



Instituto  
de Tecnologia  
& Sociedade  
do Rio

**Versão resumida**

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

# Introdução

Este estudo analisa a utilização de dados pessoais - coleta, tratamento e acesso - por bureaux de crédito<sup>1</sup> (“BdC”), com foco nos eventuais impactos que tal uso têm para grupos vulneráveis, visando identificar melhores práticas para tornar a relação entre BdC e titulares de dados pessoais mais transparente e informada. O 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 pode acarretar condutas discriminatórias na concessão de crédito. Na segunda apresentamos o panorama legislativo brasileiro relativo à proteção de dados pessoais. Finalmente, na última parte, apresentamos nossas conclusões acerca dos mecanismos de acesso de dados oferecidos por bureaux de informação, a partir da análise dos termos de uso dos serviços oferecidos pelo Serasa-Experian

(em relação ao serviço Mosaic) e Boa Vista, bem como tecemos considerações acerca de melhores práticas a serem adotadas por serviços ofertados por bureaux de informação no que se refere à coleta, ao tratamento e ao acesso de dados de terceiros. A metodologia utilizada consistiu em análise jurídica dos contratos de prestação de serviços desses BdC disponíveis tanto em suas próprias páginas de internet quanto em páginas de entes públicos com os quais os BdC mantêm contrato, assim como análise das informações sobre os produtos disponibilizados e as informações tratadas por tais BdC encontradas em suas páginas de internet.

---

1 Bureaux (ou birô, no vernáculo) de crédito tradicionalmente e 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.

# 1. Crédito e discriminação<sup>2</sup>

## 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>3</sup> o qual verifica a probabilidade de uma pessoa ser devedora<sup>4</sup> e, após, a aloca em determinada categoria de risco, de modo a fundamentar decisões relativas à concessão de crédito<sup>5</sup>, taxa de juros<sup>6</sup> e eventual conclusão do contrato.<sup>7</sup>

Para que essa análise possa ser realizada, os BdC buscam obter o máximo de informa-

2 As traduções constantes do texto foram realizadas pelos autores deste relatório.

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

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

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

6 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.

7 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.

ções possíveis sobre seus potenciais clientes, tais como informações concernentes a hábitos e, condição econômica<sup>9</sup> e, ainda, outras que possam não estar diretamente ligadas à capacidade creditícia, como, por exemplo, informações sobre saúde, incluindo aquelas sobre dados genéticos.<sup>10</sup>

A pesquisa de informações sobre consumidores para o fim de concessão de crédito foi inicialmente desenvolvida no país pelo setor comercial, através de associações como as Câmaras de Dirigentes Lojistas (“CDLs”), e por instituições financeiras. 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 surgi-

8 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.

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

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

ram no Rio de Janeiro, São Paulo e em outras unidades da federação, dotando diversas cidades com os chamados ‘serviços de proteção ao crédito’, visando conferir maior segurança à 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, 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, cartórios de protestos de títulos ou tribunais de justiça para dados sobre ações judiciais) 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 restringe à mera análise de crédito. Alguns BdC passaram, com o tempo, a oferecer outros tipos de serviço 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 ex-

trair 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. Neste estudo, contudo, consideraremos titulares apenas pessoas naturais, salvo alguma referência específica, visto que as considerações e conclusões adotadas dizem respeito àquelas que acometem estas pessoas.

Além de “titular de dados”, utilizaremos também “cliente em potencial”, “cliente” e

“consumidor” para tratar da pessoa a respeito da qual se referem as informações que estão sendo coletadas e tratadas. Essas nomenclaturas diferenciam o momento contratual em que se encontram tais pessoas - antes da tomada de crédito ou durante esta relação - ou se referem à nomenclatura específica utilizada por determinadas leis, como o Código de Proteção e Defesa do Consumidor (“CDC”), que utiliza “consumidor”, ou o projeto de lei geral de proteção de dados pessoais em tramitação na Câmara dos Deputados, que utiliza “titular de dados”.

## 1.2. Generalização e discriminação

Os BdC baseiam boa parte de suas decisões em generalizações. A generalização ocorre quando um grupo inteiro de pessoas é tratado do mesmo modo por conta do comportamento de alguns membros do grupo<sup>11</sup>. Dessa forma, quando os BdC analisam um grupo de clientes para criar um perfil de risco ou ainda quando analisam riscos individuais, fazem-no com base em comportamentos anteriores de outras pessoas que tenham características semelhantes, considerando

11 SCHAUER, Frederick. Profiles, Probabilities and Stereotypes. Cambridge, Massachusetts: Belknap Press of Harvard University Press, 2003. P. 3.

dados como idade, gênero, etnia ou até domicílio, como no uso do CEP da residência<sup>12</sup>.

Por um lado, essa generalização é necessária em razão da assimetria de informações entre clientes e fornecedores de crédito. Entretanto, por outro lado, esse tipo de generalização pode criar distorções sobre indivíduos ou grupos de indivíduos, particularmente entre aqueles em situação vulnerável, ou entre aqueles que se comportam de maneira desviante. Um exemplo disso é o valor do seguro de automóvel para jovens recém habilitados a motoristas, que se apresenta consideravelmente mais alto em relação ao de outros adultos<sup>13</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, ainda que esses jovens motoristas jamais venham a causar um acidente de trânsito.

O grande problema da generalização é a discriminação que pode ocasionar, uma vez que indivíduos desviantes do grupo alvo não têm oportunidade de demonstrar que as

12 Ibid; p. 4.

13 Ibid. p. 4.

generalizações feitas sobre o grupo não se aplicam a eles e que isso lhes pode ser prejudicial em determinadas circunstâncias<sup>14</sup>. Por outro lado, em muitas situações a generalização traz benefícios: no exemplo acima do jovem motorista, caso o preço do seguro fosse o mesmo para os que causam e os que não causam acidentes, a consequência seria um aumento geral no valor do seguro. Este mesmo raciocínio vale para a concessão de crédito.

### 1.3. Seleção adversa

A coleta e tratamento de informações pessoais<sup>15</sup> têm como finalidade reduzir a assimetria de informações na relação entre fornecedores e clientes e consequentemente a seleção adversa<sup>16</sup>. Em determinadas situações a assimetria de informações entre o titular dos dados e o fornecedor de crédito é inevitável, seja porque o potencial cliente não disponibiliza a informação voluntariamente ou porque esta, ainda que volun-

tariamente fornecida, tem sua utilização legalmente vedada, como no caso da Lei do Cadastro Positivo.<sup>17</sup> Nessas situações os BDC desempenham papel fundamental, pois conseguem reunir informações de outras fontes que não exclusivamente as fornecidas pelo titular dos dados.

Dessa forma, no caso da concessão de crédito, 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 e, nessas situações, o BDC presta um serviço importante ao fornecedor de crédito, reduzindo 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.

---

<sup>17</sup> 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.

---

<sup>14</sup> Op. cit.; p. 50.

<sup>15</sup> 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”.

<sup>16</sup> BAKER, Tom. Op. cit.; p. 2.

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 discriminação na concessão 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<sup>18</sup>.

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 buscamos identificar os limites trazidos tanto pela legislação quanto pela jurisprudência nacionais, notadamente do Superior Tribunal de Justiça, para a coleta e tratamento de

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

dados por parte dos BdC.

#### **1.4. Grupos vulneráveis**

Antes de realizarmos a análise dos limites delineados tanto pela legislação quanto pela jurisprudência nacionais no que toca à coleta e tratamento de dados por BdC, importante efetuarmos um recorte no que toca aos grupos considerados vulneráveis e o impacto que a segmentação para fins de concessão de crédito pode ter para as pessoas integrantes destes grupos.

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>19</sup>

Conforme discutido no tópico anterior,

---

19 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.

generalizações podem gerar distorções que algumas vezes afetam de maneira desproporcional alguns grupos, em particular aqueles em situação de vulnerabilidade.

No Brasil, a discriminação para fins de concessão de crédito teve sua licitude reconhecida pelo Superior Tribunal de Justiça<sup>20</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. Portanto, 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.

Neste contexto é importante destacar, ainda, que determinados outputs considerados, por exemplo, negativamente discriminatórios, sejam consolidados a partir da análise de dados que não identifiquem diretamente a natureza específica que caracteriza a vulnerabilidade de um grupo, porém funcionem como ligação para esta caracte-

terística. 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.

---

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



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

### 2.1. 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>21</sup>.

As únicas normas que tratam especificamente do tratamento de dados pessoais, além do remédio constitucional do habeas data, e que, por isso, merecerão atenção especial neste estudo, são o CDC<sup>22</sup>, a Lei do Cadastro Positivo<sup>23</sup>, a Lei de Acesso à Informação (LAI)<sup>24</sup> e o Marco Civil da Internet, este último com relação aos dados coletados online.

### 2.2 Fontes de Informação e seu uso para fins de concessão de crédito

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

O art. 31 da Lei 12.527/11 (LAI) prevê que as informações pessoais relativas à intimidade, vida privada, honra e imagem “terão

<sup>21</sup> Nesse sentido é o art. 52 do Código Civil.

<sup>22</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>23</sup> Lei n.º 12.414, de 2011.

<sup>24</sup> Lei n.º 12.527, de 2011.

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”. Inere-se, 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 Municípios, ao definir informação pessoal como “aquela relativa à intimidade, à vida privada,

à honra e à imagem das pessoas”<sup>25</sup>, repetindo a redação do art. 3º, V, do Decreto 7.724/12, que regulamentou a LAI.<sup>26</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 esferas 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

---

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

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

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.

Desta forma, considerando-se o conjunto de meios hoje disponíveis para o tratamento de dados pessoais<sup>27</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, 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.

---

<sup>27</sup> 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.

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>28</sup>

<sup>28</sup> Art. 23. São consideradas imprescindíveis à segurança da 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

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.

De acordo com o princípio da finalidade, o motivo da coleta ou fornecimento de uma informação pessoal deve ser compatível com

---

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.

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 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.

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

O CDC 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. Vale destacar, contudo, que o Superior Tribunal de Justiça a partir da edição do julgamento do caso sobre credit scoring e edição da súmula 550 afastou a exigência de consentimento do consumidor nesses casos.

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

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. 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. 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, ao contrário do CDC, exige o consentimento por parte do titular para que seus dados sejam coletados e tratados.

Portanto, 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.

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. 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 BdC, eis que muitas vezes essas entidades se valem de informações coletadas na Internet. Além disso, 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.

## 3. Estudos de Casos

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 (Serasa Experian e Boa Vista) tendo sido realizado um cotejo da transparência e natureza das informações pessoais que os alimentam, o que baseou a formulação de recomendações de boas práticas a serem implementadas pelo setor.

### 3.1. 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. Tal complexidade se reflete não apenas no elevado volume de dados passível de tratamento por estes mecanismos de forma automatizada mas também pela opacidade inerente a eles.

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. 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 também 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. Assim, 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, o que torna difícil a aplicação de mecanismos convencionais de transparência.

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. Além deste fator de ordem concorrencial, alguns algoritmos apresentam mecanismos tão complexos que dificultam ainda mais qualquer ganho objetivo em relação à transparência. Neste ponto são destaque os algoritmos que “aprendem” a partir dos dados com os quais são alimentados e que, a partir destes, modificam-se a si próprios e ao seu funcionamento, sendo que seu output não é a rigor passível de ser antecipado nem mesmo pelos seus idealizadores ou programadores, dada 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>29</sup>.

29 O tema foi abordado em detalhe em: Solon Barocas & An-



Como forma de fazer frente a este problema, diversas linhas de ação vêm sendo 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>30</sup>.

### **3.2. Utilização de dados pessoais por bureaux e data brokers: apresentação e análise e recomendação de melhores práticas**

No Brasil, diversas empresas vêm oferecendo em seu portfólio serviços de análise de informações pessoais para fins diversos de avaliação. A partir do estudo de caso de serviços oferecidos por 2 bureaux que desempenham este tipo de atividades no Brasil, nomeadamente Serasa-Experian - em relação ao serviço Mosaic - e Boa Vista, elaboramos

recomendações de melhores práticas, de forma a se cotejar transparência e natureza das informações pessoais que os alimentam.

---

drew Selbst. Big Data's Disparate Impact. In 104 California Law Review (2016).

30 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).

## 4. Recomendação de melhores práticas

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 recomendações relacionadas à transparência, boa-fé e proteção da personalidade.

No que toca à transparência, o foco está na disponibilização pelo bureau disponibilizar aos titulares dos dados a atribuição clara de sua fonte para que sejam elucidados quaisquer questionamentos quanto à legitimidade de seu uso, facilitando igualmente traçar e reconhecer a origem de problemas com informações inexatas ou com problemas de qualidade, assim como na necessidade de criação de uma estrutura de ouvidoria que possibilite aos titulares dos dados o exercício dos direitos a eles atinentes.

Em relação à boa-fé, os procedimentos a serem realizados com os dados pessoais e as

inferências e conclusões que deles poderão ser obtidas 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.

Por fim, no que toca à proteção da personalidade, 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

Atividade desenvolvida pelos BdC é de grande importância para a economia nacional. Por essa razão e considerando ainda a expansão desta atividade nos últimos anos, os BdC devem estar atentos aos potenciais riscos de discriminação negativa que sua atuação pode gerar. Neste sentido, apesar de não existir no Brasil norma específica que regule o tratamento de dados pessoais, tanto a legislação quanto a jurisprudência dos tribunais superiores 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.

A análise jurídica da conformidade da coleta e tratamento de dados efetuada pelos BdC objeto de análise constatou 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 às próprias informações utilizadas. Identificamos, ainda, que inexistem canais de comunicação próprios para que o titular dos dados possa exercer, de forma fa-

cilitada e informada seus direitos relativos ao tratamento de seus dados pessoais.