

Big Data: ranking dos cidadãos como instrumento de controlo social

Leandro César Borboleta Nogueira

**Dissertação de Mestrado em Ciências da Comunicação
Cultura Contemporânea e Novas Tecnologias**

Mai de 2020

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Ciências da Comunicação – Cultura Contemporânea e Novas Tecnologias, realizada sob a orientação científica do Professor Doutor Jorge Manuel Martins Rosa.

À Tica, por tudo.

Agradecimentos

A Deus.

Aos meus pais e irmãos, pela dedicação e carinho.

À Carol e família, pelo apoio e torcida.

Ao professor Jorge Martins Rosa, pela oportunidade e orientação.

Ao Miro Braga, pela atenção e comentários oportunos.

Ao Paulo Rocha, pelas dicas e estímulo.

Ao Miguel Hosken, pelo apoio e logística.

À Carol Delmazo, pela atenção em todos os momentos.

Ao Pery Negreiros e a Lorena Alves, pela acolhida e pela República do Ceará.

Ao Marcus Madeira e a Jocasta Luiza pela disponibilidade, receptividade e companheirismo.

A todos os amigos, pelo incentivo e apoio nessa aventura além-mar.

Big Data: ranking dos cidadãos como instrumento de controle social

Leandro César Borboleta Nogueira

RESUMO

As mudanças trazidas pela associação entre metodologias de informação e tecnologia possibilitaram alterações significativas para as sociedades industrializadas. Atualmente, o controle, a disciplina e a segmentação são potencializados pela combinação de dados e algoritmos.

Esta dissertação pretende contribuir para o debate acerca da relação das novas tecnologias da informação e metodologias de controle social, verificando como tais métodos são responsáveis por sistemas que promovem, com distintas finalidades, a categorização e o *ranking* de indivíduos.

Baseando-se na análise e contextualização de diferentes modelos, toma-se como exemplos três metodologias, sendo elas: o sistema de crédito social chinês, sistemas de governança, gerenciamento de riscos e conformidade de princípios e o cadastro positivo brasileiro.

Abordando a responsabilização sobre o uso de tais metodologias e visando contribuir para a discussão sobre os impactos da utilização de máquinas em decisões que afetam diretamente as sociedades contemporâneas, busca-se verificar a hipótese de que tais modelos podem fomentar o crescimento das diferenças sociais e econômicas.

Palavras-chave: Big Data, algoritmos, controle, disciplina, crédito social, cadastro positivo.

ABSTRACT

The changes brought about by the association between information and technology methodologies have enabled significant changes for industrialized societies. Currently, control, discipline and segmentation are enhanced by the combination of data and algorithms.

This dissertation intends to contribute to the debate about the connection between new information technologies and social control methodologies, verifying how these methods are responsible for systems that promote, with different purposes, the categorization and ranking of individuals.

Based on the analysis and contextualization of different models, three methodologies are taken as examples, namely: the Chinese social credit system, governance systems, risk and principle compliance management and the Brazilian “positive register”.

Addressing accountability on the use of such methodologies and aiming to contribute to the discussion on the impacts of the use of machines on decisions that directly affect contemporary societies, this study seeks to verify the hypothesis that such models can foster the growth of social and economic inequalities.

Keywords: Big Data, algorithms, control, discipline, social credit, positive register.

Índice

Introdução	1
Capítulo 1: Big Data: informação e tecnologia.....	5
1.1. Predição.....	11
1.2. Exclusão	13
Capítulo 2: Algoritmos: da origem ao controlo	17
2.1. Vigilância: o fim da privacidade.....	21
2.2. Pós-panóptico: o novo guardião.....	26
Capítulo 3: Controlo: disciplina, economia e sociedade.....	29
3.1. Categorização social	30
3.2. Credibilidade financeira.....	33
3.3. Metodologia	34
Capítulo 4: Modelos: oriente e ocidente	36
4.1. Sistema de Crédito Social	36
4.1.1. Tabela de Suining	38
4.1.2. O teste do Sistema de Crédito Social.....	39
4.2. Governança, gerenciamento de riscos e conformidade de princípios.....	40
4.2.1. Algoritmos e a justiça	42
4.2.2. Polícia de Chicago	42
Capítulo 5: Cadastro Positivo: o modelo brasileiro	44
5.1. Brasil: o fator desigualdade	49
5.2. Dados sensíveis.....	53
5.3. Score de crédito.....	55
5.4. O Novo Cadastro Positivo	58
5.5. Gestores do Novo Cadastro Positivo	61
5.6. LGPD e RGPD.....	63
Conclusão.....	65
Referências bibliográficas.....	69
Anexos	75

Introdução

Modelos são opiniões embutidas na matemática (O'Neil, 2016, p. 27).

A afirmação da matemática e autora estadunidense Cathy O'Neil, em seu livro *Weapons of Math Destruction* (Armas de Destruição Matemática), apresenta-nos o risco ou, ao menos, o temor em relação à autonomia e ao uso dos modelos matemáticos, sintetizados pelos algoritmos, para solução de problemas em todas as sociedades contemporâneas. A exatidão matemática é utilizada como argumento para a construção de modelos que, apesar de sua reputação de imparcialidade, refletem objetivos e ideologias, podendo, assim, aprofundar as diferenças socioculturais e econômicas. Com os algoritmos do *machine learning*, as máquinas podem aprender e amplificar preconceitos dos mais variados tipos, como de raça, gênero, credo, etnia, classe social e posicionamento político, ampliando as possibilidades de segmentação e desigualdade.

Valendo-se do Big Data e de características como conectividade, ritmo de inovação e onipresença, os sistemas de controlo executam, de forma quase invisível, um levantamento total de dados sobre os cidadãos e estabelecem uma normatização em relação às ações dos sujeitos. Os indivíduos são confrontados por dispositivos de controlo em praticamente todas as ações do quotidiano, o monitoramento e o registro funcionam por meio de aplicativos de *smartphones*, *sites* privados ou governamentais, máquinas de cartões de crédito, câmeras de segurança e redes sociais, entre outros. Contemporaneamente, no entanto, todos os pedaços da existência humana podem ser “visíveis” porque muito de quem nós somos é rastreado e apresentado através de tecnologias de *media* digitais (Cirucci, 2018, p. 17).

Neste trabalho propusemos apresentar exemplos de como governos e grandes corporações, valendo-se do uso de novas tecnologias, do Big Data e modelos matemáticos, estabelecem o funcionamento de sistemas preditivos e excludentes que balizam o desenvolvimento de políticas públicas e institucionais, podendo representar o aprofundamento de diferenças sociais e econômicas. As redes digitais e as demais tecnologias da informação facilitam a estratificação das populações, estabelecendo *rankings*, pois, assim como no “ban-óptico” proposto por Agamben (2004), ao criar mecanismos de previsão que identificam os indivíduos e ao mesmo tempo definem o

que eles vão fazer e/ou desejar em um futuro próximo, a exclusão dos sujeitos “indesejados” ocorre com ares de naturalidade.

Modelos como o sistema de crédito social, sistemas de governança, gerenciamento de riscos e conformidade de princípios e o cadastro positivo fazem uso de todo tipo de informação disponibilizada pelos cidadãos para estabelecer um *ranking* social e econômico, que Foucault trata como Disciplina: um dispositivo funcional que deve melhorar o exercício do poder, tornando-o mais rápido, mais leve, mais eficaz, um desenho das coerções sutis para uma sociedade que está por vir (1999, p. 232). Na perspectiva de Deleuze, tais modelos se enquadram como ferramenta de controle, potencializando a triagem social. O Controle é de curto prazo e de rotação rápida, mas também contínuo e ilimitado, ao passo que a disciplina era de longa duração, infinita e descontínua (1992, p. 224).

A vigilância, que na estrutura arquitetônica do Panóptico, de Jeremy Bentham, deveria ser realizada pelo guardião que ficava na torre central vigiando as celas ao redor, passa a ser efetivada pelos *bits* e *bytes* de informações fornecidas espontaneamente por milhares de cidadãos, sendo analisados e categorizados por máquinas. Sistemas que, por sua vez, são formatados com ações e impressões humanas. É importante lembrar que aqueles que têm o poder de criar estruturas digitais são os que controlam o que se naturaliza como normas sociais (Cirucci, 2018, p. 17).

Disciplina e vigilância continuam sendo pilares do modelo, como pensado por Bentham, mas com o avanço e associação das tecnologias da informação inerentes à contemporaneidade, ele passa a ser lido por Bauman (2014) como um Pós-panóptico. Com informações que são fornecidas de forma voluntária pelos indivíduos, essa versão do controle potencializa o domínio das tecnologias da informação em que os dispositivos tecnológicos são responsáveis por moldar, junto aos bancos de dados, o perfil de cada sujeito, possibilitando a segmentação mercadológica, econômica e social. A discriminação passa a ser racional, balizada por modelos matemáticos que trabalham a favor de governos e grandes corporações, realizando um processo de estratificação social e encaminhando os indivíduos que não atendem aos requisitos dos modelos para a margem do mundo tecnológico/industrializado.

A justificativa para o desenvolvimento deste trabalho se baseia na pesquisa sobre os reflexos socioculturais e econômicos do conflito entre informação e privacidade. Trata da responsabilidade de transferir, para as máquinas, as tomadas de decisões que afetam milhares de pessoas em todo o mundo, principalmente as menos favorecidas social e economicamente. Quais são e/ou serão os resultados da aplicação desses sistemas nas sociedades? Ao tratar exemplos de diferentes países, o trabalho busca verificar semelhanças entre propostas que utilizam modelos matemáticos para estabelecer um controle social e/ou econômico.

Para desenvolvermos nossa linha de análise dos sistemas supracitados, começamos por pesquisar, no primeiro capítulo, o Big Data e algumas de suas perversas funcionalidades, como predição e exclusão. Bancos de dados não são uma novidade, mas as potencialidades oriundas de sua associação com as novas tecnologias da informação podem representar sérias ameaças à privacidade. Na contemporaneidade, praticamente todos os indivíduos inseridos no mundo industrializado alimentam diariamente o Big Data com novas informações, tornando os dados uma matéria-prima valiosa.

No capítulo seguinte, trabalhamos o histórico e aplicação dos algoritmos, pesquisando como sua utilização se tornou uma ferramenta para a efetiva funcionalidade da vigilância e do controle. No complexo mundo em que o “código é lei” (Lessig, 2006), os modelos matemáticos para tratamento de dados acabam por condicionar as ações de indivíduos, governos e corporações.

No terceiro capítulo, a pesquisa trata a questão do controle na sociedade contemporânea. Busca-se verificar como o desenvolvimento tecnológico, em relação ao tratamento de dados, oferece instrumentos que viabilizam tal modalidade. No quarto capítulo, são apresentados e exemplificados os funcionamentos do sistema de crédito social chinês e dos sistemas de governança, gerenciamento de risco e conformidade de princípios.

Por fim, no quinto capítulo, a pesquisa é desenvolvida acerca do cadastro positivo brasileiro. A entrada em vigor da Nova Lei do Cadastro Positivo balizou consideravelmente o desenvolvimento dessa pesquisa. Tal metodologia de histórico de crédito já recebia críticas, mesmo ainda em sua primeira versão, sobre quais seriam os resultados junto à sociedade. O novo modelo, endossado pelo Governo Federal e

gerenciado por instituições privadas, amplia consideravelmente o acesso a dados, oriundos de diferentes fontes, de mais de 100 milhões de cidadãos brasileiros.

Dois anos após entrar em vigor, ou seja, em julho de 2021, a Nova Lei do Cadastro Positivo deve passar por uma avaliação do Congresso Nacional. O objetivo é saber se a coleta, o armazenamento e análise de dados de milhares de cidadãos serviram para aumentar o acesso ao crédito e diminuir as taxas de juros. Mesmo com êxito em relação aos objetivos econômicos, a possibilidade de danos quanto à utilização indevida dos dados é considerável, pois a ferramenta que poderia atenuar tal possibilidade, a LGPD – Lei Geral de Proteção de Dados – só começa a entrar em vigor a partir de janeiro de 2021. Portanto, quando vigente, a lei estará fragilizada no que se refere a metodologia de tratamento de dados utilizada pelos *bureaus* responsáveis pelo cadastro positivo.

Será o novo cadastro positivo o melhor modelo para inclusão da parcela da população que não tem acesso a crédito? Ele irá ampliar o problemático quadro socioeconômico brasileiro? Levando-se em consideração, dentro da realidade brasileira, a falta de informação em relação à temática da proteção de dados, os níveis de pobreza e os baixos índices de acesso aos meios digitais, há possibilidade de que uma parcela significativa da população não tenha ciência sobre o recolhimento, tratamento, análise e utilização de seus dados, sem que jamais tenha autorizado.

1. Big Data: informação e tecnologia

(...) a maioria das pessoas, pelo menos no mundo industrializado, contribui rotineiramente e experimenta os efeitos do big data. Sob esse conceito, o big data é a baleia, e todos nós somos Jonas. (Lerman, 2013, p. 56)

O Big Data pode ser entendido como uma síntese do mundo informatizado/industrializado, uma abreviação da variedade de tecnologias utilizadas para coletar e analisar dados. Com expressivo crescimento e contendo informações de utilizadores de todas as partes do planeta ele é, a cada dia, mais valioso e está em constante expansão. A coleta dos dados ocorre a todo tempo e com uso de diferentes metodologias. Todo dispositivo eletrônico conectado à internet ou plataforma de interação ou navegação é potencial coletor de dados e a maioria da população do mundo informatizado contribui, espontaneamente, para o crescimento do Big Data. Qualquer indivíduo que utilize aplicações em telefones móveis e/ou computadores, realize pesquisas, compras ou transações via internet, por exemplo, fornece dados que são armazenados e processados. O objetivo é apresentar informações sobre os indivíduos, além de estabelecer padrões e conexões que seriam invisíveis sem a utilização dos dispositivos eletrônicos.

O Big Data é um dos elementos fundamentais para desenvolvimento de novas formas de controlo social e as sociedades informatizadas experimentam seus efeitos diariamente. Representa a maximização do poder do computador, permitindo a identificação de padrões que, muitas vezes, levam a mudanças econômicas, sociais e legais (Cirucci, 2018, p. 16). Ele diverge dos bancos de dados convencionais, geridos de acordo com padrões específicos e objetivos estabelecidos previamente, além de demandarem muito tempo para serem processados. Estima-se que em 2020 serão gerados 35 Zettabytes (10^{21} bytes) de dados¹. Os dados excedem a capacidade de processamento dos sistemas de base de dados convencionais. A sua dimensão e velocidade de circulação impossibilitam que se encaixem nalgumas estruturas existentes, daí a necessidade de desenvolver novas arquiteturas (Vicente, 2018, n. p.).

No Big Data, o processamento de fluxos contínuos de dados ocorre de maneira instantânea e os resultados são apresentados em tempo real, otimizando os processos

¹ <https://www.cision.pt/2018/08/big-data-conectividade-implicac%CC%A7o%CC%83es-e-desafios-parte-i/>

de coleta, análise e resultado. Suas características distintivas são: o volume, a variedade e a velocidade. “Os dados são o novo petróleo” é um provérbio popular, e, assim como aconteceu com o petróleo, refiná-los é um grande negócio (Domingos, 2017, p. 36-37).

A administração de informações por meio de banco de dados não é uma novidade. O desenvolvimento tecnológico é um fator que transformou as metodologias de coleta e análise. O Census Bureau, dos Estados Unidos da América, implantou o primeiro equipamento de processamento automatizado do mundo em 1890 – a máquina de cartões perfurados (Body e Crawford, 2012, p. 664).

Os dados se tornaram matéria-prima de grande valor econômico e social (Tene e Polonetsky, 2012) e o Big Data desencadeia retóricas utópicas e distópicas. Se por um lado é visto como uma ferramenta resolutiva para problemas sociais, proporcionando novas ideias sobre diferentes áreas, como pesquisas sobre o cancro, o terrorismo e as mudanças climáticas, por outro, é visto como manifestação preocupante do Big Brother, permitindo invasões de privacidade, diminuição das liberdades civis e aumento do controle estatal e corporativo (Body e Crawford, 2012, p. 663). Ainda segundo Body e Crawford, a definição de Big Data determina um elemento que transpassa e interage sob diferentes perspectivas fenomenológicas:

Nós definimos Big Data como um fenômeno cultural, tecnológico e acadêmico que repousa sobre a interação de: (1) *Tecnologia*: maximizar poder de computação e precisão algorítmica para reunir, analisar e comparar grandes conjuntos de dados. (2) *Análise*: baseando-se em grandes conjuntos de dados para identificar padrões, a fim de fazer reivindicações econômicas, sociais, técnicas e legais. (3) *Mitologia*: a crença generalizada de que grandes conjuntos de dados oferecem uma forma mais elevada de inteligência e conhecimento que pode gerar insights que antes eram impossíveis, com a aura de verdade, objetividade e precisão (2012, p. 664).

Além das perspectivas apresentadas por Body e Crawford, De Mauro, Greco e Grimaldi (2016) destacam um conjunto de quatro elementos que podem formatar uma síntese do Big Data. São eles: informação, tecnologia, métodos e impactos. Para os autores, os elementos não são novos, mas juntos, permitem a formulação de um

conceito que transita entre a tecnologia, o processamento de dados e a mudança de cultura das sociedades industrializadas.

É pela linha analítica do risco embutido no controlo e utilização do Big Data que esta pesquisa se desenvolve, buscando apresentar elementos que reforçam os danosos efeitos socioeconômicos dessa manipulação. Ao longo do trabalho serão abordadas e apresentadas questões que exemplificam os riscos e erros da utilização “opaca” do Big Data, por parte de agências governamentais, privadas ou por meio da associação entre governos e iniciativa privada.

Estados e corporações gerem e monitoram, cada vez mais, todos os aspectos da vida quotidiana dos cidadãos; o Big Data potencializa o desenvolvimento de estratégias preditivas de tomada de decisão, não permitindo aos indivíduos qualquer tipo de entendimento e/ou deliberação sobre as informações coletadas e suposições criadas sobre eles. Quando se considera que o Big Data pode ser usado para tomar decisões importantes, que nos envolvem sem que sequer saibamos, a tomada de decisão social preventiva é antitética à privacidade e aos valores do devido processo (Kerr e Earle, 2013, p. 71).

À medida que novos e poderosos atores dos mercados tecnológico e/ou financeiro, como Google, Amazon, Alibaba, JP Morgan, HSBC, concentram esforços para estabelecer e/ou ampliar o controlo sobre dados reunidos das mais variadas fontes, o Big Data apresenta suas transgressões institucionalizadas, pois cria conflitos de limites e potencializa a função dos algoritmos independentes, que reduzem a função e o controlo humano. Tais características serão abordadas mais adiante neste trabalho, mas sinalizam o potencial de mudanças que podem ser geradas pela administração do Big Data.

Jonathan King e Neil Richards apontam transparência, identidade e poder como três paradoxos do Big Data, pois representam potenciais de desenvolvimento e solução de problemas que afetam milhares de pessoas e, ao mesmo tempo, riscos iminentes à privacidade e ao sigilo. A produção de dados – coleta, análise e resultados – e as ferramentas necessárias para compreender a complexidade dos resultados são desenvolvidas por grandes corporações e/ou governos com metodologia que não se baseia na clareza das ações. Sob a chancela da total transparência, proporcionada pelo Big Data, e que, teoricamente, representa um mundo mais confiável, a privacidade

passa a ser um elemento ameaçado. A mesma transparência que pode representar o acesso dos menos favorecidos a outras esferas de poder cria uma relação desigual de distribuição do conhecimento, como afirmam os autores:

Primeiro, enquanto o Big Data coleta todos os tipos de informações privadas, as próprias operações estão quase totalmente envoltas em sigilo comercial. Chamamos isso de *Paradoxo da Transparência*. Segundo, embora os evangelistas do Big Data falem em termos de resultados milagrosos, essa retórica ignora o fato de que o Big Data procura identificar, à custa dos indivíduos, a identidade coletiva. Chamamos isso de *Paradoxo da Identidade*. E terceiro, a retórica do Big Data é caracterizada por seu poder de transformar a sociedade, mas o Big Data tem efeitos de poder próprios, que privilegiam grandes empresas e governos em detrimento de indivíduos comuns. Chamamos isso de *Paradoxo do Poder* (King e Richards, 2013, p. 41).

Hansen e Poter propõem acrescentar mais linhas argumentativas aos paradoxos propostos por King e Richards. Os autores adicionam o *Paradoxo dos Objetos* e o *Paradoxo dos Limites*. No primeiro, argumentam que o Big Data permite um grande desenvolvimento das capacidades cognitivas dos humanos, mas também dá lugar à crescente autonomia de objetos que, às vezes, trabalham contra as capacidades humanas. Embora esses processos acionados por máquinas sejam fabricados em última instância por seres humanos, os processos podem tornar a agência humana secundária e os poderes em funcionamentos invisíveis (Hansen e Poter, 2013, p. 33). Já o *Paradoxo dos Limites* é o reflexo da demanda por um aumento da abertura que permita a aquisição de dados e, conseqüentemente, a implementação dos seus efeitos. Porém, de acordo com os autores, essa liberação para o acesso pode representar uma nova forma de controlo atrelado ao poder econômico de grandes corporações:

O Big Data depende da exclusão de fronteiras, incluindo as nacionais que dificultam a montagem dos dados. No entanto, aqueles que gerenciam o Big Data trabalham através de estados e empresas privadas para criar limites novos e mais fortes para implantar Big Data como uma forma de controlo ou para criar direitos comercializáveis sobre uma parte do Big Data. (Hansen e Poter 2013, p. 34).

Os modelos de vigilância, que ainda serão exemplificados e analisados ao longo deste trabalho, também sofreram alterações com o advento do Big Data. Os grandes fluxos de informação potencializaram o surgimento de metodologias de análise e vigilância com grande capacidade de trabalhar o imenso volume de dados disponibilizados a cada momento em todo o planeta, estabelecendo um novo modelo de relação das grandes corporações e governos com a privacidade.

Em um primeiro momento, o modelo tradicional de vigilância tratava os dados como elementos capazes de representar racionalmente determinadas realidades. Após o avanço na metodologia de captura das informações, a tecnologia passa a agir diretamente sobre a realidade social, mas ainda sem modificar a relação das pessoas com o uso da tecnologia. Dessa maneira, os dados ainda seriam responsáveis por uma leitura simplificada da realidade.

No atual modelo de vigilância, capaz de ser executado exclusivamente com o uso do Big Data e denominado por Jens-Erik Mai (2016) como *Datification*, o principal elemento deixa de ser a coleta e passa a ser o processamento dos dados. Segundo Mai, o modelo é viabilizado porque o Big Data consolida a relação das forças das grandes corporações com a privacidade e se baseia na análise dos dados obtidos a todo tempo por meio de sensores, máquinas, pessoas, atividades, enfim, por qualquer dispositivo ou ser humano que seja capaz de produzir informações para o Big Data. Esta perspectiva pode ser observada quando o autor afirma que:

A era do Big Data exige uma reconceituação da noção de privacidade. Modelos anteriores de privacidade limitaram seu foco na coleta e reunião de dados como o mecanismo central da preocupação com a privacidade. Desse modo, a privacidade é vista como a capacidade de restringir o acesso à informação ou a capacidade para controlar o fluxo de informações pessoais. Na era do Big Data, uma preocupação mais importante é como as novas informações pessoais são produzidas por empresas e organizações através de análise preditiva. (Mai, 2016, p. 199 *apud* Silveira, 2017, p. 769).

Os dados passam a ser vistos como possibilidades de incidir sobre os fatos, dependendo do modo como são gerados, cruzados e processados. Assim, o

processamento e análise de dados é “epistemologicamente orientado” (Silveira, 2017, p. 770).

Com a análise de dados se tornando o bem mais valioso da nossa era, apenas o estabelecimento sensato de regras de utilização pode minimizar ou atenuar os danos causados pelo uso de informações sigilosas por parte das grandes corporações. Leia-se, aqui, corporações financeiras, como bancos, agências de avaliação de risco, de tecnologia e informação. O escândalo em torno do Facebook e da Cambridge Analytica sugere o poder dos dados, dos mercados de dados e do valor de análises para gerenciar opiniões de sujeitos (Grassegger e Krogerus, 2017). Nesta questão, o papel regulamentador dos governos é de fundamental importância, pois as leis de proteção de dados têm como objetivo o controle individual das informações. No entanto, não está claro que minimizar a coleta de informações seja sempre uma abordagem prática da privacidade na era do Big Data (Tene e Polonetsky, 2012). Ainda segundo os autores:

Os formuladores de políticas devem se envolver com essa questão normativa, considerar quais atividades são socialmente aceitáveis e definir as normas padrão de acordo. Ao fazer isso, eles devem avaliar o valor do uso de dados em relação a possíveis riscos à privacidade, examinar a praticabilidade de obter consentimento verdadeiro e informado e ter em mente a aplicabilidade das restrições aos fluxos de dados. (Tene e Polonetsky, 2012).

Com os avanços nas metodologias de recolhimento e classificação, não existe sequer um único dado que possa ser ignorado ou que tenha a sua importância diminuída. Uma informação que, aparentemente, não possui significativo valor, pode, dentro de outro aspecto de utilização, receber especial destaque. Tudo depende da finalidade para qual a coleta, a análise e o tratamento de dados são realizados. Eles podem, por exemplo, ser facilitadores de complexas ferramentas que têm como objetivo a previsão, no mínimo aproximada, de determinados resultados.

1.1 Predição

O exercício de prever há muito fascina a humanidade. Do obscurantismo à análise de dados, a previsão é meta dos que pretendem exercer variados tipos de poder sobre outros sujeitos. Saber o que o futuro pode apresentar, em diferentes aspectos e contextos, é a chave para o domínio intelectual e/ou financeiro de indivíduos e nações. Tratar a probabilidade como elemento científico foi um conceito que se desenvolveu nos últimos dois séculos e meio, principalmente nas investigações realizadas por filósofos e matemáticos. Na antiguidade, chamava-se, muitas vezes, “provável” àquilo que, segundo as aparências, pode ser declarado verdadeiro ou certo (Mora, 1978, p. 324-325).

As previsões baseadas no Big Data já informam decisões dos setores público e privado todos os dias em todo o mundo (Lerman, 2013, p. 57). Como por exemplo, o *LSI-R*, um modelo de reincidência, utilizado pelo sistema penal em vários estados norte-americanos (O’Neil, 2016). Ele é um questionário destinado aos prisioneiros e desenvolvido para auxiliar juízes na definição das penas. Mas presos de diferentes classes sociais e raças poderão fornecer respostas muito distintas, que estão diretamente ligadas aos contextos socioeconômico e cultural. Tal fato pode estabelecer diferentes condenações para crimes semelhantes, além de permitir que pessoas com menor nível de instrução tenham maior índice de condenação. Como aponta O’Neil:

E embora os negros representem apenas 13% da população dos Estados Unidos, eles preenchem 40% das celas das prisões do país (...) A questão, no entanto, é se eliminamos o viés humano ou simplesmente o camuflamos com tecnologia. Os novos modelos de reincidência são complicados e matemáticos. Mas embutida nesses modelos há uma série de suposições, algumas delas prejudiciais (O’Neil, 2016, p. 29).

Outro exemplo de modelo tecnológico que pode ser prejudicial a um determinado grupo de indivíduos é a ferramenta *Concentre Scoring*, utilizada pela Serasa *Experian*², no Brasil. A empresa detém o maior banco de dados da América Latina, fornecendo informações para grandes empresas, bancos e agentes financeiros.

² <https://www.serasaexperian.com.br/>

A ferramenta estabelece uma nota de 0 (zero) a 1000 (mil) para cada consumidor, com base nas informações relacionadas ao CPF – Cadastro de Pessoas Físicas (Borges *apud* Fortes *et al*, 2015, p. 2525). Várias ações foram levadas à Justiça brasileira, pois a empresa fornecia informações apenas aos agentes que cediam crédito e não aos consumidores, impossibilitando aos cidadãos consumidores o acesso aos próprios dados.

O Big Data faz uso das funcionalidades que resultam do avanço da ciência da probabilidade, em que o desenvolvimento apurado das análises de dados permite a definição de estratégias e ações de governos e grandes corporações, potencializando a obtenção de resultados que consiste em determinar, a partir de dados, a probabilidade estatística de uma determinada ação de um indivíduo ou de um grupo. A utilização de tal metodologia, baseada em dados de frequência, remonta a um passado não muito distante, como aponta Mora:

Desde o século XVIII, procurou-se considerar a doutrina da probabilidade como a arte de julgar sobre a maior ou menor admissibilidade de certas hipóteses com base nos dados que se tem. A noção de probabilidade esteve, por isso, estreitamente relacionada com a de indução (v.); pode, pois, falar-se de uma *probabilidade indutiva*. Especialmente neste último século e meio, trabalhou-se também sobre outro conceito de probabilidade: a chamada *probabilidade estatística*, de que um dos conceitos fundamentais é o de frequência. (Mora, 1978, p. 324).

A capacidade de realizar previsões confiáveis, baseadas em estatísticas, é extremamente lucrativa em sociedades informatizadas/industrializadas, pois ela otimiza a redução de riscos. Kerr e Erale (2013) apontam que serviços de previsão têm como objetivo permitir que os indivíduos escolham determinadas linhas de ação que melhor se enquadram aos próprios interesses e, dessa forma, minimizem os resultados negativos. Muitos desses serviços não geram previsões sobre condutas de utilizadores ou prováveis consequências de consumo. Oportunamente, eles tentam “acariciar” as preferências dos utilizadores/consumidores para executar a venda de bens e serviços. Muitos dos Big Data de hoje, nas indústrias, estão focados em projeções desse tipo de material, as quais chamamos de *previsões preferenciais* (p. 67). Mecanismos de busca, como o Google, por exemplo, potencializam a demanda

por previsões preferenciais, pois o sistema desenvolvido pela corporação prevê quais informações serão demandadas pelo utilizador, baseado em combinações de dados como localização e histórico de pesquisas.

Diferentemente das previsões preferenciais, os autores argumentam que *previsões preventivas* são uma metodologia utilizada para minimizar as possibilidades de opções futuras para determinadas ações dos indivíduos. Com auxílio de algoritmos, elas realizam avaliações sobre as consequências relacionadas com a permissão ou impedimento de determinadas ações. Os exemplos dessa metodologia estão presentes em *software* que determina listas de exclusão aérea, para inibir possíveis atividades terroristas e também a liberdade condicional para presos do regime fechado, tendo como base previsões futuras de comportamento. As previsões preventivas são feitas principalmente do ponto de vista do estado, de uma corporação ou de qualquer pessoa que deseje impedir certos tipos de ações (p. 67).

1.2 Exclusão

O debate acerca do Big Data e suas capacidades é recorrente na contemporaneidade. Seu poder de coleta e processamento de informações, como citado anteriormente, tem uma dimensão primária na história da humanidade e sua grandiosidade está muito além da capacidade de simples *software* de gerenciamento de dados. Mesmo com toda essa capacidade de captura e processamento de dados, ele fomenta, com grande potência, a exclusão de sujeitos, que, de alguma maneira, não têm suas preferências e necessidades enquadradas nos parâmetros analíticos. O Big Data formatou um novo modelo de vida moderna, baseado em um padrão que até agora ajudou a aprofundar as diferenças entre ricos e pobres em todo o planeta. Em suas inúmeras possibilidades de seleção, captura e análise de informações, os parâmetros são estabelecidos principalmente pelo interesse comercial. Tal formato, muitas vezes, não leva em consideração regionalidades ou manifestações de pequenos grupos, deixando-os à margem dos contextos estabelecidos. De acordo com Lerman:

Milhares de milhões de pessoas em todo o mundo permanecem na periferia do Big Data. Suas informações não são coletadas ou analisadas regularmente, porque eles não se envolvem rotineiramente em atividades que o Big Data foi projetado para capturar. Consequentemente, suas preferências e necessidades

correm o risco de serem sistematicamente ignoradas, quando governos e setor privado usam Big Data e análises avançadas para moldar políticas públicas e o mercado. (Lerman, 2013, p. 55).

Para o autor, a proposta de solução para frear o aumento desse abismo e proteger as populações cuja existência o Big Data pode ignorar, além de preservá-las dentro de uma doutrina legal, passa pelo que chama de *antissubordinação de dados*. Questionamentos ligados a essa temática deveriam ter mais atenção nos atuais debates sobre o Big Data. Quem o Big Data exclui? Quais são as consequências da exclusão para esses excluídos, para o Big Data como tecnologia e para as sociedades? (Lerman, 2013, p. 57).

A Revolução Industrial proporcionou uma infinidade de melhorias em relação ao bem-estar e qualidade de vida de algumas populações, mas também fomentou o aumento das diferenças, separando as sociedades industrializadas daqueles que não participaram de tal transformação. Atualmente, essas diferenças são potencializadas, em grande parte, pelo desenvolvimento tecnológico. Contudo, as discrepâncias verificadas na capacidade dos países de aproveitarem as novas oportunidades são muito acentuadas, com enormes implicações no domínio da desigualdade e do desenvolvimento humano (ONU, 2019, p. 20).

Sujeitos inseridos nas sociedades industrializadas e/ou tecnológicas têm acesso ao que a vida moderna pode proporcionar em relação ao fornecimento de dados para o Big Data. O simples fato de ter um veículo com GPS, usar contas de serviços como e-mail e redes sociais e possuir um cartão de crédito já os torna pertencentes a um seletivo grupo onde, ao mesmo tempo, são fornecedores de dados e também são o público-alvo do Big Data, enquanto os sujeitos pobres residentes nas periferias não têm o mesmo valor como fornecedores de informação, pois suas rotinas nem sempre contemplam o *script* básico para a coleta de dados. Muitos não possuem conta bancária, não são assinantes, nem tampouco utilizadores de serviços via internet. Utilizam, quando possível, transporte público e residem em bolsões de miséria. Portanto, a exclusão das camadas menos favorecidas da população dos conjuntos de dados do Big Data pode ter implicações muito sérias para a definição de políticas econômicas, sociais e, principalmente, para participação democrática. De acordo com a perspectiva de Lerman:

Essas tecnologias podem criar um novo tipo de falta de voz, onde as preferências e comportamentos de certos grupos recebem pouca ou nenhuma consideração, quando atores poderosos decidem como distribuir bens e serviços e como reformar instituições públicas e privadas. (Lerman, 2013, p. 59).

A parcela da população que é colocada à margem dos parâmetros do Big Data pode sofrer danos econômicos e sociais ainda mais expressivos, pois os dados de suas preferências e hábitos de consumo são ignorados pelas ferramentas de captura e análise do Big Data. Concomitantemente, governos que se utilizam desses dados promovem a exclusão das populações menos favorecidas da atividade democrática e da participação política, construindo “uma barreira à cidadania plena” (Lerman, 2013, p. 59). A revolução tecnológica representada pelo Big Data fomenta o desenvolvimento de novas formas de desigualdade e exclusão, aprofundando, com ajuda da mais moderna tecnologia de tratamento de dados, as diferenças sociais existentes em vários países e potencializa, de forma ainda mais expressiva, em nações pobres. Dessa maneira, o Big Data representa uma ameaça na luta contra as diferenças políticas e sociais, sendo um elemento capaz de aprofundar as desigualdades ao direcionar o seu funcionamento para as camadas de população que alimentam os fluxos de dados eleitos como prioritários. Lerman afirma:

Assim, ao projetar novos programas de segurança pública e treinamento no trabalho, prevendo as necessidades futuras de moradia e transporte e alocando fundos para escolas e pesquisa médica – para citar apenas alguns exemplos – é necessário que as instituições públicas considerem e talvez trabalhem para mitigar o impacto dispar que o uso do Big Data pode ter sobre pessoas que vivem fora ou à margem dos conjuntos de dados do governo. (Lerman, 2013, p. 61).

O Big Data e seu potencial de exclusão é um expoente do novo formato de esfera pública, em que a tecnologia ocupa o espaço de deliberação e tomada de decisão, onde os dados estão a serviço do poder econômico ou de quem tiver recursos financeiros disponíveis para viabilizar a compra e/ou acesso a informações de parcelas de determinadas populações. É a manutenção de um sistema que reforça a

capacidade do poder econômico daqueles que pagam pelo melhor e maior uso dos dados. Como aponta Pasquale:

A fonte desse poder é, no fundo, o Big Data, ou seja, a capacidade das grandes empresas digitais de armazenar e analisar dados comportamentais cada vez mais íntimos dos utilizadores, traçando perfis que são de grande valor para entidades comerciais, campanhas políticas, governos ou qualquer um que deseje monitorar, monetizar, controlar e prever o comportamento humano. (Pasquale, 2017, p. 18 *apud* Silveira, 2019, p. 863).

O Big Data é um fenômeno tecnológico incapaz de ser dissociado da realidade contemporânea. Seu caráter dinâmico, repleto de mudanças, é também gerador de incertezas em relação às decisões que se irão refletir no futuro de pequenas comunidades, de países e da humanidade. Com a enorme capacidade de captura e análise de dados, com auxílio de algoritmos para formatação de padrões de comportamento humano – como veremos a seguir – é necessário e salutar que as sociedades saibam que sistemas realizam essas práticas e quem é responsável pela sua regulamentação.

2. Algoritmos: da origem ao controle

Os algoritmos não são neutros e trazem a programação imposta pelos seus programadores. (Silveira, 2017, p. 1339)

Não há como tratar as questões referentes às novas tecnologias sem abordar a importância e a influência dos algoritmos, proposições matemáticas, que, ao mesmo tempo, são icônicas e opacas nos processos de tratamento de dados. Eles não são *software*, apesar de, muitas vezes, serem confundidos com este, mas sem a sua funcionalidade talvez a revolução tecnológica da era do Big Data não estivesse em curso. Um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer (Domingos, 2017, p. 24).

Se hoje os algoritmos estão presentes em praticamente todos os dispositivos eletrônicos no dia-a-dia das pessoas – de sinais de trânsito a plataforma de redes sociais – suas origens remontam a tempos muito antigos. Como descreve Silveira:

O termo ganhou destaque com a computação, mas sua origem matemática remonta ao século IX, em Bagdá. Historiadores indicam que a palavra “algoritmo” provém de um tratado do matemático Abu Ja’far Muhammad Ibn Musa Al-Khwarizmi, que viveu entre 780 e 850 em Bagdá, tendo trabalhado na Casa da Sabedoria, uma espécie de centro de altos estudos, durante o reinado do califa al-Mamum (813-833). O tratado escrito por Al-Khwarizmi versava sobre algarismos hindu-árabes. O escrito original nunca foi encontrado e o nosso conhecimento dele se deu pela tradução em latim, denominada *Algoritmi*. Aí, encontramos a origem do termo “algoritmo”, que também pode ter tido influência da palavra grega para número, *arithmós*. (Silveira, 2019, p. 143).

A máquina desenvolvida por Alan Turing é a precursora dos computadores modernos. Com sua proposta de interpretação e resolução de problemas, ela elevou o algoritmo a um elemento central na computação, pois os complexos conjuntos de instruções para possíveis soluções de problemas só são possíveis de serem executados com auxílio dos algoritmos. De acordo com Domingos:

Os algoritmos programam voos e também pilotam aeronaves. Eles gerenciam fábricas, comercializam e entregam mercadorias, calculam os lucros e mantêm os registros. Se todos os algoritmos parassem de funcionar inesperadamente, o mundo que conhecemos chegaria ao fim. (Domingos, 2017, p. 24).

Hoje, os algoritmos cumprem um papel de destaque no funcionamento do mundo moderno. Essa importância e, em muitos casos, total dependência das resoluções apresentadas pelos esquemas matemáticos representam riscos à funcionalidade de sistemas governamentais e privados. Os algoritmos são peças fundamentais para total funcionamento do Big Data, pois são eles que potencializam a captura, análise, classificação dos dados. São eles, agora, a nova face do dispositivo de Michel Foucault (Deleuze, 1992), pois funcionam como elementos estratégicos para manutenção do poder, tanto do Estado quanto das grandes corporações. Os cientistas da computação criam algoritmos, que são, ao mesmo tempo, teorias e dispositivos (Domingos, 2017, p. 27). Lessig (2006) aponta que a estrutura social é regulada por quatro elementos, sendo eles: mercado, direito, normas sociais e arquitetura (tecnológica), ou seja, o código. Nas complexas teias de informação que compõem o Big Data, o “código é lei”, sendo uma ferramenta que funciona como regulador, para o bem ou mal, de todo o sistema:

No espaço real, reconhecemos como as leis regulam – por meio de constituições, estatutos e outros códigos legais. No ciberespaço, precisamos entender como um “código” diferente regula – como o *software* e o *hardware* (isto é, o “código” do ciberespaço) que fazem do ciberespaço o que é, também regulam o ciberespaço como ele é. Como William Mitchell coloca, esse código é a “lei” do ciberespaço. “Lex Informatica”, como Joel Reidenberg colocou pela primeira vez, ou melhor, “código é lei”. (Lessig, 2006, p. 5).

Esse condicionamento do mundo à função dos algoritmos afeta diretamente as relações sociais, levando à *algoritmização* das ações, situação em que as interações sociais são balizadas por uma profunda quantificação e *matematização* (Silveira, 2019, p. 179).

A classificação realizada mediante a utilização dos algoritmos, no caso do Big Data, facilita o controlo social por parte de governo e grandes corporações, a exemplo, as corporações do sistema financeiro. Esse processo classificatório de indivíduos facilita o exercício do poder e o controlo, além de dinamizar, muitas vezes de forma cruel em relação às questões sociais, a tomada de decisões.

Classificar, em outras palavras, é dar ao mundo uma estrutura: manipular suas probabilidades, tornar alguns eventos mais prováveis que outros, comportar-se como se os eventos não fossem casuais ou limitar ou eliminar sua casualidade (Bauman, 1991, p. 9). Para além da classificação, o controlo das sociedades também atingiu níveis nunca antes experimentados com uso da funcionalidade dos algoritmos. Eles são elementos de suma importância na atual fase da sociedade do controlo definida por Deleuze, pois sua capacidade de ação, associada à tecnologia da informação, é praticamente impossível de ser limitada.

Nessa nova versão de controlo, a barreira física, os postos de controlo e/ou fiscalização perdem lugar para a informação processada com auxílio dos algoritmos. O que conta não é a barreira, mas o computador que detecta a posição de cada um, lícita ou ilícita, e opera uma modulação universal (Deleuze, 1992, p. 225).

O poder financeiro das grandes corporações desenvolvedoras de *software* e algoritmos é um agravante para a transparência nos processos de recolha e tratamento de dados. Amarras jurídicas e comerciais protegem-nas e garantem a manutenção do uso de algoritmos de forma opaca, ou seja, sem informar aos indivíduos qual o tratamento (classificação) está sendo realizado em relação aos dados pessoais. Dessa forma, com auxílio dos algoritmos, cria-se o que Frank Pasquale denomina como “Black Box Society”, ou seja, as sociedades não têm acesso nem sabem como e de qual maneira seus dados estão sendo utilizados. Mais adiante, esse trabalho vai abordar o exemplo do cadastro positivo brasileiro – um modelo de histórico de crédito, que utiliza um sistema de *score* financeiro, autorizado pelo governo e gerido por empresas privadas, com um funcionamento algorítmico opaco e sem diretrizes muito bem explicadas à população.

Atrelado a esse poder e ofuscado pelas amarras mercadológicas, apresenta-se um outro elemento que fornece ainda mais capacidade para os modelos de seleção condicionados por algoritmos, o *machine learning*, ou seja, a capacidade de

assimilação e “aprendizado” dos computadores. Com o *machine learning*, os computadores escrevem seus próprios programas, logo, não precisamos mais fazê-lo (Domingos, 2017, p. 29). Seu desenvolvimento é, ao mesmo tempo, dinâmico e perigoso, pois a associação do uso de códigos algorítmicos secretos com a autonomia das máquinas pode gerar resultados extremamente danosos.

Algoritmos e outras formas de inteligência artificial podem deslocar ainda mais a importância da agência humana, à medida que desenvolvem automaticamente novas práticas de governança³ (Hansen e Poter, 2013, p. 35). Com o *machine learning*, os algoritmos se tornam diferentes até mesmo para os indivíduos que realizaram sua programação inicial.

Movimentos têm se realizado para tentar pressionar governos e corporações sobre esse problema. Exemplos como as organizações ProPublica⁴ e FAT/ML⁵ (Fairness, Accountability and Transparency in Machine Learning) trabalham para alertar sobre os riscos de delegar as tomadas de decisões governamentais e/ou privadas às máquinas, pois a interpretação de dados por parte dos algoritmos pode criar ou reforçar, por exemplo, problemas discriminatórios e de caráter socioeconômico. Afinal, os algoritmos são passíveis de erros e as consequências desses possíveis equívocos podem ser desastrosas. Como aponta Domingos:

Um minúsculo erro em um algoritmo faz um foguete de bilhões de dólares explodir ou milhões de pessoas ficarem sem energia elétrica. Quando os algoritmos interagem de maneiras inesperadas, o mercado de ações desaba. Se os programadores são pequenos deuses, o monstro da complexidade é o próprio demônio. Pouco a pouco, ele está vencendo a guerra. (Domingos, 2017, p. 29).

É importante ressaltar que este trabalho não preconiza a condenação do uso dos algoritmos e sua associação aos sistemas de megadados, mas trata a questão da

3 Os dicionários gerais definem governança como sinônimo de governo e governação, sendo este o termo que tradicionalmente tem sido mais usado em Portugal, quando se pretende referir o «ato de governar». E, de facto, a palavra *governance*, embora ande traduzida como governança, é também muitas vezes posta em correspondência com governação. In: <https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/governanca-e-governacao/32687>

4 propublica.org

5 fatml.org

responsabilidade de transferir para as máquinas as tomadas de decisões que afetam diretamente milhares de pessoas em todo o mundo, principalmente as menos favorecidas social e economicamente. Os avanços proporcionados pelo desenvolvimento das tecnologias referentes ao processamento de dados e ao *machine learning* são, também, muito importantes para viabilizar a solução de vários problemas, nos mais variados âmbitos, como, por exemplo, na saúde, educação e segurança.

Até que ponto esses avanços justificam o uso e o tratamento “opaco” de dados pessoais por parte de governos e grandes corporações? As estruturas de dados e seu tratamento algorítmico estão a serviço de quem tiver recursos financeiros suficientes para obter diferentes amostras de segmentos e perfis de utilizadores com os padrões especificados pelos compradores (Silveira, 2019, p. 863). Essa forma equivocada de estabelecer classificação de sujeitos representa um dos grandes problemas da nossa era, pois, cada vez mais, o processo de classificação é automatizado e está diretamente ligado ao poder financeiro, sem levar em consideração nuances dos diferentes aspectos da vida de determinados indivíduos, sociedades e/ou comunidades. Sem recursos econômicos ou visibilidade nas sociedades informatizadas, as camadas mais pobres são diretamente afetadas por governos e corporações que privilegiam os sistemas automatizados.

2.1 Vigilância: o fim da privacidade

O mundo contemporâneo é o que Manuel Castells (2002) define como um “espaço dos fluxos”, em que tudo se resume em fluxo de dados que circulam a todo momento em milhares de computadores ao redor do planeta, onde o poder regulador do Estado tem sido reduzido significativamente e a interação social, mediada por computador, contribui para essa diminuição do poder dos governos. Nesse modelo de fluxo de informação, os modernos modelos de vigilância se apresentam com tal sutileza que os fazem parecer incapazes de serem percebidos e/ou até mesmo incômodos. Bauman e Lyon (2014), por sua vez, denominam essa nova metodologia de “vigilância líquida”, pois, com auxílio da tecnologia dos algoritmos e do Big Data, sua capacidade de penetração na vida dos indivíduos atinge parâmetros nunca antes

imaginados. Como aponta Leonardo Bessa (2019), a tecnologia fomentou a mudança no conceito de privacidade:

Se é certo que, em sua origem, a privacidade estava associada ao direito de ser deixado em paz – *right to be alone* –, a preocupação de hoje é proteger o cidadão em relação aos modernos – e cada vez mais eficientes – mecanismos da informática de tratamento (coleta, armazenamento e difusão) de dados. (Bessa, 2019, p. 48).

Ancorados em políticas de privacidade, que em muitos casos não protegem os dados dos utilizadores, governos e grandes corporações fazem uso de todo tipo de informação de *sites*, aplicações, *smartphones*, etc. Muitas vezes, a captação de dados tem o consentimento individual dos utilizadores, mas nem sempre eles estão preparados para lidar com as complexas informações dos termos de autorização e terminam, por consequência, alimentando os bancos de dados. Portanto, as políticas de privacidade se tornam um elemento para isenção de responsabilidade para as empresas e governos que gerenciam dados e não, necessariamente, uma segurança jurídica para preservação da privacidade dos utilizadores.

Joseph Turow e outros mostraram que “[quando] os consumidores veem o termo ‘política de privacidade’, acreditam que suas informações pessoais serão protegidas de maneiras específicas; em particular, eles assumem que um site que anuncia uma política de privacidade não compartilha suas informações pessoais.” (Tene e Polonetsky, 2012, n.p).

O desenvolvimento de políticas públicas, como o Regulamento Geral de Proteção de Dados⁶ europeu (679/2016) e a Lei Geral de Proteção de Dados⁷ brasileira (13.709/2018), representa a tentativa de governos para equacionar os limites da privacidade e da captura de dados. A previsão é que a lei brasileira entre completamente em vigor em agosto de 2021, mas esse prazo pode ser alterado. Nos dois casos, há complexidade nas informações e legislações, pois o tema é extremamente sensível e os governos representam uma das partes interessadas na captura e processamento de dados. Além disso, o processo para a deliberação,

6 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

7 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

aprovação e aplicação dessas leis demanda tempo, enquanto o desenvolvimento tecnológico para obtenção de dados ocorre de forma mais dinâmica.

A vigilância agora deixa de se referenciar no modelo autoritário do panóptico de Jeremy Bentham – como veremos mais adiante – e cede lugar a um formato que parte da iniciativa dos próprios vigiados. Se no modelo de Bentham a proposta era manter os vigiados sempre em alerta sobre a possibilidade de estarem sendo observados e forçá-los a ter um bom comportamento, conseqüentemente mantendo a ordem e o poder, o atual modelo de vigilância opera com sutileza e conta com a colaboração de sujeitos que têm plena consciência da observação de seus atos, além de fazerem uso da tecnologia para fornecerem dados aos “observadores”. Submetemos à matança nossos direitos de privacidade por vontade própria (Bauman e Lyon, 2014, p. 28). O fornecimento de dados pessoais poderia então ser visto como uma versão tecnológica da *Servidão Voluntária* de Etienne de la Boétie (2006) e as “pegadas digitais” deixadas por todos utilizadores da internet como o maior capital de governos e grandes corporações de tecnologia.

A invisibilidade e o anonimato, elementos importantes da privacidade, são, no mundo industrializado, praticamente impossíveis de serem perenes. Não há mais possibilidade, ao menos nas sociedades profundamente atreladas à tecnologia, de um indivíduo permanecer à margem dos sistemas de recolhimento de dados. Anteriormente citado neste trabalho, as exclusões nos sistemas de recolhimento de informações podem ocorrer, principalmente por demanda socioeconômica e em países com grandes diferenças sociais.

O aprimoramento de técnicas e aplicação de metodologias de vigilância estão ligados ao desenvolvimento militar (Bauman e Lyon, 2014) e os drones não tripulados são um bom exemplo desse sistema praticamente imperceptível. A arma de guerra sintetiza o novo modelo de vigilância, pois é capaz de capturar as informações, classificá-las, agir – com auxílio do operador – e permanecer invisível. As redes sociais nos permitem traçar um paralelo com a operação dos drones.

Funcionando de uma maneira inversamente proporcional à das armas, quanto maior exposição, mais dados classificados, elas se utilizam da característica contemporânea do reconhecimento social atrelado à exposição, para categorizar perfis de utilizadores em todo o mundo. A condição de ser observado e visto, portanto, foi

reclassificada de ameaça para tentação (Bauman e Lyon, 2014, p. 30). A operação dos drones e a categorização dos utilizadores das redes sociais têm outro elemento em comum, o operador. O militar, que pilota o equipamento, e o programador, que estabelece as classificações, fazem uso de uma das principais características do desenvolvimento tecnológico das últimas décadas – a possibilidade de agir à distância.

O valor espaço-tempo tem, nesse caso, o papel de atenuar as responsabilidades dos atores que praticam e/ou coordenam a vigilância. Hannah Arendt (Bauman e Lyon, 2014) denomina essa ação à distância como “flutuação” da responsabilidade, ou seja, não há responsáveis nesses atos, pois são executadas por pessoas que não estão presentes geograficamente onde eles ocorrem.

A visibilidade se tornou uma armadilha, mas que os próprios utilizadores das redes sociais, por exemplo, ajudam a construir. O fornecimento de dados corrobora a manutenção de sistemas, muitas vezes perversos, principalmente com as esferas menos favorecidas da sociedade. A exemplo do que este trabalho se propõe a discutir, tal categorização de informações permite às grandes corporações financeiras, com auxílio da tecnologia dos algoritmos, utilizarem os mais variados dados fornecidos pelos utilizadores, muitas vezes de maneira inconsciente, para permitir acesso a crédito financeiro. Na perspectiva de Kerr e Earle, em nome de uma suposta segurança econômica, a privacidade dos sujeitos é simplesmente ignorada. De acordo com os autores:

Algumas empresas de empréstimo, por exemplo, estão começando a usar algoritmos para determinar as taxas de juros para clientes com pouco ou nenhum histórico de crédito e para decidir quem está sob alto risco de incumprimento. Milhares de indicadores são analisados, desde a presença de amigos financeiramente seguros no Facebook até o tempo gasto em sites e aplicações instaladas em vários dispositivos de dados. (Kerr e Earle, 2013, p. 69).

As redes digitais permitem uma dinâmica descomunal de seleção de dados, possibilitando que a vigilância funcione como sistema de estratificação social, permitindo, assim, que governos e grandes corporações tenham pleno conhecimento das ações de todos os indivíduos que façam uso de dispositivos ou algum serviço

eletrônico. Dessa forma, praticamente todos os aspectos da vida cotidiana das sociedades informatizadas são cobertos pela vigilância tecnológica.

(...) a vigilância cotidiana, os sistemas de reconhecimento facial das câmeras, os cartões de crédito, os caixas de supermercado, os aparelhos móveis permitem a classificação à distância. Ela é a base da organização dos sistemas de crédito, de estratificação, de seleção social, enfim, de deslocamentos físicos, econômicos e sociais das populações. (Silveira, 2017, p. 227).

Tal segmentação e tentativa de busca de um comportamento padrão das sociedades é lida por Bauman e Lyon como uma nova face da violência institucional de estados e corporações. Balizados pelas redes digitais, eles conduzem a vida de milhares de pessoas com o propósito de otimizar e potencializar ganhos financeiros, além do estabelecimento de políticas de Estado. O diferencial da era tecnológica é o não uso da violência física para obtenção desses resultados, mas os danos socioeconômicos podem ser piores do que os que ocorreram em um dos períodos mais sombrios da história moderna. O funcionamento de tal metodologia faz com que os autores apresentem o seguinte questionamento:

Será que a organização meticulosa, a cuidadosa distinção entre o agente e a vítima, a eficiência mecânica da operação observada nos comboios de gado humano e nos campos de extermínio agora se devotam não mais à violência física, mas à classificação da população em categorias, tendo em vista um tratamento diferencial? (Bauman e Lyon, 2014, p. 22).

Os novos métodos de classificação à distância revelam a face perversa dos sistemas tecnológicos de vigilância. Sua atuação silenciosa e praticamente invisível, insere todos os sujeitos do mundo industrializado em uma nova era de controle e disciplina, onde a vigilância agora ocorre em todos os lugares e a partir de todos os dispositivos.

2.2 Pós-panóptico: o novo guardião

A Vigilância, que na estrutura arquitetônica do panóptico, de Jeremy Bentham, deveria ser realizada pelo guardião que ficava na torre central observando as celas ao redor, passa a ser efetivada pelos *bits* e *bytes* de informações fornecidas espontaneamente por milhares de cidadãos, sendo analisados e categorizados por máquinas. Sistemas que, por sua vez, são formatados com dados gerados pelas ações e impressões humanas. Sendo assim, podem aprender e amplificar preconceitos dos mais variados tipos, como, por exemplo: de raça, gênero, credo, etnia, classe social e/ou posicionamento político, ampliando as possibilidades de segmentação e desigualdade.

É importante lembrar que aqueles que têm o poder de criar estruturas digitais são os que controlam o que se naturaliza como normas sociais (Cirucci, 2018, p. 17). Esses são os riscos dos sistemas que, em nome de uma segurança, seja ela sociopolítica ou econômica, demandam às máquinas as tomadas de decisões sobre temas importantes em uma sociedade. Agindo diretamente sobre cada indivíduo, os sistemas de controle, assim como o panóptico, tornam-se um intensificador de poder, pois, segundo Foucault: asseguram sua economia (em matéria, em pessoal, em tempo); asseguram a sua eficácia por seu caráter preventivo, seu funcionamento contínuo e seus mecanismos automáticos (1999, p. 229).

O papel primordial da tecnologia no processo de vigilância eleva, segundo Bauman, o modelo do tradicional panóptico, no qual era necessária a figura do guardião, ao modelo do pós-panóptico, formado por uma série de panópticos eletrônicos, onde a vigilância ocorre à distância, baseada em dados fornecidos voluntariamente pelos sujeitos vigiados. Para Bauman e Lyon, Os vigiados da era tecnológica não precisam mais estar enclausurados para permanecerem no campo de visão dos guardiões:

Assim, a segurança funciona à distância tanto no espaço quanto no tempo, circulando de maneira fluída, juntamente com os Estados-nações, mas para além deles, num domínio globalizado. Tranquilidade e recompensas acompanham esses grupos móveis para os quais essas técnicas são feitas como se fossem “naturais”. Processos de estereotipia e medidas de exclusão estão à

espera dos grupos desafortunados o bastante para serem rotulados de “indesejados”. (Bauman e Lyon, 2014, p. 13).

Nesse contexto, o modelo tradicional de vigilância, com sua observação passiva, dá lugar a um método de coleta de dados pessoais, com desempenho, resultado e volume de informações consideravelmente superiores. De acordo com Jens-Erik Mai (2016), no modelo de captura se assume que as tecnologias afetam a realidade social, mas que a coleta de dados não modifica o modo como as pessoas interagem com a tecnologia (Silveira, 2017, p. 761). Dessa maneira, dados de diferentes dispositivos podem ser cruzados e, com auxílio de algoritmos, possibilitam a reconstrução virtual da identidade dos indivíduos, decretando o fim do anonimato. David Lyon (2003), por sua vez, denomina essa reconstrução virtual dos sujeitos como *Data Doubles*. Eles estão durante todo o tempo *on-line*, são alimentados/construídos com informações dos utilizadores e têm demasiado efeito sobre a vida dos próprios utilizadores.

Para Bessa (2019), a análise dessas informações, por meio de um perfil digital, pode causar sérios danos à privacidade, além de julgamentos equivocados em relação à personalidade do indivíduo:

Cumprе ressaltar a crescente tendência de análise, juízos de valor das pessoas a partir de um perfil digital, ou seja, de dados obtidos friamente em redes eletrônicas, pela internet, por transferências não autorizadas, que invariavelmente não correspondem a situações reais, ensejando tratamento discriminatório, julgamentos rápidos e equivocados ou acesso a informações que integram dados sensíveis. (Bessa, 2019, p. 48).

Contemporaneamente, no entanto, todos os pedaços da existência humana podem ser “visíveis” porque muito de quem nós somos é rastreado e apresentado através de tecnologias de *media* digitais (Cirucci, 2018, p. 17). A pegada digital “deixada” pelos utilizadores, mesmo de maneira inconsciente, ou até mesmo inevitável durante o uso dos serviços tecnológicos, tem um efeito de corresponsabilidade no efeito da vigilância na era do pós-panóptico.

Quem está submetido a um campo de visibilidade, e sabe disso, retoma por sua conta as limitações do poder; fá-las funcionar espontaneamente sobre si mesmo; inscreve em si a relação de poder na qual ele desempenha simultaneamente os dois papéis; torna-se o princípio da sua própria sujeição. (Foucault, 1999, p. 226).

Suavidade e continuidade são marcas da vigilância pós-panóptica, funcionando como a estratégia militar da *Surveillance*⁸. Ela não perde os alvos do seu plano de observação e/ou operação. No marketing de banco de dados, a ideia é induzir os alvos potenciais a pensar que eles contam, quando tudo que se quer é contá-los e, claro, atraí-los para novas compras (Bauman e Lyon, 2014, p. 57). Com a vigilância pós-panóptica sendo viabilizada pelos utilizadores, governos e grandes corporações desenvolvem ferramentas, cada vez mais poderosas, com grande capacidade para capturar e analisar as informações que trafegam pela internet. Os programas *PRISM* e *Upstream*⁹ são apenas dois exemplos dessa gigantesca capacidade dos órgãos de inteligência de acessar, armazenar e catalogar dados. As revelações de Edward Snowden apresentaram ao mundo como os dados dos utilizadores eram tratados pelos órgãos de segurança do governo dos Estados Unidos. Uma prática que, em nome da soberania nacional ou da segurança, pode ocorrer em vários países do mundo.

8 Observação cuidadosa de uma pessoa ou local, especialmente pela polícia ou exército, por causa de um crime que aconteceu ou é esperado. Em: <https://dictionary.cambridge.org/pt/dicionario/ingles/surveillance>

9 Programas da Agência Nacional de Segurança dos EUA, ambos revelados pelo ex-analista da NSA, Edward Snowden, em 2013. Em: <https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/>

3. Controle: disciplina, economia e sociedade

*“Quis custodiet ipsos custodes?”
(Juvenal, Satire 6)*

A disciplina é uma forma de controle sobre os comportamentos, ações e interações de cada sujeito, com o intuito de garantir o argumento de um estado de controle social, como aponta Foucault: a disciplina aumenta as forças do corpo (em termos econômicos e de utilidade) e diminui essas mesmas forças (em termos políticos de obediência) (1999, p. 164). Tal garantia de disciplina é, em grande parte, fomentada, na contemporaneidade, pelo uso da tecnologia mediática. O argumento utilizado por Nick Couldry e Andreas Hepp sintetiza como essas possibilidades de uso das tecnologias podem influenciar diretamente as práticas sociais, uma vez que a dinâmica social também é determinada pelo papel dos *media* e pelo seu uso. O conceito de Mediatização Profunda é definido pelos autores como o crescente papel dos *media* na vida de milhares de pessoas, em vários países, a partir da primeira década deste século. Na perspectiva dos autores:

Primeiro, houve o fator bruto do papel crescente dos *media* na vida cotidiana em muitos países desenvolvidos em meados dos anos 2000, uma década que viu a normalização do acesso rápido à Internet, a quase universalização dos telefones móveis, a expansão massiva da capacidade de busca na *web* e o surgimento de *blogs*, *YouTube* e *media* sociais como novas formas de comunicação – em outras palavras, o fato dos *media* em nossa vida, todos os dias, como um ponto de referência básico para crianças, amigos, família, trabalho. (Hepp e Couldry, 2013, p. 2).

A mediatização profunda é, portanto, um estágio tão avançado de mediatização que os fundamentos do mundo social estão diretamente ligados aos meios de comunicação e suas tecnologias, afetando diretamente a construção social da vida contemporânea. Equipamentos como telefones móveis, *tablets*, computadores e *watches* funcionam como extensão do corpo humano e produzem informações a todo momento, tanto para os utilizadores, quanto para o Big Data. Governos e grandes corporações fazem uso de todo tipo de informação disponibilizada pelos cidadãos para estabelecer um *ranking* social e econômico, que Foucault trata como Mecanismo

Disciplinar: um dispositivo funcional que deve melhorar o exercício do poder tornando-o mais rápido, mais leve, mais eficaz, um desenho das coerções sutis para uma sociedade que está por vir (1999, p. 232). Deleuze, por sua vez, aponta que as sociedades disciplinares já deram lugar a uma nova categoria. São as sociedades de controlo que estão substituindo as sociedades disciplinares. Controlo é o nome que Burroughs propõe para designar o novo monstro, e que Foucault reconhece como nosso futuro próximo (1992, p. 220).

Os avanços tecnológicos são, portanto, base para a sustentação do controlo social. O modelo disciplinar acompanhou a evolução e tornou o controlo mais efetivo, dinâmico e imperceptível. E o ideal de liberdade da sociedade industrializada é ameaçado pelos elementos criados dentro do seu contexto de desenvolvimento.

Essa mão invisível, impulsionada pelo governo e pelo comércio, está construindo uma arquitetura que aperfeiçoará o controlo e tornará possível a regulamentação altamente eficiente. A luta nesse mundo não será do governo. Será garantir que liberdades essenciais sejam preservadas nesse ambiente de controlo perfeito. (Lessig, 2006, p. 4).

O desafio é atenuar os efeitos desse novo modelo de controlo, preservando a ideia de uma construção tecnológica que privilegie os direitos dos cidadãos.

3.1 Categorização social

Esquemas disciplinares desenvolveram, ao longo do tempo, diferentes metodologias para categorizar cidadãos. O complexo esquema de recolhimento e análise de dados, que envolve a Mediatização Profunda, o Big Data, *machine learning* e os algoritmos, possibilita uma nova leitura e união de alguns desses modelos, marcados pela individualização e pela exclusão dos sujeitos. Para Foucault (1999), o poder disciplinar ancorado na tecnologia se vale dos recortes, processos e métodos há muito estabelecidos para controlar os sujeitos e monitorar as suas relações:

(...) de um modo geral, todas as instâncias de controlo individual funcionam num duplo modo: o da divisão binária e da marcação (louco-não louco; perigoso-inofensivo; normal-anormal); e o da determinação coercitiva, da

repartição diferencial (quem é ele; onde deve estar; como caracterizá-lo, como reconhecê-lo; como exercer sobre ele, de maneira individual, uma vigilância constante, etc.). (Foucault, 1999, p. 223).

A segmentação dos sujeitos em grupos também apresenta uma variação contemporânea. Assim como o pós-panóptico representa uma leitura moderna e mais ampla da sistemática da vigilância, o Ban-óptico é o termo utilizado para sintetizar a moderna metodologia de classificação e exclusão de indivíduos, resultado da união das ideias de “bando”, defendida por Jean-Luc Nancy e desenvolvida por Giorgio Agamben (2004) e o panóptico argumentado por Foucault. A relação política originária é o *bando* (o estado de exceção como zona de indistinção entre externo e interno, exclusão e inclusão) (Agamben, 2004, p. 187).

O Ban-óptico funciona baseado na capacidade das novas tecnologias de captura e processamento de dados de separarem grupos de interesses, referenciadas por parâmetros políticos e/ou econômicos. Burocracias transnacionais de vigilância e controle, tanto empresariais quanto políticas, agora trabalham à distância para monitorar e controlar, pela vigilância, os movimentos da população (Bauman e Lyon, 2014, p. 63). A funcionalidade do Ban-óptico também se aplica às temáticas bélica e de segurança, mas este trabalho vai se ater apenas à questão do seu uso para a construção e/ou manutenção de sociedades desiguais e excludentes, principalmente no âmbito socioeconômico. Assim como aponta Neto:

Obviamente, a vida humana seria impensável sem a possibilidade de categorizar pessoas e grupos sociais. Fazemos isso instintivamente. No entanto, as novas tecnologias da informação possibilitam que essa categorização ocorra de maneira automática, a partir de algoritmos de computadores cuja função é classificar todas as informações obtidas a partir dos critérios predeterminados pelos seus criadores. Dessarte, é possível entender que tais algoritmos são “portas virtuais” que possibilitam, por meio de vários critérios desconhecidos, quem “entra” e quem “não entra” – em “lugares” físicos ou naqueles, não menos importantes, virtuais, que determinam a elegibilidade para diversos benefícios da vida real. (Neto *apud* Fortes *et al*, 2015, p. 2013).

O Ban-óptico opera nas sociedades industrializadas traçando o perfil e excluindo os grupos e sujeitos indesejados, viabilizando, dessa forma, a disciplina e o controlo. Os grupos indesejados podem ser compostos, não necessariamente por criminosos, terroristas, por exemplo, mas cidadãos comuns que não se encaixam em perfis estabelecidos previamente por governos e/ou corporações.

Ferramentas tecnológicas, como as câmeras de vigilância¹⁰ são utilizadas como sustentáculo desse modelo. A banalização do seu uso é fator que contribui para a manutenção do controlo e da disciplina. Mas, assim como outros modelos, sua utilização e funcionamento podem apresentar falhas¹¹ e, conseqüentemente, prejudicar indivíduos¹² que, até então, não figuravam nos grupos de excluídos. O rastreamento, ou *tracking*, que consiste em captura e análise dos dados deixados por utilizadores de dispositivos eletrônicos e plataformas digitais, é outra ferramenta utilizada por grandes corporações e governos, para reduzir a privacidade de quem navega pela internet. Dados sensíveis, como a orientação sexual dos utilizadores de alguns *sites* pornográficos, por exemplo, podem ser acessados por corporações como Google, Oracle e Facebook (Maris *et al*, 2019). A opacidade dos sistemas de dados não permite aos utilizadores saber como e quando esses dados são acessados. Google e Facebook¹³ alegam que os dados dos utilizadores não são destinados a publicidade, mas as informações sobre o que cada utilizador buscou nos *sites* pornográficos permanece em poder das empresas.

A compilação de dados estritamente privados e/ou sensíveis possibilita uma identificação mais detalhada dos utilizadores, mas apenas com uma pequena quantidade de interações o perfil dos utilizadores pode ser definido. É possível determinar com precisão de 95% a personalidade de cada um apenas com as informações que são disponibilizadas de maneira espontânea através do ícone “gosto” da plataforma Facebook (Kosinski *et al*, 2013).

Tais possibilidades de redução da privacidade, análise e desenvolvimento de perfis dos utilizadores fomentam a construção e/ou manutenção de sociedades

10 https://www.rtp.pt/noticias/mundo/reconhecimento-facial-cidade-chinesa-tem-26-milhoes-de-camaras-de-vigilancia_n1189532

11 <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/05/27/tecnicas-de-vigilancia-como-identificacao-facial-ainda-sao-falhas.htm>

12 <https://g1.globo.com/pop-arte/noticia/2019/05/16/san-francisco-proibe-a-policia-de-usar-reconhecimento-facial.Ghtml>

13 <https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html>

desiguais, nas quais os sujeitos são categorizados e excluídos sem averiguação ou a mínima possibilidade de argumentação. Dessa forma problemas socioeconômicos são dilatados e se alarga o abismo entre os indivíduos que beneficiam das potencialidades das sociedades industrializadas/tecnológicas e os que se encontram à margem dessas sociedades. Como indica Neto:

Fica visível, portanto, que o acúmulo indiscriminado de informação permite a criação de categorias sociais arbitrárias, evidenciando como a *surveillance* é, muito além de um problema de privacidade, uma ferramenta que amplifica a discriminação e as desigualdades sociais. A categorização dos seres humanos tem como finalidade a sua inclusão ou exclusão. Nesse sentido, a *surveillance* levanta barreiras virtuais, capazes de garantir ou impedir acesso aos elementos indispensáveis para uma vida digna. (Neto *apud* Fortes *et al*, 2015, p. 1721).

A captação e o processamento de informações pessoais extrapolam os limites da privacidade e enquadram praticamente todos os indivíduos das sociedades industrializadas em algum tipo de classificação, seja sociocultural ou econômica. Os governos são parte interessada nesses processos de coleta de dados, mas não há controle total sobre essas metodologias indiscriminadas de tratamento de informações pessoais. Como definir a legitimidade desses modelos de classificação? Somente através da democratização e da transparência desses critérios será possível proteger os direitos fundamentais, ou seja, tornar-se-á as relações de (in)visibilidade mais visíveis (Neto *apud* Fortes *et al*, 2015, p. 1738).

3.2 Credibilidade Financeira

O'Neil (2016) faz observações sobre como dados de milhares de pessoas, como códigos postais, padrões de navegação e compras, são utilizados para tentar prever uma possível credibilidade financeira. O resultado dessa análise gera uma pontuação chamada *e-score*. Os números podem possibilitar, ou não, o acesso a crédito no sistema financeiro. A autora reforça que os *e-scores* não são regulamentados, são arbitrários e, muitas vezes, injustos, pois são excludentes e reforçam diferenças. Muitos de seus modelos pseudocientíficos tentam prever nossa credibilidade, dando a cada um de nós os chamados *e-scores*. Estes números, que

raramente vemos, abrem portas para alguns de nós, enquanto as batem no rosto de outros (O’Neil, 2016, p. 118).

Deleuze também aponta como as sociedades de controlo utilizam o poder financeiro como ferramenta para manutenção do sistema. “A linguagem numérica do controlo é feita de cifras, que marcam o acesso à informação ou à rejeição. Não se está mais diante do par massa-indivíduo. Os indivíduos tornaram-se ‘dividuais’, divisíveis, e as massas tornaram-se amostras, dados, mercado ou ‘bancos’” (Deleuze, 1992, p. 222).

3.3 Metodologia

Esta pesquisa se pauta por um estudo teórico, de natureza reflexiva e caráter expositivo (Salvador, 1980, p. 35 *apud* Marconi e Lakatos, 2003, p. 238), tendo sua construção balizada pela pesquisa bibliográfica, reunindo e relacionando conteúdos oriundos de diferentes fontes.

Para fundamentação teórica, foi realizada pesquisa baseada em fontes primárias e secundárias (Marconi e Lakatos, 2003, p. 159), sendo:

Fontes Primárias: dados históricos, bibliográficos e pesquisas

Fontes Secundárias: imprensa em geral e obras literárias.

Foi feita recolha e análise de informações oriundas de fontes estatísticas e documentos escritos. O estudo de literatura pertinente e o levantamento de conteúdo informativo acerca dos sistemas estadunidense, chinês e brasileiro permitiram um esforço em relação à abordagem do tema, colocando em diálogo diferentes autores, linhas argumentativas e informações.

Após a contextualização dos conceitos de Big Data, mediatização, privacidade e vigilância, procedeu-se o levantamento de conteúdo informativo sobre exemplos de modelos de controlo desenvolvidos e aplicados em três diferentes países – os Estados Unidos, com as plataformas privadas que operam os sistemas GRC – governança, gerenciamento de riscos e conformidade de princípios, a China, com o sistema de crédito social, e o Brasil, com a Lei do Cadastro Positivo, uma metodologia de

recolha de informações para a construção de um histórico de crédito dos consumidores/cidadãos brasileiros.

Seguiu-se com a temática das metodologias de *ranking/score* e a problematização de seus usos como instrumento de controlo social. Buscando verificar a hipótese de que tais modelos podem fomentar o crescimento das diferenças socioeconômicas e culturais. Por esse motivo, julgamos importante o desenvolvimento da pesquisa acerca do tema, pois os reflexos da aplicação de tais metodologias podem afetar segmentos substanciais das sociedades em questão. Além disso, o trabalho é uma grande oportunidade para assimilação de conceitos e ampliação de conhecimento.

Busca-se apresentar: a forma como se estabelecem os sistemas, como as informações são utilizadas e os possíveis resultados dentro de cada contexto social. Partimos da ideia que as tecnologias de recolhimento e tratamento de dados podem não ser suficientes para diminuir, de forma ampla, as desigualdades sociais, além de potencializarem modelos que contribuem para o aumento da exclusão.

4. Modelos: oriente e ocidente

Como sistema operacional, a governança orientada por dados não requer espaço, mas pode gerenciar multiplicidade de ordens legais e normativas, em torno das quais, os comportamentos devem se adequar. (Backer, 2018, p.18)

4.1 Sistema de Crédito Social

O sistema de crédito social é uma iniciativa realizada pelo governo chinês sob o argumento de garantir uma abordagem global para o cumprimento da lei de responsabilidade social. O projeto do sistema foi apresentado pelo PCC – Partido Comunista Chinês, em 2014, previsto para estar em plena operação em 2020, monitorando 1,4 mil milhões de cidadãos chineses, com auxílio de 200 milhões de câmeras¹⁴ e de informações do Big Data. O objetivo é utilizar mecanismos de controlo em que indivíduos e organizações são monitorados permanentemente por meio de registo e análise de dados, incluindo imagens. Utilizando-se de argumentos como “cultura da sinceridade, promoção da honestidade e virtudes tradicionais”, o governo impõe, com o uso de mecanismos cibernéticos, um comportamento padrão para todos os cidadãos e corporações.

Um sistema de crédito social é um componente importante do sistema de economia de mercado e do sistema de governança social. É fundamentado em leis, regulamentos, normas e cartas. É baseado numa rede completa, que abrange os registos de crédito dos membros da sociedade e da infraestrutura de crédito. (...) Requisitos inerentes estão estabelecendo a ideia de uma cultura de sinceridade (...) seu objetivo é elevar a mentalidade honesta e os níveis de crédito de toda a sociedade. (República Popular da China, 2014, p. 1 *apud* Backer, 2018, p. 4-5)

O sistema é uma metodologia de controlo que fornece recompensas e/ou punições como respostas aos seus participantes, baseando-se não apenas na legalidade, mas também nas questões morais, económicas e políticas. Tal modelo utiliza as regras estabelecidas pelo governo para classificar o comportamento dos cidadãos e, com o

¹⁴ <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-adigitaldictatorship/>

uso de algoritmos, determina o resultado em um único número. Até mesmo relações de amizade e interações sociais, como as redes sociais por exemplo, são monitoradas para garantir o imperativo do modelo, afastando o cidadão com boa pontuação de indivíduos que não estejam bem avaliados pelo governo. O resultado dessa álgebra aponta se o cidadão é ou não confiável, do ponto de vista governamental. A pontuação do cidadão determina se ele irá conseguir um financiamento imobiliário, matricular o filho em uma determinada escola, fazer uma viagem ou até mesmo conseguir um emprego. Como ressalta Rogier Creemers:

Essa pontuação será baseada em pontos de dados, incluindo compras on-line, conteúdo publicado em mídias sociais e o tipo de amigos que se tem. Por sua vez, a pontuação teria um impacto amplo na vida das pessoas, influenciando sua capacidade de conseguir empregos, empréstimos e hipotecas, relações com amigos e familiares, e até mesmo a capacidade de viajar. (Creemers, 2018, p. 3).

Essa metodologia de disciplina força os indivíduos a se adequarem à normatização. Uma vez à margem ou contra normas estabelecidas, a invisibilidade social se torna uma ameaça real. Pois “enquanto os sistemas jurídicos qualificam os sujeitos de direito, segundo normas universais, as disciplinas caracterizam, classificam, especializam, distribuem ao longo de uma escala, repartem em torno de uma norma, hierarquizam os indivíduos em relação uns aos outros, e, levando ao limite, desqualificam e invalidam” (Foucault, 1999, p. 246).

Mesmo sendo sustentado por um argumento que defende a transparência nas relações comerciais e sociais, além de uma suposta ampliação do acesso a recursos financeiros para faixas da população que antes não tinham condições, o sistema de crédito social, conduzido por algoritmos, pode ampliar as diferenças sociais existentes, pois seu funcionamento sustenta uma linha de reprodução de resultados que atende a um conceito estabelecido com antecedência e caráter prioritário, como aponta Larry Catá Backer:

A análise de dados não depende de qualquer ordem normativa que não seja a da instituição cujos valores serve; e ainda pode construir seus próprios valores a partir de seu próprio universo de dados. E o algoritmo, através do qual a

análise de dados pode projetar consequências, pode servir para incorporar valores do sistema ou pode gerar os valores daqueles que podem controlar suas premissas. (Backer, 2018, p. 18).

Esse novo contexto de controlo vigilante é uma forma de legislar sobre as fronteiras do público e do privado, até então, teoricamente, reforçadas e garantidas. Com o auxílio do Big Data, os complexos sistemas de visibilidade redefinem as relações de poder entre governos e cidadãos. Essa relação é balizada pela produção de informações obtidas por meio de combinação de dados fornecidos passivamente por milhares de pessoas e analisados pelos algoritmos utilizados pelo sistema. Dessa forma, o poder do SCS contorna toda realidade da vida quotidiana dos indivíduos, controlando, de forma detalhada, os comportamentos, as atitudes, os hábitos e os discursos dos cidadãos. É a utopia da cidade perfeitamente governada (Foucault, 1999), mas agora, não mais, como uma única cidade.

4.1.1 Tabela de Suining

Em 2010, o governo do condado de Suining, na província de Jiangsu, na China, introduziu um sistema denominado Programa de Credibilidade de Massa (*dazhong xinyong*)¹⁵ que mediu e pontuou a conduta individual dos moradores locais. Cada cidadão recebeu um crédito inicial de 1.000 pontos, que seriam debitados de acordo com a tabela desenvolvida pelo governo, baseada em normas legais, administrativas e morais. O sistema recebeu várias críticas, mas também funcionou como um embrião do sistema de crédito social chinês. A tabela (Anexo A) com a pontuação seguia informações de crédito de serviços comerciais, sociais, de gestão social e de crédito social.

15 <https://bkso.baidu.com/item/睢宁县大众信用信息评估细则>

4.1.2 O teste do Sistema de Crédito Social

Uma reportagem apresentada pelo portal da rede australiana ABC, intitulada *Leave no Dark Corner*¹⁶, em português “Não deixe nenhum canto escuro”, apresenta dois lados do sistema de Crédito Social chinês. Por um lado, a boa pontuação e seus benefícios e por outro, as punições ao cidadão que não se enquadra aos aspectos estabelecidos pelo sistema.

É apresentada a rotina de Dandan Fan, uma jovem que foi selecionada para participar do programa piloto. Ela é uma profissional de marketing e é considerada uma cidadã chinesa modelo. Segundo a reportagem, ela sabe que está sendo vigiada quase 24 horas por dia e diz não se importar. No programa piloto, cada cidadão participante recebeu inicialmente 800 pontos. Aqueles com melhores pontuações recebem tratamento VIP em hotéis e aeroportos, empréstimos com taxas de juros mais baixas e oportunidades para ingressar nas melhores universidades e nos melhores empregos.

Mesmo tarefas quotidianas não escaparão ao olhar do governo chinês. Quando o sistema de crédito social for totalmente implementado, o que é adquirido no supermercado poderá afetar a pontuação social. Comprar muito álcool, por exemplo, pode sugerir dependência e, conseqüentemente, perda de pontos. Comprar um pacote de fraldas pode indicar responsabilidade e gerar mais pontos, tudo analisado em tempo real.

A reportagem também apresenta Liu Hu. Um jornalista de 43 anos, que descobriu um escândalo de corrupção nos níveis mais altos do Partido Comunista Chinês e investigou casos de assassinatos em série. Em 2015, Liu perdeu um caso de difamação após acusar um funcionário do governo de extorsão. Ele foi obrigado a publicar um pedido de desculpas e pagar uma multa, mas quando o tribunal exigiu uma taxa adicional, o jornalista se recusou a pagar. Em 2017, ele foi incluído na lista negra como “desonesto” no esquema piloto de crédito social. Ele não consegue, por exemplo, reservar passagens de trem e suas contas em plataformas de *media* sociais, onde publicou a maior parte do seu trabalho, foram encerradas.

16 <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>

4.2 Governança, gerenciamento de riscos e conformidade de princípios

Os modelos GRC – sistemas de governança, gerenciamento de riscos e conformidade de princípios – são iniciativas privadas de corporações dos Estados Unidos da América e outros países ocidentais. Muitas dessas instituições utilizam dados e algoritmos como ferramentas mercadológicas e mecanismos de governança, como reforça Backer: “o Ocidente tornou-se bem condicionado aos regimes de avaliação, autoavaliação e responsabilidade nos níveis individual e de entidade. A avaliação, é claro, presta-se bem a dados da mecânica de governança” (2018, p. 11). Para cumprir suas metas, seja governança ou retorno financeiro, as entidades – públicas ou privadas – utilizam a análise de dados como norma central para gerenciamento de seus objetivos e populações. Os sistemas GRC executam uma normatização invisível, garantindo a aplicação da lei e/ou conformidade, para controlar o comportamento dos seus públicos e sustentar um caráter de cumprimento de regras e responsabilidades.

Diferentemente do modelo chinês, em que o Estado determina as ações governamentais, baseando-se nos resultados apresentados pelos dados, no modelo ocidental é o mercado e sua força econômica, juntamente às agências reguladoras – estatais ou autônomas – que sustenta os sistemas de controle. Estas funções incluem vigilância, relatórios, incluindo a divulgação para prestação de contas (através da lei), coleta, mercados de dados, reempacotamento e distribuição de dados (Backer, 2018, p. 12).

Dessa forma, o modelo ocidental, utilizando as potencialidades do sistema e aperfeiçoando-o cada vez mais, consegue disciplinar e gerir a vida das populações, com o propósito máximo de utilização e aproveitamento, mantendo assim os controles social, político e econômico. O sistema diminui a capacidade de contestação sobre as ordens do poder, neutralizando possíveis atos de revolta e maximizando a capacidade de trabalho; enfim, tornando os sujeitos peças facilmente controláveis. A definição dos enquadramentos utilizados pelos algoritmos dos sistemas de controle funciona como um laboratório e cabe às sociedades, nas quais eles executam a funcionalidade, o papel de cobaias. Os testes são feitos na vida real com pessoas reais, enquanto os modelos de sistema de controle executam a função do panóptico, pois “pode ser

utilizado como máquina de fazer experiências, modificar o comportamento, treinar ou retrainar os indivíduos” (Foucault, 1999, p. 227).

A análise de dados ocupa agora o lugar da deliberação política e as decisões têm um valor que extrapola as decisões governamentais. Como aponta Backer:

Em vez de debate, há análises. O enquadramento dessa análise, ou seja, os juízos e princípios incorporados nessas análises não são incluídos no algoritmo. O algoritmo em si é a expressão da soma dos objetivos e perspectivas daqueles para cujos objetivos o algoritmo é implantado. Em vez de princípios, então, há presunções e limitações autocriadas de campos de dados que criam os limites dentro dos quais as escolhas são cabeadas. Estas são as estruturas da governança convencional, mas agora implantadas em um espaço bastante diferente. (Backer, 2018, p. 20).

Um exemplo do modelo GRC são as agências de classificação de risco de crédito. Elas pertencem a um número pequeno de operadores e orientam os serviços de disponibilidade de crédito. As agências também classificam os negócios públicos, obrigando os consumidores, sejam eles governos ou cidadãos, a se alinharem ao modelo de execução estabelecido por elas. Na perspectiva de Backer:

Essas agências exercem efeitos significativos de governança através da aplicação de seu julgamento de algoritmos (as classificações) que servem para gerenciar comportamentos. Eles são pautados em análises baseadas em dados aplicadas aos objetivos e seu efeito é disciplinar os comportamentos através do sistema de punição e de recompensa de suas análises. No entanto, essas agências não são controladas pelo estado, mas movidas pelo mercado. (Backer, 2018, p. 13-14).

Separados por ideologias políticas, o sistema de crédito social e o modelo GRC têm muitas características em comum. Tais metodologias fazem uso dos processos e dinâmicas estabelecidos pelos avanços tecnológicos, que trazem novas normas e hábitos comunicacionais, mas que também são ferramentas para o desenvolvimento e manutenção de uma nova forma de controle social. Ambos são baseados em monitoramento, coleta e gestão de dados, com análises produzidas por

algoritmos, e podem ser utilizadas para mudar comportamentos e/ou implementar regimes de punição e recompensa.

4.2.1 Algoritmos e a Justiça

Em alguns estados americanos são utilizados algoritmos para auxiliar a Justiça nos casos de determinação de liberdade condicional¹⁷. O caso apresentado foi auditado pela ProPublica. A análise de documentos apontou que, mesmo com a utilização dos algoritmos, os resultados eram tendenciosos. Eles indicavam os réus negros com uma potencialidade duas vezes maior de cometer novos crimes do que os réus brancos.

Como exemplo, destaca-se o caso de Brisha Borden e Vernon Prater. Brisha, mulher negra, de 18 anos, foi presa por tentativa de furto de uma bicicleta e além disso, possuía outras contravenções. Já Vernon Prater, homem branco, foi preso por furtar 85 dólares em uma loja de departamentos. Ele possuía duas condenações anteriores por roubo à mão armada. O algoritmo, no entanto, classificou Brisha como sendo de alto risco à sociedade, com pontuação 8 e Vernon de baixo risco, com pontuação 3. Dois anos após a tentativa de furto ela não tinha reincidido em nenhum crime, mas Vernon havia reincidido e está cumprindo oito anos de prisão.

4.2.2 Polícia de Chicago

O'Neil (2016) define como armas os algoritmos que têm o potencial de destruir vidas, aumentar as desigualdades e representam um risco para as democracias. Ela apresenta diversos casos em que sistemas utilizados por forças policiais americanas acabam reforçando as desigualdades sociais e raciais. Um deles ocorreu na cidade de Chicago, quando a polícia optou por usar um sistema de combate ao crime com o auxílio de algoritmos, e formou uma lista com 400 indivíduos que poderiam cometer crimes violentos ou estar envolvidos em homicídios. O jovem Robert McDaniel estava na lista, mesmo sem histórico de crime violento ou ter usado armas. O fato de ter crescido em um bairro pobre e perigoso, além de conhecer pessoas que cometeram crimes, já o torna um criminoso em potencial. Para O'Neil, a

¹⁷ https://www.ted.com/talks/zeynep_tufekci_machine_intelligence_makes_human_morals_more_important

punição ocorre pelo simples fato de as pessoas serem pobres, não-brancas e viverem em bairros menos favorecidos. De acordo com a autora:

Pessoas inocentes cercadas por criminosos são maltratadas, e criminosos cercados por um público cumpridor da lei recebem um passe. E devido à forte correlação entre pobreza e crime denunciado, os pobres continuam sendo apanhados nessas redes de arrasto digitais. (O’Neil, 2016, p. 88).

O’Neil também aponta que o funcionamento dos algoritmos, utilizados pela Justiça Criminal em algumas localidades dos Estados Unidos, se assemelha ao utilizado pela gigante do comércio, Amazon. Ambos focam nas probabilidades e possibilidades de reincidência dos indivíduos. Com objetivos distintos – comercial e jurídico – os sistemas fomentam o lucro e o controle social.

5. Cadastro Positivo: o modelo brasileiro

*“Não há crédito sem conhecimento.
Não há conhecimento sem informação.”
(Bessa, 2011, p. 23).*

Os bancos de dados de proteção ao crédito são uma espécie de banco de dados de consumo, mais especificamente entidades que têm como objetivo principal a coleta, o armazenamento e a transferência a potenciais credores de informações pessoais dos indivíduos que pretendem obter crédito (Bessa, 2019).

Este modelo de banco de dados começou a funcionar no Brasil durante a década de 1950. O aumento da demanda por crédito, atrelada ao crescimento da massa de consumidores e o desenvolvimento dos centros urbanos, impulsionou a nova metodologia de categorização. Com o crescimento do sistema de venda a prazo, os comerciantes passaram a formular fichas com informações dos consumidores, pois a dinamização do sistema de compra e venda forçou o abandono de antigos métodos, muitas vezes baseados na confiança e no relacionamento interpessoal. Constatou-se, portanto, que a atividade de coleta, armazenamento e divulgação de informações entre empresários seria mais dinâmica, racional e barata se exercida por entidade criada unicamente para este objetivo (Bessa, 2019).

Em julho de 1955, a Câmara de Dirigentes Lojistas – CDL – de Porto Alegre, no Rio Grande do Sul, fundou o primeiro Serviço de Proteção ao Crédito – SPC. Atualmente, são mais de 2.000 CDL’s em todo o país, interconectadas e formando o SPC-Brasil¹⁸, responsável por um banco de dados com dezenas de milhões de registros (Bessa, 2019, p. 25).

Essas entidades têm por principal objetivo a coleta, o armazenamento e a transferência a terceiros (credores potenciais) de informações pessoais dos pretendentes à obtenção de crédito (Bessa, 2019). A atuação desse modelo de agências de proteção de crédito remonta ao final do século XIX, nos Estados Unidos da América, sendo a Retail Credit Co. a primeira a iniciar as operações, em 1899. Em 1970, o congresso americano regulamentou a atuação dessas empresas por meio do FCRA – Fair Credit Reporting Act. Como apresenta Bessa:

¹⁸ <https://www.spcbrasil.org.br/>

A aprovação do FCRA se deveu a um grande número de reclamações relativas aos relatórios de crédito elaborados pelas agências que continham muitas informações subjetivas (ex.: estilo de vida) incompletas, inexatas, coletadas de forma ilícita. Ademais, invariavelmente, negava-se acesso do consumidor aos seus dados. (Bessa, 2011, p. 66).

Ao lado das associações de fornecedores e lojistas, o setor de proteção ao crédito começou a ser explorado economicamente por empresas privadas a partir da década de 1960 (Bessa, 2019). Assim como nos Estados Unidos, no Brasil a recolha e análise de informações de consumidores funcionaram sem marco legal durante um longo período. O CDC – Código de Defesa do Consumidor –, de 1990, garantiu a legislação sobre os bancos de dados até então vigentes.

De uma maneira simplificada, a diferenciação entre banco de dados e cadastro de consumo é realizada a partir da fonte e do destino das informações. De acordo com Bessa (2019), os bancos de dados recolhem informações no mercado para oferecê-las ao próprio mercado, entre fornecedores com alguma necessidade, enquanto no cadastro as informações são obtidas diretamente dos consumidores para uso de um fornecedor específico, com o objetivo de estreitar o vínculo entre consumidor e fornecedor.

Em 2011, o governo brasileiro editou a Lei 12.414 (Anexo B), conhecida como Lei do Cadastro Positivo, em que são estabelecidos novos sistemas de operação dos bancos de dados de proteção ao crédito. A partir dessa normativa, os bancos de dados não poderiam mais ser concebidos unicamente como entidades que negam crédito e excluem pessoas do mercado (Bessa, 2011), prática muito comum até a edição da Lei do Cadastro Positivo, pois os bancos de dados se baseavam exclusivamente em informações negativas sobre os consumidores. O argumento utilizado é que o cadastro positivo possibilita a geração de benefícios para os consumidores, como a redução das taxas de juros, diminuindo o número de pessoas endividadas e aumentando a oferta de crédito.

No período de implementação do cadastro, a taxa básica de juros no Brasil estava em torno de 12,50% ao ano¹⁹. Tendo em vista que, no Brasil, não há uma regulamentação específica sobre os juros, o próprio mercado se autorregulamenta, por essa razão, não há garantias que haverá a redução dos juros (Braunschweiger, 2014, p. 6).

Vale, aqui, apresentar a nomenclatura básica utilizada pela Lei 12.414/2011 para tratar o tema:

- I. *banco de dados*: conjunto de dados relativo à pessoa natural ou jurídica armazenado com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro;
- II. *gestor*: pessoa jurídica responsável pela administração de banco de dados, bem como pela coleta, armazenamento, análise e acesso de terceiros aos dados armazenados;
- III. *cadastrado*: pessoa natural ou jurídica que tenha autorizado inclusão de suas informações no banco de dados;
- IV. *fonte*: pessoa natural ou jurídica que conceda crédito ou realize venda a prazo ou outras transações comerciais e empresariais que lhe impliquem risco financeiro;
- V. *consulente*: pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida por esta Lei;
- VI. *anotação*: ação ou efeito de anotar, assinalar, averbar, incluir, inscrever ou registrar informação relativa ao histórico de crédito em banco de dados; e
- VII. *histórico de crédito*: conjunto de dados financeiros e de pagamentos relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica.

Aqui também ressaltamos a utilização e o significado de dois termos da língua portuguesa, muito utilizados no Brasil para tratar este e outros temas correlatos. São

¹⁹ <http://g1.globo.com/economia/noticia/2011/07/copom-sobe-juros-para-1250-ao-ano-no-5-aumento-consecutivo.html>

eles: *adimplência*²⁰ – ato de cumprir uma obrigação – e *inadimplência*²¹ – falta de cumprimento de uma obrigação.

O governo brasileiro, por meio do Relatório de Cidadania Financeira do Banco Central, indica que o cadastro tem por objetivo subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem o consulente (potencial credor, a exemplo de bancos e lojistas), permitindo melhor avaliação de risco envolvido na operação (BCB, 2018, p. 135). O próprio consumidor, sendo ele pessoa física ou jurídica, aderia ao sistema do cadastro positivo, mediante uma autorização específica – modelo denominado *opt-in*. A partir da autorização por escrito, o consumidor permite que seu histórico de crédito seja construído e acessado pela empresa que reúne informações financeiras. O cadastro do consumidor e, por essa razão, é preciso que o próprio autorize a sua criação, como também requerer seu cancelamento, a qualquer momento. Não é o consumidor que mantém, que atualiza as informações no banco de dados e, sim, a empresa (Braunschweiger, 2014). Como reforça Bessa:

Conforme o inciso VII do art. 2º., o histórico de crédito é a reunião de informações financeiras relativas aos pagamentos de operações de crédito bem como de compromissos assumidos (obrigações “em andamento”). São dados que permitem, ao consulente, verificar a data de vencimento e de pagamento efetivo de parcelas de operações creditícias, bem como o valor da prestação. (Bessa, 2011, p. 84).

Desta forma, a Lei direciona quais são as informações que deveriam constar no histórico dos cidadãos/consumidores, proibindo que sejam feitas anotações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito do cadastrado, e informações sensíveis, aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (Lei 12.414/2011). A partir da edição da Lei do Cadastro Positivo, passou-se então a ter um marco legal que autorizava os bancos de dados privados a coletarem e divulgarem informações positivas de

20 "Adimplência", in: <https://dicionario.priberam.org/adimpl%C3%Aancia>

21 "Inadimplência", in: <https://dicionario.priberam.org/inadimpl%C3%Aancia>

consumidores/cidadãos, analisando sua vida pretérita e seus hábitos de consumo, mediante autorização prévia.

Com a autorização do governo para coleta e análise de dados, empresas privadas passaram a compilar, mediante autorização dos cidadãos, informações sobre o histórico de crédito, dando origem a um grande arquivo de informações sobre as atividades financeiras de parte da população brasileira. O cadastro positivo estabeleceu a base para o seu funcionamento sob o argumento de que a exclusividade de informações negativas compromete não só o bom funcionamento dos bancos de dados, mas principalmente o próprio mercado de crédito, por não combater, de maneira adequada, a assimetria de informações em relação à seleção, ao risco moral e às informações sobre renda (Bessa, 2011).

A Lei do Cadastro Positivo também encontra argumentos que defendem a relativização da privacidade como ferramenta para o desenvolvimento social e humano, sob a alegação que o maior acesso ao crédito pode atenuar problemas relacionados a estes dois temas. (...) o desenvolvimento social, com base na acumulação de capital humano, constitui a base essencial à preservação da dignidade da pessoa humana, devendo, portanto, e para esses fins, serem valores sobrepostos ao direito à privacidade (Pinheiro, 2012, p. 77). Bessa, em oposição a tal linha argumentativa, afirma:

Todavia, ao lado da reconhecida relevância, são atividades potencialmente ofensivas à dignidade da pessoa humana, à privacidade e à honra. Com a tendência atual em ampliar o volume de informações pessoais tratadas pelos bancos de dados de proteção ao crédito, para abranger o que se tem denominado *informações positivas* (histórico de crédito), aumenta-se a tensão e a ameaça em relação ao direito à privacidade e à honra do consumidor. (Bessa, 2109, p. 21).

Mais adiante, trataremos a questão da reformulação da Lei 12.414/2011, proposta em 2017 e editada em 2019, conhecida como Nova Lei do Cadastro Positivo, onde pontos como privacidade e sigilo de informações também estarão em discussão. Antes mesmo da reformulação da Lei, questões como segurança, privacidade, juros, tempo de disponibilização das anotações e sigilo das informações disponibilizadas já

fomentavam discussões acerca do funcionamento do cadastro e da responsabilidade do Estado Brasileiro em permitir que empresas privadas executem a captação e o tratamento de informações financeiras de parte da população, além de determinarem, de maneira sigilosa, o *score* de crédito dessa população. Por esses motivos, Braunschweiger questiona:

O mencionado cadastro representa ou não uma ofensa à privacidade do consumidor? Como fica o conflito temporal de permanência das anotações frente à legislação em vigor? (...) Haverá redução da inadimplência? Haverá redução da taxa de juros? Haverá maior crescimento da economia? (...) A mencionada redução de juros será aplicada/oferecida a todos os consumidores? A redução dos juros beneficiará somente os consumidores vulneráveis financeiramente? O consumidor não vulnerável financeiramente e adimplente com suas despesas terá direito à redução da taxa de juros? (Braunschweiger, 2014, p. 5-6).

As perguntas apresentadas por Braunschweiger direcionam a uma questão de grande relevância em relação ao desenvolvimento de históricos de crédito destinados ao cadastro positivo. Quais serão os verdadeiros beneficiados com a execução da Lei? Há de se lembrar que o Brasil é uma nação com sérios problemas de desigualdade social e, portanto, o tratamento “opaco” de informações, além de ferir o princípio constitucional da igualdade, pode colaborar para potencializar o complicado quadro socioeconômico brasileiro.

5.1 Brasil: o fator desigualdade

A definição de pobreza remete à privação do bem-estar, que pode ser entendida como a limitação da capacidade que os indivíduos possuem de participar na sociedade, o que envolve fatores diversos como, por exemplo, sentir-se seguro, ter acesso a oportunidades, ter uma alimentação adequada e ter bons relacionamentos sociais (Houghton e Khan-Dker, 2009 *apud* IBGE, 2019, p. 57).

De acordo com o Relatório de Desenvolvimento Humano 2019²², da Organização das Nações Unidas, o Brasil ocupa a posição número 79 no Índice de Desenvolvimento Humano, classificado entre as nações com elevado IDH. A posição entre os 189 países que compõem o *ranking* apresenta a dimensão do desafio em relação às diferenças socioeconômicas e culturais que transpassam o corpo social brasileiro. O IBGE – Instituto Brasileiro de Geografia e Estatística²³ – aponta que um total de 13,5 milhões de brasileiros vive em condição de extrema pobreza, com uma renda mensal *per capita* inferior a US\$ 1,90 por dia – critério utilizado pelo Banco Mundial para indicar situação de extrema pobreza. Ainda de acordo com o IBGE, outros 52,5 milhões de brasileiros são pobres, ou seja, têm rendimento diário inferior a US\$ 5,50.

Essa parcela considerável, que soma mais de um quarto da população brasileira, tem poucas perspectivas em relação a um futuro melhor. Sem esperança ou dignidade, esses indivíduos assistem, às margens da sociedade, ao avanço das classes mais ricas em direção a uma prosperidade socioeconômica, cultural e tecnológica. A nível mundial, muitos escaparam à pobreza extrema, mas são ainda mais os que nunca tiveram nem as oportunidades nem os recursos para gerir suas vidas (PNUD, 2019, p. 13).

É indiscutível que o progresso tecnológico trouxe avanços na melhoria dos padrões de qualidade de vida da população mundial. Mas ainda existe um longo caminho a ser percorrido, pois as diferenças sociais se aprofundam na proporção dos avanços tecnológicos. É necessário garantir que as inovações favoreçam todas as pessoas, pavimentando um caminho para a diminuição das diferenças socioeconômicas. Como reforça o Relatório de Desenvolvimento Humano do Programa das Nações Unidas para o Desenvolvimento:

A Revolução Industrial lançou a humanidade na senda de melhorias sem precedentes ao nível do bem-estar. Também desencadeou, no entanto, a Grande Divergência, separando as poucas sociedades que se industrializaram das muitas que não o fizeram. A diferença, atualmente, prende-se com o fato de que – quiçá pela primeira vez na história – uma grande parte da tecnologia por detrás da atual transformação pode ser acedida a partir de qualquer lugar.

22 http://hdr.undp.org/sites/default/files/hdr_2019_pt.pdf

23 <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101678.pdf>

Contudo, as discrepâncias verificadas na capacidade dos países de aproveitarem as novas oportunidades são muito acentuadas, com enormes implicações no domínio da desigualdade e do desenvolvimento humano. (PNUD, 2019, p. 19).

O atual cenário exige políticas inovadoras para regulamentação no uso dos dados dos cidadãos e o Brasil não é exceção a esta regra, pois o uso da tecnologia pode reforçar ainda mais o quadro social brasileiro. O cadastro positivo pode ser ferramenta para fomentar a manutenção de desigualdades e falta de acesso aos benefícios do mundo industrializado. Ao se basear em dados oriundos de uma estrutura social desigual, em que boa parte da população se encontra abaixo ou na linha da pobreza, a sistemática do cadastro pode reforçar as desigualdades ao invés de ser uma ferramenta na luta contra a situação em que se encontra boa parte da população brasileira.

Transferir para o setor privado a responsabilidade pelo controlo de dados em relação ao acesso a crédito pode representar um risco no combate às desigualdades sociais e à pobreza. Permitir que algoritmos desenvolvidos por empresas privadas, valendo-se de metodologias pouco transparentes, sejam responsáveis, mesmo que indiretos, pela viabilidade de uma das vias de mudanças e ascensão social é, no mínimo, uma aposta arriscada. Pode-se assim criar uma categoria que Bauman (1999) denomina consumidores falhos, ou seja, aqueles indivíduos que não têm capacidade para estarem incluídos nos processos de consumo e são, por consequência, descartados da sociedade. No caso brasileiro e mais especificamente no cadastro positivo, cidadãos inaptos a terem crédito.

Todo mundo pode ser lançado na moda do consumo; todo mundo deseja ser um consumidor e aproveitar as oportunidades que esse modo de vida oferece. Mas nem todo mundo pode ser um consumidor. (...) Todos nós estamos condenados à vida de opções, mas nem todos temos os meios de ser optantes. (Bauman, 1999, p. 83).

As consequências para a camada mais pobre da população brasileira podem ser nefastas. O aprofundamento das diferenças sociais pode ser a resultante dessa

operação, sendo a metodologia do cadastro positivo um exemplo das *Weapons of Math Destruction*, apresentadas por Cathy O’Neil e anteriormente citadas neste trabalho. Dessa forma, imputa-se nas camadas mais pobres a responsabilidade pela não condição de ser um consumidor/cidadão com uma boa pontuação no *score* e retira-se das ações mercadológicas ou das políticas públicas equivocadas a responsabilidade pelo fracasso social.

É assim, reconhecidamente, devido a várias razões, mas eu proponho que a principal razão dentre elas é o fato de que os “excluídos do jogo” (os consumidores falhos – os consumidores insatisfatórios, aqueles cujos meios não estão à altura dos desejos, e aqueles que recusaram a oportunidade de vencer enquanto participavam do jogo de acordo com as regras oficiais) são exatamente a encarnação dos “demônios interiores” peculiares à vida do consumidor. Seu isolamento em guetos e sua incriminação, a severidade dos padecimentos que lhes são aplicados, a crueldade do destino que lhes é imposto são – metaforicamente falando – todas as maneiras de exorcizar tais demônios interiores e queimá-los em efígie. (Bauman, 1997, p. 57).

A natureza excludente de iniciativas como cadastro positivo reforça a inabilidade de iniciativas que se valem de metodologias de caráter mercadológico como ferramenta de combate às diferenças socioeconômicas. Simplesmente excluir quem já não possui recursos não atenua o problema em uma sociedade em que 10% da população mais rica concentra 55% de toda riqueza produzida no país²⁴. Dessa forma, o método perverso de exclusão perpetua uma das estruturas sociais mais desiguais do planeta, como argumentado por Bauman (1997), criminalizando a pobreza. Se é mais barato excluir e encarcerar os consumidores falhos para evitar-lhes o mal, isso é preferível ao restabelecimento de seu status de consumidor através de uma previdente política de emprego conjugada com provisões ramificadas de previdência (Bauman, 1997, p. 25).

24 <https://nacoesunidas.org/relatorio-de-desenvolvimento-humano-do-pnud-destaca-altos-indices-de-desigualdade-no-brasil/>

5.2 Dados sensíveis

Grupos menos favorecidos da sociedade, como já apresentado no presente trabalho, passam a ser vítimas do poder de controlo de informações executado pelo avanço tecnológico que facilita políticas de discriminação social, de redução da liberdade de escolha e de intromissão indevida nos assuntos privados (Neto, 2011, p. 90). Estefano Rodotà aponta que a privacidade ganha, nesse aspecto, um novo sentido, ampliando seu alcance, deixando-se atender apenas a individualidade de cada sujeito e atendendo a necessidade de proteção do coletivo. Na perspectiva do autor:

Tende-se a mudar o sujeito do qual emana a demanda da defesa da privacidade e muda mesmo a qualidade desta demanda: vindo em primeiro plano a modalidade do exercício do poder da parte dos detentores públicos e privados das informações, a evocação do direito à privacidade supera o tradicional quadro individualista e dilata-se em uma dimensão coletiva, no momento em que se considera não o interesse do indivíduo como tal, mas como integrante de um determinado grupo social. (Rodotà *apud* Doneda, 2001, p. 119).

Apesar de permitirem a captação de informações, no caso do cadastro positivo, os consumidores/cidadãos não têm controlo sobre a circulação e utilização dos dados que formam o seu histórico de crédito. Controlo que é ainda mais complexo de ser realizado, levando-se em consideração o grau de instrução e a disponibilidade de ferramentas tecnológicas para as camadas menos favorecidas da sociedade brasileira. Braunschweiger aponta que a Lei não oferece meios para os consumidores controlarem a circulação das próprias informações. Para tanto, ela afirma:

A segurança é de extrema importância, uma vez que a Lei nº 12.414/2011 prevê a autodeterminação e controlo dos dados pelo consumidor. Porém, a lei silencia sobre como este controlo pode ser exercido em tempo real pelo próprio consumidor! A mencionada Lei apenas afirma que o consumidor poderá ter acesso, pedir, solicitar informações sobre seu próprio cadastro. Portanto, fica claro que o consumidor não tem como gerenciar, em tempo real, a circulação de seus próprios dados. (Braunschweiger, 2014, p. 10).

De acordo com a Lei do Cadastro Positivo, é vedada a divulgação de dados excessivos e sensíveis. Excessivos são aqueles que vão além do propósito específico de formação de histórico de crédito, informações que não são exclusivamente destinadas a esta função. A regra utilizada pela legislação brasileira para definir os critérios de responsabilidade dos bancos de dados, sejam públicos ou privados, na utilização das informações é inspirada na Diretiva 95/46 da União Europeia. Tal legislação estabelece que os dados devem ser exatos e atualizados e sempre recolhidos “para finalidades determinadas, explícitas e legítimas”. Devem, também, ser adequados, pertinentes e não excessivos em relação às finalidades dos bancos de dados. (Bessa, 2011, p. 91).

Os dados sensíveis, como anteriormente citado, são definidos como aqueles pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas, filosóficas e pessoais ou quaisquer outras que possam afetar os direitos de personalidade dos cadastrados. A falta de fiscalização sobre o recolhimento e tratamento dos dados pode possibilitar sua utilização com outras finalidades, violando a privacidade dos consumidores/cidadãos. Como afirma Góis:

Sabe-se que não podemos nos valer dessas informações, porém, por haver falta de fiscalização no seu repasse, muitas vezes elas acabam sendo divulgadas sem o consentimento do cadastrado, violando, dessa forma, o direito à privacidade. Além disso, outra questão intrigante refere-se à finalidade dos dados coletados – o art. 5º, inciso VII da Lei 12.414/2011, assegura que o consumidor terá seus dados pessoais utilizados pelos comerciantes, bem como instituições financeiras, se estes estiverem em conformidade com a finalidade dos dados. Dessa maneira, é ofensivo a privacidade acessar informações por mera curiosidade ou verificar com o fito de apurar a vida pregressa do consumidor, com vistas a futuro contrato de trabalho e demais casos. (Góis, 2017, n. p.).

Como a Lei destina às empresas a responsabilidade de recolha e análise dos dados dos consumidores/cidadãos, não há uma garantia de que dados sensíveis não passem por análise, pois a formação de um histórico de crédito se baseia em informações que estão diretamente ligadas às ações realizadas no dia-a-dia dos

indivíduos, sem possibilidade de serem simplesmente desvinculadas da personalidade de cada sujeito, apresentando, assim, riscos à privacidade das pessoas cadastradas nos bancos de dados dos *bureaus* de crédito – conjunto de empresas que reúnem informações financeiras. De acordo com Bessa, a dimensão de ofensividade da informação está diretamente ligada ao contexto do tratamento:

O consulente, para uma correta avaliação dos riscos de concessão de crédito ou para reduzir a taxa de juros a ser cobrada do consumidor, precisa, por óbvio, de informações verdadeiras. O consumidor, de outro lado, cujas informações registradas são inexatas, além de avaliado incorretamente pelo consulente, é ofendido em seus direitos da personalidade, particularmente na honra, já que, no final, acabam por serem construídos perfil e fatos relativos ao consumidor que simplesmente não correspondem à realidade. (Bessa, 2019, p. 88).

Os dados pessoais formam o perfil digital, o qual representa a pessoa e define a sua reputação. Muitas decisões, as mais variadas, privadas ou governamentais, são tomadas a partir deste perfil. É nesse contexto – tanto na área da proteção ao crédito como em tantas outras – que as atenções se voltam às mais diversas modalidades de bancos de dados (Bessa, 2019, p. 49). Para tentar diminuir todo e qualquer desvirtuamento dessas informações, deve haver uma fiscalização mais eficiente de todo e qualquer tipo de repasse sobre alguma informação do consumidor, evitando-se, assim, ilegalidades e respeitando a privacidade e demais princípios (Góis, 2017, n. p.).

5.3 Score de Crédito

Com o estabelecimento do papel das empresas privadas na estratégia funcional do cadastro positivo, estas, por sua vez, desenvolvem ferramentas para dinamizar o processo de construção do histórico de crédito e, por consequência, um modelo de resposta rápida às instituições que concedem crédito. Ferramentas conhecidas como *score* ou *scoring*, por exemplo, anteriormente citadas neste trabalho, permitem às empresas oferecerem uma “nota” ou “classificação” para os consumidores/cidadãos.

O processo para obtenção de crédito junto às instituições financeiras é balizado por esse valor atribuído a cada sujeito. De acordo com o Banco Mundial²⁵, a prática de pontuação de crédito começou na década de 1960, quando o negócio de cartões de crédito automatizou seus processos de tomada de decisão. Com o tempo, o uso de técnicas de pontuação foi estendido a outras classes de clientes. Além disso, para aprimorar o valor preditivo das várias pontuações de crédito, há uma tendência crescente de coletar mais dados de uma ampla gama de provedores e outras fontes de dados. Portanto, o *score* é encarado pelas empresas como uma ferramenta fundamental para as decisões de crédito. Como apontam informações da Boa Vista Serviços:

Score é uma ferramenta que apoia com inteligência as decisões de crédito, a partir de informações comportamentais, desenvolvida pela Área de Modelagem Estatística da Boa Vista Serviços. Esse produto estima o comportamento futuro dos clientes, indicando a probabilidade de inadimplência nos próximos seis, doze ou dezoito meses, conforme a necessidade do negócio. [...] O resultado das consultas é apresentado em uma escala numérica, na qual o menor índice representa maior risco, e o maior índice, menor chance de inadimplência. (Boa Vista, 2014 *apud* Góis, 2017, n. p.).

Boa Vista Serviços²⁶ e Serasa *Experian*²⁷ são algumas das empresas privadas responsáveis pela gestão do novo cadastro positivo brasileiro, como ainda veremos neste estudo, e também realizam o trabalho de confecção de histórico de crédito e de *Score* (Anexos C e D) dos consumidores/cidadãos cadastrados. A referida metodologia é utilizada em mais de 100 países (Falcão, 2016), mas ainda é objeto de várias ações na justiça brasileira, pois apesar de utilizar informações públicas e outras disponíveis na base de dados dos cadastros de consumo coletadas de acordo com a lei, não há total transparência no processo de armazenamento, análise e transmissão das informações. Em tese, é possível que elas sejam obtidas nas mais diversas fontes, como órgãos públicos e redes sociais. É possível que sejam obtidas na internet sem o

25 <https://openknowledge.worldbank.org/bitstream/handle/10986/12792/701930ESW0P1180ting0pub010028011web.pdf>

26 <https://www.consumidorpositivo.com.br/score/>

27 <https://www.serasaconsumidor.com.br/score/>

consentimento informado do consumidor, em clara ofensa ao art. 7º, X, da Lei 12.965/2014 (Marco Civil da Internet) (Bessa, 2019, p.117). A Lei do Cadastro Positivo versa sobre a necessidade da manutenção e respeito à privacidade dos cidadãos, mas essa questão ainda abastece o embate jurídico, como observado por Falcão:

Por isso, podemos afirmar que as entidades administradoras dos bancos de dados incentivaram a edição da Lei 12.414/2011, chamada de cadastro positivo, e, visando abastecer o mercado de consumo, não só com informações negativas e positivas, desenvolveram inúmeras ferramentas para análise de crédito, com destaque para o chamado ‘Score de Crédito’, ainda objeto de enfrentamento pelo Judiciário Brasileiro no que tange à análise da sua licitude. (Falcão, 2016, p. 12).

Na verdade, existe um verdadeiro mistério de como e quais informações coletadas do consumidor são utilizadas pelas entidades de proteção ao crédito (Bessa, 2019, p. 177). O cadastro positivo foi proposto com o argumento de benefícios aos consumidores/cidadãos e à economia brasileira, mas a utilização de informações balizadas em critérios obscuros e com resultantes definidas com o auxílio de tecnologia de informação pode não significar automaticamente um denominador positivo para a população. Como indica Góis:

Por outro lado, no que tange à concessão de crédito a juros mais baixos, pensou-se que os juros iriam diminuir por causa da Lei de Cadastro Positivo, mas, na verdade, esse foi um pretexto usado pelos legisladores para maquiagem a Lei 12.414, ao induzir benefícios aos consumidores a juros menores. Notou-se que a baixa dos juros dá-se com ou sem Lei de Cadastro Positivo, basta a livre vontade dos credores e comerciantes e que o momento econômico do país possibilite, haja vista que a Lei não menciona a ocorrência de queda dos juros ao ser cadastrado nos bancos de dados de cadastro positivo. (Góis, 2017, n. p.).

Com o argumento de redução da taxa de juros em troca do tratamento de informações, o cadastro positivo estruturou uma metodologia que confronta o direito à privacidade dos cidadãos brasileiros. Na realidade, os arquivos com informações

sobre o comportamento dos consumidores/cidadãos beneficiará o sistema financeiro e o comércio em geral. Estes, sim, serão os maiores beneficiados, manipulando o crédito, os juros e as informações financeiras dos consumidores pessoas físicas ou jurídicas, conforme seus próprios interesses (Braunschweiger, 2014).

5.4 O Novo Cadastro Positivo

A Lei do Cadastro Positivo proporcionou ao setor privado um caminho legal de acesso aos dados de parte da população brasileira, mas a referida legislação garantia adesão voluntária do consumidor/cidadão aos bancos de dados, fator que se tornou um limitador para o alcance, em termos de abrangência populacional, do cadastro. Em 2017, um Projeto de Lei Complementar foi apresentado ao Congresso Nacional com a proposta de solucionar os pontos avaliados como entraves em relação ao desenvolvimento ao cadastro positivo. O principal deles: a baixa adesão dos cidadãos, pois os sistemas como o *credit scoring*, por exemplo, são guarnecidos por meios desconhecidos pelos consumidores, deixando-os, muitas vezes, sem o acesso ao crédito por estarem com uma “pontuação” não condizente com a classe “boa pagadora” (Góis, 2017, n. p.). Daí a proposta de mudança em relação à metodologia de adesão, mais uma vez, revestida com o argumento de dinamização da economia, acesso a crédito e diminuição das taxas de juros. Como apresentado pelo Banco Central do Brasil, o grande diferencial seria o número de pessoas que passariam a ter suas informações inseridas nos sistemas dos *bureaus* de crédito. Na perspectiva da instituição:

A principal proposta de aprimoramento diz respeito exatamente ao *opt-in*, pois a necessidade de autorização para ingresso no cadastro aliada ao excesso de burocracia para a criação e inclusão das informações dos cadastrados levaram à baixa adesão, alcançando pouco mais de cinco milhões de cadastrados em cerca de seis anos de vigência da Lei, ante um potencial de cadastrados superior a cem milhões. (BCB, 2018, p. 136).

Desta forma, foi apresentada a proposta de criação da Lei Complementar 166/2019, alterando a Lei 12.414/2011 e criando a Nova Lei do Cadastro Positivo Brasileiro (Anexo E), com nova redação e revogando mais da metade dos antigos

artigos. Dentre as várias mudanças, destacamos a alteração na metodologia do cadastro dos cidadãos, passando a vigorar o modelo *opt-out*. Nesse modelo, todos os cidadãos brasileiros podem ter suas informações de consumo inseridas nos bancos de dados dos *bureaus* de crédito, sem a necessidade de autorização prévia. Com a nova legislação, o cidadão deverá solicitar, caso não concorde em ter seus dados no cadastro positivo, a retirada das suas informações da base de dados das empresas que realizam análise de risco de crédito (Anexo F).

A nova Lei indica que a vontade e a liberdade do consumidor estão garantidas, pois existe a possibilidade, a qualquer tempo, de ele optar por não fazer parte do cadastro. Levando-se em conta as características socioeconômicas brasileiras, existe a possibilidade de uma parcela significativa dos cidadãos/consumidores brasileiros não saberem que estão tendo seus dados tratados com a finalidade de atender ao cadastro positivo.

Sob a ideia básica do *more is better*, ou seja, quanto maior o volume e a variedade de informações melhor será a avaliação para disponibilidade de crédito e que a assimetria de informações impede e/ou encarece o crédito, a Nova Lei do Cadastro Positivo entrou em vigor em 09 de julho de 2019. Alguns órgãos e entidades de defesa do consumidor são contrários ao cadastro positivo tanto por não acreditarem na promessa de redução da taxa de juros, como por visualizarem invasão indevida no direito à privacidade do consumidor (proteção de dados) (Bessa, 2019, p. 10).

A Nova Lei do Cadastro Positivo permitiu que as empresas que coletam e analisam informações de crédito acrescentassem em seus arquivos um maior volume de dados sobre o histórico financeiro dos consumidores. Ao utilizar dados sobre prestadores de serviços continuados, como concessionárias e/ou autarquias de água, esgoto, eletricidade, gás, telecomunicações e assemelhados, tais empresas passaram a englobar uma parcela muito maior de consumidores/cidadãos, principalmente os que pertencem aos grupos de menor renda, pois muitos destes indivíduos não possuem contas registradas no sistema bancário²⁸, até então, principal fonte de informação dos *bureaus* de crédito.

Sob o argumento de benefícios aos cidadãos, mas sem garantias obrigatórias, a Nova Lei do Cadastro Positivo fomentou o aumento das informações nos bancos de

28 <https://epocanegocios.globo.com/Brasil/noticia/2019/08/brasil-tem-45-milhoes-de-desbancarizados-diz-pesquisa.html>

dados das empresas que trabalham com o desenvolvimento do histórico de crédito. Como aponta o Banco Central do Brasil:

(...) a plena afetividade do cadastro positivo representa possibilidade concreta de reduzir a assimetria de informações no mercado creditício e, por conseguinte, melhorar a qualidade da concessão de crédito no país. (...) o cadastro positivo tem importante potencial para ser o catalisador de maior concorrência no sistema financeiro. (...) com a inclusão das informações de prestadores de serviços continuados, o Projeto ajuda a promover a inclusão financeira. (BCB, 2018, p. 137).

Tais indicações apresentam a dimensão do risco em relação à disponibilidade e acesso aos dados de uma parcela expressiva da população brasileira. No atual estágio de desenvolvimento tecnológico em relação às informações, no qual os meios automatizados têm enorme potencial ofensivo, nenhum dado, seja ele de qualquer natureza, pode ter seu valor menosprezado.

Mesmo com a utilização de dados sendo uma política incentivada pelo Banco Mundial²⁹, sob o argumento que uma economia moderna deve se basear em sistemas de informação ao crédito que garantam acesso a dados corretos e confiáveis, relativos ao histórico de crédito do tomador de empréstimo (Bessa, 2019, p. 39), as metodologias utilizadas pelos gestores dos bancos de dados podem representar tanto a viabilidade de consumo e bem-estar, em uma sociedade industrializada, quanto um risco à privacidade.

As atividades desenvolvidas pelos bancos de dados de proteção ao crédito são potencialmente ofensivas à privacidade no que concerne à ideia atual de necessidade de controlo e tutela de dados pessoais (Bessa, 2019, p. 48). Para haver uma sociedade e uma economia mais justa e segura, é preciso criar mecanismos eficientes de defesa e proteção das informações, garantindo a segurança do conteúdo dos bancos de dados, assegurando os direitos básicos dos cidadãos/consumidores, como o direito à privacidade, à honra e à proteção de dados pessoais. (Braunschweiger, 2014).

²⁹ <https://openknowledge.worldbank.org/bitstream/handle/10986/12792/701930ESW0P1180ting0pub010028011web.pdf>

5.5 Gestores do Novo Cadastro Positivo

Em 11 de outubro de 2019, o Banco Central do Brasil publicou, via Diário Oficial da União (Anexo G), a aprovação do registro de quatro empresas responsáveis por gerir o banco de dados do cadastro positivo. São elas: Boa Vista Serviços S.A., Serasa S.A., CNDL – SPC Brasil, já citadas anteriormente neste trabalho, e a Quod – Gestora de Inteligência de Crédito S.A.³⁰. A empresa, criada em 2016 pelos cinco maiores bancos do país, foi constituída pelo Banco do Brasil, Bradesco, Caixa Econômica Federal, Itaú-Unibanco e Santander, com o objetivo declarado de impulsionar o cadastro positivo (Bessa, 2019, p. 26). Vale, aqui, ressaltar que o Banco do Brasil é uma instituição de economia mista, ou seja, tem capital privado e estatal, enquanto a Caixa Econômica Federal é um banco exclusivamente estatal. Portanto, o governo brasileiro, por meio de duas de suas instituições bancárias, mesmo que em menor proporção, participa do fornecimento de informações para os bancos de dados do cadastro positivo. Bessa ressalta que:

Tanto os bancos de dados administrados por entidades públicas, como aqueles geridos por empresas ou associações (sem fins lucrativos), apresentam perigo aos direitos à vida privada e à honra. [...] a superioridade dos bancos de dados decorre mais da utilização dos resultados dos avanços tecnológicos na área de informática do que da natureza pública ou privada da entidade. (Bessa, 2003, p. 172-173 *apud* Bessa, 2019, p. 74).

Sob o argumento de acompanhar o comportamento financeiro das pessoas e valorizar os bons pagadores, as empresas gestoras de bancos de dados do cadastro positivo realizam compartilhamento das informações que integram os históricos de crédito dos consumidores. Antes mesmo de 2011, quando se editou a Lei 12.414, as entidades de proteção ao crédito estavam num processo de ampliação do número e espécie de informações pessoais que são coletadas, armazenadas e divulgadas para o mercado. (Bessa, 2019, p. 30). A Nova Lei do Cadastro Positivo proíbe a utilização de dados sensíveis para composição da nota ou pontuação de crédito e ainda determina, no Art. 7º-A, que os gestores de banco de dados devem disponibilizar, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados

30 <https://www.quod.com.br/>

peçoais para fins de elaboração de análise de risco de crédito, mas o órgão responsável por essa fiscalização, a Autoridade Nacional de Proteção de Dados, ainda não foi constituído, como ainda veremos neste trabalho.

De tal maneira, a nova metodologia de coleta de informações para o cadastro positivo está em pleno funcionamento enquanto a fiscalização não acompanha essa dinâmica, permitindo que o cidadão fique vulnerável perante os bancos de dados. A vulnerabilidade se consubstancia na situação de superioridade decorrente do fato de alguém possuir um banco de dados, com possibilidade de espalhar, em poucos segundos, informações privadas e ofensivas à honra, para locais diversos e distantes (Bessa, 2019, p. 140).

As empresas gestoras dos bancos de dados do cadastro positivo atuam, em regra, mediante remuneração, fato que, inevitavelmente, estabelece uma tratativa comercial, no caso do novo cadastro positivo, em relação ao acesso aos dados de aproximadamente 150 milhões de brasileiros. A Nova Lei do Cadastro Positivo prevê que o Banco Central do Brasil tem um prazo de dois anos, após a publicação da Lei, para elaborar um relatório com resultados obtidos com as mudanças no cadastro positivo, com devida atenção à ocorrência de redução de juros, para fins de reavaliação legislativa.

Ainda sem uma fiscalização efetiva, balizada pela Lei Geral de Proteção de Dados, como veremos adiante, sobre o tratamento das informações coletadas pelos bancos de dados destinados ao cadastro positivo, os cidadãos brasileiros terão seus dados recolhidos e tratados por empresas que têm suas atividades destinadas aos mercados financeiro e comercial. Bessa aponta uma alternativa ao modelo utilizado pelo novo cadastro positivo:

Em vez dessa pluralidade de gestores de arquivos de consumo, melhor seria que houvesse um único banco de dados de proteção ao crédito sob a responsabilidade do Poder Público. O controle sobre a atuação seria mais fácil e eficaz. As informações, hoje espalhadas entre dezenas de bancos gestores de dados, concentrar-se-iam num único arquivo, aumentando a eficiência dos propósitos das entidades de proteção ao crédito, bem como a fiscalização relativa à observância dos direitos do consumidor. (Bessa, 2019, p. 123).

Nessa hipótese, o governo brasileiro colocaria sob sua alçada o gerenciamento das informações de consumidores/cidadãos, hoje espalhadas nos bancos de dados de vários *bureaus* de crédito. Dessa maneira, seria possível atenuar problemas em relação ao tratamento e utilização das informações, além de executar uma fiscalização mais efetiva, tutelada pela Lei Geral de Proteção de Dados.

5.6 LGPD e RGPD

Assim como a primeira versão da Lei do Cadastro Positivo, de 2011, teve influência da Diretiva europeia 95/46, relativa à proteção de dados pessoais, a Nova Lei do Cadastro Positivo foi formatada para ter a sua aplicação associada à Lei Geral de Proteção de Dados (13.709/2018). A LGPD tem previsão de estar plenamente em vigor em agosto de 2021. Mais uma vez, o desenvolvimento da legislação brasileira teve como referência o modelo europeu. A LGPD teve influência direta do Regulamento 679/2016, que revoga a Diretiva 95/46 e estabelece o Regulamento Geral sobre a Proteção de Dados europeu. Como aponta Bessa:

O Regulamento 679 mantém a ideia básica de que o tratamento de dados deve, ao mesmo tempo, permitir o progresso econômico, o desenvolvimento do comércio e promover o bem-estar do homem (...) vale dizer, da dupla face que a tutela da dignidade da pessoa humana assume em relação ao tratamento de informações pelos bancos de dados de proteção ao crédito: uma que, ao facilitar a obtenção de crédito para aquisição de bens e produtos diversos, contribui para o bem-estar material e uma vida melhor; e outra que coloca em constante tensão a privacidade da pessoa, ao manipular seus dados pessoais. (Bessa, 2019, p. 58).

A lei brasileira tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade, sobre o tratamento de dados pessoais, inclusive nos meios digitais. O regulamento europeu também disciplina, nas esferas governamental e privada, o tratamento de dados, inclusive os relativos à proteção de crédito. A Lei Geral de Proteção de Dados determina que o Brasil deve possuir uma autoridade pública, independente, para fiscalizar a aplicabilidade da lei em relação aos bancos de dados de informações pessoais – Autoridade Nacional de Proteção de Dados, ANPD –

seguindo os moldes do Comitê Europeu para Proteção de Dados. Vale, aqui, ressaltar que ainda não há confirmação da data de entrada em vigor da LGPD e tampouco a constituição da ANPD. Enquanto isso, milhares de brasileiros têm seus dados coletados e tratados para construção do histórico de crédito do cadastro positivo.

O modelo europeu tem por objetivo diminuir a sujeição do homem ao computador e às novas tecnologias, buscando restringir as possibilidades de julgamentos com base em perfil digital. “O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar” (art. 22.º, item 1 *apud* Bessa, 2019). Mesmo com a Lei Geral de Proteção de Dados se baseando no modelo europeu, a Lei do Cadastro Positivo permite que o resultado produzido unicamente por definição algorítmica, após coleta de dados sem metodologia transparente, determine o *score* dos cidadãos e, conseqüentemente, a possibilidade de acesso a crédito.

Conclusão

A tecnologia caminha para assumir um papel antes reservado exclusivamente ao ser humano. A linguagem da programação vem ocupando o espaço da deliberação, das leis e normas, reduzindo o ato de governar a uma análise de dados e remodelando os sistemas de governança e/ou administração. A interpretação dos dados, em vez da interpretação das palavras, é uma característica comum aos exemplos apresentados ao longo deste trabalho.

Mesmo sendo executados em diferentes regiões do mundo e sob a tutela de diferentes modelos sociopolíticos, sistemas como o cadastro positivo, o sistema de crédito social e o modelo de governança, gerenciamento de riscos e conformidade de princípios apresentam várias semelhanças em suas metodologias de funcionamento. Nessas propostas, o ser humano fica em segundo plano e as máquinas assumem o protagonismo. As regras e o mundo passam a ser determinados pela máquina. As verdades são produzidas por elas, mesmo que operadas pelo homem (Colvara, 2007, p. 113).

A vigilância, agora, ocorre durante todo o tempo, produzindo reflexos nas sociedades e contribuindo para imposição de valores normativos, que orientem as populações altamente mediatizadas. Essa vigilância constante garante a disciplina dos atores sociais e também a eficácia dos modelos. A discriminação, baseada em análises estatísticas, possibilitada pelo uso do Big Data e dispositivos tecnológicos é capaz de isolar e excluir, dilatando o abismo existente entre as classes mais favorecidas e as demais. O poder, seja ele político ou econômico, não está atrelado a uma única figura, mas pulverizado no funcionamento dos sistemas. A internet, reconhecida pela quebra de paradigmas, como tempo e espaço, por exemplo, assume agora um novo papel. A total conectividade, antes vista como um ideal de funcionamento das sociedades, torna-se instrumento para o monitoramento e controle de todo tipo de informação que possa transitar pela rede.

Valendo-se da mediatização e travestidos de caráter de normalidade, eles segmentam e podem aprofundar ainda mais as diferenças sociais. Permitir que os sistemas legais e de acesso ao crédito sejam conduzidos por resultados produzidos por algoritmos é arriscado para qualquer tipo de sociedade, seja ela oriental ou ocidental, capitalista ou comunista. Decisões que afetam diretamente as sociedades devem ser

deliberadas levando em consideração características dos indivíduos e das comunidades que as constituem. Os bancos de dados de proteção ao crédito, no caso em questão o cadastro positivo, apresentam duas variáveis frente aos cidadãos/consumidores cadastrados, pois são ferramentas que podem viabilizar a obtenção de crédito e, conseqüentemente, garantir aquisição de bens e, ao mesmo tempo, ser uma ameaça à privacidade.

Não é possível negar os avanços trazidos pelo desenvolvimento tecnológico ao longo das últimas décadas. Os benefícios são vários e as transformações causadas por eles têm significativo valor, mas é necessário reconhecer a responsabilidade humana em relação às tecnologias baseadas na utilização dos algoritmos. Esses modelos, alimentados por algoritmos, batem as portas na cara de milhões de pessoas, geralmente pelas razões mais frágeis, e não oferecem apelo. Eles são injustos (O’Neil, 2016, p. 34).

O mantra neoliberal preconiza que não caberia ao Estado desenvolver sistemas, softwares, nem tecnologias. O Estado deve somente encomendá-los e adquiri-los do mercado. O mais grave nessa doutrina é que o Estado não deve querer regulamentar os mercados, muito menos suas empresas. Desse modo, quanto mais o Estado se automatiza, mais tenderá a ficar nas mãos das corporações. Para preservar seus produtos da concorrência feroz, os neoliberais propiciam a proliferação das caixas-pretas, das tecnologias fechadas, dos negócios sigilosos. Assim, o Estado, ao utilizar sistemas algorítmicos e soluções automatizadas, vai ficando mais opaco, menos transparente, mais subordinado às decisões tecnocráticas e mais distante de uma democratização efetiva (Silveira, 2019, p. 1638).

Abandonar a responsabilidade pelas decisões importantes na condução de uma sociedade, terceirizá-las para as máquinas ou simplesmente privatizá-las para o mercado de dados são ações que devem ser temidas e analisadas com extrema cautela. Como as sociedades responderão ao funcionamento de tais sistemas? E quando eles forem os únicos responsáveis pelas mudanças políticas e econômicas? Eles irão fomentar um crescimento das diferenças sociais?

Visando atenuar os impactos causados pela utilização dos algoritmos nas decisões sociopolíticas, a FAT/ML desenvolveu propostas que indicam um caminho responsável para diminuir os danos sociais negativos desde a modelagem até o uso. Os *Principles for Accountable Algorithms and a Social Impact Statement for Algorithms*³¹ (Princípios para Algoritmos Responsáveis e Declaração de Impacto Social para Algoritmos) são uma sugestão de caminho seguro para mitigar os danos causados pela utilização desses modelos. Dentre os princípios estão:

Responsabilidade: disponibilizar vias de reparação externamente visíveis para os efeitos individuais ou sociais adversos de um sistema de decisão algorítmica e designar um responsável interno pelo tratamento de tais questões num prazo adequado;

Explicabilidade: assegurar que as decisões algorítmicas, bem como quaisquer dados que conduzam essas decisões, possam ser explicadas em termos não técnicos aos usuários finais e outras partes interessadas;

Precisão: identificar, registrar e articular fontes de erro e incerteza em todo o algoritmo e suas fontes de dados, de modo que as implicações esperadas e as piores hipóteses possam ser compreendidas, e informar os procedimentos de mitigação;

Auditabilidade: permitir que terceiros interessados analisem, compreendam e revisem o comportamento do algoritmo por meio da divulgação de informações que permitam o monitoramento, verificação ou crítica, inclusive por meio do fornecimento de documentação detalhada, APIs tecnicamente adequadas e termos de uso permissivos;

Justiça: garantir que as decisões algorítmicas não criem impactos discriminatórios ou injustos ao comparar dados demográficos diferentes (por exemplo, raça, sexo, etc.).

Portanto, responsabilizar exclusivamente os algoritmos por possíveis erros ou consequências indesejadas em relação ao *machine learning* não é um argumento coerente. Eles são, juntamente ao Big Data, utilizados como instrumentos para os controles social e econômico, garantidores de sistemas que fazem a manutenção de

31 <https://www.fatml.org/resources/principles-for-accountable-algorithms>

uma série de desigualdades, mas tais modelos matemáticos são desenvolvidos por seres humanos e, no fim, há sempre uma pessoa responsável pela formatação das decisões por eles executadas. Será possível a construção de sociedades mais justas e igualitárias sob a tutela dos algoritmos e do Big Data? Talvez sim, desde que todos os responsáveis pelo desenvolvimento tecnológico também anseiem por isso.

Referências bibliográficas

- Agamben, G. (2004). *Homo Sacer. O poder soberano e a vida nua I*. UFMG. Belo Horizonte.
- _____, _____. (2004). *Estado de exceção*. Boitempo. São Paulo.
- Backer, L. C. (2018). And an Algorithm to Bind them All? Social Credit, Data Driven Governance, and the Emergence of an Operating System for Global Normative Orders. Entangled Legalities Workshop, Geneva. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182889.
- Banco Central do Brasil. (2018). Relatório de Cidadania Financeira. Disponível em: www.bcb.gov.br/Nor/releidfin/docs/Relatorio_Cidadania_Financeira.pdf.
- Bauman, Z. (1991). *Modernidade e ambivalência*. Zahar. Rio de Janeiro.
- _____, _____. (1997). *O mal-estar da pós-modernidade*. Zahar. Rio de Janeiro.
- _____, _____. (1999). *Globalização: As consequências humanas*. Zahar. Rio de Janeiro
- _____, _____. Lyon, D. (2014). *Vigilância líquida*. Zahar. Rio de Janeiro.
- Bessa, L. (2011). *Cadastro Positivo: comentários à Lei 12.414 de 09 de junho de 2011*. Livro eletrônico. Thomson Reuters Brasil. São Paulo.
- _____, _____. (2019). *Nova Lei do Cadastro Positivo: comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD*. Thomson Reuters Brasil. São Paulo.
- Body, D. Crawford, K. (2012). Critical Questions For Big Data: Provocations for a cultural, technological, and scholarly phenomenon. pp. 662-679. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>.
- Braunschweiger, V. (2014). Pontos Obscuros do Cadastro Positivo dos Consumidores. Disponível em: <https://www.emerj.tjrj.jus.br/paginas/rcursodeespecializacao>

_latosensu/direito_do_consumidor_e_responsabilidade_civil/edicoes/n32014/pdf/VeraMariaFBraunschweiger.pdf.

- Castells, M. (2002). *A Sociedade em Rede*. 6ª edição. Paz e Terra. São Paulo.
- Cirucci, A. M. (2018). Digitally Natural: Gender Norms in Black Mirror. Disponível em: <https://www.researchgate.net/publication/328198108>.
- Couldry, N. Heep, A. (2013). Conceptualizing Mediatization: Contexts, traditions, arguments. *Communication Theory*, 23, (3). pp. 191 - 202. doi:10.1111/comt.12019.
- Colvara, L. (2007). Tecnotemismo: a subjetividade em tempos tecnológicos. *Conexão - Comunicação e Cultura*. 6 (11), 109-122. Disponível em: <http://www.ucs.br/etc/revistas/index.php/conexao/article/view/195>.
- Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. Disponível em: <https://ssrn.com/abstract=3175792>.
- Deleuze, G. (1992). *Conversações*. Editora 34 - São Paulo.
- De Mauro, A. Greco, M. Grimaldi, M. (2016). A Formal Definition of Big Data Based on its Essential Features. *Library Review*. Volume 65. pp. 122 – 135. Disponível em: https://www.researchgate.net/publication/299379163_A_formal_definition_of_Big_Data_based_on_its_essential_features.
- Domingos, P. (2017). *O Algoritmo Mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo*. Novatec. São Paulo.
- Doneda, D. (2001). Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm#_ftnref17
- Falcão, R. (2016). Bancos de Dados de Proteção ao Crédito e a Lei do Cadastro Positivo. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/>

178706/001066922.pdf.

- Fortes, V. Bolesina, I. Cella, J. (organizadores) (2015). *Ciberdireito e Democracia: Perspectivas contemporâneas do ciberespaço, da privacidade e da surveillance*. e-book. Deviant. Erechim.
- Foucault, M. (1999). *Vigiar e Punir: o nascimento da prisão*. Vozes. Petrópolis.
- Góis, A. (2017). A eficácia do cadastro positivo e o direito à privacidade. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/a-eficacia-do-cadastro-positivo-e-o-direito-a-privacidade/#_ftn1
- Grassegger, H. Krogerus, M. (2017). The Data That Turned the World Upside Down. Disponível em: http://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.
- IBGE. (2019). Síntese de Indicadores Sociais: Uma Análise das Condições de Vida da População Brasileira. Estudos e Pesquisas – Informação Demográfica e Socioeconômica. Número 40 Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101678.pdf>.
- Mai, Jens-Erik (2016). Big data privacy: The datafication of personal information. *The Information Society*, 32:3, 192-19. Disponível em: <http://dx.doi.org/10.1080/01972243.2016.1153010>.
- Marconi, M. Lakatos, E. (2003). *Fundamentos de metodologia científica*. Atlas. São Paulo.
- Maris, E. Libert, T. Henrichsen, J. (2019). Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites. Disponível em: www.researchgate.net/publication/334478284_Tracking_sex_The_implications_of_widespread_sexual_data_leakage_and_tracking_on_porn_websites
- Mora, J Ferrater. (1978). *Dicionário de Filosofia*. Dom Quixote. Lisboa.

- Neto, A. (2011). O Poder Informático das Empresas e a Proteção do Consumidor. *Revista Dat@venia*. Vol. 3, nº 2. pp. 82-102. Disponível em: <http://revista.uepb.edu.br/index.php/datavenia/article/view/3411-10106-1>.
- Kerr, I. Earle, J. (2013). Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy. *Stanford Law Review*. Volume 65. Disponível em: https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_65_KerrEarle.pdf.
- Kosinski, M. Stillwell, D. Graepel. (2013). Private traits and attributes are predictable from digital records of human behavior. *PNAS*. Vol. 110. no 15. pp. 5802-5805. Disponível em: <https://www.pnas.org/content/110/15/5802>.
- Krause Hansen, H., & Porter, T. (2017). What do Big Data do in Global Governance? *Global Governance: A Review of Multilateralism and International Organizations*. pp. 31-42. Disponível em: <https://doi.org/10.1163/19426720-02301004>.
- La Boétie, E. (2006). *Discurso Sobre a Servidão Voluntária*. e-book. LCC Publicações Eletrônicas.
- Lerman, J. (2013). Big Data and Its Exclusions. *Stanford Law Review*. Volume 66. Disponível em: <https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/>.
- Lessig, L. (2006). *Code*. Code version 2.0. Basic Books. New York.
- Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, risk and digital discrimination*. Routledge. London and New York. Disponível em: http://www.felfel.is/sites/default/files/2016/Lyon%2C_D._%282003%29._Surveillance_and_social_sorting%26_computer_codes_and_mobile_bodies%20%281%29.pdf.

- O'neil, C. (2016). *Weapons of Math Destruction: How big data increases inequality and threatens democracy*. Crown Publishers. New York.
- ONU. (2019). Relatório do Desenvolvimento Humano 2019. Além do rendimento, além das medias, além do presente: Desigualdades no desenvolvimento humano no século XXI. Disponível em: http://hdr.undp.org/sites/default/files/hdr_2019_pt.pdf
- People's Republic of China. (2014). State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020) Disponível em: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-theconstruction-of-a-social-credit-system-2014-2020/>.
- Pinheiro, C. (2012). Cadastro Positivo: A possibilidade de acesso ao crédito como um dos caminhos para o desenvolvimento social. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/9792/Caroline%20da%20Rosa%20Pinheiro.pdf>.
- Richards, Neil M. King, Jonathan H. (2013). Three Paradoxes of Big Data. Stanford Law Review. Volume 64. Disponível em: <https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/>.
- Silveira, S. (2017). *Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais*. e-book. Sesc. São Paulo.
- _____, __. (2019). *Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas*. e-book. Sesc. São Paulo.
- Tene, O. Polonetsky, J. (2012). Privacy in the Age of Big Data: a time for big decisions. Stanford Law Review. Volume 64. Disponível em: www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/
- Vicente, F. (2018). Big Data: conectividade, implicações e desafios. Disponível em:

<https://www.cision.pt/2018/08/big-data-conectividade-implicac%CC%A7o%CC%83es-e-desafios-parte-i/>.

Anexos

Anexo A – Tabela de Suining

Informação de crédito de serviços comerciais (150 pontos)

- Empréstimos bancários (50 pontos)
- Cartão de crédito não-reembolso (50 pontos)
- Desempenho do contrato (30 pontos)
- Empréstimos pessoais (20 pontos)

Informações sobre crédito de serviços sociais (120 pontos)

- Imposto em atraso ou evasão (50 pontos)
- Pagamentos de taxas de utilidade (35 pontos)
- Pagamentos da previdência social (35 pontos)

Informações sobre crédito de gestão social (530 pontos)

- Gestão da cidade (25 pontos)
- Produzir ou vender produtos falsificados (35 pontos)
- Venda de pirâmide, fraude (35 pontos)
- Planejamento de nascimento (35 pontos)
- Atividades heréticas (50 pontos)
- Virtude do agregado familiar (50 pontos)
- Ordem social (50 pontos)
- Roubo de propriedade (50 pontos)
- Violações de trânsito (50 pontos)
- Oferecendo e aceitando subornos (50 pontos)
- Falsas acusações e difamação (100 pontos)

Informações especiais sobre crédito social (200 pontos)

- Contencioso cível (50 pontos)
- Punição administrativa (50 pontos)
- Punição criminal (100 pontos)

声明：百科词条人人可编辑，词条创建和修改均免费，绝不存在官方及代理商付费代编，请勿上当受骗。 [详情>>](#)

首页

分类

秒懂百科

特色百科

用户

权威合作

收藏 | 5 | 0

睢宁县大众信用信息评估细则

编辑 讨论

本词条缺少概述图，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

睢宁县大众信用信息评估细则，为完善睢宁县大众信用管理制度，健全社会信用体系，根据《睢宁县大众信用管理试行办法》，制定本评估细则。

中文名	睢宁县大众信用信息评估细则	B 级	较诚信级别
A 级	诚信级别	C 级	诚信警示级别
		D 级	不诚信级别

目录	1 睢宁县大众信用信息评估细则	3 二大众信用信息评估分值标准	5 四大众信用信息评估时效
	2 一大众信用级别划分	4 三大众信用信息评估计分原则	

睢宁县大众信用信息评估细则

编辑

(Suining County populace credit evaluation of information regulation ; Of credit information to assess the public details of Suining)。

一 大众信用级别划分

编辑

大众信用级别评估采用千分制。每年对个人信用信息评估一次，确定个人信用级别。

- (一) A级为诚信级别，分值在970分以上；
- (二) B级为较诚信级别，分值在850—969分；
- (三) C级为诚信警示级别，分值在600—849分；
- (四) D级为不诚信级别，分值在599分以下。

个人信用信息默认总得分1000分。默认得分为无有效诚信信息级别。有效个人信用信息超过1条以上（含1条），或有效个人信息加、减分超过50分（含50分）的，其个人信用信息进入活跃状态，其得分可以说明个人信用。

二 大众信用信息评估分值标准

编辑

大众信用信息分值由基本分和单加、减分两部分构成，个人信用信息基本分值为1000分，包含四项主要信用信息：商业服务信用信息、社会服务信用信息、社会管理信用信息、社会信用特别信息。其中，商业服务信用信息为150分，社会服务信用信息为120分，社会管理信用信息为530分，社会信用特别信息为200分。

（一）基本分值（1000分）

1. 商业服务信用信息（150分）

(1) 银行借贷（50分）。无还贷拖欠记录的，得50分；有一次还贷拖欠记录的，扣30分；有二次及以上还贷拖欠记录的，扣50分。

(2) 信用卡使用（50分）。无透支逾期未还记录的，得50分；有一次透支逾期未还记录的，扣20分；有二次及以上透支逾期未还记录的，扣50分。

(3) 合同履行（30分）。年内无违约记录的，得30分。因未履行合同，被另一方提起诉讼并被判决违约的，扣30分。

(4) 民间借贷（20分）。年内无违约记录的，得20分。有一次违约记录的，扣10分；有二次及以上违约记录的，扣20分；因非法集资、违法放贷被县有关部门查处的，扣20分。

2. 社会服务信用信息（120分）

(1) 个人纳税（50分）。无欠税记录的，得50分；有欠税、偷税、抗税记录的，扣50分。

(2) 事业费缴纳（35分）。年内无拖欠水、电、有线电视、物业费用记录的，得35分；年内恶意拖欠公用事业费用（3个月以上）发生一次的，扣20分；恶意拖欠公用事业费用二次及以上的，扣35分。

(3) 社会保险缴纳 (35分)。年内缴纳社会保险无拖欠记录的, 得35分; 年内恶意拖欠一次的, 扣20分; 恶意拖欠二次的, 扣30分; 恶意拖欠三次以上的, 扣35分。

3. 社会管理信用信息 (530分)

(1) 城市管理 (25分)。年内无违反城市市容管理记录的, 得25分; 有违反城市市容管理记录, 被公安机关予以治安处罚或被城管部门处罚或被新闻媒体曝光的, 扣25分。

(2) 制假售假 (35分)。年内个人无制假售假记录的, 得35分; 有制假售假记录的, 扣35分。

(3) 传销、欺诈 (35分)。年内个人无参与传销、商业欺诈记录的, 得35分; 有参与传销、商业欺诈记录的, 扣35分。

(4) 计划生育 (35分)。个人无超计划生育记录的, 得35分; 有超计划生育记录的, 扣35分。

(5) 邪教活动 (50分)。无参加邪教记录的, 得50分; 有参加邪教记录的, 扣50分。

(6) 家庭道德 (50分)。无家庭暴力、不赡养老人记录的, 得50分; 有家庭暴力、不履行应尽赡养、抚养义务记录的, 扣50分。

(7) 社会秩序 (50分)。无破坏社会秩序记录的, 得50分; 有围堵冲击党政机关、企业、工地、缠访、闹访等记录, 被公安机关予以治安处罚或被新闻媒体曝光的, 扣50分。

(8) 偷盗财物 (50分)。无偷盗他人财物记录的, 得50分; 有偷盗他人财物记录, 情节较轻被公安机关处以警告、罚款的, 扣50分。

(9) 交通违法 (50分)。无交通违法记录的, 得50分; 年内有轻微交通违法行为的, 扣20分; 有酒后驾驶、超载超限、交通肇事、无证驾驶、闯红灯等严重交通违法记录的, 扣50分。

(10) 行贿受贿 (50分)。无收送礼品、礼金、行贿、受贿记录的, 得50分; 有收送礼品、礼金、行贿、受贿记录的, 扣50分。

(11) 诬告诽谤 (100分)。无利用网络、短信、信函诬告、诽谤他人记录的, 得100分; 有利用网络、短信、信函诬告、诽谤他人记录的, 扣100分。

4. 社会信用特别信息 (200分)

(1) 民事诉讼 (50分)。个人无涉及诚信导致民事诉讼败诉记录的, 得50分; 个人因涉及诚信导致在民事纠纷诉讼中被判承担主要责任的, 扣30分; 承担全部责任的, 扣50分。

(2) 行政处罚 (50分)。个人无行政管理处罚记录的, 得50分; 受到警告、罚款处罚的, 扣30分, 受到吊销执照、吊销许可证、行政拘留处罚的, 扣50分。

(3) 刑事处罚 (100分)。无刑事处罚记录的, 得100分。受到刑事相对不起诉、管制、拘役、有期徒刑缓期执行处罚的, 扣

(2) 行政处罚（50分）。个人无行政管理处罚记录的，得50分；受到警告、罚款处罚的，扣30分，受到吊销执照、吊销许可证、行政拘留处罚的，扣50分。

(3) 刑事处罚（100分）。无刑事处罚记录的，得100分。受到刑事相对不起诉、管制、拘役、有期徒刑缓刑执行处罚的，扣100分。

（二）单加、减分信用信息

1. 单加分信用信息

(1) 个人积极从事志愿、义工服务、扶贫济困、资助助学、见义勇为等社会公益公德事业，有记录的当年加10分；被新闻媒体报道宣传的，当年加15分。

(2) 个人受到县级表彰的，加20分；个人受到市级表彰的，加30分；个人受到省级表彰的，加50分；个人受到国家级表彰的，加100分。

(3) 被评为“睢宁人民好榜样”、“睢宁干部好榜样”的，加100分。

2. 单减分信用信息

(1) 党员受到党内警告、严重警告处分的，扣30分；受到党内撤职、留党察看处分的，扣50分；受到开除党籍处分的，自作出处分决定之日起3年内列为诚信警示级别。

(2) 公务人员受到行政警告、记过、记大过处分的扣30分；受到降级、撤职处分的，扣50分；受到行政开除处分，自作出处分决定之日起3年内列为诚信警示级别。

(3) 个人被判处有期徒刑实刑及以上刑事处罚的，自刑满释放之日起5年内列为诚信警示级别。

(4) 因诬告、诽谤他人、偷盗财物、不赡养老人受到治安拘留以上处罚或被法院判决的，自处罚决定和判决之日起3年内列为诚信警示级别。

三大众信用信息评估计分原则

 编辑

（一）因同一事项而产生的不良信息同属于两项及以上不同信息项的，或同属于单减分信息项的，按最高减分项减分，不重复计分。

（二）同一事项加分项目按最高加分项计分，不重复计分。

（三）因同一事项而产生的不良信息减分后，在信用信息评估有效期内又重新发生同一不良信用信息，在原分值基础上加倍减分。

（四）党员干部因非诚信原因受到党纪、政纪处分的，不纳入个人单减分信用信息。

(四) 党员干部因非诚信原因受到党纪、政纪处分的, 不纳入个人单减分信用信息。

■ 四大众信用信息评估时效

 编辑

(一) 下列信用信息评估有效期为一年:

1. 事业费用缴纳; 2. 社会保险缴纳; 3. 城市管理; 4. 轻微交通违法; 5. 履行合约; 6. 民间借贷; 7. 社会公益公德。

(二) 下列信用信息评估有效期为二年:

1. 银行借贷;
2. 信用卡使用;
3. 个人纳税;
4. 党纪处分;
5. 政纪处分;
6. 行贿受贿;
7. 邪教活动;
8. 民事诉讼;
9. 行政处罚;
10. 刑事处罚;
11. 诬告诽谤;
12. 偷盗财物;
13. 严重交通违法;
14. 家庭道德;
15. 计划生育;
16. 社会秩序;
17. 传销、欺诈;
18. 制假售假。

(三) 个人被判处有期徒刑以上刑罚的, 评估有效期为五年。

(四) 个人单加分信息属市级及以下表彰、奖励的, 评估有效期为二年。

(五) 个人单加分信息属省级及以上表彰、奖励及被评为“睢宁人民好榜样”、“睢宁干部好榜样”的, 评估有效期为三年。

日期: 2010-3-15

词条标签: 组织机构, 社会

Anexo B – 1ª Lei Cadastro Positivo / 2011



CÂMARA DOS DEPUTADOS
Centro de Documentação e Informação

LEI Nº 12.414, DE 9 DE JUNHO DE 2011

Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º. Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor.

Parágrafo único. Os bancos de dados instituídos ou mantidos por pessoas jurídicas de direito público interno serão regidos por legislação específica.

Art. 2º. Para os efeitos desta Lei, considera-se:

I – banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro;

II – gestor: pessoa jurídica responsável pela administração de banco de dados, bem como pela coleta, armazenamento, análise e acesso de terceiros aos dados armazenados;

III – cadastrado: pessoa natural ou jurídica que tenha autorizado inclusão de suas informações no banco de dados;

IV - fonte: pessoa natural ou jurídica que conceda crédito ou realize venda a prazo ou outras transações comerciais e empresariais que lhe impliquem risco financeiro;

V – consulente: pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida por esta Lei;

VI – anotação: ação ou efeito de anotar, assinalar, averbar, incluir, inscrever ou registrar informação relativa ao histórico de crédito em banco de dados; e

VII – histórico de crédito: conjunto de dados financeiros e de pagamentos relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica.

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.

§ 1.º 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.

§ 2.º Para os fins do disposto no § 1.º, 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.

§ 3.º 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.

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.

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

§ 2.º 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.

§ 3.º (Vetado.).

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 – solicitar ao consultante 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.

§ 1.º (Vetado.).

§ 2.º (Vetado.).

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.

§ 1.º 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. 5.º.

§ 2.º O prazo para atendimento das informações estabelecidas nos incisos II, III, IV e V deste artigo será de 7 (sete) dias.

Art. 7º. As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:

I – realização de análise de risco de crédito do cadastrado; ou

II – subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Parágrafo único. Cabe ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar aos consulentes as informações de adimplemento do cadastrado.

Art. 8º. São obrigações das fontes:

I – manter os registros adequados para demonstrar que a pessoa natural ou jurídica autorizou o envio e a anotação de informações em bancos de dados;

II – comunicar os gestores de bancos de dados acerca de eventual exclusão ou revogação de autorização do cadastrado;

III – verificar e confirmar, ou corrigir, em prazo não superior a 2 (dois) dias úteis, informação impugnada, sempre que solicitado por gestor de banco de dados ou diretamente pelo cadastrado;

IV – atualizar e corrigir informações enviadas aos gestores de bancos de dados, em prazo não superior a 7 (sete) dias;

V – manter os registros adequados para verificar informações enviadas aos gestores de bancos de dados; e

VI – fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados.

Parágrafo único. É vedado às fontes estabelecerem políticas ou realizarem operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados que tenham autorizado a anotação de seus dados em bancos de dados.

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.

§ 1.º 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.

§ 2.º 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.

§ 3.º 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.

§ 4.º 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.

Art. 10. É proibido ao gestor exigir exclusividade das fontes de informações.

Art. 11. Desde que autorizados pelo cadastrado, os prestadores de serviços continuados de água, esgoto, eletricidade, gás e telecomunicações, dentre outros, poderão fornecer aos bancos de dados indicados, na forma do regulamento, informação sobre o adimplemento das obrigações financeiras do cadastrado.

Parágrafo único. É vedada a anotação de informação sobre serviço de telefonia móvel na modalidade pós-paga.

Art. 12. Quando solicitado pelo cliente, as instituições autorizadas a funcionar pelo Banco Central do Brasil fornecerão aos bancos de dados indicados as informações relativas às suas operações de crédito.

§ 1.º As informações referidas no caput devem compreender somente o histórico das operações de empréstimo e de financiamento realizadas pelo cliente.

§ 2.º É proibido às instituições autorizadas a funcionar pelo Banco Central do Brasil estabelecer políticas ou realizar operações que impeçam, limitem ou dificultem a transmissão das informações bancárias de seu cliente a bancos de dados, quando por este autorizadas.

§ 3.º O Conselho Monetário Nacional adotará as medidas e normas complementares necessárias para a aplicação do disposto neste artigo.

Art. 13. O Poder Executivo regulamentará o disposto nesta Lei, em especial quanto ao uso, guarda, escopo e compartilhamento das informações recebidas por bancos de dados e quanto ao disposto no art. 5.º.

Art. 14. As informações de adimplemento não poderão constar de bancos de dados por período superior a 15 (quinze) anos.

Art. 15. As informações sobre o cadastrado constantes dos bancos de dados somente poderão ser acessadas por consulentes que com ele mantiverem ou pretenderem manter relação comercial ou creditícia.

Art. 16. O banco de dados, a fonte e o consulente são responsáveis objetiva e solidariamente pelos danos materiais e morais que causarem ao cadastrado.

Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei 8.078, de 11 de setembro de 1990 – Código de Proteção e Defesa do Consumidor, aplicam-se as sanções e penas nela previstas e o disposto no § 2.º.

§ 1.º Nos casos previstos no caput, a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa.

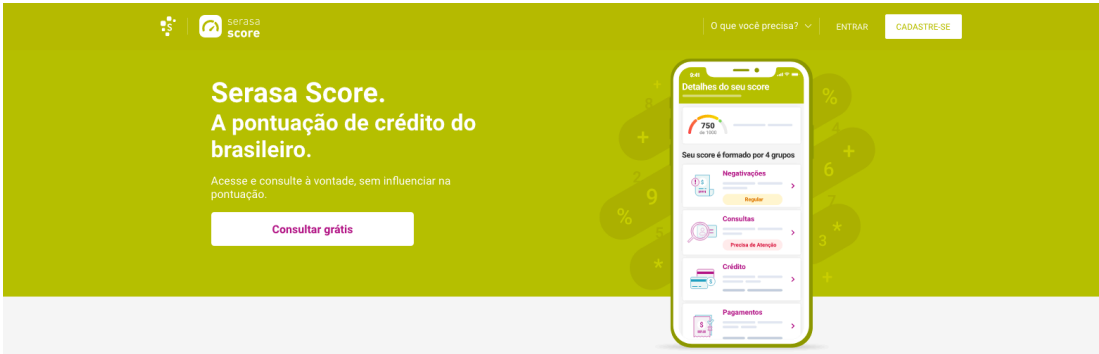
§ 2.º Sem prejuízo do disposto no caput e no § 1.º, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas, estabelecendo aos bancos de dados que descumprirem o previsto nesta Lei obrigações de fazer com que sejam excluídas do cadastro, no prazo de 7 (sete) dias, informações incorretas, bem como cancelados cadastros de pessoas que não autorizaram a abertura.

Art. 18. Esta Lei entra em vigor na data de sua publicação.

Brasília, 9 de junho de 2011; 190º da Independência e 123º da República.


DILMA ROUSSEFF
José Eduardo Cardozo
Guido Mantega

Anexo C – Serasa Experian/Score




The image shows a promotional banner for Serasa Score. On the left, the website header includes the Serasa Score logo and navigation links for 'O que você precisa?', 'ENTRAR', and 'CADASTRE-SE'. The main text reads 'Serasa Score. A pontuação de crédito do brasileiro.' followed by the instruction 'Acesse e consulte à vontade, sem influenciar na pontuação.' and a 'Consultar grátis' button. On the right, a smartphone displays the 'Detalhes do seu score' app interface, showing a score of 758 and a breakdown into four categories: Negativações, Consultas, Fretas de Aterragem, and Pagamentos.

Entenda sua pontuação




O Serasa Score é uma pontuação que vai de 0 a 1000

Indica a probabilidade de um grupo de pessoas com o mesmo perfil atrasar, ou não, uma conta.



O Score é calculado com base em algumas informações suas


Seu histórico de crédito com o mercado, dados de negativação e cadastro positivo, caso esteja aberto em seu nome.



Saiba o que influencia seu Serasa Score

Agora você pode acompanhar quais desses grupos interferem na sua pontuação: Negativações, Consultas, Crédito e Pagamentos. Assim você entende e cuida do seu Serasa Score com mais transparência.

Anexo D – Boa Vista/Score

BoaVista 

CONSULTA DE CPF | CADASTRO POSITIVO | SCORE | RADAR PESSOAL | SOS CHEQUES E DOCUMENTOS | EDUCAÇÃO FINANCEIRA

CADASTRE-SE | ENTRAR



O que é o Score Boa Vista?

No dia a dia, você faz compras, paga contas, faz um financiamento ou um pedido de empréstimo... Tudo isso contribui para formar a sua pontuação de crédito, ou como você já deve ter ouvido por aí, o seu **Score**.

Essa pontuação ajuda as empresas a analisarem o risco de uma venda e decidirem se é uma boa fechar aquele negócio. Por isso, é muito importante que você entenda como o seu Score Boa Vista é calculado para mantê-lo sempre alto.

VEJA SEU SCORE

Como funciona o Score?

O **Score Boa Vista** é calculado usando as seguintes categorias de informações:

- *Seu comportamento de pagamentos*
- *Sua busca por crédito no mercado*
- *Seus pedidos de cartão ou de aumento de limite, financiamentos e cotações, entre outros.*
- *Suas informações cadastrais.*



713

A pontuação varia de **0 a 1.000** e quanto maior, melhor. *Por isso, acompanhe a sua pontuação!*



CÂMARA DOS DEPUTADOS

Centro de Documentação e Informação

LEI Nº 12.414, DE 9 DE JUNHO DE 2011

Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor.

Parágrafo único. Os bancos de dados instituídos ou mantidos por pessoas jurídicas de direito público interno serão regidos por legislação específica.

Art. 2º Para os efeitos desta Lei, considera-se:

I - banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro;

II - gestor: pessoa jurídica que atenda aos requisitos mínimos de funcionamento previstos nesta Lei e em regulamentação complementar, responsável pela administração de banco de dados, bem como pela coleta, pelo armazenamento, pela análise e pelo acesso de terceiros aos dados armazenados; *(Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

III - cadastrado: pessoa natural ou jurídica cujas informações tenham sido incluídas em banco de dados; *(Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

IV - fonte: pessoa natural ou jurídica que conceda crédito, administre operações de autofinanciamento ou realize venda a prazo ou outras transações comerciais e empresariais que lhe impliquem risco financeiro, inclusive as instituições autorizadas a funcionar pelo Banco Central do Brasil e os prestadores de serviços continuados de água, esgoto, eletricidade, gás, telecomunicações e assemelhados; *(Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

V - consulente: pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida por esta Lei;

VI - anotação: ação ou efeito de anotar, assinalar, averbar, incluir, inscrever ou registrar informação relativa ao histórico de crédito em banco de dados; e

VII - histórico de crédito: conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica. (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

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.

§ 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.

Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a: (“Caput” do artigo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

I - abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas; (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

II - fazer anotações no cadastro de que trata o inciso I do *caput* deste artigo; (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

III - compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados; e (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

IV - disponibilizar a consulentes:

a) a nota ou pontuação de crédito elaborada com base nas informações de adimplemento armazenadas; e

b) o histórico de crédito, mediante prévia autorização específica do cadastrado. (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 1º (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 2º (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 3º (VETADO).

§ 4º A comunicação ao cadastrado deve:

I - ocorrer em até 30 (trinta) dias após a abertura do cadastro no banco de dados, sem custo para o cadastrado;

II - ser realizada pelo gestor, diretamente ou por intermédio de fontes; e

III - informar de maneira clara e objetiva os canais disponíveis para o cancelamento do cadastro no banco de dados. (Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 5º Fica dispensada a comunicação de que trata o § 4º deste artigo caso o cadastrado já tenha cadastro aberto em outro banco de dados. (Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 6º Para o envio da comunicação de que trata o § 4º deste artigo, devem ser utilizados os dados pessoais, como endereço residencial, comercial, eletrônico, fornecidos pelo cadastrado à fonte. (Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 7º As informações do cadastrado somente poderão ser disponibilizadas a consulentes 60 (sessenta) dias após a abertura do cadastro, observado o disposto no § 8º deste artigo e no art. 15 desta Lei. (Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 8º É obrigação do gestor manter procedimentos adequados para comprovar a autenticidade e a validade da autorização de que trata a alínea b do inciso IV do *caput* deste artigo. (Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 5º São direitos do cadastrado:

I - obter o cancelamento ou a reabertura do cadastro, quando solicitado; (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado; (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

III - solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação; (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;

V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; *(Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e

VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

§ 1º (VETADO).

§ 2º (VETADO).

§ 3º O prazo para disponibilização das informações de que tratam os incisos II e IV do *caput* deste artigo será de 10 (dez) dias. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

§ 4º O cancelamento e a reabertura de cadastro somente serão processados mediante solicitação gratuita do cadastrado ao gestor. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

§ 5º O cadastrado poderá realizar a solicitação de que trata o § 4º deste artigo a qualquer gestor de banco de dados, por meio telefônico, físico e eletrônico. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

§ 6º O gestor que receber a solicitação de que trata o § 4º deste artigo é obrigado a, no prazo de até 2 (dois) dias úteis:

I - encerrar ou reabrir o cadastro, conforme solicitado; e

II - transmitir a solicitação aos demais gestores, que devem também atender, no mesmo prazo, à solicitação do cadastrado. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

§ 7º O gestor deve proceder automaticamente ao cancelamento de pessoa natural ou jurídica que tenha manifestado previamente, por meio telefônico, físico ou eletrônico, a vontade de não ter aberto seu cadastro. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

§ 8º O cancelamento de cadastro implica a impossibilidade de uso das informações do histórico de crédito pelos gestores, para os fins previstos nesta Lei, inclusive para a composição de nota ou pontuação de crédito de terceiros cadastrados, na forma do art. 7º-A desta Lei. *(Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)*

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; (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

V - cópia de texto com o sumário dos seus direitos, definidos em lei ou em normas infralegais pertinentes à sua relação com gestores, bem como a lista dos órgãos governamentais aos quais poderá ele recorrer, caso considere que esses direitos foram infringidos; e (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

VI - confirmação de cancelamento do cadastro. (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 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 de que tratam os incisos II, III, IV e V do *caput* deste artigo será de 10 (dez) dias. (Parágrafo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 7º As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:

I - realização de análise de risco de crédito do cadastrado; ou

II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Parágrafo único. Cabe ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar aos consulentes as informações de adimplemento do cadastrado.

Art. 7º-A. Nos elementos e critérios considerados para composição da nota ou pontuação de crédito de pessoa cadastrada em banco de dados de que trata esta Lei, não podem ser utilizadas informações:

I - que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas;

II - de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica; e

III - relacionadas ao exercício regular de direito pelo cadastrado, previsto no inciso II do *caput* do art. 5º desta Lei.

§ 1º O gestor de banco de dados deve disponibilizar em seu sítio eletrônico, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito.

§ 2º A transparência da política de coleta e utilização de dados pessoais de que trata o § 1º deste artigo deve ser objeto de verificação, na forma de regulamentação a ser expedida pelo Poder Executivo. (Artigo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 8º São obrigações das fontes:

I - (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

II - (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

III - verificar e confirmar, ou corrigir, em prazo não superior a 2 (dois) dias úteis, informação impugnada, sempre que solicitado por gestor de banco de dados ou diretamente pelo cadastrado;

IV - atualizar e corrigir informações enviadas aos gestores, em prazo não superior a 10 (dez) dias; (Inciso com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

V - manter os registros adequados para verificar informações enviadas aos gestores de bancos de dados; e

VI - fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados.

Parágrafo único. É vedado às fontes estabelecer políticas ou realizar operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados. (Parágrafo único com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 9º O compartilhamento de informações de adimplemento entre gestores é permitido na forma do inciso III do *caput* do art. 4º desta Lei. (“Caput” do artigo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 1º O gestor que receber informação por meio de compartilhamento equipara-se, para todos os efeitos desta Lei, ao gestor que anotou originariamente a informação, inclusive quanto à responsabilidade por eventuais prejuízos a que der causa e ao dever de receber e processar impugnações ou cancelamentos e realizar retificações. (Parágrafo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 2º O gestor originário é responsável por manter atualizadas as informações cadastrais nos demais bancos de dados com os quais compartilhou informações, sem nenhum ônus para o cadastrado. (Parágrafo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 3º (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

§ 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.

Art. 10. É proibido ao gestor exigir exclusividade das fontes de informações.

Art. 11. (Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 12. As instituições autorizadas a funcionar pelo Banco Central do Brasil fornecerão as informações relativas a suas operações de crédito, de arrendamento mercantil e de autofinanciamento realizadas por meio de grupos de consórcio e a outras operações com características de concessão de crédito somente aos gestores registrados no Banco Central do Brasil. (*“Caput” do artigo com redação dada pela Lei Complementar nº 166, de 8/4/2019*)

§ 1º (*Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

§ 2º (*Revogado pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

§ 3º O Conselho Monetário Nacional adotará as medidas e normas complementares necessárias para a aplicação do disposto neste artigo.

§ 4º O compartilhamento de que trata o inciso III do *caput* do art. 4º desta Lei, quando referente a informações provenientes de instituições autorizadas a funcionar pelo Banco Central do Brasil, deverá ocorrer apenas entre gestores registrados na forma deste artigo. (*Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

§ 5º As infrações à regulamentação de que trata o § 3º deste artigo sujeitam o gestor ao cancelamento do seu registro no Banco Central do Brasil, assegurado o devido processo legal, na forma da Lei nº 9.784, de 29 de janeiro de 1999. (*Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

§ 6º O órgão administrativo competente poderá requerer aos gestores, na forma e no prazo que estabelecer, as informações necessárias para o desempenho das atribuições de que trata este artigo. (*Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019*)

§ 7º Os gestores não se sujeitam à legislação aplicável às instituições financeiras e às demais instituições autorizadas a funcionar pelo Banco Central do Brasil, inclusive quanto às disposições sobre processo administrativo sancionador, regime de administração especial temporária, intervenção e liquidação extrajudicial. (*Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

§ 8º O disposto neste artigo não afasta a aplicação pelos órgãos integrantes do Sistema Nacional de Defesa do Consumidor (SNDC), na forma do art. 17 desta Lei, das penalidades cabíveis por violação das normas de proteção do consumidor. (*Parágrafo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

Art. 13. O Poder Executivo regulamentará o disposto nesta Lei, em especial quanto: (*“Caput” do artigo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

I - ao uso, à guarda, ao escopo e ao compartilhamento das informações recebidas por bancos de dados; (*Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação*)

II - aos procedimentos aplicáveis aos gestores de banco de dados na hipótese de vazamento de informações dos cadastrados, inclusive com relação à comunicação aos órgãos responsáveis pela sua fiscalização, nos termos do § 1º do art.

17 desta Lei; e (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

III - ao disposto nos arts. 5º e 7º-A desta Lei. (Inciso acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 14. As informações de adimplemento não poderão constar de bancos de dados por período superior a 15 (quinze) anos.

Art. 15. As informações sobre o cadastrado constantes dos bancos de dados somente poderão ser acessadas por consulentes que com ele mantiverem ou pretenderem manter relação comercial ou creditícia.

Art. 16. O banco de dados, a fonte e o consulente são responsáveis, objetiva e solidariamente, pelos danos materiais e morais que causarem ao cadastrado, nos termos da Lei nº 8.078, de 11 de setembro de 1990 (Código de Proteção e Defesa do Consumidor). (Artigo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor, aplicam-se as sanções e penas nela previstas e o disposto no § 2º.

§ 1º Nos casos previstos no *caput*, a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa.

§ 2º Sem prejuízo do disposto no *caput* e no § 1º deste artigo, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento, conforme disposto no inciso I do *caput* do art. 5º desta Lei. (Parágrafo com redação dada pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 17-A. A quebra do sigilo previsto na Lei Complementar nº 105, de 10 de janeiro de 2001, sujeita os responsáveis às penalidades previstas no art. 10 da referida Lei, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 (Código de Proteção e Defesa do Consumidor). (Artigo acrescido pela Lei Complementar nº 166, de 8/4/2019, publicada no DOU de 9/4/2019, em vigor 91 dias após a publicação)

Art. 18. Esta Lei entra em vigor na data de sua publicação.

Brasília, 9 de junho de 2011; 190º da Independência e 123º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Guido Mantega

Anexo F – Comunicação Cadastro Positivo (e-mail) / janeiro 2020

16/01/2020

Comunicamos que o seu Cadastro Positivo foi aberto nas empresas Boa Vista, Quod, Serasa Experian e SPC Brasil, devidamente aderentes aos requisitos legais para atuação como gestoras de banco de dados.

Com a alteração da Lei 12.414/2011, em vigor desde 9 de julho de 2019, passou a ser automática a abertura do seu cadastro, com informações de histórico de crédito e pagamentos, o chamado Cadastro Positivo.

Mas o que é o Cadastro Positivo?

O Cadastro Positivo é uma forma mais abrangente e mais justa de avaliar o seu acesso ao crédito, levando em consideração todo o seu histórico de pagamentos de obrigações, e não somente uma ou mais dívidas atrasadas.

Dessa forma, as empresas com as quais você quer se relacionar poderão analisar seu potencial de bom pagador com base no seu comportamento ao longo do tempo, e não apenas com base no cadastro negativo. Antes, somente as contas que você deixou de pagar eram analisadas. Com o novo Cadastro Positivo, será possível mostrar também todos os seus pagamentos em dia, que serão considerados pelas empresas ao realizar negócios com você.

Ou seja, com o seu Cadastro Positivo, você terá mais chances de ter melhores condições e acesso a crédito. E não precisa se preocupar, pois os seus dados serão usados apenas para o cálculo do seu Score de Crédito (pontuação de crédito, calculada a partir das informações do cadastro). Se você autorizar, os dados também poderão ser detalhados para as empresas que você escolher.

Mesmo conhecendo os seus benefícios e vantagens, caso você não queira participar do Cadastro Positivo, é possível solicitar o cancelamento do seu cadastro, gratuitamente, nos mesmos canais de atendimento de qualquer um dos birôs participantes acima. Caso seja solicitado o cancelamento, nenhuma empresa terá acesso aos seus dados positivos. Para mais informações, ou contatos das empresas, acesse o site www.brasilnositivo.com.br



Anexo G – Diário Oficial da União – Brasil – 11/10/2019

AVISOS PROCESSOS APROVADOS PELA DIRETORIA CO...

<http://www.in.gov.br/web/dou/-/avisos-processos-aprovados-pela-...>

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 11/10/2019 | Edição: 198 | Seção: 3 | Página: 43

Órgão: Ministério da Economia/Banco Central do Brasil/Área de Organização do Sistema Financeiro e de Resolução/Departamento de Organização do Sistema Financeiro

AVISOS PROCESSOS APROVADOS PELA DIRETORIA COLEGIADA

162290 - Boa Vista Serviços S.A. (CNPJ 11.725.176). Assunto: Registro de gestor de banco de dados. Data: 9.10.2019.

162098 - Gestora de Inteligência de Crédito S.A. (Quod) (CNPJ 28.042.871). Assunto: Registro de gestor de banco de dados. Data: 9.10.2019.

162421 - Serasa S.A. (CNPJ 62.173.620). Assunto: Registro de gestor de banco de dados. Data: 9.10.2019.

162913 - Confederação Nacional de Dirigentes Lojistas (CNDL - SPC Brasil) (CNPJ 34.173.682). Assunto: Registro de gestor de banco de dados. Data: 9.10.2019.

PROCESSOS APROVADOS PELO DEPARTAMENTO DE ORGANIZAÇÃO DO SISTEMA FINANCEIRO

161629 - Banco Bradesco Cartões S.A. (CNPJ 59.438.325). Assuntos: incorporação da totalidade das ações da Amapari Administradora de Cartões S.A. (CNPJ 15.012.678), nos termos do artigo 252 da Lei nº 6.404, de 1976; alteração do capital de R\$2.600.000.000,00 para R\$5.470.960.776,27 (AGE de 30.6.2019). Decisão: Chefe-Adjunto. Data: 9.10.2019.

161629 - Banco Bradescard S.A. (CNPJ 04.184.779). Assuntos: incorporação da Amapari Administradora de Cartões S.A. (CNPJ 15.012.678), mediante versão da totalidade de seu patrimônio e consequente extinção, sucedendo-lhe o incorporador em todos os direitos e obrigações; alteração do capital de R\$ 1.991.716.406,54 para R\$4.862.677.182,81 (AGE de 30.6.2019). Decisão: Chefe-Adjunto. Data: 9.10.2019.

161861 - Cooperativa de Economia e Crédito Mútuo dos Funcionários das Instituições de Serviço Social Autônomo em Manaus Ltda. (CNPJ 02.321.862). Assunto: mudança da denominação social para Coopsebram - Cooperativa de Economia e Crédito Ltda. (AGE de 5.7.2019). Decisão: Gerente-Técnico da GTREC. Data: 9.10.2019.

1601616463 - Banco XP S.A. (CNPJ 33.264.668). Assuntos: autorização para funcionamento como banco múltiplo, com as carteiras comercial e de investimento, cuja constituição foi autorizada pela Diretoria Colegiada em 13.12.2018; sede no Rio de Janeiro (RJ); capital social de R\$100.000.000,00; autorização para realizar operações no mercado de câmbio; controladores: Guilherme Dias Fernandes Benchimol, Julio Capua Ramos da Silva, Carlos Alberto Ferreira Filho, Daniel Albernaz Lemos, Gabriel Klas da Rocha Leal, Pedro Henrique Cristoforo da Silveira e Fabricio Cunha de Almeida (AGC de 30.1.2019; AGE de 5.9.2019). Decisão: Chefe. Data: 10.10.2019.

JOSE REYNALDO DE ALMEIDA FURLANI

Chefe

Este conteúdo não substitui o publicado na versão certificada.