideradas como “pessoais” na classificação da empresa correspondem, de fato, a um subgrupo daquilo que se entende por informação pessoal (isto é, toda informação relacionada a uma pessoa determinada ou determinável<sup>80</sup>) e também extrapolam as informações usualmente consideradas como cadastrais<sup>81</sup>, por incluir, por exemplo, dados sobre escolaridade e informação empregatícia. Neste sentido, não consistem em um grupo homogêneo e pode-se afirmar que, ainda que algumas das informações aqui contidas possuam natureza de acesso público, o que facilita a sua utilização, mesmo neste caso possa ser levantado o questionamento sobre de que forma chegou-se a determinada informação, processo que pode revelar um tratamento prévio de informações pessoais que também há de ser considerado (e que não pode ser simulado por conta da ausência de informações sobre as fontes específicas utilizadas). Por exemplo, ao se considerar o estado civil ou o núme-

80 Cf. Lei 12.527/2011, art 4º, IV.

81 Cf, entre outras, Lei 12.965/2014, art.10º, § 3º.

ro do cadastro de pessoa física (CPF), muito embora este possa ser recuperado a partir do nome de um cidadão, resta sempre também a elucidar de qual forma o próprio nome foi considerado como apto a fazer parte de um determinado banco de dados para utilização pelo sistema *Mosaic*.

Já em relação a outras informações, de natureza empregatícia, exceto para aquelas que correspondem às obrigações de transparência do poder público e que dizem respeito a servidores públicos, estas possuem natureza a princípio privada e sua utilização deve ter sido objeto de autorização do titular.

### **(b) Endereço**

O endereço, seja aquele pessoal como o profissional, é informação cuja divulgação irrestrita não encontra amparo na legislação brasileira, com a exceção de casos referentes a servidores públicos e a sede de seu exercício profissional. Desta forma, sua utilização deve levar em conta a sua fonte e, quando necessário, que o titular esteja ciente e a tenha autorizado.

Há ainda de se verificar a eventualidade do endereço ser efetivamente fornecido como parte de algum outro serviço que o tenha inserido em um determinado banco de dados. Caso o fornecimento seja do endereço individualizado, este fato pode levantar questionamentos inclusive referentes à segurança pessoal do titular dos dados; de toda forma, ainda que o endereço seja fornecido de forma agregada, dependendo da granularidade deste dado e da sua utilização, este pode eventualmente possibilitar que medidas de caráter discriminatório sejam tomadas em relação a grupos de cidadãos em um determinado endereço. Tais fatos não de ser levados em conta no momento da utilização dos dados.

### **(c) Telefones e Outros Endereços**

Em relação aos telefones e outros endereços, deve-se reputar válidas as observações feitas anteriormente em relação ao endereço, com o acréscimo de que os dados telefônicos permitem a interpelação de um cidadão, prática que deve ser considerada em relação ao impacto em sua esfera pessoal e familiar e, ainda, ter a sua legalidade considerada a partir de legislações estaduais e municipais que, em determinadas unidades

da federação, restringem a possibilidade de *marketing* telefônico, tornando necessária a prévia consulta a uma lista de cidadãos que optaram por negar o recebimento de tais chamadas telefônicas<sup>82</sup>.

### **(d) Anotações de Inadimplência**

As anotações de inadimplência, em sentido estrito, têm sua utilização permitida pelo CDC, desde que sejam verificados alguns requisitos como a comunicação prévia por escrito da inscrição ao inadimplente, dentre outras. Desta forma, há que se verificar que dados que diretamente deem conta desta inscrição devem ter sido necessariamente obtidos a partir de um banco de dados que cumpriu estes requisitos, sob pena de viciar todo o sistema.

Outras informações que possam ter significância análoga, como a inscrição em cadastro de cheques sem fundos, por exemplo, devem responder, respectivamente, à sua regulamentação específica, com os mesmos efeitos. Note-se ainda que, em todos estes casos, a utilização destes cadastros muitas vezes somente é estritamente permitida

<sup>82</sup> São as chamadas leis do “não perturbe” ou “no call”. Como exemplo podemos citar a Lei nº 13.226 de 2008, do Estado de São Paulo.

para fins de apuração de viabilidade de fornecimento de crédito e operações financeiras, sendo bastante discutida e mesmo com viés negativo a sua possibilidade de utilização para outras finalidades não relacionadas à concessão de crédito (como ocorre atualmente com a discussão na justiça trabalhista acerca da utilização de dados creditícios no processo de contratação de empregado). Desta forma, é essencial verificar o nexo entre a finalidade para qual a informação sobre inadimplência foi obtida e a finalidade de sua utilização, sendo que o potencial de discriminação presente em determinadas utilizações pode ser fator determinante para caracterizar eventual ilegitimidade.

#### **(e) Outras Anotações**

Esta rubrica é bastante heterogênea e apresenta certas singularidades resultantes deste fato. Nela, constam informações relacionadas ao ritmo com que certas atividades (que não são limitadas em sua frequência por legislação) são praticadas (como a frequência de consultas a cheque ou a crédito ou a contumácia de sustação), que têm sido eventualmente reputadas abusivas como critério para valoração de crédito, revelando

potencial discriminatório consistente.

De forma análoga, a eventual valoração sobre registro de grafias semelhante ou sobre documentos extraviados e furtados, dependendo da forma como possam ser valorados pelo sistema *Mosaic*, ainda que baseados em tratamento estatístico que revele algum resultado que possa ser considerado útil para fins de segmentação, podem igualmente levar a resultados discriminatórios - veja-se o caso eventual de um alto índice de furto de documentos de uma pessoa que vive em região com escassa segurança.

Desta forma, a utilização de grande parte dos dados desta rubrica deve considerar não somente a formalidade e regularidade de sua obtenção, mas o potencial de risco que pode trazer aos seus titulares, individual ou coletivamente.

#### **4. Análise do Data Plus, da Boa Vista SCPC**

##### **4.1. A coleta do dado pessoal se deu diretamente do titular ou por intermediário?**

Idem ao *Mosaic*

**4.2. Caso a coleta tenha sido feita junto ao titular, esta foi consentida?**

Idem ao *Mosaic*

**4.3. Caso a coleta tenha sido feita de intermediário, este possui legitimidade para utilizar o dado e repassá-lo a terceiro?**

Idem ao *Mosaic*

**4.4. O dado em questão pode ser considerado como enquadrado em alguma hipótese legal ou regulamentar de uso permitido?**

Idem ao *Mosaic*

**4.5. O output do serviço permite a identificação pessoal de cidadãos ou apresenta como resultados informações em forma agregada e anônima?**

O serviço contempla a identificação pessoal e o fornecimento de dados pessoais de cidadão de forma individualizada e específica.

**4.6. Existe alguma modalidade de estratificação já implementada na apresentação dos dados?**

Idem ao *Mosaic*

**a) Em caso positivo, pode-se afirmar que os critérios de estratificação são direta ou potencialmente discriminatórios?**

Idem ao *Mosaic*

**4.7. O serviço e as suas características essenciais (em particular a informação sobre os dados pessoais tratados, o escopo do serviço e potenciais efeitos que a sua utilização pode ocasionar para o titular dos dados) são informações acessíveis publicamente?**

Tal qual as fontes dos dados não são disponibilizadas pelo bureau, da mesma forma o escopo do tratamento e as potenciais utilizações que podem ser aplicadas aos dados coletados não são transparentes aos titulares de dados, que podem ter noção da destinação a ser dada às suas informações basicamente por inferências tomadas a partir das informações fornecidas a potenciais clientes do serviço por ocasião da oferta do serviço. Há apenas uma menção que tais dados poderiam ser utilizados para “ações de marketing direto, rentabilização de carteira, fidelização, cobrança e atualização do banco de dados”.

Assim como no caso do *Mosaic*, merece destaque a ausência de um canal de comunicação do bureau dirigido aos titulares de dados, capaz de tornar o processo transparente e, eventualmente, de permitir ou facilitar a estes o exercício de direitos sobre seus próprios dados.

**a) em caso positivo, estas informações são facilmente acessíveis, claras, compreensíveis e completas?**

Não se aplica, dada a indisponibilidade da informação mencionada

**4.8. O titular de dados pessoais utilizados pelo bureau tem acesso aos dados e informações sobre o tratamento de seus dados e sobre critérios para a realização de avaliações a seu respeito?**

Não há um canal ou outra estratégia de comunicação ou transparência destinada ao esclarecimento aos titulares de dados sobre a utilização de suas informações.

## **4.9 Accountability check - Boa Vista SCPC**

### **4.9.1. Adequação dos dados utilizados à normativa brasileira**

Os dados considerados pelo bureau Boa Vista SPPC para oferecimento de serviços a seus clientes – especialmente o serviço Data Plus - serão classificados de acordo com a sua origem, procurando identificar se se tratam de dados de acesso público ou se são passíveis de serem obtidos somente com alguma modalidade de privilégio de acesso (p.ex. mediante pagamento ou para pessoas ou agentes específicos), usando-se os mesmos critérios atribuídos à análise relativa ao serviço *Mosaic* ofertado pelo Serasa Experian, e serão apresentados de forma compilada, juntamente com as informações utilizadas por aquele BdC.

### **4.9.2. Verificação da proporcionalidade dos dados utilizados em relação à sua finalidade e adequação dos dados utilizados aos princípios de proteção de dados pessoais**

Para a verificação da proporcionalidade da informação coletada com as finalidades almejadas pelo bureau, os dados que alimentam o

sistema serão considerados a partir de categorias gerais pré-definidas pela Boa Vista SCPC, utilizando-se os mesmos critérios empregados na análise do serviço *Mosaic* da Serasa Experian. Caso a informação ofereça algum risco específico, este será igualmente ressaltado.

#### **(a) Informações pessoais**

As informações consideradas como “pessoais” na classificação da empresa correspondem, de fato, a um subgrupo daquilo que se entende por informação pessoal e também extrapolam as informações usualmente consideradas como cadastrais, por incluir, por exemplo, dados sobre estilo de vida e de classe social, informações essas que poderiam ser enquadradas como excessivas na linha do que foi decidido pelo Superior Tribunal de Justiça no julgamento do caso do credit scoring.

Tais informações, conforme destacado na análise sobre o serviço *Mosaic* do Serasa Experian, não consistem em um grupo homogêneo e pode-se afirmar que, ainda que algumas das informações aqui contidas possuam natureza de acesso público, o que faci-

lita a sua utilização, mesmo neste caso possa ser levantado o questionamento sobre de que forma chegou-se a determinada informação, processo que pode revelar um tratamento prévio de informações pessoais que também há de ser considerado (e que não pode ser simulado por conta da ausência de informações sobre as fontes específicas utilizadas).

Já em relação a outras informações, como o Número de Identificação Social (NIS), que é atribuído a pessoas que serão beneficiadas por algum projeto social, ainda que eventualmente venham a ser divulgadas para fins de transparência do poder público, possuem natureza a princípio privada e sua utilização deve ter sido autorizada pelo seu titular.

#### **(b) Endereço**

Idem ao *Mosaic*

#### **(c) Telefone e e-mail**

Em relação aos telefones, deve-se reputar válidas as observações feitas anteriormente em relação ao endereço, com o acréscimo de que os dados telefônicos permitem a interpeção de um cidadão, prática que deve ser

considerada em relação ao impacto em sua esfera pessoal e familiar e, ainda, ter a sua legalidade considerada a partir de legislações estaduais e municipais que, em determinadas unidades da federação, restringem a possibilidade de *marketing* telefônico, tornando necessária a prévia consulta a uma lista de cidadãos que optaram por negar o recebimento de tais chamadas telefônicas, serviço esse igualmente disponibilizado pela Boa Vista SCPC sob a rubrica “Flag Not Call”.

#### **(d) Outras Anotações**

Esta rubrica é bastante heterogênea e apresenta certas singularidades resultantes deste fato. Nela, constam informações relacionadas ao ritmo com que certas atividades (que não são limitadas em sua frequência por legislação) são praticadas (como a frequência de consultas a crédito ou a contumácia de sustação), que têm sido eventualmente reputadas abusivas como critério para valoração de crédito, revelando potencial discriminatório consistente.

Por outro lado, informações relativas a restrição creditícia encontram amparo no CDC, desde que sejam verificados alguns requisitos já destacados anteriormente. Des-

ta forma, há que se verificar que dados que diretamente deem conta desta inscrição devem ter sido necessariamente obtidos a partir de um banco de dados que cumpriu estes requisitos, sob pena de viciar todo o sistema.

Além disso, a consulta a certas informações, como aquelas relativas a Pessoas Politicamente Expostas (PPE), decorrem de obrigações internacionais assumidas pelo Estado Brasileiro<sup>83</sup>, e sua utilização, portanto, além de permitida, mostra-se uma exigência legal a incidir sobre diversos setores de atividades.

Desta forma, a utilização de grande parte dos dados desta rubrica deve considerar não somente a formalidade e regularidade de sua obtenção, mas o potencial de risco que pode trazer aos seus titulares, individual ou coletivamente.

---

<sup>83</sup> Nesse sentido é a Resolução nº 16, de 28 de março de 2007, do Conselho de Controle de Atividades Financeiras – COAF. Disponível em <http://www.coaf.fazenda.gov.br/backup/legislacao-e-normas/normas-do-coaf/coaf-resolucao-no-016-de-28-de-marco-de-2007-1>. Acesso em 03.11.2016.



## 4. Recomendação de melhores práticas

Levando em consideração os pontos levantados quanto à crescente importância da utilização de dados pessoais pelos setores privado e público, a importância fundamental de que seu uso respeite os direitos humanos e impulse a cidadania e, finalmente, o cenário atual em que a regulamentação no Brasil a respeito está ainda em momento de definição, identificamos uma série de recomendações a serem levadas em conta nas atividades que utilizem dados pessoais no contexto do *Big Data*<sup>84</sup>.

As recomendações levaram em conta, à parte as particularidades do uso de informações pessoais e do *big data*, as características específicas do contexto regulatório brasileiro, no qual, apesar da atual indefinição sobre um modelo regulatório específico so-

bre proteção de dados pessoais, a legislação vigente, seja a partir da Constituição Federal como de diversas leis ordinárias e de decisões de tribunais – conforme discutido neste estudo -, já aponta para um perfil do que se pode considerar como elementos básicos de um sistema de proteção de dados no ordenamento brasileiro, no qual destacam-se elementos como a proteção da personalidade, a transparência e a boa-fé.

Com base nas particularidades da atividade de tratamento de dados pessoais e de *big data* levantadas e nos elementos presentes em nossa legislação atual, bem como em projetos de lei atualmente em discussão pelo Congresso Nacional sobre proteção de dados, elaboramos as recomendações a seguir:

### a. Transparência

**a.1. Especificação das fontes:** todo dado utilizado deve ter a atribuição clara de sua fonte para que sejam elucidados quaisquer questionamentos quanto à legitimidade de

---

84 “*Big Data* é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.” In Instituto de Tecnologia e Sociedade. *Big Data* no projeto Sul Global Relatório sobre estudos de caso. RIO DE JANEIRO 2016. Disponível em [http://itsrio.org/wp-content/uploads/2016/03/ITS\\_Relatorio\\_Big-Data\\_PT-BR\\_v2.pdf](http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf). Acesso em 27.01.2017. P. 9.

seu uso, facilitando igualmente traçar e reconhecer a origem de problemas com informações inexatas ou com problemas de qualidade. Importante ressaltar que à maior transparência corresponde maior confiança da sociedade acerca da legitimidade do sistema.

**a.2.** Sempre que necessário, seja para cumprimento de obrigação legal ou para alertar sobre o uso de informações pessoais em hipóteses que excedam as expectativas de seus titulares, o bureau deve tomar as providências necessárias para, de forma ativa, levar ao conhecimento dos titulares de dados sobre o tratamento e as informações relevantes a este respeito.

**a.3.** Os procedimentos a serem utilizados na análise dos dados pessoais, seja quanto à mineração destes seja quanto à inteligência analítica e algoritmos utilizados, deverão ser tornados públicos, de forma que sejam claros e compreensíveis ao titular dos dados os parâmetros principais destas operações e seus possíveis resultados, bem como seus potenciais efeitos para o titular. Eventuais restrições quanto à propriedade intelectual e segredo comercial relacionados à divulgação de algoritmos utilizados, antes que uti-

lizados como justificativas para a opacidade do sistema como um todo, devem fomentar a elaboração de estratégias que permitam ao cidadão ter ciência e segurança quanto aos elementos básicos e fundamentais do funcionamento do sistema de processamento de seus dados para que possa ter ciência das suas consequências e ter elementos para identificar e notificar por eventuais abusividades quanto ao tratamento de seus dados e a operação do sistema.

**a.4.** Os *bureaux* deverão requerer dos destinatários de seus serviços que sejam transparentes perante o titular dos dados caso venham a ter acesso a seus dados pessoais, assumindo o compromisso de alertar publicamente que estão tendo acesso a estes, a finalidade da sua utilização e quaisquer outros elementos que sejam de interesse do titular dos dados.

**a.5.** Os *bureaux* deverão estabelecer meios para a divulgação pública de suas práticas e operações realizadas com informações pessoais, incluindo a criação de espaço em seus portais exclusivamente para veicular tais informações.

**a.6.** Os *bureaux* devem estruturar mecanismos – no formato de uma ouvidoria, por exemplo – que possibilitem aos titulares dos dados exercerem seus direitos no que toca ao tratamento de suas informações pessoais, tais como acesso, retificação, conhecimento da fonte e das informações pessoais utilizadas em determinado tratamento.

## **b. Boa-fé**

**b.1.** Os procedimentos a serem realizados com os dados pessoais e as inferências e conclusões que deles poderão ser obtidos deverão respeitar as expectativas legítimas de seus titulares, consideradas estas como aquelas que possam ser consideradas legítimas em relação às finalidades para as quais os titulares esperam que seus dados sejam utilizados.

**b.2.** A utilização de dados pessoais deve ser um recurso do qual se lance mão com cuidado, procurando, sempre que possível, utilizar o mínimo de dados pessoais necessários para que uma determinada finalidade almejada seja alcançada e também utilizá-los somente quando esta finalidade não puder ser atingida por outros meios ou instrumentos.

**b.3.** O tratamento de dados não deverá ser realizado de forma a permitir a reidentificação de indivíduos ou grupos de indivíduos cuja identidade não era conhecida em alguma das bases de dados utilizadas em tal tratamento.

**b.4.** As informações fornecidas aos destinatários dos serviços dos *bureaux* deverão ser, sempre que possível, fornecidas em formato anônimo e com segmentação realizada de forma a dificultar a reidentificação dos titulares dos dados.

## **c. Proteção da personalidade**

**c.1.** Os serviços oferecidos aos clientes dos *bureaux* não poderão proporcionar ou facilitar a realização de práticas discriminatórias por seus clientes, não podendo, em nenhuma hipótese, se valer de informações sensíveis ou excessivas, ou ainda incompatíveis com as finalidades que razoavelmente poderiam ser vislumbradas pelo titular do dado no momento de sua coleta e, em particular, não realizar nenhum tipo de tratamento que, a despeito de ser feito a partir de dados pessoais legitimamente coletados, resulte em inferências ou conclusões que revelem dados sensíveis ou ensejem práticas discriminatórias.

## 5. Conclusão

Ao abordarmos conceitos como avaliação de risco e de seleção adversa, constatamos que a atividade desenvolvida pelos BdC é de grande importância para a economia nacional, o que, aliás, foi reconhecido por nossos tribunais. Por outro lado, essas empresas devem estar atentas aos potenciais riscos de discriminação negativa que sua atuação pode gerar, o que discutimos no capítulo 1 deste estudo, especialmente com relação a grupos vulneráveis, em razão da prática de generalização que realizam.

Identificamos, também, que apesar de não existir no Brasil uma norma específica que regule o tratamento de dados pessoais, tanto a legislação nacional quanto a jurisprudência do Superior Tribunal de Justiça e do Supremo Tribunal Federal trazem parâmetros que estabelecem limites claros para o tratamento de dados pessoais com a finalidade de análise de risco para fins de obtenção de crédito.

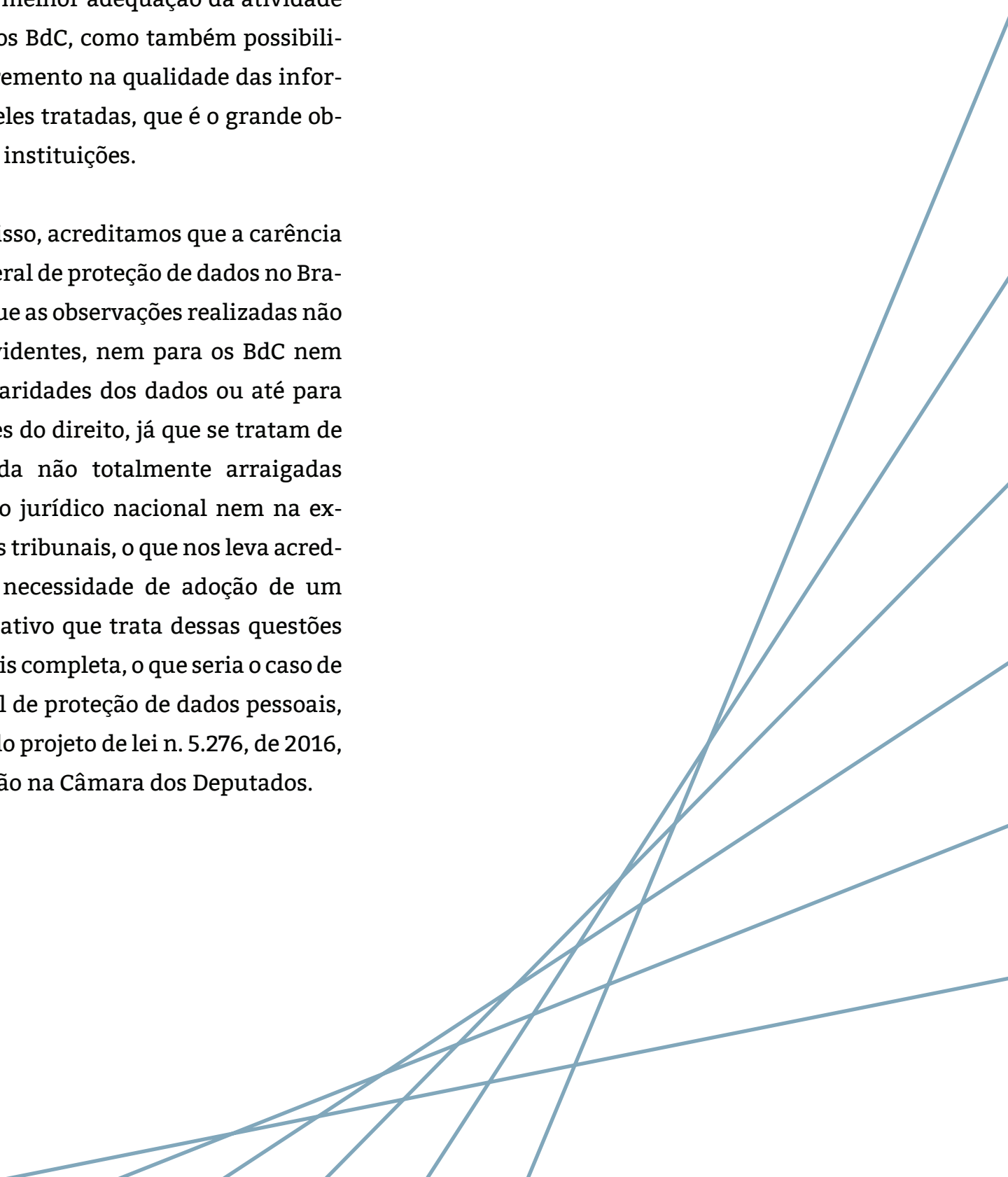
Com base nesses parâmetros realizamos análise da conformidade da coleta e tratamento de dados efetuada pelos BdC objeto de

análise e constatamos que o item de maior preocupação diz respeito à transparência no que toca à atuação dessas entidades, em especial com relação às fontes das informações e até mesmo das informações utilizadas. Nessa linha, identificamos, ainda, que inexistem canais de comunicação próprios para que o titular dos dados possa exercer, de forma facilitada e informada seus direitos relativos ao tratamento de seus dados pessoais.

Diante desse cenário apresentamos uma série de recomendações de boas práticas a serem observadas pelos BdC, divididas em três eixos: transparência, boa-fé e proteção da personalidade, com o que acreditamos que a atuação dessas entidades irá estar mais em consonância com os ditames trazidos pelo nosso ordenamento jurídico e os aproximará dos titulares dos dados que, por duas vias, são a grande fonte e finalidade do seu negócio, visto que são a matéria prima do serviço que oferecem – por meio de seus dados pessoais – e são a razão de contratação dos seus serviços pelas instituições financeiras – por serem os tomadores de crédito.

Portanto, aproximar as duas pontas dessa operação, BdC e titular de dados, não apenas propiciará a melhor adequação da atividade exercida pelos BdC, como também possibilitará um incremento na qualidade das informações por eles tratadas, que é o grande objetivo dessas instituições.

Apesar disso, acreditamos que a carência de uma lei geral de proteção de dados no Brasil faz com que as observações realizadas não sejam tão evidentes, nem para os BdC nem para os titularidades dos dados ou até para os operadores do direito, já que se tratam de questão ainda não totalmente arraigadas no arcabouço jurídico nacional nem na experiência dos tribunais, o que nos leva acreditar que há necessidade de adoção de um marco normativo que trata dessas questões de forma mais completa, o que seria o caso de uma lei geral de proteção de dados pessoais, nos moldes do projeto de lei n. 5.276, de 2016, em tramitação na Câmara dos Deputados.



# Anexo 1: Tabelas com os dados utilizados pelos BdC analisados

## Informações pessoais

### Disponibilidade

### Comentário

1. CPF	pública	O acesso público ao CPF é somente realizado de forma individualizada. Discute-se se é dado que possa ser considerado como fornecido publicamente em lote
2. Nome	pública	Disponível no registro civil
3. Situação Insc. CPF	pública	Disponível via Receita Federal (a partir do nome)
4. Data Nascimento	pública	Disponível no registro civil
5. RG	privada	–
6. Grau de Instrução	privada	–
7. Naturalidade	pública	Registro civil
8. Estado Civil	pública	Registro civil
9. Cônjuge	pública	Registro civil
10. Ocupação	privada*	Dados públicos somente para servidores públicos
11. Empregador	privada*	Dados públicos somente para servidores públicos
12. Profissão	privada*	Eventualmente a informação pode ser pública para categorias que tenham o rol de inscritos aptos a praticar a profissão público

## Endereço pessoal

### Disponibilidade

### Comentário

1. Logradouro

privada\*

Informações sobre endereço não podem ser consideradas públicas. Elas podem estar disponíveis em alguma base de dados à qual se tenha acesso (seria necessária a indicação)

2. Número

privada\*

Idem

3. Complemento

privada\*

Idem

4. CEP

privada\*

Idem

5. Bairro

privada\*

Idem

6. Município

privada\*

Idem

7. UF

privada\*

Idem

## Outras informações

### Disponibilidade

### Comentário

Sexo

pública

Disponível no registro civil

Nome da mãe

pública

Disponível no registro civil

NIS

privada\*

Necessário verificar a origem desta informação. Esse cadastro é gerido pelo Ministério da Previdência Social e sua divulgação não é pública. Eventualmente essa informação pode ter sido obtida diretamente do titular do dado.

Classificação de índice de desenvolvimento urbano (Data-Geo)

pública

Disponível no IBGE e relacionada à cidade, portanto, ao endereço do titular do dado.

Código do IBGE

pública

Disponível no IBGE

Estilo de vida

privada

Necessário verificar a origem desta informação. Não há um banco de dados conhecido a respeito, portanto as informações devem ser resultantes do cruzamento de diversas fontes.

Classe Social

privada

Idem

Escolaridade

privada

Idem

Classe de Risco

privada

Idem

Classe de propensão de consumo

privada\*

Idem

Georreferenciamento

privada

Informações sobre georreferenciamento não podem ser consideradas públicas. Elas podem estar disponíveis em alguma base de dados a qual se tenha acesso (seria necessária a indicação)

E-mail

privada\*

Endereço de e-mail, assim como outras informações de contato, somente podem ser consideradas de acesso público no caso de servidores públicos.



## Informações profissionais

Profissão

### Disponibilidade

privada\*

### Comentário

Eventualmente a informação pode ser pública para categorias que tenham rol público de inscritos aptos a praticar a profissão

## Endereço profissional

1. Logradouro

privada\*

### Comentário

Endereço e informações de contato, da mesma forma, somente podem ser consideradas de acesso público no caso de servidores públicos.

2. Número

privada\*

Idem

3. Complemento

privada\*

Idem

4. CEP

privada\*

Idem

5. Bairro

privada\*

Idem

6. Município

privada\*

Idem

7. UF

privada\*

Idem

## Notações de inadimplência

### Disponibilidade

### Comentário

1. Protestos

pública

-

2. Ações Judiciais executivas, de busca e apreensão, de execução fiscal federal, estadual e municipal

pública

-

3. Participação em insucessos empresariais

privada\*

Necessário verificar a origem desta informação. Não há um banco de dados conhecido a respeito, portanto as informações devem ser resultantes do cruzamento de diversas fontes. De toda forma, como interessam os dados pessoais, esta informação somente é relevante para análise no que tange à pessoa natural dos sócios.

4. Cheques sem fundos, extraviados, sustados, cancelados e roubados

privada\*

O cadastro de emitentes de cheques sem fundos mantido pelo Banco Central é de consulta restrita, não podendo ser equiparado a dados públicos, remanescendo o dever de notificação por parte da Serasa em caso de negativação derivada de tais informações." REsp 1033274, Min. Luis Felipe Salomão, julg. 06.08.2013.

5. Pefin/Refin

privada\*

Produtos fornecidos e administrados pela própria Serasa

## Outras anotações

	Disponibilidade	Comentário
1. Grafia semelhante em outro CPF	pública	Disponível no registro civil
2. Outras grafias no mesmo CPF	pública	Disponível no registro civil
3. Registro de consultas a cheque	privada*	Necessário verificar a origem desta informação. Esse cadastro é gerido pelo Ministério da Previdência Social e sua divulgação não é pública. Eventualmente essa informação pode ter sido obtida diretamente do titular do dado.
4. Registro de consultas a crédito	privada*	Disponível no IBGE e relacionada à cidade, portanto, ao endereço do titular do dado.
5. Participação societária	pública*	Disponível no IBGE
6. Documentos roubados e extraviados	privada*	Necessário verificar a origem desta informação. Não há um banco de dados conhecido a respeito, portanto as informações devem ser resultantes do cruzamento de diversas fontes.
7. Contumácia de sustação	privada*	Idem
8. Compromissos e hábitos de pagamento da própria instituição	não aplicável	Idem

## Flags

## Disponibilidade

## Comentário

1. Flag restritivo

privada\*

Acessível a clientes do bureau

2. Flag de PPE

privada\*

Acessível a clientes do bureau

3. Flag de Sócios

privada\*

Acessível a clientes do bureau (esta informação deve ter como base a participação societária disponível na Junta Comercial ou no Registro Civil de Pessoas Jurídicas)

4. Flag de Atividade de Crédito

privada\*

Acessível a clientes do bureau

5. Flag Óbito

pública

Disponível no registro civil

6. Flag Not Call

pública

Disponível nos procons e outros órgãos públicos que gerem bancos de dados de bloqueio do recebimento de ligações de *telemarketing*

7. Participação societária

pública

Disponível na Junta comercial ou Registro Civil de Pessoas Jurídicas