FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

YASMIN SILVA BARRÊTO

FRAGILIDADE NA PROTEÇÃO DOS BANCOS DE DADOS DE INFORMAÇÕES PESSOAIS DO CONSUMIDOR

ARACAJU
2017

YASMIN SILVA BARRÊTO

FRAGILIDADE NA PROTEÇÃO DOS BANCOS DE DADOS DE INFORMAÇÕES PESSOAIS DO CONSUMIDOR

Monografia apresentada como requisito de aprovação na disciplina TCC II e graduação no Curso de Bacharelado em Direito da Faculdade de Administração e Negócios de Sergipe - FANESE.

Orientador: Prof. Me. Afonso Carvalho de Oliva

ARACAJU
2017

B273f

BARRETO, Yasmin Silva.

Fragilidade Na Proteção Dos Bancos De Dados De Informações Pessoais Do Consumidor / Yasmin Silva Barreto. Aracaju, 2017. 63f.

Monografia (Graduação) Faculdade de Administração e Negócios de Sergipe. Coordenação de Direito.

Elaborada Pela Bibliotecária Lícia de Oliveira – CRB-5/1255

YASMIN SILVA BARRÊTO

FRAGILIDADE NA PROTEÇÃO DOS BANCOS DE DADOS DE INFORMAÇÕES PESSOAIS DO CONSUMIDOR

Monografia apresentada à banca examinadora da Faculdade de Administração e Negócios de Sergipe, como pré-requisito para obtenção do grau de bacharel em Direito.

Aprovada em: 02/12/17

BANCA EXAMINADORA

Prof. Me. Afonso Carvalho de Oliva (Orientador)

Faculdade de Administração e Negócios de Sergipe

Prof. Me. Emerson Pracz

Faculdade de Administração e Negócios de Sergipe

Luis Anderson Ribeiro Leite

Prof. Dr. Luis Anderson Ribeiro Leite

Faculdade de Administração e Negócios de Sergipe

RESUMO

O presente trabalho tem como objetivo investigar a fragilidade na proteção dos bancos de dados de informações pessoais do consumidor pelas empresas que os detêm. O estudo aborda desde a origem da necessidade da criação dos bancos de dados, até as formas de tratamento e procedimentos realizados nestes dados de informações pessoais, evidenciando os princípios e garantias constitucionais, bem como os direitos básicos dos consumidores. As informações fornecidas pelo consumidor, com prévio consentimento expresso, ocasionam a circulação dos dados entre as empresas com o objetivo de dinamizar o mercado de consumo. Com essa circulação, ilegal ou não, surge a responsabilidade civil dessas empresas, onde a intervenção do Estado é necessária para solucionar os conflitos oriundos desse compartilhamento. A análise destes dados em consonância com o direito à privacidade e à proteção dos dados pessoais do consumidor deve obedecer às normas do Código de Defesa do Consumidor e às demais leis existentes que tratem desses bancos, a exemplo da Lei de Cadastro Positivo e da Lei de Informação. Essas leis surgem da necessidade de proteger os dados do consumidor das empresas no mercado de consumo, já que estas são as detentoras das informações pessoais e possuem o rápido desenvolvimento tecnológico ao seu dispor, tornando o consumidor ainda mais vulnerável.

Palavras-chave: Banco de dados pessoais. Consumidor. Código de Defesa do Consumidor. Legislação.

ABSTRACT

The present work aims to investigate the fragility in the protection of the databases of personal information of the consumer by the companies that hold them. The study addresses from the origin of the need to create databases, to the forms of treatment and procedures performed in these personal information, highlighting the principles and constitutional guarantees, as well as the basic rights of consumers. The information provided by the consumer, with prior express consent, causes the circulation of the data among the companies with the purpose of dynamizing the consumer market. With this movement, illegal or not, there arises the civil responsibility of these companies, where the intervention of the State is necessary to solve the conflicts resulting from this sharing. The analysis of these data in accordance with the right to privacy and the protection of the personal data of the consumer must comply with the rules of the Consumer Protection Code and other existing laws dealing with these banks, such as the Positive Registration Law and the Information. These laws arise from the need to protect consumer data of companies in the consumer market, as these are the holders of personal information and have the rapid technological development at their disposal, making the consumer even more vulnerable

Keywords: Personal database. Consumer. Legislation. Code of Consumer Protection.

Dedico à Deus, aos meus pais Miguel e Maria da Conceição e ao meu irmão Michel Gustavo, por todo o apoio durante esses cinco anos

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer aos meus pais, Miguel e Maria da Conceição, fundamentais nessa caminhada, por todo o apoio e assistência durante esse longo período acadêmico, na minha decisão de abandonar o curso de Design Gráfico e escolha do curso de Direito. Sou muito grata a tudo que fizeram e fazem por mim, espero superar sempre suas expectativas. Muito obrigada e amo vocês!

Ao meu irmão, Michel por todas as ajudas possíveis durante esses cinco anos, nas indicações e empréstimos de livros e na retirada de dúvidas, mesmo que de forma nada forçada. Obrigada.

A minha avó materna, Maria Isabel por me receber tão bem à oito anos após a mudança de João Pessoa pra Aracaju. Posso não demonstrar o quanto sou grata por tudo que fez por mim, por isso, muito obrigada.

A minha avó paterna, Maria das Neves, mesmo distante, sempre rezando e pedindo o meu bem, me recepcionando maravilhosamente bem quando vou à São Paulo. Quero ter a força e garra que a sra. tem, muito obrigada por tudo.

As minhas amigas Rebeka, Mariana, Karla e Sueli e a minha cunhada, Tamara Isis por todo o apoio durante o curso, principalmente nessa reta final, sempre me motivando e ajudando nos momentos felizes e tristes, saibam que vocês são demais e amo vocês. Obrigada!

Aos meus amigos Felipe e Kelvin (os tops), Rhuan Felipe, Juan, Marco Antônio e Rafael Pimenta por sempre que solicitava me ajudavam, alguns mais próximos do que outros. Adoro vocês.

Ao meu orientador e professor Afonso Oliva por todo o auxilio com seus conhecimentos e disponibilidade em ajudar durante o período do TCC, muito obrigada.

Aos primos Carla (e Pepê), Diego e Victor pelos momentos de descontração e piadas ruins e as minhas tias Suzaneide, Rosemary e Silvanete por apoio durante esses anos.

A todos primos(as), tios(as) e colegas, alguns mais presentes do que outros, por toda a contribuição, mesmo que indireta, durante a conclusão desse longo percurso.
Por ultimo e não menos importante agradeço a Deus por sempre iluminar meu caminho e escolhas nesse caminho árduo. Devo tudo a Ti Senhor.

.

SUMÁRIO

1. INTRODUÇÃO

Desde a antiguidade já ocorriam práticas comerciais entre os povos, mesmo que primitivas. Passando pelo Império Romano, pelo feudalismo e pelas revoluções ao redor do mundo, resultando na prática do capitalismo, que visa a obtenção de lucros.

A necessidade da circulação da moeda, ocasionado pelo crescimento continuo do comércio a partir do desenvolvimento das cidades, transformando-as em grandes centros, com o surgimento do capitalismo demonstrou a necessidade de ampliação do mercado de consumo, com o processo de industrialização e massificação das relações de consumo, na qual o fornecedor não conhecia mais o consumidor, extinguindo as relações pessoais.

Com a massificação do mercado de consumo, tecnologias cada vez mais avançadas e o fim das relações pessoais entre o fornecedor e consumidor, fez necessário a existência de uma norma jurídica que regulamentasse essas novas relações, originando a Lei 8.078/1990, conhecida como Código de Defesa do Consumidor (CDC).

Devido a grande quantidade de empresas que disputam um espaço no mercado de consumo, que obedecem ao principio da livre concorrência e que buscam sempre o aumento da produção e sua comercialização, gerou-se a necessidade de um método efetivo para constatar informações acerca dos consumidores a fim de facilitar o dinamismo neste mercado.

Os bancos de dados surgem com o intuito de analisar informações pessoais e devem atender às normas e aos princípios constitucionais que estão contidos no próprio Código de Defesa do Consumidor. Mesmo sendo o marco jurídico que regulamenta as relações de consumo no Brasil, este não normatizava completamente esses bancos, necessitando de leis que abordassem desde o modo de coleta, armazenamento e a possível difusão desses dados pessoais do consumidor, a fim de resguardar o seu direito à privacidade.

Este trabalho apresenta a aplicação do ordenamento jurídico brasileiro acerca dos bancos de dados, desde a aplicação dos princípios salvaguardados aos consumidores, até a regulamentação pelo Código de Defesa do Consumidor.

O capítulo inicial trata das normas específicas de funcionamento destes bancos, abordando a Lei 12.414/2011, chamada de Lei do Cadastro Positivo, regula, em seu artigo primeiro, a formação e consulta dos dados a partir dos bancos de dados. Embora criada para regular a formação dos bancos de dados que continham informações "negativas", com o passar do tempo, adveio a necessidade de conter informações chamadas de "positivas", referentes aos pagamentos feitos pelo consumidor sem nenhum atraso.

O segundo capítulo discute a necessidade e a origem dos bancos de dados, e de que forma estes coletam, tratam e realizam a possível cessão desses dados. Embora seja necessária a autorização expressa por parte do consumidor para realização desta cessão, muitas vezes os bancos violam esta norma.

O terceiro e último capítulo aborda o posicionamento do Superior Tribunal de Justiça a respeito dos bancos de dados e faz uma breve análise de jurisprudências e a responsabilização civil destes quando infringirem as normas jurídicas que as regulam. Ao fim do capítulo foi analisado o funcionamento do Sistema "*scoring*" e o modo que o STJ julga suas práticas no Brasil.

A partir dos apontamentos surgiram os seguintes questionamentos:

- Quão seguro é a transferência desses dados pessoais por parte dos bancos de dados?
- Quais princípios devem ser obedecidos pelos bancos de dados?
- Esses bancos de dados devem obedecer a qual ordenamento jurídico brasileiro?
- De que modo os dados coletados devem ser tratados?
- Qual o dever deles quanto à proteção e à privacidade dos dados?
- Se desrespeitarem esses ordenamentos, quais serão as consequências à luz do direito brasileiro?

No desenvolvimento do trabalho utilizou-se o método dedutivo para demonstrar a maneira como os bancos de dados utilizam os dados pessoais dos consumidores, à luz do ordenamento jurídico, e quais medidas devem ser adotadas por eles ao ceder informações pessoais, impossibilitando de violar o direito à privacidade e proteção dos seus dados.

O trabalho foi iniciado realizando-se uma pesquisa bibliográfica em obras e artigos científicos especializados sobre o tema. Baseado na literatura selecionada, o trabalho avançou pela abordagem do método dedutivo, com o auxilio do método histórico para a melhor compreensão do tema. A natureza da pesquisa é qualitativa e exploratória, visando aprofundar a discussão e obtenção dos resultados. O trabalho também foi desenvolvido através de estudos de casos e verificando o histórico relacionado ao tema.

O objetivo geral deste presente trabalho foi verificar a fragilidade dos bancos de dados de informações pessoais na proteção dessas informações ao transferirem à terceiros, dados que violam direito à privacidade e à honra do consumidor.

2. ORDENAMENTO JURIDICO BRASILEIRO NA PROTEÇÃO DO CONSUMIDOR

Para analisar os bancos de dados e como são regulados legalmente, faz-se necessário a análise de princípios dispostos em todo o ordenamento jurídico para garantir ao consumidor seus direitos, através das aplicações de legislações que serão discutidas a seguir.

2.1. Princípios Constitucionais e Informadores do Consumidor

A Constituição Federal de 1988, por estar acima de todas outras normas, juridicamente falando, dissipa em todo seu corpo princípios que protegem o ser humano como um todo.

A Carta Magna elenca o princípio da Dignidade da Pessoa Humana, em seu artigo 1º, inciso III, como base para todos os outros princípios e ordenamentos jurídicos e fora positivado com a Declaração Universal dos Direitos Humanos.

É inegável que o consumo passou a ser essencial a vida do ser humano, em consequência, o consumidor é a parte vulnerável da relação com o fornecedor e deve ficar protegido a luz da justiça, conforme a Constituição Federal.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor. (BRASIL, 1988)

Vale ressaltar que, para que seja posto em prática a dignidade da pessoa humana, primeiro há de se garantir os direitos básicos do consumidor.

> A honra [...] compreende-se desde atributos ou qualidades inerentes a qualquer pessoa, pelo fato de ser pessoa, e decorrentes da dignidade da pessoa humana, quanto a outros atributos que o indivíduo passa a ter em vista de suas relações ao longo da vida. (MIRAGEM, 2015, p.191)

A Constituição Federal prevê o direito à privacidade, em seu artigo 5º, inciso X sendo “invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente da sua violação”, atuando como direito a personalidade dos seres humanos, possibilitando a ameaça direta desse por parte dos bancos de dados.

O direito à proteção de dados pessoais foi aproximado ao conceito do princípio à privacidade pelo Ministro Ruy Rosado no julgamento do REsp 22.337/RS, pela 4º Turma do STJ, que será discutido mais adiante.

O Princípio da Liberdade, disposto nos artigos 1º, inciso IV, 3º, inciso I e 5º, *caput* alude à liberdade que o consumidor têm em adquirir determinado serviço ou produto, sem que contenha qualquer vício de vontade. Pelo fato do fornecedor deter algumas informações que o consumidor não tem acesso, este é a parte vulnerável da relação.

> Assim, por exemplo, o negócio jurídico de consumo há se ter transparência (consciência do consumidor do alcance de seu ato jurídico de consumo), boa-fé (dever de lealdade, sinceridade e honestidade máxime diante da fragilidade já conceitual, já efetiva do consumidor)[...] (AMARAL, 2010, p.57)

O consumidor teve sua vulnerabilidade reconhecida pela ONU na resolução 39/248 de 1985, conquistando uma tutela jurídica específica acerca do comportamento dos bancos de dados.

O princípio da igualdade, disposto no *caput* do artigo 5º da Constituição Federal, o texto de lei “todos são iguais perante a lei” não seria facilmente aplicável na relação de consumo entre consumidor e o banco de dados pelo fato deste ser vulnerável de maneira genérica.

O principio da vulnerabilidade do consumidor, disposto no artigo 4º, inciso I do Código de Defesa do Consumidor, dissipado por todo o texto do código, está interligado aos princípios constitucionais da dignidade da pessoa humana e da igualdade.

A vulnerabilidade do consumidor independe da condição social, financeira ou cultural, possibilitando ser pessoa física ou jurídica, pelo fato dele não possuir controle e informações técnico-jurídicas do funcionamento dos bancos de dados e nem tão pouco as implicações econômico-financeiras acerca desses.

> Consumidor é sempre pessoa física ou jurídica, cuja necessidade (*lato sensu*) de consumo torna-a subordinada às condições e interesses que o titular dos bens e serviços impõem. (AMARAL, 2010, p.65)

Para Amaral (2010) a vulnerabilidade está restrita às pessoas físicas ou jurídicas, não profissionais e que não visam lucro, adotando a teoria subjetiva a partir do conceito de consumidor.

> Todo consumidor é vulnerável, por conceito legal. A vulnerabilidade não depende da condição econômica, ou de quaisquer contextos outros. A hipossuficiência [...] como dissemos, deve ser aferida no caso concreto [...]. A hipossuficiência diz respeito, nessa perspectiva, ao direito processual, ao passo que a vulnerabilidade diz respeito ao direito material. (NETTO, 2015, p.57)

Faz-se necessário distinguir hipossuficiência de vulnerabilidade. A hipossuficiência refere-se ao direito processual e a capacidade probatória, ou seja, quando configurada a inversão de ônus da prova auferida pelo juiz da demanda.

Já a vulnerabilidade diz respeito ao direito material e não depende de condição econômica, jurídica ou técnica, isto é, pessoa física ou jurídica não possui os mesmo conhecimentos e informações acerca dos produtos/serviços que o fornecedor.

Logo, todo consumidor é vulnerável embora nem todo consumidor seja hipossuficiente.

Não importa se é uma pessoa física ou jurídica, ambas são consumidoras de acordo com o artigo 2º do Código de Defesa do Consumidor em que “consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final” e pode ter suas informações armazenadas nos arquivos de consumo.

Netto (2017) afirma que a hipossuficiência técnica é aquela em que o consumidor não possui conhecimento técnico acerca de determinado produto/serviço, gerando a inversão de ônus da prova em seu favor.

No atual mercado de consumo há uma escassez de opções, que faz com que o consumidor seja escolhido ao invés de escolher, onde é de iniciativa do fornecedor oferecer como, o que e quando seus serviços e produtos, ou seja, a oferta é maior do que a procura.

> O principio da boa-fé objetiva, ligado ao princípio da Dignidade da Pessoa Humana, nas relações de consumo com os bancos de dados trata acerca da regra de conduta que os bancos devem possuir ao está em posse dos dados pessoais do consumidor, ou seja, “dever de agir de acordo com os padrões socialmente determinados e reconhecidos”. (MANDELBAUM, 1996 *apud* AMARAL, 2010, p. 75)

Os bancos de dados, ao cederem os dados pessoais do consumidor a outros, devem estar de posse de um consentimento expresso por parte deste, se não estará violando o princípio da boa-fé objetiva. Acerca do consentimento dado ao banco de dados será refletido mais a frente do presente trabalho.

2.2. O Código de Defesa do Consumidor

A Lei 8.078 de 1990, conhecido como Código de Defesa do Consumidor passou a regular, de forma incompleta, os bancos de dados que, até então, não existiam legislações regulamentadoras a respeito desses.

Veremos adiante que, o Código possui diversos princípios aplicáveis ao consumidor que o protegem dos bancos de dados.

A seção VI do Código de Defesa do Consumidor dispõe sobre a regulamentação dos bancos de dados e cadastros de consumidores, classificados em espécies de arquivos de consumo, conforme expresso no artigo 43 do código.

Segundo Zanon (2013) os arquivos de consumo são previstos na lei com uma finalidade determinada, qual seja, a de servir de apoio para as relações de consumo, não devendo conter informações adversas com a finalidade prevista e autorizada por lei.

Os bancos de dados são caracterizados por quatro elementos, de acordo com Herman Benjamin. São eles: uma coleta de dados arbitrária com o intuito de aumentar a base de dados ao máximo; organização das informações pessoais; cessão de dados tratados, ou seja, objetiva a transmissão dos dados pessoais do consumidor a terceiros e, o não conhecimento do consumidor, isto é, não há o consentimento desse pelo simples fato de não conhecê-lo em particular.

Por outro lado, os cadastros de consumidores têm por características uma delimitada base de dados “cadastráveis”, marcado pela aleatoriedade; breve permanência dos dados nos cadastros pelo fato de apenas serem necessários durante a relação com o consumidor e à não transmissibilidade à

terceiros, ou seja, os dados ficam destinados apenas ao arquivista, contrariando a destinação dos bancos de dados.

> Tanto os bancos de dados como os cadastros podem ser compostos com dados pessoais de identificação da pessoa [...] e com dados pessoais comportamentais de consumo (histórico financeiro e de crédito da pessoa). (ZANON, 2013, p.135)

[...]

> A preocupação maior do legislador foi com a dignidade da pessoa. Consequentemente, não importa se o organizador do banco de dados de consumo é pessoa jurídica privada ou pública. Neste setor, como a ameaça e violação ao *direito à proteção dos dados pessoais* pode advir tanto do setor público como da iniciativa privada, a eficácia do direito fundamental deve ser ampla, atuando nos planos vertical e horizontal. (ZANON, 2013, p.135)

Os arquivos de consumo possuem caráter público, mesmo que tenham origem privada, como os cadastros de consumo e os bancos de dados, a exemplo do SPC e SERASA, submetendo-se ao controle através do remédio constitucional *habeas data*, de acordo com o inciso LXXII, do artigo 5º da Constituição Federal interligado ao artigo 43, §4º do CDC.

O artigo 43 do Código de Defesa do Consumidor prevê alguns princípios implícitos, a exemplo do parágrafo 2º, que alude o princípio da transparência já que “a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele”, isto é, é proibido o colhimento de dados pessoais sem uma comunicação prévia do consumidor feita pelo banco.

O caput do artigo 43 dispõe acerca do princípio da informação onde o consumidor “terá acesso às informações existentes em cadastros, fichas,

registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas fontes", ou seja, deve haver uma comunicação prévia tanto por parte do organizador do banco de dados quanto do fornecedor do dado originário.

Exige-se seguir a regra da acessibilidade limitada – os dados só devem ser transmitidos a terceiros a partir de uma necessidade na relação de consumo. O CDC estipulou no artigo 72 crime a quem "impedir ou dificultar o acesso do consumidor às informações".

O organizador do banco de dados possui informações pessoais de pessoas físicas ou jurídicas, facilitando o espalhamento destas a terceiros em questões de segundos.

Os parágrafos 1º e 3º do artigo 43 dissertam sobre o principio da veracidade e determina que os dados sejam "objetivos, claros, verdadeiros e em linguagem de fácil compreensão" e o consumidor "sempre que encontrar exatidão nos seus dados e cadastros, poderá exigir sua imediata correção". A não correção dos dados pelo arquivo de consumo constitui-se em crime previsto no artigo 73 do CDC.

O principio da temporalidade do uso, elencado nos parágrafos 1º e 5º do artigo 43 do Código de Defesa do Consumidor, institui que as informações não podem constar nos arquivos de consumo no período superior a 5 (cinco) anos. Serão abordados os prazos de permanência das informações mais a frente deste presente trabalho.

2.3. Normas Jurídicas Complementares

Em 2011 foi aprovada pelo Congresso Nacional a Lei 12.414/2011, Lei de Cadastro Positivo, regulada pelo Dec. 7.829/2012, que disciplina a formação e consulta dos bancos de dados, com a finalidade de formação de um histórico de crédito ao consumidor, seja pessoa física ou jurídica.

> [...] que "o conceito de histórico de crédito abrange a expressão "conjunto de dados financeiros", o que a princípio admite

> conceitualmente observar também a totalidade das obrigações, inclusive as inadimplidas [...] (MIRAGEM, 2012, p.7)

Antes da Lei de Cadastro Positivo, o CDC era o único dispositivo legal que abordava, mesmo que superficialmente, como os bancos de dados se comportariam.

Primeiramente, é de extrema importância distinguir as informações positivas das negativas, elementos compostos dos bancos de dados de proteção ao crédito.

Antes da Lei de Cadastro Positivo, a concessão de crédito era realizada apenas com as informações “negativas” dos consumidores, discriminando aqueles que não eram considerados “bons pagadores”. Entretanto, as informações positivas já eram utilizadas pelos bancos, de forma não regular.

Foi a partir desta lei que os bancos de dados de formação ao crédito passariam a conter informações “positivas” a respeito dos consumidores, não os distinguindo de maneira negativa.

> Então, atentos às novas mudanças de mercado, o legislador resolveu acompanha-las [...] o sistema legal brasileiro passou a dispor de um diploma que permite, expressamente, o registro de informações positivas junto aos órgãos de proteção ao crédito, relacionadas ao histórico de pagamentos e de compromissos assumidos pelo consumidor, viabilizando-se o cadastro positivo, objetivando avaliar o risco de uma operação de crédito. (ALESSIO, 2013)

Zanon (2014) entende que, a Lei de Cadastro Positivo, ao controlar o modo como os bancos de dados tratam as informações pessoais, elevam o direito à proteção dos dados pessoais em nosso ordenamento jurídico, escasso referente aos bancos de dados.

Como já exposto anteriormente, o CDC possui ao longo do seu texto, princípios que protegem o consumidor da ação dos bancos de dados, embora a

Lei de Cadastro Positivo também possua alguns princípios que regulam como esses devem atuar.

Constam-se os princípios da finalidade, proporcionalidade e da necessidade, nada mais é que os bancos de dados de cadastro positivos só podem conter dados pessoais do consumidor para uma futura possível concessão de crédito, a partir do histórico. Esses dados só podem ser coletados e tratados se os bancos de dados mantiverem uma relação de consumo com o consumidor, vedado o uso destes para uma futura propositura de marketing ou qualquer outro uso não previsto em lei, sempre primando pela clareza da sua utilização.

O princípio da finalidade trata acerca de como os fornecedores – os bancos de dados utilizam as informações pessoais, notificando previamente os consumidores.

Os princípios da proporcionalidade e necessidade diz respeito de como a coleta das informações pessoas do consumidor são necessárias para a finalidade a que se destinam, de forma harmônica.

O artigo 3º da Lei 12.414/2011 veda também a coleta e tratamento de dados sensíveis, ou seja, informações relacionadas “à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”.

Ao falar sobre a personalidade humana, o doutrinador alemão Heinrich Henkel entende que esta se divide em esfera individual e esfera privada, de acordo com Oliva (2016). Há uma subdivisão da privada em esfera da privacidade, da intimidade e do segredo, onde os dados sensíveis elencados no artigo 3º, se encaixam na esfera da intimidade, já que são informações que o consumidor não pretende compartilhar com terceiros.

> Dessa esfera exclui-se grande parte da população, mesmo pessoas com as quais o indivíduo tenha um relacionamento diário, e, portanto, afeitas à esfera da privacidade colegas de trabalho ou estudo, por exemplo. (OLIVA, 2016, p.56)

Ora, se essas informações são restritas às pessoas conhecidas do consumidor, quiçá dos bancos de dados, os quais o consumidor não tem um real conhecimento de quem estão em posse seus dados pessoais.

Os artigos 4º e 9º da Lei 12.414/2011 dissertam que é necessária notificação prévia ao titular dos dados, assinando em documento específico, para que ocorra a formação do histórico de crédito sem violações à lei.

De acordo com a Lei fica a critério do consumidor a possibilidade do banco de dados realizar apenas a abertura do histórico de crédito ou o compartilhamento destes dados à terceiros, tendo ciência de que esse compartilhamento, no futuro, possa prejudica-lo mais a frente.

O Serasa, principal banco de dados de proteção ao crédito, em seu site, afirma que quem apenas terão acesso aos dados do consumidor no Cadastro positivo serão “o comércio, os bancos, as financeiras e as prestadoras de serviço”.

A nota técnica nº 40 de 2013 do Ministério da Justiça analisa o Decreto nº 7.962/2013 acerca da contratação em comércio eletrônico com o objetivo de garantir os direitos referentes ao consumidor neste tipo de relação de consumo.

> [...] a relação de consumo em meio eletrônico deve se pautar pelo respeito ao uso consentido e proporcional dos dados pessoais do consumidor, em respeito tanto à sua privacidade quando ao pleno exercício de sua autodeterminação informativa, consistente no poder de tomar pessoalmente as decisões fundamentais sobre a utilização de seus dados pessoais, estando informado e consciente das consequências desta decisão” (BRASIL, 2013)

A nota alude que os bancos de dados devem comunicar previamente ao consumidor como utilizará as informações pessoais, prezando pelo direito à privacidade e à proteção dos dados pessoais.

O Decreto nº 5.903 de 2016, no seu artigo 1º, parágrafo 1º inciso I diz que a informação deve ser “verdadeira que não seja capaz de induzir o consumidor em erro”.

Este objeto jurídico aplica-se aos bancos de dados com relação à finalidade do tratamento destas, isto é, o consumidor deve estar ciente, mediante prévia notificação.

Outras leis regulam ou abordam o funcionamento dos bancos de dados, tais como a Lei da Informática e a Lei do Acesso à Informação Pública.

A Lei da Informática, lei 7.232/1984, dispõe, em seu artigo 1º sobre os “princípios, objetivos e diretrizes da Política Nacional de Informática, seus fins e mecanismos de formulação”. Esta lei estabelece de que modo os dados pessoais serão processados, coletados e cedidos, sempre prezando pela proteção do sigilo destes das pessoas físicas ou jurídicas, públicas ou privadas.

A Lei da Informática estipulou de que modo e como funcionariam a exploração dos dados pessoais, desde a coleta até a transmissão a terceiros, e, que, lei especifica as regularizariam, embora com a vigência da Lei 12.414/2011, essa não atende a todas as exigências.

A Lei 12.527/2011, Lei do Acesso à Informação Pública, foi sancionada para haver uma transparência no acesso e na divulgação das informações públicas, da Administração Pública direta e indireta, até então não eram acessadas facilmente, consagrando o inciso XXXIII do artigo 5º da Constituição Federal, dissertando assim:

> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. (BRASIL, 1988)

O artigo 4º, inciso I da Lei 12.527/2011 define que informações são “dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”.

Necessário estabelecer que, quanto ao sigilo das informações, os artigos 22 a 30 da lei as classifica como: ultrassecretas, secretas e reservadas. Essa classificação é baseada no grau de restrição da informação e “deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível”. O parágrafo 5º do artigo 24 estabelece tempo em que as informações deverão permanecer em sigilo.

O prazo máximo de restrição da informação ultrassecreta é de 25 anos, renovável apenas uma única vez. Para a informação secreta, o prazo é de 15 anos e para a reservada, é de 5 anos.

Por exemplo, o parágrafo 2º do artigo 24 da Lei de Acesso a Informação Pública, diz que as informações sobre o “Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as)” são reservadas e devem permanecer em sigilo até o fim dos mandatos.

A Lei 12.654/2012 acrescenta ao parágrafo único no artigo 5º da Lei 12.037/2009, que dispõe sobre a “identificação criminal do civilmente identificado”, a possibilidade da coleta de dados genéticos de cidadãos que praticaram delitos. A lei afirma que esses dados genéticos são sigilosos, Zanon (2014, p.145).

Esses dados se encaixariam na esfera do segredo, conforme mencionado no presente trabalho (p.12) que guardam informações íntimas, portanto, como Oliva (2016, p. 57) traz “trata-se de um local que não pode ser violado, nem mesmo por ordem judicial específica”.

Para compreender o funcionamento e regramento dos bancos de dados, faz-se necessária uma análise conjunta de todas as leis existentes no ordenamento jurídico brasileiro.

3. OS BANCOS DE DADOS DE INFORMAÇÕES PESSOAIS NO BRASIL

A seguir, analisa quais motivos fomentaram a criação dos bancos de dados de informações pessoais no Brasil, elencando a coleta, tratamento e cessão dos dados, expondo a fragilidade nessa transferência à terceiros.

3.1. Origem e Necessidade de Controle no Brasil

Os bancos de dados surgiram na década de 50 com a intensificação das relações comerciais, impulsionados pelo crescimento econômico do país a partir do desenvolvimento de novas tecnologias, como a estimada chegada da televisão e divulgação em massa de propagandas em rádios.

Foi no Governo Vargas que o processo de industrialização se exorbitou no Brasil, com a substituição de produtos importados e a abertura da possível entrada do capital estrangeiro no desenvolvimento da economia brasileira.

> As grandes lojas acabaram criando setores próprios com a única função de realizar pesquisa sobre os hábitos de pagamento do pretendente a realizar a compra de determinado produto ou serviço por intermédio de crediário. (BESSA, 2007, p.2)

Com o mercado de consumo expandindo cada vez mais, as grandes empresas observaram a possibilidade de agrupar dados acerca dos consumidores a fim de direcionar a fabricação de seus produtos, e futura concessão de crédito a estes, consequentemente, ampliando sua base de consumidores.

Para Bessa (2007, p.2) “hoje, os negócios são realizados entre anônimos, em lojas de departamentos, pela internet, por telefone”.

Nítida era a grande demanda em criar um único órgão responsável para obtenção de dados pessoais dos consumidores, acarretando ainda mais, a expansão de clientes às empresas, criou-se então o primeiro banco de dados de proteção ao crédito no Brasil, em 1955.

Posteriormente, com a maior dependência do comércio desses bancos, empresas passaram a sondá-los, explorando a atividade a fim da "coleta, o armazenamento e a transferência a terceiros (credor potencial) de informações pessoais", sempre objetivando uma possível cessão de crédito ao consumidor.

Para Bessa (2007, p.2) "a concessão de crédito pressupõe certo grau de confiança no beneficiário da operação", ou seja, a empresa que estar disposta a ceder crédito ao consumidor tem uma confiança "prévia" a respeito dele, através das informações contidas nos bancos de dados, por sua vez, proporciona uma rapidez na concessão do crédito por conhecer o "histórico de pagamento" do consumidor.

> É neste contexto, e considerando os perigos decorrentes da rápida evolução tecnológica no setor da informática, que as atenções se voltam às diversas modalidades de bancos de dados que coletam, armazenam e transferem para terceiros as mais variadas espécies de informações pessoais. (BESSA, 2007, p.3-4)

É evidente, tanto a essencialidade da existência dos bancos de dados de proteção ao crédito quanto à fragilidade na proteção dos dados pessoais do consumidor a partir desses.

O banco de dados, por não ter conhecimento de quem seja cada consumidor, isenta o gestor da responsabilidade por apenas receber informações repassadas pelo fornecedor dos dados.

> [...] o ordenamento jurídico veda, de regra, a veiculação de fato concernente à mora de alguém, pois tal tipo de notícia afeta,

> inexoravelmente, a reputação da pessoa, sua consideração no meio em que vive. (BESSA, 2007, p.4)

A partir dessa violação se viu a necessidade do ordenamento jurídico interferir, legislando-se sobre a prática desses bancos a partir do Código de Defesa do Consumidor e, segundo Bessa (2007, p.5) “exige do intérprete análise sistemática do ordenamento jurídico, *diálogo das fontes* entre diplomas diversos”, referindo-se tanto ao CDC quanto a Lei de Cadastro Positivo e a Lei da Informação, entre outras.

Para que seja válida a transferência dos dados pessoais à terceiros por parte dos bancos de dados é de suma importância a autorização expressa do consumidor, conforme indica o CDC.

Não há de negar que a cessão de crédito futuro ao consumidor fomenta a economia do país, gerando um aumento no mercado de consumo.

3.2. Formas de Tratamentos dos Dados Pessoais do Consumidor

Primordialmente, faz-se necessário esclarecer que o tratamento dos dados pessoais não trata apenas da coleta desses, mas como e para quais finalidades eles foram devidamente tratados, de acordo com o ordenamento jurídico aplicado aos bancos de dados de informações pessoais. Abordaremos as formas como são realizados esses tratamentos e quais requisitos devem ser cumpridos para que tenham validade perante a lei.

3.2.1. Momento da coleta dos dados

Antes da massificação do mercado de consumo, as empresas conheciam seus consumidores de maneira individualizada, isto é, conheciam seus gostos e modos de atuação no mercado de consumo.

Os bancos de dados fornecem a essas empresas um método de aumentar o conhecimento acerca dos antigos ou futuros consumidores, com dados que possibilitem oferecer seus produtos ou serviços.

A priori, para validar a coleta dos dados pessoais é necessário que o consumidor expresse consentimento prévio, ou ainda com a previsão em lei, com o conhecimento para qual finalidade aqueles dados que estão sendo fornecidos por parte dos bancos de dados.

Ao coletar os dados, esses bancos devem sempre prezar pela boa-fé objetiva e o direito à privacidade e à proteção dos dados pessoais do consumidor.

Mendes (2014) elenca as principais fontes de dados utilizadas pelos bancos ao coletarem as informações. São essas: transações comerciais, censos e registros públicos, pesquisas de mercado e de estilo de vida, sorteios e concursos, comercialização e cessão de dados e tecnologias de controle na internet.

Ao realizar uma compra em determinado estabelecimento de consumo a primeira vez, geralmente, as empresas solicitam informações para efetivar um "cadastro" daquele consumidor, certificando-se da segurança desses dados.

> Nesses registros, é comum constar não apenas os dados do consumidor, mas também os seus hábitos de consumo, possibilitando que posteriormente a empresa possa ofertar-lhe produtos específicos. (MENDES, 2014, p.96-97)

Com esses registros, com informações pessoais a respeito dos hábitos de consumo, é possível que acarrete uma discriminação do consumidor que não se adequa às especificações dessas empresas, interessando-lhes apenas aqueles classificados como bons consumidores.

Mendes (2014, p.97) cita como exemplo os cartões de fidelidade oferecidos pelas empresas com o intuito de direcionar seus produtos aos consumidores, embora ele não tenha total ciência de que esses cartões são utilizados como "monitoramento e o armazenamento dos dados referentes ao seu comportamento de consumo".

Vale ressaltar que, para que a coleta desses dados pessoais seja considerada válida nos termos da lei, requer o consentimento do consumidor, desde que notificado acerca da utilização destes.

Nos anos 70, os EUA negociaram a venda de fitas magnéticas constando dados pessoais do censo dos consumidores a empresas, possibilitando uma análise geográfica a respeito desses, embora este modo de análise acarrete um pré-julgamento do consumidor, classificado de modo coletivo, não o analisando de modo individual.

> Além disso, é bastante questionável que os dados pessoais que foram coletados com o proposito de servir ao censo demográfico possam ser utilizados para fins de *marketing* direto ou avaliação de risco, sem o consentimento do titular, uma vez que isso viola o princípio da finalidade da proteção de dados pessoais. (MENDES, 2014, p.98-99)

A massificação do consumo faz com que empresas não conheçam os consumidores de forma individualizada, mas elas realizam pesquisas de mercado, onde o consumidor é entrevistado diretamente, ou por vários meios de comunicação, com objetivo de conhecer os hábitos de consumo a fim de oferecer benefícios em relação às outras empresas no mercado.

Para que as pesquisas de estilo de vida (utilizada pelas empresas de *geomarketing*[1]) e as pesquisas de mercado tenham validade legal é imprescindível que os bancos informem aos consumidores como e de que modo os dados são tratados, assim como sua finalidade. As empresas de *marketing*, de forma generalizada, devem informar previamente ao consumidor a futura possível cessão dos dados à terceiros.

A Lei 12.965/2014, conhecida como Marco Civil da Internet, trata dos "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" como

[1] *Geomarketing* é utilizada pelas empresas com o intuito de dinamizar as vendas e no direcionamento do *marketing*, "auxiliando a Entender, Planejar, Estruturar e Implementar Estratégias e Táticas relacionadas à dinâmica de consumo no território". Disponível em: <https://www.geomarketing.com.br/o-que-e>.

disposto no seu artigo 1º. De acordo com a legislação, artigo 5º, inciso I, dessa lei, internet é “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

Para Mendes (2014, p.101) “a internet, que é uma estrutura aberta de rede de computadores, é um marco no fluxo de informações, por ampliar radicalmente as possibilidades de comunicação”.

É inegável o avanço e a facilidade nas relações de consumo com o surgimento e desenvolvimento da internet, ocasionando um estímulo nas novas tecnologias de proteção dos dados, onde “somente é possível a partir da flexibilidade dos protocolos de comunicação” de acordo com o entendimento de Mendes (2014, p.101).

> De tal forma, são diversos os riscos à privacidade a que os usuários de internet estão sujeitos, em razão das inúmeras tecnologias de controle existentes e, principalmente, pela facilidade de disfarce dessas tecnologias. (MENDES, 2014, p.102)

Entretanto, com a flexibilidade nas relações, abre um paradigma em relação à violação da privacidade e proteção dos dados pessoais do consumidor, ficando ainda mais vulnerável porque no espaço virtual a violação é “mais imperceptível e silenciosa que o ambiente físico”, ou seja, vislumbrar a violação no ambiente virtual é complexo por não ter conhecimento do momento exato da captura ou espalhamento dos dados.

De acordo com Mendes (2014) Castells classifica essas tecnologias de controle de dados em três tipos: de identificação, de vigilância e de investigação.

As tecnologias de identificação[2], a exemplo dos *cookies*, são aquelas que possibilitam a identificação dos dados, tais como senhas e movimentações em *sites* na internet.

> Assim, desde a entrada em vigor da Diretiva [...] a legitimidade da coleta de informações por meio de *cookies* instalados no navegador do usuário depende tanto do seu consentimento prévio como do fornecimento de informações completas a respeito da coleta. Não basta [...] o consentimento presumido até manifestação ao contrário do usuário; faz-se necessário o seu consentimento expresso e declarado antes da instalação dos *cookies* em seu navegador. (MENDES, 2014, p.104)

Essas tecnologias proporcionam uma memorização dos dados, muitas vezes sem o consentimento do consumidor, infringindo a Diretiva 2009/136/EG[3], que "determinou a necessidade de consentimento prévio do usuário para qualquer tipo de coleta de informações armazenadas no seu equipamento" (Mendes, 2014, p.103), e de acordo com o inciso IX, do artigo 7º da Lei 12.965/2014 "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais", violando o direito à privacidade ao memorizar estes dados.

Por sua vez, tecnologias de vigilância[4] geram uma dúvida questionável a respeito da sua utilização pelo fato, segundo Mendes (2014, p.104), que "permitem a interceptação de mensagens, o rastreamento dos fluxos de comunicação e o monitoramento ininterrupto das atividades", ou seja, é evidente que esse meio tecnológico, a exemplo de *spyware* (tipo de s*oftware)*, viola diretamente o princípio constitucional da Dignidade da Pessoa Humana provocando danos à privacidade do consumidor.

---

[2] São tecnologias que possibilitam a identificação da movimentação do internauta.

[3] Diretiva 2009/136/EG altera a Diretiva 2002/58/CE relativa ao "tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas".

[4] São tecnologias utilizadas pelas empresas para monitorar as ações dos internautas.

Com a internet e seus meios de controles surgiu a necessidade de criação de tecnologias que protejam informações, à privacidade e à honra do consumidor como disposto no artigo 10º da Lei 12.965/2014.

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

Uma das mais usadas tecnologias de proteção, a criptografia "protege a identidade dos internautas e possibilita a realização de transações anônimas na internet" (Mendes, 2014, p.105), ou seja, o internauta, ao utilizar internet e criptografia, tem seus dados protegidos, mantendo sigilo das operações realizadas.

A aplicação da criptografia no Brasil não foi bem aceita, no inicio, pelo governo, já que, o entendimento é que facilitaria a prática de crimes além de violar diretamente o direito à privacidade, não apenas do internauta, como da sociedade e do Estado em si, de acordo com entendimento de Mendes (2014).

Segue um entendimento de Belleil (2002) acerca da tecnologia de proteção:

> Cada internauta predefine o que está disposto a aceitar por parte dos sítios da web em matéria de coleta e de utilização de seus dados pessoais. em seguida, à medida que vai surfando, instaura-se automaticamente um diálogo entre o navegador do internauta e o sítio web visitado. Efectua-se uma comparação automática entre as praticas do sítio web, ou seja, a sua política de dados pessoais e os desejos do internauta. Se as práticas do sítio web excederem os limites fixados pelo utilizador ou se ele não reunir condições para aceitar a plataforma P3P, então o utilizador é automaticamente

> prevenido. Cabe-lhe prosseguir ou interromper a sua visita, sabendo que a solução não prevê um bloqueio automático de conexão. (BELLEIL, 2002 apud MENDES, 2014, p.106)

Essas tecnologias, juntamente com a legislação vigente e outras medidas jurídicas, garantem o direito à privacidade do internauta.

3.2.2. Método de tratamento dos dados

Como visto anteriormente, o primeiro momento dos bancos de dados com as informações pessoais do consumidor é o da coleta desses, com requisitos a serem cumpridos para terem validade perante o mundo jurídico.

> Isso se torna possível com a submissão dos dados coletados a processos técnicos de lapidação da informação, a fim de buscar informações mais completas sobre os hábitos e o comportamento dos consumidores ou clientes em potencial. (MENDES, 2014, p.107)

Neste momento, será analisado como devem ser tratados e aprimorados os dados coletados a partir de tecnologias desenvolvidas com o passar do tempo, analisando os riscos oriundos desse refinamento.

> A partir desses instrumentos tecnológicos, a empresa pode lograr a classificação de seus clientes e a sua segmentação em grupos diversos, diferenciando entre os consumidores de maior valor para a companhia e os de menor valor. (MENDES, 2014, p.108)

É no momento do tratamento dos dados em que a empresa analisará o consumidor, a partir dos seus hábitos de consumo, visando obter vantagem à

frente de outras empresas do mesmo ramo comercial, direcionando os produtos e/ou serviços àqueles que o procuram.

O refinamento de informações pessoais pelo banco de dados pode gerar uma discriminação do consumidor a depender da técnica utilizada, violando o direito à privacidade, à honra e ao princípio da isonomia.

Serão elencadas a seguir algumas das técnicas mais utilizadas pelos bancos de dados no processamento dos dados pessoais coletados anteriormente.

O *data warehouse* nada mais é do que um grande bancos de dados utilizado em conjunto com outras técnicas de processamento de dados que contém informações organizadas a fim de colaborar no conhecimento dos consumidores, elaborando relatórios acercas desses.

> A expressão *data warehouse* denota a atividade de organizar dados de inúmeros sistemas operativos e heterogêneos de acordo com sua relevância, transformando-os e selecionando-os, com vistas a possibilitar a tomada de decisão estratégica. (MENDES, 2014, p.104)

Os relatórios podem classificar os consumidores de acordo com a necessidade da empresa, a fim de uma futura relação consumerista.

A mineração de dados, ou *data mining*, une informações consideradas incompreensíveis do banco de dados, modificando-as através de tecnologias de informática, tornando-as aproveitáveis e valiosas para as empresas.

Segundo Mendes (2014, p.109) a mineração “é o produto de rápido desenvolvimento no domínio das técnicas aplicadas à analise estatísticas”, ou seja, essa técnica é vista como um método “fácil” no tratamento dos dados, ampliando sua utilização em todos os ramos.

A OLAP (*Online Analytical Processing*) também é uma técnica de processamento de dados, equivalente à mineração, utilizada a partir de uma base de variáveis.

Embora a mineração destes dados sejam ágeis, por ter “como finalidade gerar regras para a classificação de pessoas”, diferenciam alguns consumidores, excluindo-os e, assim, descumprem o princípio da isonomia. Para Laura Mendes, a discriminação do consumidor não se dá a partir da técnica de processamento dos dados, mas sim, de como ela será utilizada pelos bancos.

> [...] a utilização da técnica do *data mining* somente será legítima se, além do prévio consentimento do consumidor, o processamento se der de forma transparente, de modo que o consumidor seja informado sobre o objetivo da coleta e do processamento de seus dados [...]. (MENDES, 2014, p.110)

A grande preocupação a respeito dessa técnica é o modo de processamento dos dados, transformando-os em dados sigilosos ao ponto de vista do consumidor. E também se os bancos de dados informaram previamente ao consumidor a destinação de uso das informações.

A construção de perfil é a técnica que dispõem de dados referentes à imagem do consumidor visto pelas empresas, a fim de conhecer os hábitos de consumo, gostos e disponibilidades do consumidor acerca dos produtos e/ou serviços oferecidos por essas empresas.

O maior risco desta técnica ocorre devido a grande quantidade de combinações possíveis dos dados, isto é, ao combinar o dado “a” com o “b”, e o dado “a” com o “c” gera uma enorme possibilidade de análise desses dados, promovendo a discriminação do consumidor.

Para que o banco de dados possa usufruir dessa técnica é, imprescindível o consentimento prévio do consumidor de que modo os dados serão combinados, e se necessário, a alteração desses com iniciativa do próprio consumidor.

O sistema de avaliação, conhecido como *Scoring*, é uma espécie de “ranking” dos consumidores, evidenciando aqueles considerados “bons consumidores” a partir de critérios elencados pelos próprios bancos de dados.

> Como é de se esperar, a identificação dos melhores também pressupõe a identificação daqueles considerados “piores consumidores”. Esses são aqueles para quem as empresas têm interesse de oferecer as piores ofertas ou nenhuma oferta. (MENDES, 2014, p.112)

Os bons consumidores são analisados a partir do nível de “inadimplência”, sendo esse baixo, ofertando-lhes vantagens e melhores produtos. A empresa, ao oferecer as piores ofertas ou nenhuma aos consumidores elencados por elas como “piores” está ferindo diretamente o princípio da igualdade.

A Diretiva 95/46/CE (1995), principal diploma do direito europeu que dispõe acerca da proteção aos dados pessoais, em seu artigo 1º diz que: “Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, notadamente o direito à vida privada, no que diz respeito ao tratamento de dados pessoais”.

A doutrinadora Catarina Sarmento e Castro entende que não é possível somente a aplicação do sistema de avaliação, ou seja, deve aplicar junto à outra técnica de processamento, elencando os dados de acordo com a classificação adotada.

> Como regra geral, pode-se afirmar que apenas as informações relativas à capacidade financeira do consumidor podem ser utilizadas para formar o seu *scoring*, pois, afinal, um valor objetivo, como ele se pretende, não poderia basear-se em dados subjetivos ou questionáveis. (MENDES, 2014, p. 144)

Para tanto, a Diretiva fixa padrões mínimos a serem respeitados por aqueles que utilizem esse método de processamento de dados pessoais.

As informações a serem utilizadas no sistema de avaliação devem ser objetivas e corresponderem à realidade, e se não, pode o consumidor sair lesado por um “erro” do banco de dados. Por isso é necessário que o consumidor tenha conhecimento de que formas seus dados estão sendo utilizados e, devem ser corrigidos assim que notado a inexatidão com a realidade.

3.2.3. Fragilidade na cessão dos dados

Foi feita a análise de dois momentos importantes na utilização dos dados pessoais por parte dos bancos de dados. A primeira foi o momento da coleta desses e o segundo as técnicas adotadas pelas empresas e bancos, de processamento e análise das informações pessoais.

> Algumas entidades de proteção ao crédito tem realizado a troca de informações ‘por espelhamento’, o que significa divulgar as informações provenientes de outros bancos de dados, sem, contudo, realizar, quando necessário, a retificação ou cancelamento das informações difundidas, sob o argumento de que os dados não são incluídos na base da entidade que recebeu as informações. (BESSA, 2014, p.9)

A partir deste ponto, será analisado de que forma se dá a transferência dos dados pessoais à terceiros por parte do banco de dados, e o quão frágil é essa cessão, acarretando violações a direitos básicos do consumidor.

> O resultado é a ampla circulação das informações pessoais na sociedade, gerando benefícios aos setores envolvidos, mas também grandes riscos aos consumidores, cujos dados são coletados, processados e transferidos. (MENDES, 2014, p.117)

É com a cessão de dados a terceiros que há o dinamismo acerca da utilização dos dados pessoais, isto é, a partir da transferência das informações

o mercado de consumo se amplia, onde empresas podem ofertar seus produtos a novos consumidores.

Algumas empresas configuram uma espécie de consórcio com o intuito de compartilhar entre membros os dados pessoais que possuem acerca dos seus consumidores.

Com a transferência de dados a terceiros aumenta o mercado de consumo e surgem empresas “cujo a única finalidade é a comercialização de dados”, de acordo com Mendes (2014, p.118).

> Ademais, a entidade que divulga informações negativas ou positivas de outros bancos de dados (em razão de compartilhamento) deve facultar ao consumidor o direito de acesso e retificação da informação. É ilegal a conduta de sugerir ao consumidor que se dirija diretamente ao banco de dados que “gerou” a informação para – somente lá – exercer o direito a exigir o cancelamento ou correção da informação. (BESSA, 2014, p. 8)

A respeito da cessão de dados pessoais, quando há inexatidão de um dado e este é compartilhado, a dificuldade em corrigi-lo é absurda, pelo simples fato de analisar o quanto esse dado errôneo já foi compartilhado, lesando o consumidor de uma maneira incoerente.

Embora o compartilhamento de dados contribua no conhecimento de hábitos de consumo, direcionando seus produtos e/ou serviços e expandindo seus consumidores deve-se tratar esse assunto com bastante atenção, pois, para que não violem o direito à privacidade, à honra e a proteção de dados pessoais, é previsto na lei que somente será possível a cessão desses dados com o consentimento prévio do consumidor, e que ele seja ciente da finalidade da utilização dos dados.

> Isso ocorre porque os riscos advindos da coleta e do processamento de dados indevidos podem se multiplicar

> infinitamente, caso essas informações sejam repassadas a terceiros. Afinal, se essas informações circulam na sociedade, de forma equivocada, sem se constituir em uma representação fidedigna do consumidor, a sua liberdade e a igualdade de acesso aos bens de consumo poderão ser gravemente violadas. (MENDES, 2014, p.119)

A Lei de Cadastro Positivo, em seu artigo 6º, inciso III determina que “os gestores de bancos de dados obrigados, quando solicitados, a fornecer ao cadastrado: [...] III – indicação dos gestores de bancos de dados com os quais as informações foram compartilhadas”. É necessária que seja feita uma análise com o diálogo das fontes, entre o Código de Defesa do Consumidor e a Lei de Cadastro Positivo.

Mendes (2014) entende que deve haver um equilíbrio entre a proteção dos dados pessoais (princípio de igualdade, direito à privacidade e à honra do consumidor) e a livre iniciativa por parte das empresas, responsabilizadas por desenvolver economicamente o país e expandir seu mercado de consumo.

Embora seja necessário o consentimento prévio do consumidor para a transferência de dados pessoais a terceiros, esse consentimento não será essencial se forem dados públicos, a exemplos dos salários dos servidores públicos, já que quem “paga” seus salários é o povo brasileiro. Outros dados que são dispensáveis o consentimento são àqueles relativos à saúde e de repartições públicas.

4. POSICIONAMENTO DO SUPERIOR TRIBUNAL DE JUSTIÇA

Será verificado a seguir como o Superior Tribunal de Justiça compreende a atividade dos bancos de dados de informações pessoais, responsabilizando-os e posicionando-se quando violarem direitos e garantias inerentes ao consumidor.

4.1. Responsabilização Civil dos Bancos de Dados

Ao falar da responsabilidade dos bancos de dados em função dos dados de informações pessoais do consumidor, é necessário analisar preliminarmente a responsabilidade civil.

A responsabilidade civil tem alguns pressupostos quando se trata do dever de indenizar, são eles: a conduta, o dano e nexo de causalidade.

O Código Civil em seu artigo 186 define: “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”.

Alguns doutrinadores adotam a teoria que a conduta só se aplica a responsabilidade subjetiva, quando há ação ou omissão. Quando se trata da responsabilidade objetiva (aplicada aos bancos de dados) “vai haver em relação a uma atividade desenvolvida por aquele a quem se imputa a responsabilidade” de acordo com Miragem (2015, p.117).

Para haver a responsabilização civil é necessária que haja uma violação a partir de um ato ilícito a um direito estabelecido, causando dano ao detentor do direito.

> [...] a conduta antijurídica que figura como pressuposto da responsabilidade civil será aquela que, ao violar norma ou direito alheio, der causa, por isso, a um dano injusto,

> independentemente de haver norma proibitiva genérica ou especifica. (MIRAGEM, 2015, p.122)

Miragem (2015, p.119) entende que o ilícito deve preencher alguns requisitos como a existência e acusação de uma conduta, um ordenamento jurídico violado e a incidência na esfera jurídica alheia, porque “ilicitude é espécie de antijuridicidade, mas não esgota sua definição”.

O artigo 187 do Código Civil nos traz outra definição de ato ilícito que: “também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes”.

> A antijuridicidade decorre da violação de dispositivo de lei ou de preceito integrante do ordenamento jurídico, como é o caso da violação do comando reconhecido de um princípio jurídico, como aquele que viola um dever de informar não escrito, porém advindo do princípio da boa-fé. (MIRAGEM, 2015, p.118)

Como já abordado no presente trabalho os bancos de dados ao coletar, tratar e ceder dados pessoais dos consumidores se responsabilizam civilmente por se tratar da atividade do agente, isto resultará no dever de indenizar se violar dispositivos legais, a exemplo da violação ao direito à privacidade.

> A noção de dano toma o sentido de perda, uma lesão a um patrimônio compreendido em sentido amplo como conjunto de bens e direitos de que seja titular a pessoa. (MIRAGEM, 2015, p.155)

Essa se refere aos danos causados pela transferência de dados pessoais errôneos a terceiros por parte dos bancos de dados, pois viola, inegavelmente, o direito à honra e à proteção dos dados pessoais.

O nexo de causalidade trata-se da conexão entre a conduta antijurídica do agente e o dano causado à vítima, neste caso, ao consumidor por ter suas informações repassadas à terceiros com alguma violação prevista em lei ou mediante atitudes inadequadas dos bancos de dados.

> Realmente, não há como se pretender excluir a responsabilidade civil do bancos de dados de proteção ao crédito perante o consumidor. Todos os pressupostos legais (*veracidade*, clareza, objetividade, limites temporais etc.) que legitimam o registro, são dirigidos a todos que praticam do tratamento das informações" (BESSA, 2011, p.6)

Não pode excluir a responsabilidade civil dos bancos de dados de proteção ao crédito, mas também, de todos os bancos de dados pessoais que utilizam técnicas de processamento e refinamento das informações pessoais, já discutidas no presente trabalho.

O CDC, no artigo 6º, inciso VI determina que a responsabilidade civil é objetiva, pois, de acordo com Bessa (2011, p.6) "o dispositivo em nenhum momento se refere à *culpa* [...] como pressuposto ou requisito para gerar o dever de indenizar".

O parágrafo único do artigo 7º do Código de Defesa do consumidor ordena que: "tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo".

Faz-se necessária uma análise e verificação a respeito das duas ou mais pessoas que causaram o fato danoso.

> Sem dúvida, há concorrência entre fornecedor e banco de dados na realização do ato ilícito. O fornecedor apresentou, desatendendo o disposto no art. 43, § 1.º, do CDC, informação inverídica. A entidade arquivista aceitos como verdadeira a informação e a colocou à disposição de terceiros [...] reforça o

> dever da entidade de proteção ao crédito de zelar, a todo momento, pela exatidão do registro. (BESSA, 2011, p.7)

Pressupõe, de acordo com esses dispositivos, a responsabilidade solidária entre o banco de dados e o arquivista dos dados quando violarem direitos básicos do consumidor e os ordenamentos jurídicos.

O exemplo claro é a cessão de dados pessoais do consumidor à terceiros quando possuem ambiguidade a respeito da veracidade dos dados, onde o consumidor não tem ciência de qual entidade proferiu a informação inexata.

O Código de Defesa do Consumidor, no artigo 6º e seus incisos dispõem os direitos básicos do consumidor, disciplinando a respeito da responsabilidade civil objetiva dos bancos de dados, juntamente com o artigo 16 da Lei de Cadastro Positivo que trás a seguinte redação: “O banco de dados, a fonte e o consulente são responsáveis objetiva e solidariamente pelos danos materiais e morais que causarem ao cadastrado”.

Embora o parágrafo único do artigo 7º do Código de Defesa do consumidor e o artigo 16 da Lei 12.414/2011 abordem a solidariedade dos bancos de dados e o fornecedor, é fundamental diferenciá-las.

A solidariedade abordada no CDC é direta, isto é, não precisa de indagação a respeito da conduta ou nexo de causalidade, como caracterizada a responsabilidade civil subjetiva. Por outro lado, a solidariedade disposta na Lei do Cadastro Positivo, de acordo com o entendimento de Bessa (2011, p.7) “enseja debate processual no sentido de se questionar se o dano do consumidor foi causado, direta ou indiretamente, por ambos”.

O Código Civil Brasileiro também regula acerca da responsabilidade civil, no dispositivo 927, parágrafo único: “Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”.

Sempre evidente que, para determinar a responsabilidade civil dos bancos de dados ou do fornecedor das informações pessoais é imprescindível

que ocorra o diálogo das fontes, a fim de melhor aplicação da responsabilidade àqueles que causaram prejuízos e danos à privacidade e honra do consumidor.

4.2. Entendimentos e Análise Jurisprudenciais

Devido ao rápido desenvolvimento das tecnologias, tanto as de mercado como as de processamento dos dados pessoais do consumidor já discutidas anteriormente, o STJ viu a necessidade de se posicionar a respeito destas utilizadas pelos bancos de dados de proteção ao crédito.

Ao perceber a importância da atuação dos bancos de dados na sociedade, definiu limites a partir do direito à privacidade, à honra e à proteção de dados pessoais em consonância com o Código de Defesa do Consumidor, baseado nos princípios e garantias constitucionais.

O STJ compreende a relevância jurídica acerca dos bancos de proteção ao crédito além do que, fomentam a economia do país ao conceder empréstimos aos consumidores mesmo sem conhecê-los.

> Não há como negar a importância que as entidades de proteção ao crédito exercem na atualidade, pois afastando ou mitigando o anonimato dos atores da sociedade de consumo, possibilita que o crédito seja concedido com maior agilidade e rapidez. (BESSA, 2010, p.2)

No ano de 1995, o ministro Ruy Rosado de Aguiar, proferiu o REsp 22.337, criando o precedente de como os bandos de dados pessoais coletam, tratam e transfere à terceiros de maneira generalizada, gerando uma discriminação daqueles que não se encaixam no perfil formalizado.

Segue abaixo um trecho dessa decisão:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade

> de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular, para alcançar fins contrário à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o numero imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito à autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do *ombudsmon*, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação. (REsp 22.337/RS, Relator: Min, Ruy Rosado de Aguiar. 4ª Turma. Brasília, DF, julgado em 20 de março de 1995. DJ 20/3/2005)

Como analisado anteriormente, as formas de tratamentos das informações pessoais controlam como e quais dados são realmente utilizados pelos bancos de dados, protegendo sempre os direitos básicos inerentes ao consumidor.

O STJ se posiciona em relação a pratica dos bancos de proteção ao crédito em espalhar a outros bancos de dados informações referentes ao consumidor sobre dívidas vencidas e não pagas e diz que essa divulgação pressupõe indenização por danos morais, pelo fato de ferir o direito à privacidade e à honra do consumidor que teve essas informações dissipadas indevidamente, gerando uma responsabilidade objetiva e solidária aos danos causados ao cadastrado, conforme o artigo 16 da Lei 12.414/2011.

> […] ainda que verdadeiro, o ordenamento jurídico veda, de regra, a veiculação de fato concernente à mora de alguém, pois tal tipo de notícia afeta, inexoravelmente, a reputação da pessoa, sua consideração no meio em que vive. (BESSA, 2010, p.4)

Quando se trata dos danos morais e materiais, o STJ entende que, para que os bancos de dados e o fornecedor (responsabilidade civil objetiva e solidária, de acordo com o parágrafo único do artigo 7º do Código de Defesa do Consumidor) basta que o consumidor comprove “que o registro foi irregular, ou seja, que não atendeu a um dos requisitos exigidos pelo art. 43”, segundo entendimento do Bessa (2010, p.5), ou seja, não é necessário a comprovação que tal equivoco tenha afetado diretamente a pessoa física do consumidor, embora viola o direito à privacidade.

No REsp 273.250 pretendia julgar a exclusão da responsabilidade de um banco de dados alegando que essa deveria pertencer apenas à fornecedora das informações, embora o relator Ministro Ruy Rosado deu o seguinte parecer:

> O SPC presta um serviço ao seu associado, mas atua diante daquele cujo nome é registrado em seus arquivos, dai por que deve zelar também ele pela veracidade do que anota; se não o faz, corre risco inerente à sua atividade e, em caso de erro, deve indenizar o dano que decorre dessa falha. (REsp

> 273.250. Relator: Min. Ruy Rosado de Aguiar. 4º Turma. Brasília, DF, julgado em 19 de fevereiro de 2001)

Em 2001 o STJ modificou o entendimento do Tribunal de Justiça do Estado de São Paulo para a não exclusão do Serasa da responsabilidade civil, entendeu o relator Ministro Ruy Rosado de Aguiar que toda informação registrada indevidamente por envio de terceiros gera a responsabilidade deste, embora não exclua a obrigação de quem cadastrou, ou seja, o Serasa ao divulgar quais consumidores estão com dívidas vencidas e não pagas, já é solidário na responsabilização por também ser detentor dos dados pessoais desses consumidores.

O STJ criou um precedente a respeito da proibição de transferência de informações referentes a cartões de crédito ao julgar o REsp 1.348.532/SP.

O relator reconhece a vulnerabilidade do consumidor ao falar que ele "desconhecia as condições técnicas dos profissionais responsáveis pelos esclarecimentos prestados" e declarando a prática feita pelo banco como abusiva, violando o CDC, devendo este, retirar a cláusula de compartilhamento de dados pessoais do consumidor dos seus contratos de cartão de crédito.

No tocante à responsabilidade civil, destrinchada no tópico anterior, o STJ se posiciona, em sua súmula 37: "São cumuláveis as indenizações por dano material e dano moral oriundos do mesmo fato", indenizações essas tratadas como "resultado" da violação do direito à privacidade e à honra do consumidor.

À luz do entendimento do STJ, a ausência de comunicação, seja por parte do fornecedor quanto dos bancos de dados, das informações quando transferidas a terceiros também são passíveis de indenização por danos morais e materiais, pelo fato da comunicação ser prévia à esta cessão.

O julgado precursor a respeito da ausência de comunicação foi o REsp 165.727, proferido pelo relator Ministro Sálvio de Figueiredo quando decidiu que é "efetivamente necessária a comunicação ao consumidor de sua inscrição no cadastro de proteção ao crédito, tendo-se, na ausência dessa comunicação,

por reparável o dano moral oriundo da indevida inclusão", ou seja, os bancos de dados, ao incluírem os consumidores no cadastro de proteção ao crédito devem avisá-los previamente, responsabilizados civilmente se não o fizer.

O Código de Defesa do Consumidor, em seu artigo 43, § 2° regula que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele", fundamento para os julgados do Tribunal Superior.

Posteriormente a este julgado, outros surgiram, pacificando o entendimento da Corte em que é característica da inscrição indevida a não comunicação prévia por parte dos bancos de dados de proteção ao crédito e empresas interligadas a esses.

Mas em que momento deve ser feita essa comunicação prévia ao consumidor?

O entendimento do Superior Tribunal de Justiça é que deve disponibilizar ao consumidor a chance de impugnar o registro de informações equivocadas, com o intuito de evitar prejuízo à honra e à privacidade, antes mesmo de ceder à terceiros esses dados, aumentando ainda mais a lesão ao consumidor.

Na súmula 359, o STJ se posiciona da seguinte maneira: "Cabe ao órgão mantenedor do cadastro de proteção ao crédito a notificação do devedor antes de proceder à inscrição", ou seja, é dever do banco de dados informar o consumidor da possível inscrição no nome no cadastro de proteção ao crédito.

O inciso VI do artigo 6º do CDC já prevê essa ideia onde "a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos".

Como já aludido previamente, algumas informações são "consideradas imprescritíveis à segurança da sociedade", conforme Zanon (2013, p.143), o STJ chegou ao entendimento que os serviços de proteção ao crédito não devem constar dados pessoais do consumidor no tocante a prescrição de ação de cobrança por mais de cinco anos, prezando pelo princípio da caducidade.

> A discursão chegou ao STJ que pacificou seu entendimento através da Súmula 323, de seguinte teor: “A inscrição no nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução”. (ZANON, 2013, p. 137)

A súmula acarretou ao consumidor uma garantia de um direito de prescrição da cobrança da dívida, ou seja, após os cincos anos o credor não tem a possibilidade de cobrar a dívida existente.

Vejamos um recente julgado do STJ:

> RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. REPARAÇÃO POR DANOS MORAIS. INSCRIÇÃO EM CADASTRO DE PROTEÇÃO AO CRÉDITO. PRAZO DE PERMANÊNCIA. ART. 43, §1º, DO CDC. CINCO ANOS. TERMO INICIAL. DATA DO FATO GERADOR DO REGISTRO. INTERPRETAÇÃO LITERAL, LÓGICA, SISTEMÁTICA E TELEOLÓGICA DO ENUNCIADO NORMATIVO. 1. Pacificidade do entendimento, no âmbito deste Superior Tribunal de Justiça, de que podem permanecer por até 5 (cinco) anos em cadastros restritivos informações relativas a créditos cujos meios judiciais de cobrança ainda não tenham prescrito. 2. Controvérsia que remanesce quanto ao termo inicial desse prazo de permanência: (a) a partir da data da inscrição ou (b) do dia subsequente ao vencimento da obrigação, quando torna-se possível a efetivação do apontamento, respeitada, em ambas as hipóteses, a prescrição. 3. Interpretação literal, lógica, sistemática e teleológica do enunciado normativo do §1º, do art. 43, do CDC, conduzindo à conclusão de que o termo 'a quo' do quinquênio deve tomar por base a data do fato gerador da informação depreciadora. 4. Vencida e não paga a obrigação, inicia-se, no dia seguinte, a contagem do prazo, independentemente da efetivação da inscrição pelo credor. Doutrina acerca do tema. 5.

> Caso concreto em que o apontamento fora providenciado pelo credor após o decurso de mais de dez anos do vencimento da dívida, em que pese não prescrita a pretensão de cobrança, ensejando o reconhecimento, inclusive, de danos morais sofridos pelo consumidor. 5. RECURSO ESPECIAL DESPROVIDO. (REsp 1.316.117-SC, Rel. Min. João Otávio de Noronha, Rel. para acórdão Min. Paulo de Tarso Sanseverino, julgado em 26/4/2016, DJe 19/8/2016.)

O Tribunal Superior se posicionou baseando-se na súmula 323 e no artigo 43, § 3º do Código de Defesa do Consumidor, garantindo-lhe a prescrição da dívida cobrada.

O STJ sumulou, a partir do REsp nº 1.149.998, relatado pela Ministra Nancy Andrighi, acerca do prazo que os credores têm para efetivar a exclusão do registro da dívida devido o CDC não estabelecer um prazo, ocasionando uma violação do direito à honra do consumidor, já que a permanência do nome no cadastro de proteção ao crédito acarretaria possíveis danos.

Verificamos, como exemplo, o seguinte julgado:

> RECURSO ESPECIAL Nº 1.626.073 - SP (2016/0241175-4) RELATOR : MINISTRO MARCO BUZZI [...] Com efeito, a Segunda Seção desta Corte Superior de Justiça, sob o rito dos recursos especiais repetitivos, no julgamento do Recurso Especial n.º 1.424.792/BA, consolidou o entendimento nos termos do acórdão assim ementado: INSCRIÇÃO DO NOME DO DEVEDOR EM CADASTRO DE INADIMPLENTES. RECURSO ESPECIAL REPRESENTATIVO DA CONTROVÉRSIA. QUITAÇÃO DA DÍVIDA. SOLICITAÇÃO DE RETIFICAÇÃO DO REGISTRO ARQUIVADO EM BANCO DE DADOS DE ÓRGÃO DE PROTEÇÃO AO CRÉDITO. INCUMBÊNCIA DO CREDOR. PRAZO. À MÍNGUA DE DISCIPLINA LEGAL, SERÁ SEMPRE RAZOÁVEL SE EFETUADO NO PRAZO DE 5 (CINCO) DIAS ÚTEIS, A

> CONTAR DO DIA ÚTIL SUBSEQUENTE À QUITAÇÃO DO DÉBITO. [...] Nessa esteira, ainda que havendo regular inscrição do nome do devedor em cadastro de órgão de proteção ao crédito, após o integral pagamento da dívida, incumbe ao credor requerer a exclusão do registro desabonador, no prazo de 5 (cinco) dias úteis. No presente caso, assiste, portanto, razão ao recorrente quanto à reparação dos danos morais, já que o seu nome foi indevidamente mantido no cadastro de inadimplentes por 13 (treze) dias, mesmo após a realização do pagamento da dívida vencida. [..] Portanto, o pedido de condenação em danos morais deve ser acolhido e fixado com moderação, respeitando os critérios de razoabilidade e proporcionalidade. (REsp 1.626.073, Rel. Min. Marco Buzzi, julgado em 30/04,2017, DJe 09/05/2017).

A Súmula 548, do STJ trás a seguinte redação: “incumbe ao credor a exclusão do registro da dívida em nome do devedor no cadastro de inadimplentes no prazo de cinco dias úteis, a partir do integral e efetivo pagamento do débito”.

Vale-se dizer que o princípio ordena que os bancos de dados e arquivos de consumo não podem utilizar informações negativas superiores a cinco anos, e quando prescritas, devem ser excluídas dos seus bancos a fim de preservar o possível futuro crédito ao consumidor.

4.3. Sistema “*Scoring*”

O sistema *scoring* ou “*credit scoring*” foi originado nos Estados Unidos após a carência de métodos de distinção dos bons e maus pagadores, utilizado pelo banco de dados de formação ao crédito com o intuito de facilitar a concessão de crédito com base em análise de resultados oriundos das relações consumeristas.

Essa análise é baseada em fórmulas matemáticas realizada pelos bancos de dados, gerando uma pontuação a partir de informações pessoais dos consumidores. Quanto mais alta a pontuação atingida, maior a probabilidade de ser concedido o crédito por ser considerado um “bom pagante”.

Essa prática, embora comum, viola diretamente o princípio da isonomia a partir da discriminação dos consumidores com um “baixo *scoring*” por não atingir a meta imposta por estes bancos de dados.

Ao analisar informações como idade e sexo do consumidor no sistema comprova-se o descumprimento do parágrafo 3º, do artigo 3º da Lei 12.414/2011 onde “ficam proibidas as anotações” das informações excessivas e sensíveis do consumidor.

> § 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. (BRASIL, 2011)

A Lei de Cadastro Positivo, no inciso IV do artigo 5º regula, de forma indireta, o direito básico do consumidor em “conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial”, isto é, a prática do *scoring* adotada pelos bancos de dados de formação ao crédito.

Embora a lei traga essa redação, o SJT posicionou-se acerca do sistema “*scoring*”, entendendo que não se enquadra na categoria de “bancos de dados”, considerando lícita a utilização dos dados pessoais mesmo sem o consentimento do consumidor.

Essa decisão originou-se de uma demanda em que o autor da ação aludiu, na exordial, que o cadastro de consumidor manuseou suas informações pessoais sem o consentimento dele e, ainda não houve notificação prévia acerca do uso dos dados.

Após várias demandas semelhantes, criou-se o precedente a partir do julgado do REsp 1.419.698/RS, relatado pelo Min. Paulo de Tarso Sanseverino, configurando o sistema “scoring” apenas como:

> [...] uma metodologia de cálculo do risco de crédito, utilizando-se de modelos estatísticos e dos dados existentes no mercado acessíveis via “internet”. Constitui, em síntese, uma fórmula matemática ou uma ferramenta estatística para avaliação do risco de concessão do crédito.

Esse entendimento está representado na Súmula 550, do STJ.

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. (REsp1.419.697/RS, relator: Min. Paulo de Tarso Sanseverino. 2º Turma. DF, julgado em 12/11/2014)

Embora o sistema de crédito *scoring* não seja configurado como um banco de dados, os limites aplicados a ele são regidos pelo Código de Defesa do Consumidor e a Lei de Cadastro Positivo. Como já aludido, não é crucial o consentimento prévio do consumidor, mas sim uma notificação prévia acerca da finalidade do uso das informações.

Fica evidenciado a violação clara do direito à privacidade, à honra e à proteção dos dados pessoais do consumidor com essa prática, ainda que com súmula do STJ.

Ressalta que antes implementação da Lei de Cadastro Positivo e do CDC, o acesso a essas informações de histórico de crédito por parte do consumidor eram dificultadas.

Para que o consumidor tenha acesso ao seu “score”, de acordo com o site do SERASA, basta ele acessa-lo e realizar um cadastro. Nesse score constará o calculo apresentado de 0 a 1000 e observado este, conhecerá o comportamento do consumidor em um grupo de pessoas semelhantes.

Observa-se um “retrocesso” ao direito do consumidor, este sendo o vulnerável da relação consumerista, principalmente neste sistema, por estar “resguardado o segredo empresarial”, conforme o inciso IV do artigo 5º da Lei 12.414/2011 e o CDC.

5. CONSIDERAÇÕES FINAIS

Com o avanço e desenvolvimento das empresas a partir do princípio da livre concorrência, que objetivavam a expansão do mercado de atuação, surgiu a necessidade de mecanismo que abranja informação, a fim de facilitar o conhecimento do mercado de consumo através dos gostos e preferências dos consumidores.

Os arquivos de consumo surgem para dinamizar a reunião dos dados e a possível troca de informações entre si. Com a expansão destes, a lei 8.090 de 1990 - Código de Defesa do Consumidor aparece para regular o seu funcionamento, embora de maneira superficial.

Pelo fato do Código ser omissão em algumas questões, a Lei 12.414/2011 conhecida como Lei do Cadastro Positivo manifestou-se sobre quais e de que modo informações contidas nos bancos de dados para uma formação de um histórico de crédito ao consumidor seriam utilizadas.

A Constituição Federal, em consonância com o Código de Defesa do Consumidor abordam garantias, princípios e normas que o consumidor adquiriu com o passar do desenvolvimento das relações consumeristas.

Ao usufruir de dados pessoais, alguns considerados “sensíveis” à luz de doutrinadores, os arquivos de consumo violam princípios constitucionais e inerentes ao consumidor, como o direito à privacidade e à honra, se não manuseados de acordo com o ordenamento jurídico brasileiro.

Embora a Constituição expresse que “todos são iguais perante a lei”, na relação dos consumidores e bancos de dados não aplica o princípio da isonomia pelo fato da vulnerabilidade ser adotada às pessoas físicas ou jurídicas que não detêm de informações técnicas acerca do funcionamento do serviço praticado por estes arquivos de consumo.

Os bancos de dados instituíam a concessão de crédito essencialmente em informações negativas, ou seja, dívidas vencidas e não pagas, ainda que existente em seus bancos as informações positivas.

A partir da Lei de Cadastro Positivo os bancos passaram a utilizar todas informações necessárias a fim de formar um histórico de crédito completo do consumidor, não os discriminando como antes.

Os dados pessoais contidas nestes arquivos de consumo devem ter a finalidade devidamente expressa antes do consumidor fornece-las, por meio de um documento específico a fim de garantir o direito à privacidade e à proteção de dados pessoais.

Cada arquivo de consumo define de que modo coletará, processará e transferirá – salvo os cadastros de consumidores, os dados pessoais, respeitando os parâmetros legais.

No modo de coletar as informações pessoais por parte dos bancos de dados é indispensável o consentimento do consumidor, notificando-os sobre os riscos e finalidades do uso destas informações, com existência de proibições previstas em leis.

Os dados pessoais são aqueles referentes à hábitos, preferências e interesses do consumidor, salvaguardados pelo direito à privacidade e à proteção.

É no momento de processamento e cessão destes dados em que se demonstra a fragilidade maior na proteção dos dados pessoais do consumidor.

No processamento, a depender do método utilizado pelo banco de dados, gera uma discriminação do consumidor por “aproveitar” apenas informações que esse considera essencial á formação de um histórico de crédito, a exemplo do Serasa e SCP. A utilização de um mecanismo de processamento pode transforma-los em “mais pessoais” ainda, ao ponto de vista do consumidor, ofendendo a honra desse.

Para que um fornecedor ou um banco de dados transmita a outros informações já devidamente tratadas, é imprescindível o consentimento para este fim.

Embora essa prática contribua para que empresas ampliem seus mercados de atuação, uma informação que contenha inexatidão acarreta uma violação grave ao princípio da informação e do direito à honra do consumidor,

já que este pode ficar “mau visto” perante aqueles que detiverem do dado impreciso.

Quando há a cessão de dados à terceiros, o ordenamento jurídico brasileiro compreende que existe a responsabilização civil solidária entre o fornecedor ou arquivista e o bancos de dados quando se encontra imprecisão nas informações repassadas.

Entretanto há uma divergência quanto a notificação prévia e o consentimento do consumidor. O STJ entende que é necessário o consentimento do consumidor quando notificado acerca de como suas informações pessoais serão utilizadas, mas desconstitui um sistema utilizado pelos bancos de dados, afirmando que este é apenas um método de cálculo, violando diretamente o direito à privacidade e à honra.

Por isso, conclui-se a extrema necessidade do consumidor ter ciência de quais informações estão sendo coletadas, tratadas e cedidas à outros, a fim de evitar maiores prejuízos à sua honra e privacidade.

REFERENCIAS BIBLIOGRÁFICAS

ALESSIO, Marcio. **Evolução Histórica dos Bancos de Dados e a Aplicação da Nova Lei de Cadastros Positivos**. 2013. 78 f. Monografia (Especialização em Direito do Consumidor). Universidade Federal do Rio Grande do Sul, Porto Alegre. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/156527/001016565.pdf?sequence=1>. Acesso em: 10 out. 2017.

AMARAL, Luiz Otavio de Oliveira. **Teoria Geral do Direito Do Consumidor.** São Paulo: Editora Revista dos Tribunais Ltda., 2010.

BRASIL. Constituição (1988). **Constituição da República do Brasil**. Brasília, DF: Senado, 1988.

BESSA, Leonardo Roscoe. **Abrangência da disciplina conferida pelo Código de Defesa do Consumidor aos bancos de dados de proteção ao crédito**. Doutrinas Essenciais de Responsabilidade Civil, v. 8, p. 393, out. 2011.

BESSA, Leonardo Roscoe. **Banco de dados de proteção ao crédito: contornos jurídicos do compartilhamento de informações.** Revista de Direito do Consumidor, v. 95, p. 77, set. 2014.

BESSA, Leonardo Roscoe. **Os bancos de dados de proteção ao crédito na visão do Superior Tribunal De Justiça.** Revista de Direito do Consumidor, v. 63, p. 202, jul. 2007.

BESSA, Leonardo Roscoe. **Responsabilidade civil dos bancos dos dados de proteção ao crédito**. Revista de Direito do Consumidor, v. 94, p. 49, mar. 2014.

BESSA, Leonardo Roscoe. **Responsabilidade civil dos bancos de dados de proteção ao crédito: diálogo entre o CDC e a Lei do cadastro positivo**. Revista do Ministério Público do Consumidor, v. 1, n. 1º, 2014.

BRASIL. **Decreto nº 5.903** de 20 de setembro de 2006. **Regulamenta a Lei nº 10.962, de 11 de outubro de 2004, e a Lei nº 8.078, de 11 de setembro de 1990**. D.O.U em 21/09/2006.

BRASIL. **Decreto nº 7.829** de 17 de outubro de 2012. **Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que 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**. D.O.U de

18/10/2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7829.htm>. Acesso em: 19 out. 2017

BRASIL. **Decreto nº 7.962** de 15 de março de 2013. **Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico**. D.O.U de 15/03/2013.

BRASIL. Lei nº 7.232 de 29 de outubro de 1984. **Dispõe sobre a Política Nacional de Informática, e dá outras providências**. D.O.U. de 30/10/1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7232.htm>. Acesso em: 19 out 2017.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. D.O.U. de 12/9/1990.

BRASIL, Lei nº 10.406 de 10 de janeiro de 2002. **Institui o Código Civil**. D.O.U. de 11/01/2002.

BRASIL. Lei nº 12.037 de 1º de outubro de 2009.
Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. D.O.U. de 02/10/2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm>. Acesso em 19 out. 2017

BRASIL. Lei nº 12.414 de 09 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**. D.O.U de 10/06/2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em 19 out. 2017.

BRASIL. Lei nº 12.527 de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências**. D.O.U. de 18/11/2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 19 out.2017.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. **Estabelece princÍpios, garantias, direitos e deveres para o uso da Internet no Brasil**. D.O.U. de 24/4/2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 19 out.2017.

BRASIL. Nota Técnica nº40. **Análise do Decreto nº 7.962, de 15 de março de 2013**. D.O.U. em 11/11/2013. Disponível em: <http://justica.gov.br/seus-

direitos/consumidor/notas-tecnicas/anexos/nota-tecnica-no-40-2013-comercio-eletronico.pdf/view>. Acesso em: 23 out.2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 22.337/RS**. Relator: Min, Ruy Rosado de Aguiar. 4ª Turma. Brasília, DF, julgado em 20 de março de 1995. DJ 20/3/2005.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 165.727/DF**. Relator: Min. Sálvio de Figueiredo Texeira. 4º Turma. Brasília, DF. DJ 21/8/1998.

BRASIL. Superior Tribuna de Justiça. **Recurso Especial 273.250/CE**. Relator: Min, Ruy Rosado de Aguiar. 4º Turma. Brasília, DF, julgado em 19 de fevereiro de 2001.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.149.998/RS**. Relator: Min. Nancy Andrighi. 3º Turma. Brasília, DF, julgado em 07 de agosto de 2012.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.316.117/SC**. Relator: Min. João Otávio de Noronha, Rel. para acórdão Min. Paulo de Tarso Sanseverino. 3º Turma, julgado em 26 de abril de 2016. DJe 19/8/2016.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.348.532/SP**. Relator: Min. Paulo de Tarso Sanseverino. 4º Turma. DF, julgado em 24 de agosto de 2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.419.697/RS**. Relator: Min. Paulo de Tarso Sanseverino. 2º Turma. DF, julgado em 12 de novembro de 2014.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.626.073/SP**. Relator: Min. Marco Buzzi. 4º Turma. Brasília, DF, julgado em 30 de abril de 2017. DJe 09/5/2017.

BRASIL. Superior Tribunal de Justiça. **Súmula n.º 37**. São cumuláveis as indenizações por dano material e dano moral oriundos do mesmo fato. In: ___. **Súmulas**. São Paulo: Editora Saraiva. p. 2054.

BRASIL. Superior Tribunal de Justiça. **Súmula n.º 323**. A inscrição do nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução. Disponível em: https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_26_capSumula323.pdf. Acesso em: 18 out. 2017.

BRASIL. Superior Tribunal de Justiça. **Súmula n.º 548**. Incumbe ao credor a exclusão do registro da dívida em nome do devedor no cadastro de inadimplentes no prazo de cinco dias úteis, a partir do integral e efetivo

pagamento do débito. Disponível em: < https://www.legjur.com/sumula/busca?tri=stj&num=548>. Acesso em: 18 out. 2017.

Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. **Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Acesso à legislação da União Europeia. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046>. Acesso em 19 out. 2017.

Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009. **Altera a Diretiva 2002/58/CE**. Acesso à legislação da União Europeia. Disponível em: < https://www.anacom.pt/render.jsp?contentId=1174139>. Acesso em: 30 out. 2017.

GEOMARKETING. Disponivel em: <https://www.geomarketing.com.br/o-que-e>. Acesso em: 30 out. 2017.

LEONARDI, Marcel. **Vigilância tecnológica, bancos de dados, Internet e privacidade**. 2001. Disponível em: < https://jus.com.br/artigos/5899/vigilancia-tecnologica-bancos-de-dados-internet-e-privacidade>. Acesso em: 30 out. 2017.

LUPION, Ricardo. **O caso do sistema "credit scoring" do cadastro positivo**. Revista da Ajuris, v. 42, n. 137. 2015. Disponível em: <http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/391>. Acesso em: 20 out. 2017.

MENDES, Laura Schertel. **O direito básico do consumidor à proteção de dados**. Revista de Direito do Consumidor, v. 95, p. 53, set. 2014.

MENDES, Laura Schertel**. Privacidade, proteção de dados e defesa do consumidor.**, São Paulo: Editora Saraiva, 2014.

MIRAGEM, Bruno. **Direito Civil: responsabilidade civil**. São Paulo: Editora Saraiva, 2015.

MIRAGEM, Bruno. **Regulamentação da lei que disciplina a formação e consulta dos bancos de dados com informações de adimplemento e formação de histórico de crédito comentários ao Dec. 7.829/2012**. Revista de Direito do Consumidor, v. 84, p. 317, out. 2012.

NETTO, Felipe Peixoto Braga. **Manual de Direito do Consumidor**. 10ª ed. Bahia: Editora JusPodivm, 2015.

NETTO, Felipe Peixoto Braga. **Manual de Direito do Consumidor**. 12ª ed. Bahia: Editora JusPodivm, 2017.

OLIVA, Afonso Carvalho de. **Direitos do Consumidor: proteção de dados pessoais**. Sergipe: DireitoMais Editora, 2016.

SANTANA, Hector Valverde. **Proteção internacional do consumidor: necessidade de harmonização**. Revista de Direito Internacional, Brasília, v. 11, n. 1, 2014. Disponível em: < https://bdjur.stj.jus.br/jspui/bitstream/2011/81418/protecao_internacional_consumidor_santana.pdf>. Acesso em: 30 out. 2017.

SERASA. Cadastro Positivo. Disponível em: <https://www.serasaconsumidor.com.br/cadastro-positivo/>. Acesso em 22 out. 2017.

SERASA. Sistema Score. Disponível em: <https://www.serasaconsumidor.com.br/score/>. Acesso em 22 out. 2017.

ZANON, João Carlos. **Direito à Proteção dos Dados Pessoais.** São Paulo: Editora Revista dos Tribunais, 2014.