UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO (UNIRIO)
CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS (CCJP)
ESCOLA DE CIÊNCIAS JURÍDICAS

JOÃO LUCAS MORAES PAVÃO

A RESPONSABILIZAÇÃO CIVIL OBJETIVA NO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS E NO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS SOB O REGIME DA LEI GERAL DE PROTEÇÃO DE DADOS

RIO DE JANEIRO
2021

JOÃO LUCAS MORAES PAVÃO

A RESPONSABILIZAÇÃO CIVIL OBJETIVA NO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS E NO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS SOB O REGIME DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de conclusão de curso apresentado à Escola de Ciências Jurídicas da Universidade Federal do Estado do Rio de Janeiro como requisito parcial à obtenção do grau de Bacharel em Direito.

Profº Drº. Emerson Affonso da Costa Moura

Rio de Janeiro

2021

JOÃO LUCAS MORAES PAVÃO

A RESPONSABILIZAÇÃO CIVIL OBJETIVA NO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS E NO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS SOB O REGIME DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de conclusão de curso apresentado à Escola de Ciências Jurídicas da Universidade Federal do Estado do Rio de Janeiro como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovado em: de 2021.

BANCA EXAMINADORA

_____

Profª. Drº. Emerson Affonso da Costa Moura (Orientador)

Universidade Federal do Estado do Rio de Janeiro

_____

Profª Drª.Edna Raquel Hogemann

Universidade Federal do Estado do Rio de Janeiro

_____

Profª Drª. Rosalina Corrêa de Araujo

Universidade Federal do Estado do Rio de Janeiro

Rio de Janeiro

2021

AGRADECIMENTOS

Agradeço primeiramente a Deus e à minha família, que me deram o apoio e os alicerces necessários para chegar tão longe. Sei que posso contar especialmente com meus pais, meus irmãos, meus avós Salvador e Isabel. Gratidão também ao meu finado avô, Lucas Lopes Pavão, que investiu e acreditou em mim, e que deixou muitas saudades entre seus familiares.

Agradeço aos meus amigos de faculdade que estiveram sempre ao meu lado, me ensinaram tanto sobre a vida e sobre o Direito. Em especial, Fabiana, Lucas, Estela, Gabriel, Luciana, tenho muita sorte de ter amigos brilhantes e companheiros como vocês.

Agradeço aos meus amigos de outras datas, que fizeram parte da minha vida, me deram apoio e conselhos quando precisei. Roberto, Beatriz, Renan, Marcos, Carol, Alessandra, entre tantos outros que não caberiam aqui neste pequeno texto, vocês não sabem como foram importantes para mim.

Agradeço em especial à minha namorada, Gabriela de França Scarpa, que além de namorada é uma amiga e colega de profissão. As suas palavras de ânimo, a sua admiração, os seus conselhos e a sua intuição certeira foram decisivos nesses momentos finais.

Também agradeço aos meus professores, que tanto me inspiraram e me deram suporte. Professor Emerson Moura, obrigado pela orientação e pela oportunidade, professora Edna Raquel e Professora Rosalina, obrigado pela disponibilidade e empenho como membros da minha banca examinadora, e, finalmente, obrigado a todos os professores desde o maternal até o presente momento, sem vocês nada disso seria possível.

Por fim, e não menos importante, agradeço aos meus colegas de trabalho, que acompanharam de perto alguns degraus dessa minha caminhada e me ensinaram a parte prática de tudo que aprendi na faculdade e muito do que foi transmitido nesse trabalho. Obrigado Dra. Vanuce, pelo apoio e pela confiança. Obrigado Dra. Laura, por me ensinar a tratar com esmero cada pequena tarefa que me fosse dada.

The tools of the Industrial Age extended the capacities of our muscles. The tools of the digital age extend the capacities of our minds.

(GATES, 2001, p. 98).

RESUMO

O presente trabalho propõe-se a analisar a possibilidade de responsabilização objetiva pelos danos causados pelo tratamento de dados sensíveis e pelo tratamento automatizado de dados sob o regime da Lei Geral de Proteção de Dados brasileira, partindo-se da hipótese de que tais atividades carregam em si um risco inerente. Em meio ao estudo proposto, encontra-se o desafio de se obter respostas que respeitem o binômio desenvolvimento econômico e tecnológico e a privacidade dos dados. Para atingir os objetivos pretendidos, busca-se evidenciar como as espécies de tratamento de dados mencionadas podem gerar danos ao indivíduo no tocante à sua segurança, privacidade e autodeterminação informativa. Como a nova lei de proteção de dados não define o regime de responsabilidade adotado como regra geral na seara da proteção de dados, busca-se, também, analisar esse regime, a fim de que seja possível definir se o mesmo comporta ou não exceções. Desse modo, utiliza-se o procedimento bibliográfico para, de forma descritiva, estudar e comparar as teorias de reconhecidos doutrinadores acerca do tema, o Regulamento Geral de Proteção de Dados europeu e o próprio texto legal da Lei Geral de Proteção de Dados brasileira. Após, por uma abordagem qualitativa, verifica-se que o regime geral que melhor se adequa à proteção de dados no Brasil é o da responsabilidade subjetiva, em razão das disposições da Lei Geral de Proteção de Dados. Ademais, valendo-se de análise dedutiva, encontra-se, na lei brasileira de proteção de dados, normas específicas para o tratamento de dados sensíveis, as quais são consideravelmente mais rigorosas em relação ao tratamento de dados comuns, restando notória a possibilidade de defesa de um regime de responsabilidade objetiva para os danos produzidos pelo tratamento de dados sensíveis. Todavia, não se comprova a hipótese inicial quanto ao tratamento automatizado de dados, vez que para este tipo de tratamento não há qualquer diferenciação dada pela lei em relação ao regime geral. Por fim, conclui-se que, embora a responsabilidade subjetiva seja a regra na Lei Geral de Proteção de Dados, o titular de dados não ficou desamparado, vez que os agentes de tratamento de dados devem cumprir uma série de deveres de transparência e prestação de contas, a fim de testificarem sua boa-fé e compromisso com a proteção de dados.

Palavras-chave: Responsabilidade civil. Responsabilidade objetiva. Proteção de dados. Dados pessoais. Tratamento automatizado.

ABSTRACT

This work proposes to analyze the possibility of strict liability for the damages caused by the treatment of sensitive data and the automated treatment of data under the regime of the brazilian General Data Protection Law, starting from the hypothesis of that such activities carry an inherent risk. In this regard, it is proposed to analyze the possibility of objective liability for the damages caused by the treatment of sensitive data and the automated treatment of data, starting from the hypothesis that such activities carry an inherent risk. In the midst of the proposed study, there is the challenge of obtaining answers that respect the binomial economic and technological development and privacy data. In order to achieve the intended objectives, are showed how the types of data processing mentioned can cause harm to the individual with regard to his security, privacy and informational self-determination. As the new Brazilian data protection law does not define the liability regime adopted as a general rule in the field of data protection, it is necessary to analyze this regime, so that it is possible to define whether or not it includes exceptions. Thus, the bibliographic procedure is used to, in a descriptive way, study and compare the theories of recognized doctrines on the subject, the European General Data Protection Regulation and the legal text of the Brazilian General Data Protection Law. Then, through qualitative approach, it appears that the general regime that best suits data protection in Brazil is that of subjective responsibility, due to the provisions of Brazilian General Data Protection Law. Furthermore, using the deductive analysis, in Brazilian data protection law, specific rules for the treatment of sensitive data are found, which are considerably more rigorous in relation to the treatment of common data, leaving the notorious possibility of defense of a strict liability regime for damages caused by the processing of sensitive data. However, the initial hypothesis regarding the automated processing of data is not proven, since for this there is no differentiation given by the law in relation to the general regime. Finally, it is concluded that, although subjective responsibility is the rule in the General Data Protection Law, the data subject has not been left unprotected, since data processing agents must comply with a set of transparency and accountability duties. accounts in order to testify their good faith and commitment to data protection.

Keywords: Civil liability. Strict liability. Data protection. Personal Data. Automated treatment.

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, a economia mundial sofreu drásticas mudanças, em razão do impacto causado pela internet e pela digitalização das informações. Como as pessoas estão cada vez mais conectadas à rede mundial de computadores, as interações sociais e comerciais se dão cada vez mais de forma online, provocando um grande crescimento no fluxo de informações compartilhadas na internet e, consequentemente, criando um novo nicho onde empresas buscam capitalizar essas informações.

Não à toa cunhou-se o termo "sociedade da informação" para designar uma sociedade onde a informação figura como elemento fundamental para reorganizar a sociedade. Nesse contexto, a internet desempenha o papel de catalisador para acelerar a influência dos dados sob a economia, pois por meio dela uma infinidade de conhecimento é acumulada em bancos de dados, disponíveis a qualquer momento e lugar, e as distâncias são encurtadas, permitindo a comunicação em tempo real onde quer que se esteja.

Em razão de todo esse avanço cibernético, milhares de serviços são disponibilizados por meio de aplicativos de celulares, como os serviços de entrega e de entretenimento, que podem ser contratados no conforto de casa, apenas fornecendo os seus dados cadastrais e de cartão de crédito no *app*. Contudo, ao se fazer um cadastro em um site ou aplicativo, são deixados rastros de informações que perduram na internet por tempo indeterminado e que podem ser utilizados para os mais diversos fins.

Nas redes sociais, por exemplo, as pessoas compartilham livremente suas vidas privadas por meio de fotos, vídeos, textos, preferências etc. com milhares de outras pessoas, muitas vezes desconhecidas, gerando verdadeiros relatórios detalhados de suas vidas que são armazenados e utilizados para traçar perfis precisos de usuários, que podem servir para fomentar campanhas de publicidade, *trending topics*, estatísticas comportamentais etc.

Assim, à medida que as pessoas realizam buscas, compras e demonstram predileções por determinado conteúdo na *web*, algumas empresas já perceberam uma oportunidade de captar os rastros deixados pelas pessoas na internet, utilizando-os para aprimorar produtos e serviços e para promover um marketing mais eficiente de suas empresas.

Em razão disso, algumas companhias vêm se especializando em capturar e gerir dados pessoais – chamadas de operadoras – em nome de outras empresas que possuem o interesse econômico direto nesses dados – chamadas de controladoras. Entrementes, nota-se uma nova

dinâmica de mercado estruturada, na qual os dados pessoais são barganhados como moeda de troca por agentes econômicos em suas atividades empresariais.

Fato é que, os rastros de informações deixados pelas pessoas ao navegarem na internet adquirem uma certa perpetuidade, pois quando os agentes econômicos compartilham essas informações uns com os outros, perde-se o controle sobre eles. E depois, caso o indivíduo não deseje mais que determinada informação seja a ele vinculada, ou que alguma informação sua seja corrigida por qualquer motivo, torna-se tarefa praticamente impossível encontrar e excluir todos os seus registros na *web*.

Com isso, a exploração econômica das informações pessoais se torna um fator de risco e preocupação para a segurança, privacidade e autodeterminação dos indivíduos. Isso porque, na ausência de uma regulamentação apropriada, as empresas buscam, em última instância, o lucro e a eficiência em seus negócios, havendo pouca reflexão, por parte delas, sobre as consequências aos direitos e liberdades individuais e coletivos.

Além do mais, existem algumas informações pessoais sensíveis que devem ser mantidas longe do conhecimento de terceiros, pois o seu conteúdo diz respeito a intimidade do indivíduo, que só deve ser compartilhada com quem ele consinta. Imagine-se, por exemplo, que sejam divulgadas informações como o posicionamento político de alguém em uma conjuntura de perseguição política, ou que sejam utilizados dados sobre a origem étnica do indivíduo como critério para contratação de emprego.

Essas situações mencionadas certamente acarretariam danos difíceis de se reparar, pois provocariam injustiças e discriminação. A situação é ainda mais crítica quando se fala em algoritmos e inteligência artificial, pois essas tecnologias de programação podem ser capazes de prever e antecipar comportamentos humanos, aprendendo e reproduzindo em larga escala preconceitos enraizados na sociedade.

Para além disso, mesmo quando não há a reprodução de preconceito propriamente dito por essas tecnologias, é necessário reconhecer que sistemas de decisão automatizados podem eventualmente atingir resultados incorretos, imprecisos ou enviesados, capazes de prejudicar quem quer que seja alvo deles. Portanto, deve haver também uma preocupação quanto à penalização dos responsáveis por esses danos.

Assim, em razão do rápido desenvolvimento da programação e da exploração econômica dos dados, o direito à proteção de dados clamou por posição de destaque no ordenamento jurídico brasileiro. Tornou-se salutar, portanto, haver a criação de medidas para regulamentar o tratamento de dados e para criar meios de responsabilização eficientes para inibir e reparar os danos causados pelos agentes econômicos nesse campo de ação.

Em atenção ao exposto, a LGPD, que entrou em vigor muito recentemente, visa a complementar o entendimento sobre proteção de dados, já iniciado no Brasil com a Lei de Acesso à Informação (Lei Federal nº 12.527/2011) o Marco Civil da Internet (Lei Federal nº 12.965/2014 – MCI) e o Código de Defesa do Consumidor (Lei Federal nº 8.078/1990 – CDC). Dessa maneira, embora a nova lei protetiva de dados brasileira tenha muito do seu texto inspirado em sua congênere europeia, a General Data Protection Regulation (Regulation 679/2016 – GDPR), a interpretação da LGPD deve ser realizada de forma harmônica e sistemática em relação às normas que a antecedem no ordenamento jurídico brasileiro.

Por isso, a LGPD visa a consolidar conceitos e a pacificar discussões acerca da proteção de dados no Brasil, além de estabelecer uma série de novos direitos e deveres objetivos, o que deve ser feito levando em conta a árdua tarefa de se equilibrar o desenvolvimento econômico e tecnológico e os direitos individuais e coletivos de proteção de dados.

Não obstante, não se pode esperar que, em seus sessenta e cinco artigos, a nova LGPD esgote o tema da proteção de dados em toda a sua abrangência, ou que essa lei seja a palavra final sobre essa questão que carece de atualização constante, em virtude do acelerado desenvolvimento tecnológico. Reconhecendo tal limitação, o legislador adicionou ao texto da nova lei a criação um órgão de fiscalização, a Agência Nacional de Proteção de Dados (ANPD) com atribuições bastante abrangentes, principalmente para estipular critérios técnicos, com o fito de inibir e reparar práticas lesivas aos titulares de dados.

Isto posto, deve-se reconhecer que a responsabilidade civil pela proteção de dados pessoais foi um assunto insuficientemente abordado pela LGPD, pois, embora essa lei preveja a responsabilização dos agentes de tratamento de dados em seu escopo, foram deixadas de fora questões importantes como qual o regime de responsabilidade teria sido adotado por ela.

Em adendo, deve ser levado em conta que algumas atividades envolvendo dados pessoais podem ser mais lesivas que outras, por isso tem-se como objetivo geral verificar a possibilidade de aplicação da responsabilidade objetiva para os casos de incidentes envolvendo o tratamento de dados pessoais sensíveis e o tratamento automatizado de dados pessoais, com base na teoria do risco.

Em vista disso, este trabalho tem como problema central investigar se a responsabilidade civil é um instituto suficiente para dirimir os riscos trazidos pelo tratamento de dados sensíveis e pelo tratamento automatizado de dados, considerando a necessidade de se encontrar respostas que não onerem excessivamente o desenvolvimento econômico e tecnológico, mas que também não deixem o titular de dados desprotegido de abusos cometidos nesta seara.

Parte-se da hipótese de que as atividades envolvendo dados sensíveis e decisões automatizadas carregam em si um risco inerente, vez que não se poderia executá-las sem que o resultado lesivo se tornasse muito provável. Por essa razão, se justificaria o regime da responsabilidade objetiva para os casos de incidentes envolvendo o tratamento de dados pessoais sensíveis e o tratamento automatizado de dados pessoais.

Com isso em mente, o presente trabalho, como primeiro objetivo específico, propõe-se a analisar a exploração econômica de dados pessoais sensíveis e através do tratamento automatizado de dados, a fim de se verificar a real existência de riscos inerentes dessas atividades. Posteriormente, como segundo objetivo específico, discorre-se sobre qual teria sido o regime de responsabilidade civil adotado pela LGDP como regra, com o intuito de verificar se a referida legislação comporta exceções ao regime geral e, portanto, se admitiria a hipótese do presente trabalho.

Os capítulos desse trabalho são embasados no procedimento bibliográfico de análise da doutrina, da regulamentação europeia de proteção e dados – a qual é referência mundial sobre o certame –, e do próprio texto legal da LGPD. Também são resgatadas algumas jurisprudências com o fito de se demonstrar como os tribunais vêm entendendo a tratativa de dados sensíveis e a automatização de processos de tomada de decisão.

Objetiva-se descrever o conhecimento já existente sobre a responsabilidade civil no âmbito da proteção de dados, com o intuito de se criar um arcabouço jurídico suficiente para analisar qualitativamente a responsabilidade civil da proteção de dados nas hipóteses específicas abordadas nesse trabalho, quais sejam, o tratamento automatizado de dados e o tratamento de dados sensíveis.

Assim, utiliza-se, predominantemente, o método dedutivo de pesquisa, para, a partir das premissas encontradas como verdadeiras acerca da proteção de dados, tanto na doutrina quanto no texto da LGPD, explicar a configuração da responsabilidade nas situações mais específicas, quais sejam a do tratamento automatizado de dados e do tratamento de dados sensíveis.

A finalidade básica-estratégica é preponderante nesta pesquisa, uma vez que são tratados assuntos de relevante interesse acadêmico e prático, evidenciados pelo avanço da tecnologia e a necessidade de adaptação do Direito ao novo contexto de regulação de dados, motivo pelo qual o presente trabalho poderá ser futuramente utilizado como o ponto de partida de novas pesquisas.

Dedica-se, desse modo, a segunda sessão deste trabalho a explicar a necessidade de se criar um ambiente de regulação em que não se impeça o desenvolvimento econômico e tecnológico, sem perder de vista o dever fundamental da proteção de dados. Nos subtópicos

dessa mesma sessão, almeja-se, no primeiro subtópico, contextualizar a proteção de dados ao cenário econômico, e, nos subtópicos seguintes, explicar as particularidades do tratamento de dados sensíveis e do tratamento automatizado de dados, evidenciando quais os riscos envolvidos nessas atividades.

Já na terceira sessão desse trabalho, aborda-se qual teria sido o regime geral de responsabilidade civil adotado pela nova lei protetiva de dados brasileira e as possíveis exceções ao referido regime, considerando os riscos do tratamento automatizado de dados e as particularidades trazidas por essa lei em relação aos dados sensíveis.

Derradeiramente, na última sessão, conclui-se o trabalho, buscando resumir as ideias construídas, e confirma-se que o regime de responsabilidade trazido pela LGPD leva em conta o cumprimento de uma série de obrigações, a serem detalhadas pela ANPD, mas que já demonstram uma tendência à responsabilidade subjetiva e a se criar um elevado padrão de transparência e diligência às empresas, que deverão demonstrar engajamento e robustez documental afim de promover a governança de dados necessária para efetivar a máxima segurança aos seus titulares.

2 A REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

A LGPD, sem dúvidas, irá revolucionar a proteção de dados no Brasil, tal qual a GDPR fez na Europa. Isto se dá porque o Brasil, até então, somente contava com normas esparsas que tratavam do assunto (MONTEIRO FILHO; DE CASTRO, 2019). Pode-se citar, a título de exemplo, a Lei de Acesso à Informação (Lei Federal nº 12.527/2011) o Marco Civil da Internet (Lei Federal nº 12.965/2014 – MCI) e o Código de Defesa do Consumidor (Lei Federal nº 8.078/1990 – CDC).

Ocorre que, nos últimos anos, os debates sobre a exploração de dados pessoais vem se intensificando no Brasil há alguns anos, e ganharam ainda mais notoriedade em 2018, com o caso da Microsoft, que foi processada pelo Ministério Público Federal de São Paulo (MPF/SP) pela coleta não autorizada de dados de seus usuários (FEDERAL, 2018), e, em 2019, com o caso do Aplicativo "FaceApp" desenvolvido pelo Google em parceria com a Apple, que foram multadas pelo Procon-SP em quase R$ 10 milhões e em R$ 7,7 milhões, respectivamente, por disponibilizar o aplicativo sem termos de uso em português e impondo cláusulas abusivas aos usuários (VENTURA, 2019).

Por essa razão, já não era sem tempo para que fosse editada uma lei específica que regulasse a matéria da proteção de dados no Brasil com completude, pois a falta de regulamentação específica sobre o tema começou a se mostrar preocupante, haja vista a possibilidade de que decisões esparsas e desalinhadas, criassem um cenário de insegurança jurídica. Em adendo, esse novo campo de atuação do direito carece de conceituações legais mais claras e uniformes, pois o estudo desta matéria está repleto de termos eminentemente técnicos, que podem gerar confusão tanto para o cidadão, quanto para as empresas e também para os próprios intérpretes da lei em atuação no judiciário.

Nesse contexto de incertezas, a LGPD, que entrou em vigor em setembro de 2020 (SENADO, 2020), promete ser um divisor de águas na esfera da proteção de dados, pois se propõe a unificar o debate acerca do tema no Brasil. Contudo, levanta-se o questionamento sobre alguns conceitos abstratos trazidos pela nova lei e sobre do rigor das punições trazidas por ela, que são capazes de gerar impactos econômicos desastrosos até mesmo para grandes empresas.

As punições previstas na LGPD se aproximam daquelas estipuladas pela GDPR, pois, a título de comparação, as companhias que violarem a proteção de dados no Brasil se sujeitarão a multas de até 2% (dois por cento) da receita bruta da empresa no exercício anterior, limitadas

ao total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração cometida[1]. Enquanto isso, sob a vigência da regulamentação europeia, as multas podem chegar a 4% (quatro por centro) do faturamento global anual ou 20 milhões de euros, o que for maior, para aqueles que violarem suas disposições[2].

Com isso em mente, é evidente que devem ser estabelecidas diretrizes justas e equilibradas ao se interpretar os termos da LGPD, a fim de que não se onere demais as empresas, e, consequentemente, não sejam gerados impactos desproporcionais à economia. Por outro lado, assim como ocorre no âmbito do direito do consumidor e do direito trabalhista, a legislação precisa ser mais incisiva em determinadas situações para garantir a tutela de direitos fundamentais e a igualdade entre todos perante a lei.

Nesse prisma, deve-se reconhecer que algumas atividades, mais que outras, aviltam a segurança e a incolumidade psicofísica das pessoas, pois, devido à sua natureza, geram riscos à coletividade e ao indivíduo. Para essas atividades, o Direito reserva a responsabilidade objetiva, conforme prenuncia o art. 927, parágrafo único, do CC/2002, ao dizer que deve haver reparação, "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" (BRASIL, 2002).

Portanto, na seara da proteção de dados, muito embora se reconheça que não se deva onerar excessivamente o desenvolvimento econômico e tecnológico, existem algumas atividades que merecem atenção especial ao se analisar a responsabilização pelos erros ocasionados por elas.

Como será abordado mais à frente, a própria lei de proteção de dados brasileira já reconhece expressamente a responsabilidade objetiva pelas falhas ocorridas no tratamento de dados realizado na esfera da atividade consumerista. Nesse caso, a responsabilidade objetiva é

---

[1] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL, 2018, art. 52, inciso II):

[2] 5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[…] (EUROPEIA, 2016, p. 119/83) Tradução do autor: Infrações às seguintes previsões podem, de acordo com o parágrafo 2, estarem sujeitas à multa administrativa de até 20 000 000 EUR, ou no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:

um reflexo do risco da atividade evidenciado pela disparidade econômica e técnica existente e reconhecida amplamente no Direito brasileiro entre o consumidor e o fornecedor[3].

Além das atividades desenvolvidas no âmbito do direito do consumidor, conquanto não ter sido expressamente positivada a responsabilidade objetiva nessas ocasiões pela LGPD, pretende-se demonstrar que entendimento análogo pode ser despendido ao tratamento de dados pessoais sensíveis e ao tratamento automatizado de dados, em decorrência da natureza dessas atividades.

Sendo assim, no subtópico a seguir serão abordados os principais conceitos e princípios da LGPD, com o intuito de clarificar os termos utilizados por essa lei e de contextualizá-los com a necessidade de se promover o equilíbrio entre a proteção de dados e o desenvolvimento econômico e tecnológico. Posteriormente, nos demais subtópicos, passa-se a dissertar sobre as atividades aviltantes dos direitos dos titulares de dados, quais sejam, o tratamento de dados sensíveis e o tratamento automatizado de dados.

2.1 O equilíbrio entre a proteção de dados e o desenvolvimento econômico

O art. 2º da LGPD (BRASIL, 2018) estipula os fundamentos da proteção de dados, sobre os quais destacam-se o respeito à privacidade e o desenvolvimento econômico e tecnológico, respectivamente nos seus incisos[4] I e V. Esses fundamentos merecem destaque, pois expressam muito bem a máxima a ser seguida pela regulação de dados no direito brasileiro, qual seja, o equilíbrio entre os direitos à proteção de dados e o desenvolvimento econômico.

Dessa forma, é preciso compreender que a proteção de dados deve ser o liame entre o respeito à privacidade e o desenvolvimento econômico e tecnológico. Em outras palavras, a empreitada da proteção de dados deve criar um ambiente digital de confiabilidade, no qual o

[3] Nesse sentido, Bessa e de Moura (2014, p. 77): "A Lei nº 8.078/90 (CDC) parte do pressuposto de que o consumidor é um sujeito vulnerável ao adquirir produtos e serviços ou simplesmente se expor a práticas do mercado. A vulnerabilidade é o ponto fundamental do CDC e, na prá□ca, traduz-se na insuficiência, na fragilidade de o consumidor se manter imune a práticas lesivas sem a intervenção auxiliadora de órgãos ou instrumentos para sua proteção.". Em concordância, Leonardo Garcia (2020, .p. 24): "Assim, da leitura do art. 5º, XXXII da CF (o Estado promoverá, na forma da lei, a defesa do consumidor); extrai-se quatro conclusões imediatas: 1) o reconhecimento da vulnerabilidade do consumidor pela CF, isso porque quando a CF previu que o Estado deverá promover a "defesa do consumidor", é porque reconheceu que este indivíduo se apresenta vulnerável frente ao outro parceiro contratual (no caso o fornecedor, expert da relação). De outro modo, se fossem parceiros (consumidor e fornecedor) que agissem na relação em "pé de igualdade", não faria sentido a CF prever a defesa de um deles.". E, também, Fabio Ulhoa Coelho (2012, p. 71): "Em geral, o consumidor tem, relativamente ao produto ou serviço que pretende adquirir, apenas as informações prestadas pelo fornecedor. Caracteriza-se, no caso, a vulnerabilidade do consumidor, fundamento para o tratamento legal mais benéfico liberado pelo direito do consumidor"

[4] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; V - o desenvolvimento econômico e tecnológico e a inovação; (BRASIL, 2018, art. 2º, incisos I e II)

titular de dados tem os seus direitos à privacidade e à autodeterminação informativa respeitados, ao passo que os agentes de tratamento de dados possam, também, ter plena convicção do que podem ou não fazer com os dados pessoais.

Nesse sentido, assevera Bruno Bioni (2019):

> as leis de proteção de dados procuram conferir segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados. E, em última análise, assegurar confiança entre todos os atores desse ecossistema para que não haja paralisia nessas trocas econômicas. (BIONI, 2019, p. 108)

Assim, para se criar esse cenário de segurança jurídica e confiabilidade, os agentes de tratamento de dados deverão internalizar em suas atividades os valores fundamentais da proteção de dados. Ou seja, a atividade econômica deve ser realizada de forma a garantir o controle dos dados por parte de seus titulares e a incolumidade da vida privada.

Isto posto, é necessário conceituar o direito à proteção de dados e definir alguns outros termos e implicações que surgem ao seu entorno, tais como o conceito de "dado pessoal" e de "dado pessoal sensível", a relação entre o fundamento da autodeterminação informativa e o fundamento do desenvolvimento econômico e tecnológico, além de se analisar brevemente quais são os princípios básicos que devem reger a proteção de dados.

Conforme a leitura do art. 5º, inciso I[5], da LGPD (BRASIL, 2018), entende-se que os dados pessoais são aquelas informações que podem ser atreladas a uma pessoa identificada ou identificável, ou seja, são informações pertencentes a um titular conhecido, ou que, mediante mero raciocínio lógico se possa conhecer, de modo que enquanto perdurar a possibilidade de identificação do titular de uma determinada informação, também perdurará a tutela da proteção destes dados.

Destarte pode-se falar sobre a *anonimização* de dados, conceituada pela nova lei de proteção de dados brasileira como sendo a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (BRASIL, 2018, art. 5º, inciso X). Essa técnica procura desassociar uma informação de seu titular, de modo a preservar os resultados comerciais, estatísticas, avaliações, censos demográficos, pesquisas científicas, dados da medicina, enfim, todo tipo de informação necessária ao desenvolvimento econômico, tecnológico e à inovação, sem, contudo, expor os titulares dessas informações.

Importante destacar que a *anonimização* somente é considerada eficaz quando o processo de identificação da pessoa titular de dados se torna realmente dificultoso. Isso significa

[5] I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (BRASIL, 2018, art. 5º, inciso I)

dizer que não serão considerados *anonimizados* os dados que, por mero cruzamento de informação, puderem ser associados novamente aos seus titulares. Por isso a lei brasileira de proteção de dados prevê que o processo de anonimização somente será considerado efetivo quando o procedimento de reversão demandar esforços razoáveis de terceiros, ou exclusivamente por meios próprios puder ser realizado, nos termos do art. 12º, *caput*[6], da LGPD.

Outro conceito importante dentro desse escopo é o de dados pessoais sensíveis, que são aqueles que, além de pertencerem a uma pessoa identificada ou identificável, dizem respeito às informações de cunho íntimo, como por exemplo, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural. Esses exemplos podem ser encontrados no art. 5º, inciso II[7], da LGPD (BRASIL, 2018), porém, este não se trata de um rol exaustivo, visto que, a depender do contexto, um dado pessoal trivial poderá revelar traços profundos da personalidade de seu titular.

Nesse mesmo raciocínio, afirma Leonardi (2011, p.74), ao explicar as relevantes palavras de Conesa (1984, p. 45) acerca dos dados sensíveis:

> [CONESA] afirma que existem dados irrelevantes a priori do ponto de vista da intimidade, mas que, em conexão com outros dados, quiçá igualmente irrelevantes, sob a mesma perspectiva, quando isoladamente considerados, podem servir para tornar totalmente transparente a personalidade de um indivíduo, "tal como ocorre com as pequenas pedras que formam os mosaicos: em si mesmas, não dizem nada, mas unidas podem formar conjuntos plenos de significado". (LEONARDI, 2011, p. 74)

De igual modo, a Consideração nº 51 da GDPR (EUROPEIA, 2016) considera que dados sensíveis são aquelas informações que, em razão da sua natureza, quando submetidas ao tratamento, podem causar riscos significativos aos direitos e liberdades fundamentais:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. [...] Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. (EUROPEIA, 2016, p. 119/10, tradução do autor)

---

[6] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. (BRASIL, 2018, art. 12)

[7] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018, art. 5º, inciso II)

Portanto, os dados sensíveis carregam em si uma fragilidade inerente, pois dizem respeito às informações mais íntimas do indivíduo, as quais ele deseja manter resguardadas do conhecimento de terceiros não autorizados. Evidentemente os dados pessoais sensíveis receberam uma atenção especial na LGPD, estando o seu uso restrito a algumas situações específicas que serão melhor abordadas adiante, normalmente relacionadas com o consentimento do titular, o cumprimento de deveres legais e o interesse coletivo.

Esclarecido o conceito de dados pessoais e feita a diferenciação entre dados pessoais e dados pessoais sensíveis, argumenta-se que os dados pessoais podem ser entendidos como uma projeção da personalidade do seu titular, conforme assevera Bioni (2019, p. 64-65) ao dizer que, sob a perspectiva da tutela jurídica, "um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular."

Nesse sentido, valiosa é a lição do jurista e professor italiano Stefano Rodotà (2012 Apud BIONI, 2019), segundo o qual o homem constrói sua identidade a partir dos recursos disponíveis que encontra na sociedade[8]. Por essa razão, à medida que a tecnologia se torna cada vez mais facilitadora da vida moderna, mais o homem a utiliza para se relacionar com seus semelhantes, para auxiliar em decisões importantes em sua vida e para expressar suas opiniões, e com isso ele próprio se distingue dos seus iguais, expressando sua individualidade e desenvolvendo sua própria identidade.

Verifica-se, desta maneira, que estas informações associadas ao indivíduo são bens da sua própria personalidade, pois, como expõe Catala (1983, p. 19) citado por Leonardi (2011, p. 78): "quando o objeto dos dados é um sujeito de direito, a informação representa um atributo de sua personalidade.".

É oportuno, portanto, enfatizar que os direitos à proteção de dados, são direitos fundamentais da personalidade, haja vista os dados figurarem como a projeção do indivíduo na esfera cibernética. Assim, para Thiago Neves (2019, p. 11) os direitos da personalidade "decorrem diretamente da pessoa humana, [...] pelo postulado da dignidade da pessoa humana",

[8] "Tutto questio, oggi, può essere considerato anche nella dimensione de diritti, di uma construzione dell'indetitá che finisce com il coincidere con la costruzione stessa dell'umano (...) costruire liberamente la própria indetitá utilizando tutte le oportunità socialmente disponibili. La nuova dimensione dell'umano sige uma diversa misura giuridica, che dilata l'ambito de diritti fondamentali della persona" (RODOTÀ, 2012, p. 314 Apud: BIONI, 2019, p. 65). Tradução do autor: Tudo isso, hoje, pode ser pensado também na dimensão dos direitos, de uma construção do indefinido que acaba coincidindo com a própria construção do humano (...) construir livremente a própria identidade aproveitando todas as oportunidades socialmente disponíveis. A nova dimensão do humano requer uma medida jurídica diferente, que amplia o alcance dos direitos fundamentais da pessoa.

portanto, não há um rol taxativo para esses direitos, vez que decorrem da própria condição de pessoa humana.

Por esse entendimento, é evidente a importância dos dados pessoais para o desenvolvimento da personalidade humana, pois funcionam como um instrumento de identificação e de individuação do seu titular. Desta forma, essas informações devem refletir fielmente as características e os anseios do indivíduo a quem elas se referem.

É o que preceitua o art. 6º, inciso V[9] da LGPD (BRASIL, 2018), ao tratar do princípio da qualidade dos dados. Esse princípio exige que os agentes de tratamento, ou seja, aqueles agentes que utilizam os dados com interesses econômicos, garantam que os dados pessoais serão tratados com exatidão, clareza, relevância e atualização.

O princípio da qualidade dos dados autoriza, inclusive, ao titular de dados exigir a retificação de informações incorretas e de processos discriminatórios que tenha sofrido conforme art. 20 da LGPD (BRASIL, 2018). Dessa maneira, atrelado aos princípios da finalidade, adequação, necessidade, livre acesso e transparência, o princípio da qualidade dos dados vigora como autorizador da gestão dos dados pessoais pelo seu titular, garantindo o exercício da autodeterminação informativa.

Por sua vez, a autodeterminação também é um dos fundamentos estabelecidos pela LGPD, em seu art. 2º, inciso II (BRASIL, 2018) e tem por significado a garantia ao indivíduo de poder tomar suas próprias decisões sem interferências externas indesejadas. Esse direito nasce, portanto, como um desdobramento do direito à privacidade, porém visto sob uma nova perspectiva, que não aquela cunhada no final do século XIX, a qual definia a privacidade como o "direito a ficar só". Essa nova perspectiva, encara a privacidade como sendo o direito do indivíduo de ter controle sobre suas próprias informações e liberdade de escolhas existenciais. Nesse sentido, Carlos Nelson Konder (2019) afirma:

> Nessa toada, o direito à privacidade supera o viés individual e passivo do tradicional "direito a ficar só", cunhado no final do século XIX para defender a esfera íntima contra as invasões da imprensa, para assumir novo papel, restabelecendo ao sujeito o controle sobre suas informações: passa-se do domicílio à rede, do sigilo à circulação, da proteção estática à proteção dinâmica, de um poder de exclusão a um poder de controle. Sob essa perspectiva de empoderamento, a privacidade desdobra-se no direito à autodeterminação informativa e no "espaço (inviolável) da liberdade de escolhas existenciais". (KONDER, 2019, p. 262)

[9] V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (BRASIL, 2018, art. 6º, inciso V)

Portanto, por essa nova perspectiva, impedir a intervenção de terceiros na vida privada não é mais suficiente para proteger o titular de dados, é preciso haver atuação direta para conceder a ele o poder de gerência sobre suas informações pessoais e garantir que o indivíduo tenha poder decisório, realizando suas próprias escolhas existenciais.

Em consonância Mulholland (2018) arremata o conceito da privacidade, sob o novo prisma da autodeterminação informativa, em três principais aspectos:

> Seriam, assim três as concepções sobre o direito à privacidade acima apresentadas, quais sejam, (i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial. (MULHOLLAND, 2018, p. 173)

Por conseguinte, como um direito de escolha, a autodeterminação também admite que o indivíduo renuncie a certos direitos para que possa usufruir de outros que lhe convenha. É o que ocorre, por exemplo, quando o indivíduo decide publicar uma foto sua em uma rede social, ou, ao realizar uma compra online, permite que o Google memorize seus dados bancários. Ao fazer essas coisas pretere-se parte da privacidade e da segurança em prol da interatividade e da comodidade.

A princípio, não há problemas ao se realizar tais escolhas, pois trata-se de um desdobramento normal da autodeterminação informativa que elas sejam feitas. Contudo, há de se levado em conta o dever de informar do agente de tratamento de dados, a fim de garantir que o usuário está plenamente consciente das suas escolhas. Nesse aspecto, o uso de sistemas de inteligência artificial, pode gerar algum problema, haja vista a característica de serem capazes atuar sem interferência humana e automaticamente.

Embora se reconheça que os direitos à proteção de dados possam sofrer limitações voluntárias, não se pode admitir, contudo, que o indivíduo disponha de forma genérica ou permanente sobre sua privacidade, imagem, honra, ou qualquer outro direito de sua personalidade, conforme entendimento consagrado no Enunciado nº 4[10] da I Jornada de Direito Civil promovida pelo Conselho de Justiça Federal (FEDERAL, 2012).

Observe-se que a limitação de que trata o enunciado mencionado deve ser temporária e específica, pois é de suma importância que a disposição volitiva acerca de um direito da personalidade seja feita de forma restrita. De fato, os direitos fundamentais – e, portanto, o direito à proteção de dados – podem sofrer limitações, principalmente para permitir o exercício de outro direito fundamental, entretanto deve ser observado que há um núcleo intangível destes

[10] O exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral. (FEDERAL, 2012, p.18, Enunciado nº 4)

direitos, o qual precisa ser preservado, justamente para se proteger a dignidade da pessoa humana.

Há, portanto, uma problemática exposta, pois nem sempre as pessoas possuem plena consciência dos riscos aos quais se expõem na internet ou em qualquer meio digital, desconhecendo a destinação conferida a seus dados, as condições de tratamento dessas informações, ou mesmo que teve suas informações coletadas. Por essa razão, é preciso pensar em soluções que possam criar um ambiente justo e transparente, onde seja realmente possível haver direito de escolha e não somente uma aparência de escolha pelo titular de dados.

Nesse sentido, para resguardar os direitos fundamentais da proteção de dados e da autodeterminação informativa, a LGPD restringiu o tratamento de dados às hipóteses autorizativas previstas em seus artigos 7º e 11 (BRASIL, 2018). Como será melhor visto adiante, tais artigos buscam delimitar as condições em que as operações envolvendo dados poderão ocorrer, privilegiando o consentimento do titular, o interesse social, o interesse do titular de dados e o cumprimento de contratos e obrigações legais.

Contudo, criar uma base legal autorizativa para o tratamento de dados é somente o primeiro passo, pois também é necessário acompanhar se o consentimento do usuário, oferecido no exercício da autodeterminação informativa, está sendo respeitado, além de se garantir a devida reparação e indenização pelos danos causados pelo desrespeito à proteção de dados.

Por essa razão, a LGPD (BRASIL, 2018) elenca, em seu art. 6º um arcabouço principiológico, mediante o qual é possível se interpretar situações complexas que não necessariamente estarão previstas nos artigos 7º e 11 da mesma Lei. Esses princípios são: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A boa-fé, ocupa posição de destaque em relação aos demais princípios, pois foi alocada ao *caput*[11] do art. 6º da LGPD (BRASIL, 2018), enquanto os demais foram enumerados nos incisos. A boa-fé ora citada é aquela objetiva, isto é, quando se pode depreender, pelas condutas e resultados obtidos pelas partes, haver colaboração, lealdade, retidão e probidade durante as relações jurídicas estabelecidas.

O art. 6º, inciso I[12], da LGPD (BRASIL, 2018) prevê o princípio da finalidade, o qual determina que, no momento da coleta, sejam claros os propósitos do tratamento que se pretende

[11] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (BRASIL, 2018, art. 6º)

[12] I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (BRASIL, 2018, art. 6º, inciso I)

dar aos dados pessoais. Portanto tais propósitos precisam ser legítimos, pois não podem fundar-se em atividades ilícitas; específicos, pois não podem ser genéricos a ponto de se autorizar toda e qualquer atividade; e explícitos, pois veda-se a prática de cláusulas dúbias ou obscuras que possam induzir os titulares de dados ao erro.

O princípio da adequação está previsto no art. 6º, inciso II[13], da LGPD (BRASIL, 2018), e complementa o sentido do princípio da finalidade, pois ele consagra justamente a necessidade de haver compatibilidade entre o tratamento e as finalidades informadas, de acordo com o contexto em que ocorra. Assim, o controlador deverá afastar ao máximo aquelas tecnologias, metodologias e protocolos de segurança que possam provocar algum tipo de constrangimento, importunação ou tratamento discriminatório.

O princípio da necessidade, previsto no art. 6º, inciso III[14], da LGPD (BRASIL, 2018), estabelece que os dados colhidos devam ser somente aqueles estritamente imprescindíveis para a persecução do fim almejado com o tratamento. É evidente que esse princípio objetiva preservar a privacidade de seus titulares, e, sobretudo, aplica-se aos dados pessoais sensíveis, pois estes merecem ainda mais cuidado, devido à sua natureza e às preocupações a eles inerentes.

O livre acesso, previsto no art. 6º, inciso IV[15], da LGPD (BRASIL, 2018), é a garantia que deve ser oferecida aos titulares de dados da consulta gratuita e facilitada sobre a forma e a duração do tratamento conferido à integralidade de suas informações pessoais. A forma facilitada de acesso pode ser implementada por meio de canal de atendimento, que pode ser remoto e, se possível, presencial, pois é possível que o titular de dados tenha pouco ou nenhum domínio sobre o uso da tecnologia remota.

O já mencionado princípio da qualidade dos dados, previsto no art. 6º, inciso V da LGPD (BRASIL, 2018), preceitua que, os agentes de tratamento devem garantir que os dados pessoais serão tratados com exatidão, clareza, relevância e atualização. Desta forma, essas informações devem refletir fielmente as características e os anseios do indivíduo a quem elas se referem. Nesse aspecto, o art. 18, inciso III[16] da LGPD (BRASIL, 2018), assegura a possibilidade de se

[13] II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (BRASIL, 2018, art.6º, inciso II)

[14] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (BRASIL, 2018, art.6º, inciso III)

[15] IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (BRASIL, 2018, art.6º, inciso IV)

[16] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] III - correção de dados incompletos, inexatos ou desatualizados; (BRASIL, 2018, art. 18, inciso III)

exigir a correção dos dados, o que deve ser solicitado pelo titular ou seu representante mediante requerimento expresso.

O princípio da transparência, previsto no art. 6º, inciso VI[17], da LGPD (BRASIL, 2018), se correlaciona intimamente com o princípio do livre acesso, pois exige a difusão e efetiva transmissão do conhecimento da informação. A transparência exige que as informações sejam amplamente difundidas, claras, objetivas e não somente disponíveis, mas também compreensível a todos.

A segurança é o princípio elencado no art. 6º, inciso VII[18], da LGPD (BRASIL, 2018), e consiste na utilização de medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão da informação pessoal. Portanto, não se trata somente da segurança contra invasões externas aos sistemas e bancos de dados, mas também há a preocupação com a organização interna das empresas que administram esses dados, pois muitos vazamentos ocorrem por descuido dos administradores.

O princípio da prevenção, estabelecido no art. 6º, inciso VIII[19], da LGPD (BRASIL, 2018), objetiva que as medidas de segurança devem ser adotadas desde o primeiro momento do tratamento de dados. Destacar o princípio da prevenção de forma apartada do princípio da segurança demonstra a preocupação do legislador para que as medidas de segurança sejam adotadas na base de qualquer operação, antes que qualquer dano seja infligido.

O princípio da não discriminação, previsto no art. 6º, inciso IX[20], da LGPD (BRASIL, 2018), veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos. Este princípio orienta o tratamento de dados segundo a isonomia material, de forma a identificar e combater as ações discriminatórias, sejam elas explícitas ou veladas. Esse combate dependerá, por conseguinte, da transparência das empresas, da fiscalização dessas práticas pela ANPD e de estudos estatísticos acerca de práticas potencialmente abusivas, para que se demonstre percentualmente a produção de impactos diferenciados sobre um grupo, em comparação a outros (CORBO, 2017).

---

[17] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (BRASIL, 2018, art.6º, inciso VI)

[18] VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; (BRASIL, 2018, art.6º, inciso VII)

[19] VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (BRASIL, 2018, art. 6º, inciso VIII)

[20] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; (BRASIL, 2018, art. 6º, inciso IX)

Por fim, o princípio da responsabilização, previsto no art. 6º, inciso X[21], da LGPD (BRASIL, 2018), visa a analisar, por meio da exigência de prestação de relatórios e auditorias, a eficiência dos meios utilizados pelos agentes de tratamento de dados para assegurar a proteção de dados pessoais. Seu sentido é ainda complementado com a possibilidade de que sejam exigidos relatórios de impactos dos agentes de tratamento de dados, conforme art. 38[22], da mesma lei (BRASIL, 2018).

É possível observar que os princípios acima possuem o condão de estabelecer diretrizes para o tratamento de dados, que devem ser respeitadas tanto pelos agentes de tratamento, no desempenho de seus negócios, quanto pela ANPD, ao regulamentar as normas técnicas de segurança.

Ademais, conquanto o Capítulo VII (BRASIL, 2018) inteiro da LGPD tenha sido dedicado à segurança e boas práticas, observa-se que os deveres ora elencados são bastante genéricos. Isso ocorre, porque, com o avanço constante da tecnologia, disposições muito específicas se tornariam rapidamente obsoletas, por isso a lei protetiva de dados brasileira somente cuidou das diretrizes gerais de proteção de dados, delegando à ANPD regulamentar os padrões técnicos mínimos de segurança a serem adotados pelos agentes de tratamento de dados, conforme art. 46, §1º[23] (BRASIL, 2018), da lei em comento.

Logo, pode-se concluir que a LGPD, mesmo de forma genérica e abstrata, demonstra a necessidade de se criar mecanismos capazes de rastrear e prevenir a ocorrência de danos, principalmente no tocante aos princípios da transparência, segurança, prevenção e responsabilização e prestação de contas.

Diante disso, é possível inferir que muito do equilíbrio entre o desenvolvimento econômico e tecnológico e a proteção de dados dependerá da capacidade da ANPD de criar mecanismos justos de fiscalização e regulamentação, que deverão levar em conta "a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, em especial no caso de dados pessoais sensíveis" (BRASIL, 2018, art. 46, §1º).

---

[21] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas; (BRASIL, 2018, art. 6º, inciso X)

[22] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. (BRASIL, 2018, art. 38)

[23] Art. 46 [...] § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. (BRASIL, 2018, art. 46, §1º)

A bem da verdade, a legislação protetiva de dados tem o intuito de regulamentar e frear abusos, e não de impedir o progresso e a produção de riquezas. Em um cenário hipotético em que haja excessos regulatórios, poderia ser causado um consequente colapso da economia, e assim não haveria espaço para o livre desenvolvimento da personalidade e poucos recursos para se viver com dignidade e para garantir o exercício da cidadania.

Nesse sentido, Fabio Ulhoa Coelho (2012) ensina o conceito de direito-custo, significando o efeito econômico causado pelas normas de regulamentação na atividade empresarial. Essas normas são, em regra, consideradas pelas sociedades econômicas ao realizar o cálculo final dos preços dos seus produtos e serviços. Nas palavras do referido autor:

> Há normas jurídicas que importam aumento do custo da atividade produtiva. Quando a lei cria um novo direito trabalhista, por exemplo, os empresários alcançados refazem seus cálculos para redefinir o aumento dos custos de seu negócio. Esse aumento de custos implica, quase sempre, aumento dos preços dos produtos ou serviços que o empresário oferece ao consumidor. Conceitua-se 'direito-custo' como as normas dessa categoria. (COELHO, 2012, p. 42)

Assim, a regulamentação deve sempre ser pautada na razoabilidade, buscando equilibrar os direitos individuais com o desenvolvimento econômico e tecnológico. Nesse aspecto, andou bem o legislador, pois muniu a LGPD de diversos dispositivos que levam em consideração a situação fática e o porte dos agentes de tratamento de dados no momento de se atribuir a responsabilidade civil ou administrativa por incidentes.

Em última análise, não se pretende, por meio da regulamentação do uso de dados, criar entraves ao progresso, mas sim evitar que o cidadão seja tolhido de seus direitos em favor de interesses econômicos abusivos e do desenvolvimento tecnológico desenfreado. Portanto, procura-se, no Direito, soluções para que o desenvolvimento econômico e tecnológico ocorra de forma ponderada e responsiva.

2.2 Os riscos do tratamento de dados sensíveis

Para iniciar o debate sobre o tratamento de dados sensíveis e os possíveis riscos inerentes dessa atividade, é preciso, primeiro, compreender o que vem a ser o tratamento de dados, quais são as hipóteses autorizadas para o tratamento e de que forma a LGPD se refere aos dados pessoais sensíveis. Isto porque, como será visto, o tratamento de dados pessoais sensíveis possuem restrições particulares dadas pela lei protetiva de dados.

Deste modo, segundo o art. 5º, inciso X[24], da LGPD (BRASIL, 2018) tratamento de dados se define como sendo toda operação realizada com dados pessoais, cuja coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Fica claro, pois, que o legislador optou por um conceito bastante abrangente de tratamento de dados, provavelmente com o intuito abarcar o máximo de possibilidades possíveis.

Logo, todas essas possibilidades deverão se enquadrar nas hipóteses autorizativas para o tratamento de dados pessoais, dentre as quais, respeitado o consentimento do titular de dados é a principal e mais importante, conforme artigos 7º, inciso I[25], e 11, inciso I[26], da LGPD (BRASIL, 2018). O consentimento de que tratam os referidos incisos deve ser oferecido pelo titular de dados de forma livre, informada e inequívoca e devem ser claras, inclusive, as finalidades que se pretende dar aos dados coletados.

O consentimento do titular é a principal hipótese autorizativa para que seja realizado o tratamento de dados pessoais. Contudo, a LGPD (BRASIL, 2018) também o autoriza, nos casos previstos nos incisos[27] II ao X de seu art. 7º e nas hipóteses de tratamento de dados pessoais sensíveis elencadas no inciso II, alíneas “a” a “g"[28] do art. 11 da mesma Lei.

---

[24] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018, art. 5º, inciso X)

[25] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; (BRASIL, 2018, art. 7º, inciso I)

[26] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; (BRASIL, 2018, art. 11, inciso I)

[27] Art. 7º [...] II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018, art. 7º, incisos II ao X)

[28] Art. 11. [...] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por

É importante verificar que os artigos 7º e 11 da LGPD (BRASIL, 2018) possuem hipóteses que autorizam o tratamento de dados sem a necessidade de consentimento. Sobre essas hipóteses Konder (2019) destaca que estará autorizado o tratamento de dados pessoais, sendo eles sensíveis ou não, quando o tratamento servir:

> ao cumprimento de obrigação legal ou regulatória pelo controlador; ao tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; à realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; ao exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitrário; à proteção da vida ou da incolumidade física do titular ou de terceiro; e à tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias. (KONDER, 2019, p. 264)

Há, ainda, no §3º do art. 11 da LGPD (BRASIL, 2018) a possibilidade de que a ANPD venha vedar ou restringir o compartilhamento de dados pessoais sensíveis entre controladores com o intuito de se obter proveito econômico, além da expressa vedação, no §4º do mesmo artigo, para o tratamento de dados sensíveis, quando referentes à saúde, com o objetivo de se obter vantagem econômica.

> § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir[...] (BRASIL, 2018, art. 11, §§3º e 4º)

Quando se está diante do tratamento de dados sensíveis, que naturalmente vulnerabilizam o seu titular, justifica-se a adoção de um padrão ainda mais rigoroso de proteção. Por isso, o legislador afastou os interesses patrimoniais das hipóteses de dispensa do consentimento no caso dos dados sensíveis (KONDER, 2019, p. 264), apenas se justificando a ausência do consentimento quando relacionada com os interesses dos titulares (BRASIL, 2018, art. 11, inciso II, alíneas "e" e "g"), com o exercício regular de direitos (BRASIL, 2018, art. 11, inciso II, alínea "d"), com o estrito cumprimento do dever legal (BRASIL, 2018, art. 11, inciso

---

profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018, art. 11º, incisos II, alíneas "a" a "g")

II, alíneas “a” e “d”), com a supremacia do interesse público e com a garantia da ordem pública, do contraditório e da ampla defesa (BRASIL, 2018, art. II, alíneas “b”, “c”, “f” e “g”).

Dada a natureza dos dados sensíveis, pode-se inferir que a exploração de tais dados sujeita os seus titulares a uma maior fragilidade, decorrente do risco da discriminação (BIONI, 2019, p.85), capaz de criar disparidades sociais injustificáveis. A LGPD, inclusive, prevê em seu art. 6º, inciso IX (BRASIL, 2018), o princípio da não discriminação, o qual orienta o tratamento de dados segundo a isonomia material, de forma a identificar e combater as ações discriminatórias ilícitas ou abusivas, sejam elas explícitas ou veladas.

Vale ressaltar que a discriminação, concebida como o tratamento de forma injusta ou desigual a uma pessoa ou um grupo de pessoas, por motivos relacionados com suas características pessoais específicas como cor de pele, nível social, religião, sexualidade etc. pode ocorrer de modo individual, mas também pode ocorrer de modo coletivo, como ocorre nas práticas discriminatórias de *geo princing*[29] e *geo blocking*[30], gerando cenários de disparidade econômica e social.

Quanto ao modo em que ocorre, a discriminação pode ser direta ou indireta. Quando direta, prática discriminatória gera um efeito negativo e injustificável para alguém propositalmente, por exemplo, a preterição de um indivíduo para uma vaga de emprego por causa de sua cor da pele. Por sua vez, a discriminação será indireta, quando a prática discriminatória, embora desprovida de intencionalidade, produz impactos desproporcionais a determinadas pessoas ou grupos sociais ao se utilizar de critérios aparentemente neutros, como apontado na ADI 5543/DF (BRASIL, 2020), em que o STF reconheceu a inconstitucionalidade do posicionamento do Ministério da Saúde e da Agência Nacional de Vigilância Sanitária (ANVISA) ao impedir homossexuais de doar sangue.[31]

É notório que as práticas de discriminação direta não ocorrem com a mesma frequência de alguns anos atrás, tendo havido uma mudança de “estratégia” dos agentes de discriminação para prática de discriminações indiretas (CORBO, 2017). Embora ambas as práticas devam ser combatidas com a mesma veemência, a discriminação indireta é mais difícil de ser detectada, dado que ela se encontra na configuração da sociedade, e pode ser reproduzida também no meio digital sem que se perceba.

---

[29] Geoprincig é a prática de modificar a lista básica de preços baseado na localização geográfica do comprador. (WIKIPEDIA, 2020a. tradução do autor)

[30] Geoblocking é a tecnologia que restringe o acesso a um conteúdo da internet baseado na localização geográfica do usuário. WIKIPEDIA, 2020b. tradução do autor)

[31] Nesse sentido, o Ministro Relator Edson Fachin (BRASIL, 2020, p. 27) explica: “há que se diferenciar a discriminação direta – aquela munida de intuito discriminatório – da discriminação indireta – aquela que, desprovida dessa intencionalidade, produz impactos desproporcionais a determinadas pessoas ou grupos sociais.”

Como evidenciado, o tratamento discriminatório perpassa pela intenção do indivíduo, ou mesmo pelas práticas sociais discriminatórias reiteradas e inconscientes. Assim, é possível concluir que há um risco inerente sobre o tratamento de dados pessoais sensíveis, uma vez que não é possível prever ou evitar de forma contundente que lhes sejam dadas destinações discriminatórias.

As consequências do tratamento irregular de dados pessoais sensíveis podem ser desastrosas, posto que, a violação de direitos da personalidade, não acarreta apenas danos materiais, mas também danos morais. Enquanto o dano material é aquela transgressão que afeta o patrimônio de um indivíduo, podendo sempre tal ofensa ser mensurada economicamente, o dano moral se trata de uma lesão injustificável que causa aflição, angústia e/ou desequilíbrio ao bem-estar do ofendido o que o torna muito difícil de ser mensurado economicamente.

Este foi o caso dos usuários da página "Ashley Madison", um site de encontros para pessoas casadas, o qual manteve em seus arquivos tanto os dados de usuários ativos como os de usuários não ativos, tendo, no ano de 2015, seus bancos de dados invadidos e divulgados publicamente (GARCIA, 2015). Nesse caso, a simples associação ao site e a posterior divulgação dos dados pessoais, ainda que comuns, dos usuários, categoriza essas informações como dados sensíveis, pois os prejuízos de tal associação serão muito prováveis.

Desse modo, milhares de casamentos foram desfeitos, pessoas perderam seus empregos e tiveram suas imagens manchadas diante da sociedade, há relatos até mesmo de suicídios por conta do escândalo (O GLOBO, 2015) em relação ao vazamento de dados do site "Ashley Madison". Em situações como essa, não obstante a possibilidade de haver uma condenação que obrigue o ofensor a pagar uma indenização generosa, não é possível sequer mensurar o prejuízo sofrido pelo cidadão, nem tampouco retornar ao estado anterior à lesão.

Considerando a excepcionalidade dos dados sensíveis, é possível se presumir que quando ocorre uma violação às proteções conferidas aos seus titulares, o dano é presumido, isto é, torna-se muito provável que tal fato tenha ocorrido de maneira a causar algum prejuízo considerável ao ofendido. A essa espécie de dano que decorre da dimensão do próprio fato, chama-se dano *in re ipsa*, que nas palavras de Sergio Cavalieri Filho (2012) prescinde da demonstração do dano, apenas sendo necessário provar a ocorrência do fato:

> Se a ofensa é grave e de repercussão, por si só justifica a concessão de uma satisfação de ordem pecuniária ao lesado. Em outras palavras, o dano moral existe in re ipsa; deriva inexoravelmente do próprio fato ofensivo, de tal modo que, provada a ofensa, ipso facto está demonstrado o dano moral à guisa de uma presunção natural, uma presunção *hominis oufacti*, que decorre das regras da experiência comum. Assim, por exemplo, [...]; provado que a vítima teve o seu nome aviltado, ou a sua imagem vilipendiada, nada mais ser-lhe-á exigido provar, [...]; decorre inexoravelmente da

> gravidade do próprio fato ofensivo, de sorte que, provado o fato, provado está o dano moral. (CAVALIERI FILHO, 2012, p. 97)

Cavalieri Filho (2012, p. 89) defende que, estando o ordenamento jurídico voltado a proteger a dignidade da pessoa humana, esta proteção não está restrita àquelas situações em que o ofendido esteja profundamente amargurado pelas ofensas sofridas. Do mesmo modo, pode alguém em estado de coma sofrer danos à sua imagem mesmo não podendo reagir, nítido é que sua dignidade foi maculada independente de sua indignação.

Deveras, o tratamento irregular realizado em virtude de dados pessoais sensíveis não pode ser considerado um mero aborrecimento para o seu titular, mesmo se este não conseguir provar as angústias sofridas. Diferentemente do que ocorre com os dados pessoais comuns, que apenas identificam o indivíduo, a utilização dos dados sensíveis tornam o seu titular um potencial alvo de discriminação.

Nesse sentido, Konder (2019) assevera a especialidade dos dados sensíveis:

> os dados sensíveis são dados pessoais especialmente suscetíveis de utilização para fins discriminatórios, como estigmatização, exclusão ou segregação, de modo que seu tratamento atinja a dignidade de seu titular, lesionando sua identidade pessoal ou privacidade. (KONDER, 2019, p. 263)

Sendo assim, a não observância dos deveres de proteção de dados pessoais sensíveis pode acarretar um dano *in re ipsa*, tendo em vista que o tratamento dessas informações vulnerabiliza os seus titulares, por ter o potencial de atingir a sua dignidade. Como explicado, pode ocorrer até mesmo que o indivíduo sofra sanções sociais em razão deste tratamento, sem sequer tomar consciência de que está sendo vítima de uma discriminação indireta.

Isto posto, é perfeitamente cognoscível a hipótese de que o tratamento de dados pessoais sensíveis realmente carrega um risco inerente da atividade, haja vista as consequências negativas discriminatórias que podem dela surgir. Desse modo, é preciso verificar tão somente se a LGPD comporta a possibilidade de aplicação de um regime de responsabilidade objetiva em razão do risco criado pelo tratamento irregular de dados sensíveis.

2.3 Os riscos do tratamento automatizado de dados

Outra atividade cujo potencial lesivo pode exacerbar a medida do razoável é o tratamento automatizado de dados pessoais. Isto porque, as decisões envolvidas no processo são tomadas por máquinas, sem qualquer intervenção humana, observando apenas a associação de informações concedidas anteriormente, históricos de comportamento e de preferências.

Com base em detalhes como idade, etnia, gênero, patrimônio, origem, religião, posição política etc., o indivíduo é classificado em categorias[32], como se estas informações fossem suficientes para definir um ser humano ou predizer sua capacidade e comportamento diante de determinada situação. No entendimento de Goodman e Flaxman (2017, p. 53), os algoritmos que categorizam e classificam pessoas são inerentemente discriminatórios.

Pode-se citar alguns casos em que o uso de *profiling*[33] gerou constrangimentos aos seus usuários, como o caso da professora Latanya Sweeney, da Universidade de Harvard, que em 2012 percebeu que as pesquisas de alguns nomes afro-americanos no Google resultavam no recebimento de publicidades de empresas que realizavam checagem de antecedentes criminais (NEWS, 2013). Esta mesma empresa, a Google, protagonizou outro caso de racismo, quando classificou pessoas negras como gorilas em seu recurso de buscas por imagem (CRAWFORD, 2016).

É imperioso reconhecer que a técnica de *profiling* pode gerar danos concretos à dignidade da pessoa humana, criando situações em que os dados fornecidos por seus titulares são usados para constrangê-los ou para discriminá-los. Aliás, até mesmo dados que não eram originariamente sensíveis, podem passar a ser entendidos como tais, pois o tratamento discriminatório dessa técnica pode prejudicar, importunar e preterir pessoas em relação a outras.

Outro exemplo de incidentes gerados pelo uso desregulado de processamento automatizado de dados aconteceu em 2016, quando o robô criado pela Microsoft, apelidado de Tay, que deveria interagir e aprender com pessoas no Twitter, em questão de poucas horas, adquiriu tendências neonazistas e declarou repúdio às mulheres integrantes do movimento feminista (VICENTE, 2018).

Do mesmo modo, o uso de inteligência artificial pode usurpar o poder de decisão do usuário, violando a sua autodeterminação informativa. Isso ocorre porque a decisão

---

[32] Nesse sentido, Solove (2006, p.46) citado por Bioni (2019,. p. 89): "We are partially captured by details such as our age, race, gender, net worth, property owned, and so on, but only in a manner that standardizes us into types or categories. Indeed, database marketers frequently classify consumers into certain categories based on stereotypes about their values, lifestyle, and purchasing habits." Tradução do autor: Somos parcialmente capturados por detalhes tais como nossa idade, raça, gênero, patrimônio, propriedades, e assim por diante, mas somente de maneira que nos padroniza em tipos ou categorias. Na verdade, os profissionais de marketing de banco de dados frequentemente classificam os consumidores em certas categorias com base em estereótipos sobre seus valores, estilo de vida e hábitos de compra.

[33] *Profiling* nada mais é do que a criação de categorias de pessoas, que recebem um tratamento diferenciado a depender do grupo em que se enquadram. O Artigo 4º da GDPR dá a seguinte definição para *profiling*: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person." (Tradução do autor: qualquer forma de processamento automático de dados pessoais que consista no uso dos dados pessoais para valorar certos aspectos pessoais relacionados a uma pessoa natural.).

automatizada baseada em históricos de decisões anteriores tomadas pelo próprio usuário, cria um certo determinismo sobre o que essa pessoa irá ver, ouvir e ler.

Exemplos que permitem visualizar tal situação se encontram nas opções de *playlists* aleatórias indicadas por aplicativos como Youtube ou o Spotfy, ou o catálogo de filmes recomendados do Netflix. Nesses casos o indivíduo abdica de parte de sua autonomia para que o algoritmo do aplicativo decida o que ele irá ouvir e assistir.

Abre-se um pequeno parêntese para frisar a importância desses últimos exemplos, que a princípio não parecem oferecer grandes preocupações. Porém, se operados em larga escala, os processos de decisões automatizadas são capazes de criar padrões comportamentais replicados em massa na sociedade, fenômeno que Eli Pariser (2012, p. 132), citado por Bioni (2019, p.91), chamou de efeito bolha[34]. Desta forma, os grupos sociais se estratificam, e os indivíduos deixam cada vez mais de ter contato com opiniões e culturas diferentes.

O efeito bolha faz com que as pessoas se tornem intolerantes com quem não faz parte de sua 'bolha', de forma que todo e qualquer desentendimento é resolvido com um simples *click*, capaz de finalizar uma amizade, como acontece no *facebook*, no *instagram*, no *telegram*, no *whatsapp* e etc.

Por conseguinte, é salutar que os processos automatizados de tomadas de decisão sejam submetidos a constante vigilância, vez que estes processos influenciam de forma silenciosa a vida das pessoas e constituem riscos ao pleno exercício da autonomia informativa. A diversidade cultural e de opiniões é condição sem a qual não seria possível o livre desenvolvimento da personalidade humana.

Para se começar a pensar em soluções para esses problemas, é preciso compreender primeiro a linguagem por trás do processo automatizado de tomada de decisão, pois atualmente, quase todo tipo de máquina como computadores, tablets, celulares etc. são programadas por meio de algoritmos.

Embora outrora tenham sido utilizados por matemáticos para solucionar equações complexas, os algoritmos, como entendidos hoje, são códigos linguísticos elaborados para dar instruções aos computadores modernos (FARIAS; MEDEIROS, 2013, p. 54), a fim de que se chegue a um resultado lógico mediante um estímulo inicial, ou melhor, um *input*.

---

[34] "Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes, ocasionais e fortuitas, que escapariam dessa catalogação." (BIONI, 2019, p. 91)

Os algoritmos são, portanto, uma sequência finita de ações executáveis e que visam a obter uma solução para um determinado tipo de problema (ZIVIANI, 2011, p.1). Esse conceito foi cunhado originalmente pelo engenheiro Alan Turing, em 1936, para quem algoritmos são "um conjunto não ambíguo e ordenado de passos executáveis que definem um processo finito" (FARIAS; MEDEIROS, 2013, p.58).

A evolução da programação permitiu que estes códigos se tornassem muito eficientes na obtenção de resultados lógicos, o que, associado ao avanço da engenharia da computação e ao desenvolvimento de poderosos computadores, permitiu a criação de algoritmos tão arrojados que são capazes de aprender e reproduzir o comportamento humano[35]. A essa tecnologia chamou-se de *machine learning* (ou aprendizado de máquina).

O grande diferencial do *machine learning* está no fato de que ele permite que as máquinas sejam capazes de acumular "experiências" próprias e de aprender com elas de forma espontânea, como um autodidata (PIRES; SILVA, 2017, p. 242). Com essa nova tecnologia é possível que um programa de computador aprenda as tendências mercadológicas, os padrões de consumo, os perfis de usuários, os perfis de colaboradores de alguma empresa e, inclusive, os preconceitos já enraizados na sociedade, para tomar decisões objetivas com base em seu aprendizado.

Há ainda outra tecnologia muito importante chamada *deep leaning*, na qual, por meio do aprendizado de máquina, os programas de computador tornam-se capazes de programarem a si mesmos (KNIGHT, 2017), produzindo resultados inalcançáveis e imprevisíveis pelos seres humanos. Essa tecnologia faz jus ao termo "inteligência artificial", pois com ela é possível que o os computadores executem tarefas sobre as quais os seus criadores não possuem expertise alguma.

Em matéria do site MIT Technology Review (KNIGHT, 2017), o líder de um grupo de pesquisas sobre o uso de inteligência artificial em hospitais, Joel Dudley, admite à página que embora seu grupo tenha desenvolvido um programa de diagnose para doenças psicológicas, não sabiam mais como ele funcionava, pois ele já era capaz de diagnosticar, sem auxílio humano, distúrbios psicológicos complexos como a esquizofrenia.

[35] Nesse sentido, Goodman e Flaxman (2017. p.53) conceituam: "machine learning depends upon data that has been collected from society, and to the extent that society contains inequality, exclusion, or other traces of discrimination, so too will the data". (Tradução do autor: "o aprendizado de máquina depende dos dados coletadas da sociedade, e à medida que a sociedade contém desigualdade, exclusão o outros traços de discriminação, então também terão os dados"). Em consonância, Marrafon e Medon (2019): "Entretanto, o que tem se visto é que, em verdade, a neutralidade é aparente: as máquinas herdam o conteúdo a que possuem contato, seja por carregamento inicial de programadores, seja por aprendizado na interação humana, inclusive o preconceito."

É por essa razão que o termo *blackbox*, utilizado para qualificar essa nova tecnologia, se difundiu tanto nos últimos anos, pois ele denota a imprevisibilidade das ações das máquinas, dado que nem mesmo os seus programadores conseguem conjecturar os resultados.

Talvez por esses motivos, a GDPR tenha abordado a questão do tratamento automatizado de dados de maneira restritiva, tendo o admitido apenas quando houver consentimento do titular de dados ou nas previsões legais abaixo descritas, conforme tradução do texto legal europeu:

> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
> 2. O nº 1 não se aplica se a decisão:
> a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
> b) quando autorizado por Lei da União ou Estado Membro, com o intuito de salvaguardar os interesses legítimos e liberdades do titular de dados.
> c) quando baseado no explícito consentimento do titular de dados. (EUROPEIA, 2016, p. 119/46)

O §2º do art. 22º da GDPR (EUROPEIA, 2016) explica, ainda, que o tratamento automatizado proveniente das hipóteses "a" e "c", obrigam o Controlador a implementar medidas adequadas para salvaguardar os direitos do titular de dados, minimamente garantindo ao internauta o direito de obter a intervenção humana para revisar as decisões tomadas pelos sistemas do Controlador, a fim de permitir ao titular dos dados expressar seu ponto de vista ou contestar a decisão.

Nesse aspecto, andou mal o atual Presidente da República Federativa do Brasil, ao vetar parte do art. 20 da LGPD (BRASIL, 2018), a qual conferia ao titular de dados tal direito à revisão humana. Na atual redação, em razão da retirada da expressão "por pessoa natural" do texto original, as decisões tomadas por máquinas poderão ser revisadas por outras máquinas, gerando insegurança jurídica a respeito do funcionamento e eficácia de tais revisões.

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL, 2018, Lei nº 13.709, art. 20)

Apesar do veto, ainda prevalece a previsão da revisão das decisões automatizadas, e, portanto, a possibilidade de o ofendido defender-se contra abusos sofridos, posto que o direito de revisão envolve também o direito a oposição, contestação e explicação a respeito desse tratamento.

Além disso, não necessariamente estará impossibilitada a revisão humana, uma vez que a alteração do artigo em comento não a proibiu, apenas lhe desprestigiou. Certamente, como a história mostra, a *práxis* adotada pelos agentes de tratamento será aquela menos custosa para a produção, ou seja, optarão pela revisão por máquina.

Porém é bem provável que os juízes e órgãos de fiscalização reconheçam a obscuridade dos algoritmos e a disparidade técnica do usuário em relação aos controladores e operadores. Assim, por meio da construção jurisprudencial e de regulamentação dada pela ANPD, é possível que sejam determinadas revisões humanas de algoritmos nos casos concretos.

No que diz respeito a configuração do dano *in re ipsa* sobre o tratamento automatizado de dados, o Superior Tribunal de Justiça (STJ) se manifestou no Recurso Especial nº 1419697/RS, sob relatoria do Ministro Paulo de Tarso Sanseverino, para não reconhecê-lo, quando se pronunciou sobre os sistemas de *credit scoring*:

> RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL.
> I – TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito).2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. 4) **Apesar de desnecessário o consentimento do consumidor consultado**, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. 5) **O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011),** bem como **nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.**
> II – CASO CONCRETO:
> 1) Não conhecimento do agravo regimental e dos embargos declaratórios interpostos no curso do processamento do presente recurso representativo de controvérsia; 2) Inocorrência de violação ao art. 535, II, do CPC. 3) Não reconhecimento de ofensa ao art. 267, VI, e ao art. 333, II, do CPC. 4) **Acolhimento da alegação de inocorrência de dano moral "in re ipsa".** 5) **Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie.** 6) Demanda indenizatória improcedente.
> III – NÃO CONHECIMENTO DO AGRAVO REGIMENTAL E DOS EMBARGOS DECLARATÓRIOS, E RECURSO ESPECIAL PARCIALMENTE PROVIDO." (BRASIL, 2014, *on-line*)

No caso em tela, o que se discute é a incidência de danos causados pelo sistema de *credit scoring*, que, nas palavras do Ministro Relator, trata-se de "um sistema de pontuação do risco de concessão de crédito a determinado consumidor". Ou seja, trata-se de um sistema automático que, por meio de estatísticas comportamentais, apura a probabilidade de inadimplência de um determinado consumidor.

O STJ entendeu que não houve o dano moral, pois, a autoria não comprovou efetivamente nenhuma negativa de crédito por conta de seu cadastro não autorizado no sistema. Além disso, por não ter havido comprovada utilização de informações excessivas ou sensíveis, também não teria havido infração à Lei 12.414/2011 (Lei do Cadastro Positivo). O posicionamento do STJ leva a crer que, em casos similares, deve haver comprovação de dano, ou seja, qualquer implicação negativa que decorra do cadastro.

Não obstante, haveria de se questionar a possibilidade de revisão do processo automático que conferiu a baixa pontuação no sistema de *credit scoring* à autora. É preciso verificar se os critérios adotados pelo sistema não foram abusivos ou preconceituosos e, neste caso, seria inválida a negativa de crédito efetivada, a prática seria considerada abusiva e seria configurado um dano ao titular de dados decorrente da discriminação e não necessariamente do tratamento automatizado em si.

Portanto, embora o cadastro positivo esteja autorizado, ainda terá de demonstrar transparência que permita o contraditório ao consumidor. Pois do contrário, nas palavras do Exmo. Desembargador Alexandre Morais da Rosa, relator da decisão reformada pelo STJ, o *Concentre Scoring*, "avilta a vulnerabilidade jurídica e de informação do consumidor" e "ofende o Estado Democrático de Direito" (SANTA CATARINA, TJSC, 2013, *on-line*).

Nessa toada, a transparência, princípio elencado no art. 6º, inciso VI, da LGPD (BRASIL, 2018), ganha papel de destaque para tentar frear os atos lesivos provenientes do tratamento automatizado de dados. A transparência exige que as informações sejam amplamente difundidas, sejam claras, objetivas e não somente disponíveis, mas também compreensível a todos.

A transparência deve estar presente em todo o "ciclo de vida" dos dados pessoais dentro da empresa, desde o momento em que são captados e armazenados, até quando são divulgados. Logicamente, para cumprir tais exigências, as empresas precisarão mapear todo esse processo de maneira detalhada e documentada.

Em matéria do site da PriceWaterhouseCoopers Brasil (PwC Brasil), uma das maiores empresas de auditoria do mundo, os sócios de Cibersegurança desta empresa asseveram que:

> O primeiro passo para adequação é realizar um mapeamento detalhado dos dados pessoais tratados e o seu ciclo de vida. Saber onde estão, como estão armazenados, quem tem acesso, se os dados são compartilhados com terceiros no Brasil ou exterior e quais riscos associados ao ciclo de vida, são algumas perguntas essenciais que todas as organizações devem responder antes estabelecer o programa de implementação. (D'ANDREA; BATISTA; JURICIC, 2020)

Sob o mesmo raciocínio, Ana Frazão (2019, pp. 512-518), ao defender a responsabilidade subjetiva dos administradores de sistemas automatizados, recomenda a adoção de diversos critérios de segurança, que visam a dirimir os riscos do tratamento automatizado de dados, seguindo o Guia divulgado pela Comissão Europeia em 2017, as Diretrizes Éticas para a Inteligência Artificial Confiável:

> o Guia está também alicerçado em sete exigências, que devem ser avaliadas continuamente ao longo de todo o ciclo de vida do sistema de inteligência artificial: (i) *human agency* e supervisão humana, (ii) robustez técnica e segurança, (iii) privacidade e governança de dados, (iv) transparência, (v) diversidade, não discriminação e justiça, (vi) bem-estar e ambiental e social e (vii) *accountability* (FRAZÃO, 2019, p. 513-514)

Pela exigência de *human agency* requer-se a possibilidade de contínua supervisão humana desde a concepção dos programas de computador, até o seu acompanhamento por meio de *feedbacks* externos acerca de falhas ou mal funcionamentos. Esse conceito se comunica, inclusive, com a lógica de *privacy by design*, que representa a adoção de medidas de proteção de dados desde a concepção dos algoritmos. (FRAZÃO, 2019, p. 514)

A robustez técnica é exigida no sentido de se garantir a previsibilidade do comportamento dos programas algorítmicos, a fim de se minimizar os danos não esperados. Isto gera no usuário a confiança de que serão reproduzidos os mesmos comportamentos pela máquina, quando submetida às mesmas condições.(FRAZÃO, 2019, p. 515)

A governança de dados é uma exigência que ressalta a manutenção da qualidade e a integridade dos dados, e conversa diretamente com a exigência de transparência, pois sem a governança não é possível rastrear os dados, explicar o tratamento e comunicar ao usuário sobre seus interesses. Assim, a transparência exige que os processos de tomada de decisão sejam muito bem documentados. (FRAZÃO, 2019, p. 515)

A exigência da diversidade, não discriminação e justiça, requer que os programas de computadores sejam supervisionados para garantir que não estão adotando vieses discriminatórios, seja na fase de concepção, ou na fase de funcionamento, intencionalmente ou não. Também exige a promoção de inclusão e diversidade, ressaltando a importância de se ouvir a opinião de todos os usuários, pois a inteligência artificial deve ser utilizada para promover o bem-estar social.(FRAZÃO, 2019, p. 516)

Por fim, a exigência de *accoutability*[36] ressalta a importância de que as empresas promovam auditorias, a fim de que sejam avaliados os seus processos de tomada de decisão, os códigos algorítmicos e a sua capacidade de identificar, avaliar, documentar e minimizar os potenciais impactos negativos de seus sistemas. (FRAZÃO, pp. 516-517)

Esses deveres comungam com a ideia de transparência, responsabilização e prestação de contas trazidas pela LGPD, mas, por outro lado, essa Lei também demonstra a necessidade de se resguardar o segredo comercial e industrial, conforme se vê em seu art. 6º, inciso VI (BRASIL, 2018). De toda forma, é imprescindível que seja possível a revisão das decisões tomadas de forma automática e que sejam feitos relatórios periódicos e completos sobre o fluxo de dados e processos de tomadas de decisão.

Portanto, é razoável se concluir que o tratamento automatizado de dados pode ser considerado uma atividade cujos riscos são adquiridos quando os responsáveis pelo seu desenvolvimento não consideram a segurança e a privacidade como padrão de configuração em todas as fases do processo. Outrossim, deve-se reconhecer que, a despeito de haver um potencial lesivo no trato automatizado de dados, a própria LGPD demonstra ser possível dirimir esses riscos mediante a adoção de critérios que promovam a transparência e a prestação de contas, como será visto no capítulo adiante.

[36] "Accountability é um termo da língua inglesa que pode ser traduzido para o português como responsabilidade com ética e remete à obrigação, à transparência, de membros de um órgão administrativo ou representativo de prestar contas a instâncias controladoras ou a seus representados." (WIKIPEDIA, 2020c)

3 O REGIME DE RESPONSABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS

O Direito brasileiro classificou a responsabilidade civil em objetiva ou subjetiva. Na responsabilidade subjetiva a análise do elemento culpa *latu sensu* é primordial para que se possa configurar o dever de reparação. Assim, se o infrator não tiver agido com dolo ou culpa *strico sensu*, que se manifesta como erro, negligência, imprudência ou imperícia, não há que se falar em responsabilidade civil.

Já na responsabilidade objetiva o elemento culpa não será levado em conta, tão somente precisando existir um resultado lesivo para ensejar a responsabilização, sendo irrelevante qual tenha sido a intenção do agente. Este instituto, notoriamente mais severo, visa a garantir que um indivíduo em situação desfavorável em relação ao seu ofensor seja elevado à paridade.

A regra da responsabilidade civil adotada pelo direito brasileiro, no art. 186[37] do CC/2002 (BRASIL, 2002), é a responsabilidade subjetiva, dado que não se pode penalizar alguém sem que se tenha faltado com o dever de cautela em seu agir (CAVALIERI FILHO, 2012, p. 17). Entretanto, em algumas ocasiões, quando a comprovação da culpa se torna muito onerosa para a vítima ou quando o resultado lesivo já é esperado, o ordenamento jurídico admite a incidência da responsabilidade objetiva, podendo estar expressamente designada em lei ou ser invocada em razão da natureza das atividades.

A LGPD, todavia, não deixou explícito qual seria o regime de responsabilidade adotado como regra na seara da regulação de dados, apenas prevendo o dever de reparação em razão do dano causado no desenlace da atividade de tratamento de dados pessoais: “art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.” (BRASIL, 2018, art. 42).

Por essa razão, é conveniente buscar na jurisprudência como se tem entendido a questão da responsabilização pela proteção de dados no direito brasileiro até então, isso com o intuito de se encontrar parâmetros comparativos e para verificar uma possível inclinação de entendimento.

Observa-se que a jurisprudência atual é bastante consolidada em determinar o dano *in re ipsa* quando alguém tem seu nome inscrito indevidamente em cadastro de inadimplentes,

[37] Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. (BRASIL, 2002, art. 186)

conforme entendimento do STJ no Recurso Especial 718618/RS 2005 e no Agravo ao Recurso Especial nº 1379761/SP 2011:

> EMENTA: RESPONSABILIDADE CIVIL. DANO MORAL. REGISTRO NO CADASTRO DE DEVEDORES DO SERASA. EXISTÊNCIA DE OUTROS REGISTROS. INDENIZAÇÃO. POSSIBILIDADE. **A existência de registros de outros débitos do recorrente em órgãos de restrição de crédito não afasta a presunção de existência do dano moral, que decorre in re ipsa, vale dizer, do próprio registro de fato inexistente.** Precedente. Hipótese em que o próprio recorrido reconheceu o erro em negativar o nome do recorrente. Recurso a que se dá provimento. (BRASIL, 2005, *on-line*, grifos do autor).

> EMENTA: AGRAVO REGIMENTAL NO AGRAVO DE INSTRUMENTO. RESPONSABILIDADE CIVIL. INSCRIÇÃO INDEVIDA EM ÓRGÃOS DE PROTEÇÃO AO CRÉDITO. DÍVIDA ORIUNDA DE LANÇAMENTO DE ENCARGOS EM CONTA CORRENTE INATIVA. DANO MORAL.
> VALOR DA CONDENAÇÃO. 1. Inviável rever a conclusão a que chegou o Tribunal a quo, a respeito da existência de dano moral indenizável, em face do óbice da Súmula 7/STJ. 2**. É consolidado nesta Corte Superior de Justiça o entendimento de que a inscrição ou a manutenção indevida em cadastro de inadimplentes gera, por si só, o dever de indenizar e constitui dano moral in re ipsa, ou seja, dano vinculado a própria existência do fato ilícito, cujos resultados são presumidos.** 3. A quantia fixada não se revela excessiva, considerando-se os parâmetros adotados por este Tribunal Superior em casos de indenização decorrente de inscrição indevida em órgãos de proteção ao crédito. Precedentes. 4. Agravo regimental a que se nega provimento. (BRASIL, 2011, *on-line*, grifos do autor)

Esse entendimento foi construído devido à dimensão das consequências da inclusão indevida de alguém em cadastro de inadimplente, posto que presumem-se os danos à dignidade da pessoa humana, tanto em sua honra subjetiva, quanto objetiva, perante a sociedade. Cabe ressaltar que a associação do nome de alguém a um cadastro de inadimplentes, torna essa informação um dado sensível, deduzível pelo contexto de repercussões negativas às quais seu titular é submetido.

Do mesmo modo, percebe-se que a Corte Especial já reconheceu no REsp nº 1758799/MG (BRASIL, 2019), inclusive, o dano *in re ipsa* pela violação de deveres legais quanto a proteção de dados pessoais com base no CDC:

> EMENTA: RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a

> Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. **5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.** 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus artigos 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais **9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa.** 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. (BRASIL, 2019, *on-line*, grifos do autor)

A Ministra Nancy Andrighi reconheceu, com base no Marco Civil da Internet e no CDC, o dano *in re ipsa* nos casos em que o gestor do banco não comunica o titular das informações sobre o uso desses dados pessoais. Afirmou, ainda, em suas razões, que, na hipótese do compartilhamento das informações sem a prévia comunicação – como ocorreu no caso analisado –, o dano moral é presumido, sendo desnecessário ao consumidor comprovar prejuízo.

A Ministra também aduziu o caráter pecuniário das informações no atual mercado de consumo, e, por isso, a manutenção de bancos de dados constitui serviço de grande utilidade, seja para o fornecedor, seja para o consumidor, mas, ao mesmo tempo, afigura-se como atividade potencialmente ofensiva aos direitos do consumidor.

Não obstante o referido julgamento tenha se baseado na esfera do direito do consumidor e, por isso, não permita estender seus efeitos aos demais ramos do direito, é possível se

averiguar a excepcionalidade com que a Excelentíssima Ministra trata dos dados sensíveis no trecho abaixo de sua decisão.

> O fato, por si só, de se tratar de dados usualmente fornecidos pelos próprios consumidores, quando da realização de qualquer compra no comércio, **que não se afiguram como os chamados dados sensíveis ou sigilosos**, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado (STJ, 2019, *on-line*, grifos do autor)

Portanto, o reconhecimento do dano *in re ipsa*, ou seja, a desnecessidade de dilação probatória em relação a existência do dano, demonstra que a Corte Especial já circula a tese da fragilidade do titular de dados em relação ao tratamento de dados na esfera do consumidor. Além disso, também se trata com certo grau de excepcionalidade o tratamento de dados sensíveis.

Nesse diapasão, percebe-se que a LGPD, em relação ao tratamento de dados sob o direito do consumidor, concorda com a jurisprudência atual, bastando analisar o teor do seu art. 45: "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente." (BRASIL, 2018, art. 45)

Tal previsão legal faz referência clara ao CDC, o que significa dizer que, nestas hipóteses, os agentes de tratamento de dados passam a ser equiparados à figura do fornecedor. Portanto, os agentes não poderão escusar-se da reparação do dano que vierem a causar, seja pelo produto fornecido ou pelo serviço prestado, pois, em consonância com os artigos 12 e 14 da Lei 8.078/1990 (BRASIL, 1990), não haverá o exame da culpa nestes casos:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. (BRASIL, 1990, artigos 12 e 14)

Como se observa nesses casos, a responsabilização objetiva do agente de tratamento de dados decorre diretamente da aplicação do CDC, o qual tem por objetivo promover a proteção do consumidor dos abusos e desmandos das empresas. Considerando a disparidade de poder econômico e de conhecimento técnico entre as empresas e os consumidores, funda-se a

responsabilidade objetiva em razão da dificuldade de produção de provas encontrada pelo consumidor e no risco inerente da atividade desenvolvida pelas empresas.

Para Mendes e Doneda (2018, p. 477), a teoria do risco se aplicaria para o tratamento de dados de maneira geral, pois, para estes autores, a LGPD leva em conta os riscos intrínsecos dessa atividade. Por esse raciocínio, a legislação restringe o tratamento de dados apenas às hipóteses estritamente úteis e necessárias, sendo certo que até mesmo essas podem ser limitadas quando verificados riscos aos direitos e liberdades do titular de dados.

De fato, a LGPD (BRASIL, 2018) procura restringir o tratamento de dados unicamente a uma base legal definida por ela, em seus artigos 7º e 11, exigindo que apenas seja utilizado o mínimo necessário de informações – art. 6º, inciso III, da LGPD –, unicamente através dos meios adequados – art. 6º, inciso II, da LGPD – para atingir a finalidade do tratamento pretendida – art. 6º, inciso I, da LGPD.

Somado a esse entendimento, a exigência de eliminação dos dados ao término do tratamento, prevista no art. 16[38] da LGPD (BRASIL, 2018), levam Mendes e Doneda (2018) a concluírem que a responsabilidade sobre o tratamento de dados é objetiva:

> a Lei procura minimizar as hipóteses de tratamento àquelas que sejam, em um sentido geral, úteis e necessárias, e que mesmo estas possam ser limitadas quando da verificação de risco aos direitos e liberdades do titular de dados. Trata-se, dessa forma, de uma regulação que tem como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares.
> Assim justifica-se o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais. (MENDES; DONEDA, 2018, p. 477)

Em sintonia com esta corrente, Caitlin Mulholland (2020) justifica a responsabilidade objetiva pelo tratamento irregular de dados pessoais em razão teoria do risco inerente do tratamento de dados. Para essa autora, os riscos dessa atividade podem ferir os direitos fundamentais difusos, o que por si só já justificaria a adoção da responsabilidade civil objetiva.

De maneira diferente, mas ainda defendendo a responsabilização objetiva no caso de tratamento irregular de dados, Dresch e Stein (2020) defendem uma teoria de responsabilidade objetiva especial, que decorre do cometimento de um ilícito, qual seja, o não cumprimento de deveres impostos pela legislação de proteção de dados, em especial, o dever geral de prover a "segurança que o titular dele pode esperar", previsto no art. 44, da LGPD (BRASIL, 2018).

[38] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (BRASIL, 2018, art. 16)

Para Dresch e Stein (2020), é crucial haver o cometimento dos ilícitos previstos nos artigos 42 e 44 da LGPD (BRASIL, 2018), e, não obstante haver a necessidade de se averiguar a análise externa de práticas do agente de tratamento de dados, defendem que tal análise não passa pelo crivo da intenção ou falta de cuidado do sujeito, caracterizada pela negligência, imprudência ou imperícia. Trata-se de uma análise tão somente da conduta do agente de tratamento de dados de forma objetiva, com o intuito de se perquirir o cumprimento ou não do padrão de conduta imposto, ou melhor, utilizando as palavras dos autores, o cumprimento de "standards" técnicos de mercado e regulatório.

Contudo, entende-se que essa teoria reforça, na verdade, a ideia de subjetividade, haja a vista a evidente necessidade de se comprovar o cumprimento de deveres por parte dos controladores e operadores de dados. Ademais, é notório que o legislador elencou uma série de critérios subjetivos, que dizem respeito às condições fáticas e às características dos agentes de tratamento, quando da análise da violação à proteção de dados.

Observa-se, por exemplo, as expressões "segurança que o titular dele pode esperar" e "técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.", ambas previstas no art. 44, *caput* e inciso III, da LGPD (BRASIL, 2018), respectivamente.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a **segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais **disponíveis à época em que foi realizado**. (BRASIL, 2018, art. 44, incisos I ao III, grifos do autor)

Tais expressões demonstram juízos de razoabilidade trazidos pela Lei, os quais possuem o condão de resguardar a defesa do desenvolvimento econômico e tecnológico e a inovação, valores consagrados como fundamentos da proteção de dados pessoais pelo art. 2º, inciso V, da LGPD (BRASIL, 2018). Logo, a desnecessidade de comprovação de culpa contraria esses valores, pois isso geraria um rigor exacerbado da regulação e poderia inibir as atividades voltadas ao progresso e ao desenvolvimento.

De fato, como se infere do artigo em comento, nenhum sistema de segurança é impenetrável, de maneira que agentes mal intencionados sempre encontrarão alguma forma de burlá-los. Reconhecendo essa realidade, o art. 44º, inciso III (BRASIL, 2018), mencionado acima, foi oportuno ao garantir que a lei não poderá exigir do agente de tratamento de dados esforços além daqueles disponíveis à época do fato danoso.

Na mesma medida, o art. 46, *caput*, da LGPD (BRASIL, 2018), utiliza-se de termos extremamente abertos ao se referir aos deveres de adoção de segurança para proteção de dados:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018, art. 46)

Em decorrência dessa previsão, o agente de tratamento de dados poderia arguir ter cumprido todas as medidas aptas a proteger os dados pessoais, inobstante ter ocorrido algum dano a terceiros. A vagueza dos termos utilizados leva à possibilidade interpretativa ampla, o que aumenta as chances de análise de culpa.

Sobre o artigo em comento, Bioni e Dias (2020, p. 7) defendem um regime subjetivo de responsabilidade, pois, para os autores, quando a LGPD dispõe sobre a necessidade de violação à segurança dos dados para que seja deflagrada a responsabilidade, se está a afastar o sistema de responsabilidade objetiva.

Ainda sob esse raciocínio, o art. 12, §1º da LGPD (BRASIL, 2018), ao se referir ao processo de anonimização de dados, salienta que os dados não serão considerados anonimizados a depender do tempo, custos e esforços necessários para que se tenha êxito em reverter a medida de segurança.

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. (BRASIL, 2018, art. 12, *caput* e §1º)

É possível compreender, pela leitura do artigo, que a LGPD admite a possibilidade de que sistemas de segurança venham a ser violados, sem que, contudo, o agente de tratamento seja punido penalizado pela não anonimização de dados. Tal punição dependerá, não obstante, do esforço empregado por esse agente em garantir a anonimização, de forma que não seja qualquer investida capaz de burlar o processo, mas somente aquelas consideradas extraordinárias.

Ainda por esse ângulo, a LGPD, ao destacar as competências da ANPD, também reforça a ideia de subjetividade na análise da culpa dos agentes de tratamento. Basta observar a diferenciação de tratamento prevista no art. 55-J, incisos VIII e XVIII (BRASIL, 2018), a depender do porte e das especificidades das atividades das empresas:

> VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, **os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis**; [...]

> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, **para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação**, possam adequar-se a esta Lei; (BRASIL, 2018, art. 55-J, incisos VIII e XVIII, grifos do autor)

O que se está a dizer nos referidos incisos é que não seria razoável exigir o mesmo nível de segurança de uma empresa multinacional, no tratamento de dados sensíveis de seus clientes, como o de uma empresa de pequeno porte, que apenas coleta o primeiro nome e o endereço de seus clientes quando estes optam por um serviço de entrega, por exemplo.

Outro indício de que a responsabilidade se apresenta, em regra, subjetiva na LGPD é a previsão do art. 43, inciso II desta Lei, que possui seguinte teor: "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: [...] II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (BRASIL, 2018, art. 43, *caput* e inciso II).

Esta previsão isenta o agente de tratamento de dados de culpa nos casos em que este puder provar sua estrita observância às leis de proteção de dados, em que se presume estarem incluídas a CRFB/1988, o CDC, o Marco Civil da Internet e outras legislações que vierem a ser editadas sobre o tema de proteção de dados, não se esgotando na LGPD.

Sobre o artigo em comento, Gisela Sampaio Guedes, no I Simpósio de Responsabilidade Civil e Proteção de Dados realizado pelo Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC, realizado em 2020 (GUEDES, 2020), defendeu a adoção da culpa presumida pela LGPD, tendo em vista o uso da expressão "só não serão responsabilizados", a qual denota que a culpa seria a regra, mas que podem ser aplicadas as exceções previstas nos incisos daquele artigo.

A culpa presumida é uma forma de se inverter o ônus da prova (FARIAS; NETTO; ROSENVALD, 2018, p. 916), pois quem deverá provar não ter agido com dolo, negligência ou imperícia será o infrator e não a vítima. Portanto, essa teoria se diferencia da responsabilidade objetiva, pois admite prova em contrário por parte de quem realizou a conduta lesiva, e, para Braga Netto, Farias e Rosenvald, trata-se de uma fase intermediária entre as duas teorias:

> a teoria da presunção de culpa se insere na teoria subjetiva, com o mérito de construir uma fase intermediária de evolução entre aquela e a teoria objetiva (a teoria do risco, por exemplo, na Itália, é hipótese de responsabilidade civil por culpa presumida, não é objetiva). (FARIAS; NETTO; ROSENVALD, 2018, p. 917)

Em defesa do regime subjetivo de responsabilidade, Guedes e Meireles (2019, p.123) argumentam que a retirada da referência expressa de responsabilidade objetiva do projeto de lei da LGPD; a existência de um capítulo dedicado à "segurança e boas práticas", responsável por

criar um *"standard"* de condutas a serem seguidas pelos agentes de tratamento; e o art. 43, inciso II, da LGPD (BRASIL, 2018), o qual prevê a isenção da responsabilidade caso haja prova do cumprimento das leis de proteção de dados, seriam verdadeiras "pistas" do regime subjetivo de responsabilidade.

Guedes e Meireles (2019, p. 122) argumentam que não faria sentido lógico ou jurídico a LGPD prever tantos deveres de cuidado para, no fim, não ser aplicado um regime de responsabilidade subjetiva e, além do mais, punir-se os agentes mesmo que tenham zelado por cada um desses deveres. Concluem, outrossim, que para a lógica da responsabilidade objetiva não cabe a discussão de cumprimento de deveres.

Dadas tais circunstâncias, a consequência lógica da responsabilização subjetiva, conferida pela LGPD, é que o fator probatório ganha grande relevância para se auferir a culpabilidade dos agentes de tratamento. Essa questão é reforçada pelo princípio da LGPD da responsabilização e prestação de contas, que nitidamente traz um dever de *accountability*.

Ou seja, os controladores e operadores de dados deverão manter regras de *compliance* e governança efetivas, capazes de mapear riscos e criar planos de ação para conter impactos à proteção de dados, sendo facultado à ANPD criar os padrões de segurança mínimos exigíveis e requerer relatórios de impacto aos controladores de dados.

Pelos motivos expostos, acredita-se que realmente a responsabilidade objetiva não foi adotada como padrão no âmbito da regulação da exploração de dados no Brasil. Nesse sentido, Bioni e Dias (2020, p.4), arrematam a ideia central da presente exposição, pois para esses autores, a LGPD, ao qualificar intensamente as obrigações dos agentes de tratamento de dados, e ao traçar de forma vaga os parâmetros normativos para mensurar a reprovabilidade de uma conduta danosa, deixa uma margem interpretativa para que a culpa exerça um papel importante nessa seara.

Entretanto, a regra da subjetividade pode comportar exceções, pois, como antes elucidado, algumas atividades no convívio humano podem ser mais ameaçadoras que outras. Nesse sentido, aliás, Bioni e Dias (2020) asseveram que há, na LGPD, margem para o encaixe de exceções ao regime subjetivo,

> a (in)evolução do texto da LGPD não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado. Pelo contrário, demanda-se uma análise casuística para se desdobrar um juízo de valor sobre o modo pelo qual deve ser realizado um tratamento de dados e os riscos que dele razoavelmente se esperam. (BIONI; DIAS, 2020, p. 16)

Por esse seguimento, é inegável que a LGPD despende de certa excepcionalidade ao se referir aos dados sensíveis. Verifica-se, por exemplo, um regime diferenciado de autorização

para tratamento de dados sensíveis previsto no art. 11 da LGPD (BRASIL, 2018), a necessidade de especificação dos dados sensíveis no relatório de impacto referida em seu art. 38 (BRASIL, 2018) e a expressão "especialmente no caso de dados sensíveis" prevista no §1º do art. 46 (BRASIL, 2018), o qual prevê o papel da ANPD de criar padrões mínimos de segurança, evidenciam a excepcionalidade para o tratamento de dados sensíveis.

Como se pretendeu demonstrar em capítulos anteriores, o referido posicionamento legal decorre do fato de que os dados pessoais sensíveis são mais facilmente utilizados como meio de discriminação, por isso argumenta-se (GUEDES; MEIRELES, 2019, p. 124) que a falha no tratamento de dados sensíveis enquadra-se na cláusula geral de responsabilidade objetiva, fundamentada no parágrafo único do art. 927, do CC/2002 (BRASIL, 2002), em decorrência da natureza dessa atividade.

Deve ser esclarecido que, diferentemente do tratamento de dados pessoais comuns, que apenas podem conter um risco adquirido, pode-se concluir que o tratamento de dados sensíveis comporta um risco inerente. Em relação ao risco inerente, Cavalieri Filho (2012, p.188) conceitua: "é aquele intrinsicamente atado à própria natureza da atividade, à sua qualidade ou modo de realização, de tal forma que não se pode exercer essa atividade sem arrostar certos riscos".

Esse conceito se contrapõe ao de risco adquirido, que para o mesmo autor surge "quando a atividade normalmente não oferece perigo a alguém, mas pode se tornar perigosa (eventualmente) em razão da falta de cuidado de quem a exerce" (CAVALIERI FILHO, 2012, p. 188). Complementa, ainda, Cavalieri Filho, que somente o risco inerente poderia invocar a responsabilidade objetiva.

Deveras, entender de forma diversa, seria admitir que toda e qualquer atividade poderia invocar a responsabilidade objetiva. Assim, considerando que há riscos necessários e aceitáveis no cotidiano do homem moderno (CAVALIERI FILHO, 2012, p. 188), o art. 927, parágrafo único, do CC/2002 não abarca atividades que podem se tornar perigosas, mas sim aquelas que são inerentemente arriscadas.

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> 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 (BRASIL, 2002, art. 927, *caput* e par. único)

Levando em conta o risco inerente ao tratamento de dados sensíveis ora exposto e a excepcionalidade com que a LGPD tratou do tema, não resta dúvidas de que é perfeitamente

plausível a aplicação da teoria do risco e, por conseguinte, a aplicação da responsabilidade objetiva para o tratamento de dados sensíveis.

Denota-se, além do mais, que o art. 927, parágrafo único, do CC/2002 (BRASIL, 2002), prevê duas hipóteses de aplicação da teoria do risco, sendo a primeira quando a lei assim o declara e a segunda quando a atividade normalmente desenvolvida, por sua natureza, implicar riscos para os direitos de outrem. Esta segunda hipótese poderia, inclusive, ser o caso do tratamento automatizado de dados, em razão da já demonstrada opacidade sobre o funcionamento dos algoritmos, sobretudo aqueles que utilizam inteligência artificial.

A teoria do risco se prestaria, portanto, a impedir que ocorra uma espécie de terceirização das responsabilidades dos agentes para as máquinas, conforme explica Ana Frazão (2018) em artigo criado para a revista eletrônica JOTA. Entende a autora que a complexidade de funcionamento dos algoritmos não deve justificar uma isenção de responsabilidade por meio de um processo de *mathwashing*[39].

Como foi visto anteriormente, robôs de inteligência artificial estão aptos a agir sem a necessidade de instruções de seus desenvolvedores, são verdadeiros autodidatas capazes de resultados imprevisíveis. Isto posto, ao mesmo tempo em que as possibilidades de avanços na ciência e em outras áreas são promissoras, também devem ser consideradas as consequências negativas para as pessoas cujos dados sejam tratados por essas máquinas.

Novamente se está diante do binômio proteção de dados e desenvolvimento econômico e tecnológico, pois, ao passo que deve ser garantido o livre desenvolvimento econômico e tecnológico, isto não pode se tornar um pretexto para perpetração de violações de direitos fundamentais, mascarados por uma ideia de falsa neutralidade.

Assim, diante da complexidade do tema, o Parlamento Europeu reconheceu, inclusive, a incapacidade da responsabilidade civil nos ordenamentos jurídicos atuais suportarem as implicações dos sistemas autônomos, conforme Parágrafos AF, AG e AH da Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com Recomendações à Comissão de Direito Civil sobre Robótica (2015/2103(INL)) (EUROPEIA, 2017).

---

[39] Lavagem matemática (tradução literal) é o termo em inglês usado para designar uma forma de burlar o cumprimento de obrigações sob um viés de falsa neutralidade proporcionado pelo uso de números, estatísticas, cálculos e etc., que validam ações ilícitas ou imorais. Sobre o tema, Fred Benenson, em entrevista ao site TechnicallyMedia (WOODS, 2016): "Mathwashing can be thought of using math terms (algorithm, model, etc.) to paper over a more subjective reality. For example, a lot of people believed Facebook was using an unbiased algorithm to determine its trending topics, even if Facebook had previously admitted that humans were involved in the process." (tradução do autor: Mathwashing pode ser pensando como o uso de termos matemáticos (algoritmos, modelos, etc.) para encobrir uma realidade mais subjetiva. Por exemplo, um grande número de pessoas acreditou que o Facebook estava usando um algoritmo não enviesado para determinar seus *trending topics*, mesmo o Facebook tendo previamente admitido que humanos foram envolvidos no processo.)

> AF. Considerando que, perante o cenário em que um robô pode tomar decisões autónomas, as normas tradicionais não serão suficientes para suscitar problemas de responsabilidade jurídica pelos danos causados por um robô, uma vez que não seria possível identificar a parte responsável para prestar a indemnização e para lhe exigir que reparasse os danos causados; AG. Considerando que as insuficiências do atual quadro jurídico são evidentes também no domínio da responsabilidade contratual, na medida em que as máquinas concebidas para escolher as suas contrapartes, para negociar as condições contratuais, para celebrar contratos e para decidir se e como os aplicam, invalidam a aplicação das normas tradicionais; considerando que isto sublinha a necessidade de novas normas, eficientes e mais atualizadas, que correspondam ao desenvolvimento tecnológico e às inovações recém-surgidas e utilizadas no mercado; AH. Considerando que, no que respeita à responsabilidade extracontratual, a Diretiva 85/374/CEE apenas pode abranger os danos provocados por defeitos de fabrico de um robô, e sob reserva de a pessoa lesada poder comprovar os danos efetivos, o defeito do produto e a relação de causalidade entre o dano e o defeito, pelo que o quadro de responsabilidade objetiva ou de responsabilidade sem culpa pode não ser suficiente. (EUROPEIA, 2017, p. 8)

Muito embora se deva admitir a complexidade e controvérsia do tema, porquanto trata-se de uma questão pioneira no âmbito legal para a qual o direito ainda não encontrou respostas concretas, diversas teorias já foram formuladas para explicar a responsabilidade pelo tratamento automatizado de dados, muitas das quais, reforçam a ideia da responsabilidade objetiva.

Sobre a responsabilidade de entes autônomos, em estudo publicado na Revista Brasileira de Políticas Públicas, Pires e Silva (2017, p. 240-252) expõem as diversas propostas de abordagem da doutrina estrangeira e do Parlamento Europeu de 2017. Passa-se pela viabilidade da criação de personalidade jurídica para máquinas automatizadas; em seguida, analisa-se a responsabilidade vicária, que considera a inteligência artificial uma ferramenta e a possibilidade da responsabilidade indireta do usuário; depois, a teoria do fato do produto, que revela familiaridade com o regime adotado no CDC; a teoria do risco criado; e, por fim, a teoria do risco proveito, a qual acredita que a responsabilidade de quem se beneficia do risco deve ser objetiva.

A primeira tese abordada foi sugerida pela Resolução do Parlamento Europeu de 2017 (EUROPEIA, 2017). Nela propunha-se a criação de personalidade jurídica especial para robôs, pois entende-se que alguns possuem tamanha autonomia que deveriam estar envolvidos por uma "personalidade eletrônica", capacitando-lhes a assumir direitos e deveres na ordem jurídica (PIRES; SILVA, 2017. p. 246). [40]

[40] Também é possível verificar essa previsão na Cláusula 59, alínea 'f' da Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações à Comissão de Direito Civil sobre Robótica (2015/2103(INL)): "f) Criar um estatuto jurídico específico para os robôs a longo prazo, de modo a que, pelo menos, os robôs autónomos mais sofisticados possam ser determinados como detentores do estatuto de pessoas eletrónicas responsáveis por sanar quaisquer danos que possam causar e, eventualmente, aplicar a personalidade eletrónica a casos em que os robôs tomam decisões autónomas ou em que interagem por qualquer outro modo com terceiros de forma independente;"

Essa possibilidade foi rechaçada duramente por aqueles que afirmam que inteligências artificiais não possuem os atributos necessários para receberem personalidade jurídica, pois lhes faltaria capacidade volitiva, já que operam em nome de seus desenvolvedores. Para essa corrente doutrinária, as decisões tomadas por robôs devem ser imputadas à entidade jurídica em nome da qual o sistema é operado, e conferir essa responsabilidade a uma máquina seria demasiadamente inspirado em ideias fictícias (ČERKA; GRIGIENĖ; SIRBIKYTĖ, 2015. p. 376-389 Apud PIRES; SILVA, 2017, p. 246).

Todavia se argumente a possibilidade de criação de personalidade jurídica para robôs inteligentes, é necessário reconhecer os riscos de que se crie um cenário de "irresponsabilidade organizada", que, segundo Ana Frazão (2019, p. 505), "certamente ocorreria se os agentes econômicos que se utilizassem de sistemas de inteligência artificial não mais respondessem pelos danos daí decorrentes".

A segunda teoria, entende os robôs inteligentes como sendo ferramentas em favor de quem deles obtém proveito (PIRES; SILVA, 2017, p. 248). Por esse ponto de vista, ao encará-los como ferramentas, a responsabilidade objetiva se assimilaria àquela advinda da chamada responsabilidade vicária, decorrente do dever de cuidado ou de vigilância de quem a manuseia.

Nesse seguimento, haveria a responsabilidade objetiva do agente de tratamento de dados quando este estivesse utilizando a inteligência artificial na prestação de seus serviços, decorrente do dever de vigilância. Contudo, essa teoria poderia embasar a excludente de responsabilidade baseada em culpa exclusiva da vítima, posto que um usuário comum, utilizando-se, para proveito próprio, de um software de inteligência artificial, incorreria nos deveres de cuidado e vigilância sobre a ferramenta sob sua tutela (PIRES; SILVA, 2017, p. 248).

Por essa linha, o usuário seria o responsável por realizar maus *inputs*, ou seja, instruções baseadas em imperícia e/ou preconceitos do próprio usuário, capazes de interferir no funcionamento e no padrão de respostas dos robôs, o que de certa forma personaliza o funcionamento da inteligência artificial, fazendo com que este robô passe a desempenhar uma função nova não prevista nos códigos originais.

Pelos conceitos construídos ao longo deste trabalho, não é forte o argumento de que seria possível imputar uma responsabilidade de dever de vigilância ao usuário comum, em vista de sua fragilidade técnica em relação aos sistemas automatizados de tomada de decisão. Na realidade, incumbe ao agente que criou e comercializou o programa de inteligência artificial supervisionar as suas atividades e criar maneiras de instruir os usuários sobre a sua correta operação.

Ainda sob esse raciocínio, a doutrina (PAGALLO, 2013 Apud PIRIS; SILVA, 2017, p. 249) levanta a possibilidade de se atribuir a responsabilidade objetiva ao criador ou fabricante da inteligência artificial, com base na teoria do fato do produto. Para essa corrente, o dano causado pela inteligência artificial é oriundo de uma "falha humana *res ipsa loquitor*, seja uma falha de projeto, de fabricação, de montagem ou de informação suficiente ao usuário acerca da segurança e do uso apropriado do produto" (PIRES; SILVA, 2017, p. 250).

Fato é que, mesmo que sejam respeitados todos os deveres objetivos de segurança e informação, e que a inteligência artificial não apresente qualquer mau funcionamento técnico, ainda é possível que sejam causados danos ao titular de dados. Isso se deve ao fato de que o próprio conceito de inteligência artificial envolve a autoaprendizagem e autoaperfeiçoamento, tornando muito difícil precisar quais falhas são resultantes desse processo e quais são provenientes do defeito de fabricação do produto (PIRES; SILVA, 2017, p. 250).

Assim, considerando essa característica da autoaprendizagem e a imprevisibilidade de resultados, a teoria do risco do desenvolvimento complementa o entendimento sobre a responsabilidade no tratamento de dados automatizado. Para essa teoria, o risco do desenvolvimento é aquele que não pode ser conhecido no momento do lançamento do produto no mercado, em virtude do estado da Ciência e da Técnica à época (BENJAMIN, 1991, p. 67 Apud CAVALIERI FILHO, 2012, p. 199).

Em adendo, para Cavalieri Filho a responsabilidade civil objetiva pode ser sustentada também pela teoria do risco do desenvolvimento, sendo um caso de fortuito interno:

> Em nosso entender, os riscos de desenvolvimento devem ser enquadrados como fortuito interno – risco integrante da atividade do fornecedor, pelo que não-exonerativo da sua responsabilidade. Nesse sentido o Enunciado nº 43 aprovado na Jornada de Direiro Civil promovida pelo Centro de Estudos Judiciários do Conselho da Justiça Federal (Brasília, 11 a 13 de setembro de 2002): "A responsabilidade civil pelo fato do produto, prevista no art. 931 do novo Código Civil, também inclui os riscos do desenvolvimento." (CAVALIERI FILHO, 2012, p. 200)

Por fim, concluindo seu estudo, Pires e Silva (2017, p. 251) ressaltam a teoria do *deep-pocket*, por meio da qual todos os agentes que obtiveram proveitos econômicos daquele determinado robô causador de dano estariam objetivamente obrigados a ressarcir às vítimas pelas perdas e danos sofridos. Assim, destaca-se a proposta da Resolução do Parlamento Europeu de 2017 (EUROPEIA, 2017), de que haja a adoção, pelos controladores e operadores de dados que utilizam de inteligência artificial em suas atividades, de um seguro obrigatório para prevenir os riscos inerentes dessas atividades.

Como se nota, há diversas teorias no sentido de se defender a incidência da responsabilidade objetiva pelo tratamento automatizado de dados, seja pela teoria do risco

proveito, do fato do produto, do risco criado ou do risco do desenvolvimento. Contudo, deve ser observado o caso brasileiro com atenção, considerando as peculiaridades trazidas pela nova LGPD.

Certo é que o tratamento automatizado de dados, assim como ocorre com os dados sensíveis, diferencia-se pelo seu potencial lesivo ao titular, motivo pelo qual, justifica-se defender a incidência da teoria do risco e, consequentemente, a incidência da responsabilidade objetiva para essa espécie de tratamento de dados.

Não se pode olvidar, entretanto, que o assunto carece ainda de amadurecimento e provavelmente será objeto de muitas demandas judiciais. Isso porque, pelo fato de não haver a LGPD conceituado o que vem a ser atividade de risco e, tampouco, definido o tratamento automatizado de dados como tal, há margem para interpretação diversa, para defender a responsabilidade subjetiva em prol do desenvolvimento econômico e tecnológico.

Para responder à pergunta do que viria a ser uma atividade de risco, Maria Celina Bodin de Moraes (2006, p. 28), citada por Guedes e Meireles (2019, p. 125), vale-se da doutrina italiana, que adota comumente dois critérios de definição, quais sejam: "i) a quantidade de danos habitualmente causados pela atividade em questão; ii) a gravidade de tais danos.".

Dessa forma, pode-se concluir que atividade de risco é aquela que estatisticamente causa danos graves e com frequência. Por conseguinte, embora a responsabilidade objetiva se mostre adequada para evitar a "socialização dos danos"[41] provocada pelo tratamento automatizado de dados, o levantamento de estatísticas acerca da frequência e das dimensões dos danos mostra-se necessário para que se possa invocar a sua incidência.

Além disso, conquanto se possa argumentar a responsabilidade objetiva no tratamento automatizado de dados em razão do risco da atividade, a redação dada à LGPD vai em sentido contrário a esse entendimento, pois a Lei não trata o tema de forma específica e, como regra, privilegia o cumprimento de deveres, a prestação de contas, o porte econômico da empresa, o nível de segurança que se espera do agente de tratamento etc.

Esse entendimento é reforçado, aliás, no art. 20, §§ 1º e 2º, da LGPD (BRASIL, 2018), o qual consagra o o direito à revisão de decisões automatizadas e a possibilidade de o controlador se negar a fornecer informações a respeito dos critérios e procedimentos utilizados para tomada de decisão.

> Art. 20 [...]

[41] Nas palavras de Cavalieri Filho (2012, p. 166): "O dano, por esse novo enfoque, deixa de ser apenas contra a vítima para ser contra a própria coletividade, passando a ser um problema de toda a sociedade".

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (BRASIL, 2018, art. 20, §§ 1º e 2º)

Isto posto, constata-se que, quanto ao tratamento automatizado de dados, a LGPD impõe um especial dever de transparência aos controladores, os quais poderão ser alvos de auditoria para verificação de aspectos discriminatórios em suas atividades, caso não cumpram com tal dever de transparência.

Como abordado anteriormente, não há de se falar em cumprimento de deveres ou diligências quando se está diante de uma responsabilidade objetiva. A comprovação de falta no cumprimento de deveres, bem como a instauração de auditoria para investigar tais descumprimentos, são características da responsabilidade subjetiva.

Em vista do exposto, pode-se afirmar que a responsabilidade pelo tratamento automatizado de dados seguirá o regime geral adotado pela LGPD, ou seja, a responsabilidade subjetiva. Tal posicionamento reforça ainda mais os deveres de transparência e prestação de contas que precisam ser cumpridos pelas empresas, pois o uso sem regulação de algoritmos, que funcionam como *black boxes*, podem expor o titular de dados a sérios riscos.

Em concordância, Ana Frazão (2019) destacou que a transparência e *accountability* são essenciais para se criar um ambiente capaz de garantir a proteção de dados diante da opacidade algorítmica:

> Com efeito, um dos principais objetivos da lei é o de assegurar a autodeterminação informacional dos titulares de dados por meio de diversos princípios e garantias, dentre os quais se destacam os princípios do livre acesso aos dados e também da transparência e *accountability*, a fim de colocar um freio no ambiente de opacidade que vem caracterizando as decisões algorítmicas. Isso quer dizer que todo aquele que se utiliza de sistemas de inteligência artificial precisa se acercar de garantias de que o sistema é razoavelmente adequado, seguro, robusto, inteligível e suscetível de ser explicado e justificado. (FRAZÃO, 2019, p. 507)

Considerando o prestígio dado pela LGPD aos deveres de transparência e prestação de contas, que coloca os agentes de proteção de dados na posição de proverem, por conta própria, a adoção de parâmetros adequados de segurança, sob pena de que sejam presumidamente culpados pelos danos causados, Maria Celina Bodin de Moraes e João Quinelato de Queiroz (2019) defendem a tese de que a LGPD adotou um regime de responsabilidade proativo:

> Trata-se da sua união ao conceito de "prestação de contas". Esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa" encontra- se indicada no inciso X do art. 6º, que

> determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente". (DE MORAES; DE QUEIROZ, 2019, p. 129)

Assim sendo, as companhias precisarão demonstrar o quão aptas estão para mapear os riscos e impactos de seu negócio, o quanto se empenham para buscar programas de segurança da informação, o quão robusto e transparente é o seu canal de comunicação com o titular de dados – e aqui se incluem tanto a comunicação antes do tratamento de dados, os termos de uso, os contratos, como também a possibilidade de denúncias e reclamações – e qual o nível de documentação sobre os seus sistemas a empresa possui.

4 CONSIDERAÇÕES FINAIS

Na atual sociedade informatizada, os dados pessoais tornaram-se uma extensão da personalidade humana, e a exploração econômica desses dados vem sendo realizada de forma desregulada e inconsequente. Por esse motivo, a LGPD criou suporte legal para responsabilizar os agentes de tratamento de dados pelos desrespeitos aos direitos à autodeterminação informativa e à privacidade.

Não obstante, a LGPD não deixou claro qual teria sido o regime de responsabilidade civil adotado por ela, se objetiva ou subjetiva. Por essa razão, o presente trabalho propõe respostas sobre a configuração da responsabilidade civil na LGPD, bem como sobre a possibilidade de aplicação da teoria do risco para embasar a responsabilidade objetiva quanto ao tratamento automatizado de dados e o tratamento de dados sensíveis.

Portanto, atingiu-se o primeiro objetivo específico deste trabalho, ao se analisar a existência de um risco inerente nas atividades de tratamento automatizado de dados e de tratamento de dados sensíveis. Verificou-se que, enquanto os dados sensíveis podem expor o seu titular ao risco da discriminação, comprovando a existência de um risco inerente à atividade, o tratamento automatizado de dados pode se tornar potencialmente lesivo, caso seus desenvolvedores não se ocupem em proporcionar transparência no funcionamento de seus sistemas e em combater comportamentos enviesados e preconceituosos destes.

Do mesmo modo, o segundo objetivo específico do presente trabalho foi atingido, ao se demonstrar que o regime geral da responsabilidade civil, adotado pela LGPD, é o da responsabilidade subjetiva, haja vista a existência de deveres legais a serem cumpridos pelo agente de tratamento, as evidências dadas pelo próprio texto da LGPD, que levam em conta fatores subjetivos na apuração da responsabilidade, e em razão do fundamento do desenvolvimento econômico e tecnológico elencado no art. 2º, inciso V, dessa Lei (BRASIL, 2018).

Pelo exposto, também foi atingido o objetivo geral do presente trabalho, ao se demonstrar a possibilidade de aplicação da teoria do risco para fundamentar a responsabilidade objetiva dos agentes de tratamento de dados, quando do tratamento de dados sensíveis, adotando-se a teoria do risco criado, prevista no art. 927, parágrafo único do CC/2002 (BRASIL, 2002), haja vista a existência do risco inerente da exploração desses dados.

Ainda sobre o objetivo geral desse trabalho, verificou-se que a responsabilidade pelo tratamento automatizado de dados deve ser subjetiva. Isso porque, muito embora se reconheça

a complexidade do funcionamento algorítmico, ao se estudar a doutrina e o texto da própria LGPD, verificou-se que não há indícios fortes o bastante para que se possa concluir haver responsabilidade objetiva nessa hipótese.

Sendo assim, com base nos §§1º e 2º, do art. 20 da LGPD (BRASIL, 2018), os quais preveem o dever de transparência e a possibilidade de auditoria para se averiguar atividades discriminatórias no tratamento automatizado de dados, e com base no regime geral de responsabilidade da LGPD, só é possível concluir pela subjetividade da responsabilidade nesta seara.

Desta forma, a hipótese inicial de que se poderia adotar a teoria do risco para fundamentar a responsabilidade civil objetiva pelo tratamento de dados pessoais sensíveis e pelo tratamento automatizado de dados pessoais, somente se confirma na primeira suposição, restando refutada quanto à segunda, pois, nesse caso, não há um risco inerente da atividade, mas sim a possibilidade de que haja um risco adquirido pela não observância dos deveres de cuidado.

Outrossim, com base nos resultados obtidos pela presente pesquisa, é possível observar que o problema do equilíbrio entre a proteção de dados e o desenvolvimento econômico e tecnológico, dependerá do assentamento da jurisprudência acerca do tema e da regulamentação a ser dada pela ANPD sobre os padrões técnicos de segurança a serem a serem respeitados pelos controladores de dados, observando as particularidades de cada setor da economia e o porte econômico das empresas.

Entretanto, não se pode negar que a LGPD determinou diretrizes razoáveis para que esse binômio seja equalizado de forma satisfatória, pois a previsão da responsabilidade objetiva do tratamento de dados pessoais sensíveis cria maior proteção ao titular de dados. Sem embargo, o legislador também atendeu ao princípio do livre desenvolvimento econômico e tecnológico, ao adotar o regime geral de responsabilidade subjetiva para o tratamento de dados; e, ao criar deveres de transparência e prestação de contas, cuidou de inibir eventuais excessos cometidos pelos controladores e operadores de dados.

Quanto à metodologia, o procedimento bibliográfico demandou grande esforço na busca por diversos autores, livros, artigos e notícias, os quais foram obtidos em meio digital ou físico. O caráter descritivo se encontra em todos os capítulos dessa pesquisa, haja vista a necessidade de se embasar as formulações teóricas realizadas, para, ao final, realizar a análise qualitativa das teorias abordadas.

Por fim, o método dedutivo foi utilizado para chegar às conclusões acerca da responsabilização no âmbito do tratamento de dados sensíveis e do tratamento de dados

automatizado, vez que há poucos escritos acerca dessa temática, já que as legislações e a doutrina estudadas voltam-se mais a descrever o regime geral da responsabilidade.

As limitações e dificuldades encontradas se revelam em razão do fato de que a LGPD, cuja vigência começou em setembro de 2020, ainda é muito recente no ordenamento jurídico brasileiro, não havendo, por conseguinte, muitos casos que invoquem tal legislação para dirimir questões da responsabilidade civil. Ademais, em virtude do pouco espaço de tempo, também não foi possível realizar estudos de direito comparado na jurisprudência de países específicos regidos pela GDPR.

Com toda certeza, futuros estudos deverão indicar o entendimento jurisprudencial acerca do tema, bem como deverão indicar análises estatísticas sobre a quantidade de incidentes de proteção de dados e quantos deles foram devidamente punidos. Tal análise será importante para demonstrar se a LGPD encontrou eficácia para inibir o tratamento abusivo de dados e para verificar quais das teorias da responsabilidade foram adotadas nos casos concretos.

Cumpre frisar que este trabalho, por se propor a estudar as principais teorias acerca da responsabilidade civil na área da proteção de dados, poderá contribuir para a melhor compreensão da matéria, principalmente no tocante ao tratamento de dados pessoais sensíveis e no tratamento de dados automatizados, pois o tema ainda é pouco explorado pelos tribunais brasileiros, e a doutrina diverge bastante em acerca das teorias que explicariam o regime de responsabilidade adotado pela LGPD.

Diante de todo exposto, é possível concluir que a LGPD arquitetou um sistema de responsabilidade civil coerente, que não se distancia tanto do sistema geral do CC/2002, mas que irá exigir um esforço adaptativo muito grande dos controladores e operadores de dados, pois estes deverão agir proativamente para implementar em suas companhias programas efetivos de *compliance* e governança de dados, que sejam capazes de testificar a boa-fé e o compromisso para com as boas práticas de tratamento de dados.

REFERÊNCIAS

LIVROS

BESSA, Leonardo Roscoe; MOURA, Walter José Faiad de. **Manual de direito do consumidor**. 4ª Ed. Brasília: Escola Nacional de Defesa do Consumidor. 2014. Disponível em: <https://www.defesadoconsumidor.gov.br/images/manuais/manual-do-direito-do-consumidor.pdf> Acesso em 08 jan. 2021

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Editora Forense. 2019.

CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 10ª Ed. São Paulo: Editora Atlas S.A. 2012. Disponível em: <https://www.academia.edu/7722953/SERGIO_CAVALIERI_Programa_de_Responsabilidade_Civil_2012> Acesso em 09 dez. 2020.

COELHO, Fábio Ulhoa. **Curso de direito comercial**. 16ª Ed. v.1. São Paulo: Saraiva, 2012. Disponível em: <https://docero.com.br/doc/nss551e> Acesso em 08 jan. 2021.

FARIAS, Cristiano Chaves de; NETTO, Felipe Braga; ROSENVALD, Nelson. **Manual de Direito Civil**. 2ª Ed. Salvador: JusPodivm. 2018.

FARIAS, Gilberto; MEDEIROS, Eduardo Santana. **Introdução à Computação**. 1ª Ed. Paraíba: Universidade Federal da Paraíba, 2013. Disponível em: <http://producao.virtual.ufpb.br/books/gilbertofarias/introducao-a-computacao-livro/livro/livro.pdf> Acesso em 09 dez. 2020.

FRAZÃO, Ana. **Responsabilidade**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coordenadoras). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Editora RT. 2019.

GARCIA, Leonardo. **Código de defesa do consumidor comentado: artigo por artigo**. 15ª Ed. Jus2020. Salvador: Editora Juspodivm. 2020. Disponível em: <https://www.editorajuspodivm.com.br/cdn/arquivos/4faa91c73af1ee00a9b3718da851f62e.pdf> Acesso em 08 jan. 2021.

GATES, Bill. **Business @ the Speed of Though**. Harlow, England: Pearson Education Limited. 2001. Disponível em: <https://www.pdfdrive.com/business-the-speed-of-thought-chiakhoathanhcong-d17576090.html> Acesso em 03 jan. 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. **Término do tratamento de dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coordenadores). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1ª Ed. São Paulo: Editora RT. 2019. *E-book*. Disponível em: <https://pt.scribd.com/document/461238367/LGPD-e-Suas-Repercussoes-no-Direito-Brasileiro-Gustavo-Tepedino-2019-1> Acesso em: 28 dez. 2020.

KONDER, Carlos Nelson. **O tratamento de dados sensíveis à luz da Lei 13.709/2018** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coordenadores). Lei Geral de Proteção de Dados Pessoais. 1 Ed. São Paulo: Thomson Reuters Brasil. 2019. *E-book.* Disponível em: < https://pt.scribd.com/document/461238367/LGPD-e-Suas-Repercussoes-no-Direito-Brasileiro-Gustavo-Tepedino-2019-1> Acesso em: 30 dez. 2020.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva. 2011. Disponível em: <http://leonardi.adv.br/wp-content/uploads/2012/01/mltpi.pdf> Acessado em 09 dez. 2020.

MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. **Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018)** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coordenadores). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1ª Ed. São Paulo: Editora RT. 2019. *E-book*. Disponível em: <https://pt.scribd.com/document/461238367/LGPD-e-Suas-Repercussoes-no-Direito-Brasileiro-Gustavo-Tepedino-2019-1> Acesso em: 28 dez. 2020.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP**. IN: THEMOTEO, Reinaldo J. (Coordenador). Proteção de dados pessoais: privacidade versus avanço tecnológico. Cadernos Adenauer, volume 3, Ano XX. Rio de Janeiro: Fundação Konrad Adenauer. 2019. Disponível em: <https://www.academia.edu/41132175/Autodetermina%C3%A7%C3%A3o_informativa_e_responsabiliza%C3%A7%C3%A3o_proativa_novos_instrumentos_de_tutela_da_pessoa_humana_na_LGDP> Acesso em 07 jan. 2021.

NEVES, Thiago Ferreira Cardoso. **Autonomia privada e privacidade nas redes sociais: renunciabilidade e responsabilidade por danos**. 1ª Ed. Rio de Janeiro: LMJ Mundo Jurídico, 2019.

ZIVIANI, Nivio. **Projeto de algoritmos: com implementações em Java e C++**. 3ª Ed. São Paulo: Cengage Learning. 2011. Disponível em: <https://www.academia.edu/35019244/Projeto_de_Algoritmos_com_Implementacoes_em_Java_e_C_Nivio_Ziviani> Acessado em: 09 dez. 2020.

ARTIGOS

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais**: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em 06 jan. 2021.

CORBO, Wallace. **Discriminação indireta: o que é e como superá-la?**. JOTA. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/Art.s/discriminacao-indireta-o-que-e-e-como-supera-la-09112017#:~:text=Como%20j%C3%A1%20afirmado%2C%20a%20discrimina%C3%A7%C3%A3o,efeitos%20discriminat%C3%B3rios%20contra%20esses%20grupos.> Acesso em 27 dez. 2020.

CRAWFORD, Kate. **Artificial Intelligence's White Guy Problem**. The New York Times. 2016. Disponível em: <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html> Acesso em 27 nov. 2020.

D'ANDREA, Edgar; BATISTA, Eduardo; JURICIC, Maressa. **LGPD: o que muda na prática com a Lei 13.709/18**. PwC Brasil. 2020. Disponível em: <https://www.pwc.com.br/pt/sala-de-imprensa/artigos/lgpd-muda-pratica-plc-53.html> Acesso em 27 dez. 2020.

DRESCH, Rafael de Freitas Vale; STEIN, Lilian Brandt. **Direito fundamental à proteção de dados e responsabilidade civil**. Migalhas. 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/336997/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil> Acesso em 07 jan. 2021.

FRAZÃO, Ana. **Algoritmos e inteligência artificial**. JOTA. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018#sdfootnote6anc> Acesso em 28 dez. 2020.

GOODMAN, Bryce; FLAXMAN, Seth. **European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"**. 3ª Ed. Nova York: Al Magazine. 2017. Disponível em: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/2741/2647> Acesso em 09 dez. 2020.

KNIGHT, Will. **The dark secret at the heart of AI: no one really knows how the most advanced algorithms do what they do - that could be a problem**. MIT Technology Review. 2017. Disponível em: <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/>. Acesso em 16 jun. 2020.

MARRAFON, Marco Aurélio; MEDON Filipe. **Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados**. Consultor Jurídico (Conjur). 2019. Disponível em: <https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd#_ftn3)> Acesso em 16 jun. 2020.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor. vol. 120, ano 27. São Paulo: Editora. RT. 2018. Disponível em: <https://www.academia.edu/42741127/Reflex%C3%B5es_iniciais_sobre_a_nova_lei_geral_de_prote%C3%A7%C3%A3o_de_dados> Acesso em 27 dez. 2020.

MULHOLLAND, Caitlin Sampaio. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?**. Migalhas. 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco> Acesso em 07 jan. 2021.

_____, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18)**. Vitória: Revista de Direitos e Garantias Fundamentais. v. 19, n. 3, p. 159-180. 2018. Disponível em:

<https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603> Acesso em 06 jan. 2021.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. **A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu**. Vol. 7. 3ª Ed. Brasília: Revista Brasileira de Políticas Públicas. 2017. Disponível em <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4951/3643> Acessado em 09 dez. 2020.

VICENTE, João Paulo. **Preconceito das máquinas: como algoritmos podem ser racistas e machistas**. Tilt: O canal sobre tecnologia do UOL. 2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/04/24/preconceito-das-maquinas-como-algoritmos-tomam-decisoes-discriminatorias.htm> Acesso em: 27 nov. 2020.

PALESTRAS E SEMINÁRIOS

GUEDES, Gisela Sampaio. **I Simpósio de Responsabilidade Civil e Proteção de Dados**. Moderadores: Nelson Rosenvald e Carlos Edison do Rêgo Monteiro Filho. Coordenação Técnica: José Faleiros Jr. [S.I.]: Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. 2020. 1 vídeo (2h23min). Publicado pelo canal IBERC - Responsabilidade Civil. Disponível em: <https://youtu.be/igbbxkbqeKI> Acesso em 28 dez. 2020.

LEGISLAÇÕES, ENUNCIADOS E RESOLUÇÕES

BRASIL. **Lei 8.078/1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília-DF, 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em 01 jan. 2021.

_____. **Lei nº 10.406/2002**. Institui o Código Civil. Diário Oficial da União, Brasília-DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm> Acesso em 01 jan. 2021.

_____. **Lei nº 13.709/2018**. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília-DF, 14 ago 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em 01 jan. 2021.

EUROPEIA, União. **Regulation (EU) 2016/679**. General Data Protection Regulation. Bruxelas: Parlamento Europeu e Conselho de 27 abr. 2016. Official Journal of the European Union. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> Acesso em 01 jan. 2021.

EUROPEIA, União. **Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL))**. Estrasburgo: Parlamento Europeu. Publicado em 16 fev. 2017. Disponível em: <https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.pdf> Acesso em 28 dez. 2020.

FEDERAL, CONSELHO DE JUSTIÇA. **Jornadas de direito civil I, III, IV: Enunciados aprovados**. Ministro Ruy Rosado Júnior (coord. científico). Brasília: Conselho de Justiça Federal, Centro de Estudos Judiciários. 2012. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/EnunciadosAprovados-Jornadas-1345.pdf> Acesso em 08 jan. 2021.

JURISPRUDÊNCIA

BRASIL. Supremo Tribunal Federal – STF. **Ação Direta de Inconstitucionalidade nº 5543/DF**. Ação direta de inconstitucionalidade. Direito constitucional. Art. 64, iv, da portaria n. 158/2016 do ministério da saúde e art. 25, xxx, "d", da resolução da diretoria colegiada – rdc n. 34/2014 da anvisa. Restrição de doação de sangue a grupos e não condutas de risco. Discriminação por orientação sexual. Inconstitucionalidade. Ação direta julgada procedente.Tribunal Pleno. Requerente: Partido Socialista Brasileiro – PSB. Intimados: Ministro de Estado da Saúde; Agência Nacional de Vigilância Sanitária – Anvisa. Relator: Ministro Edson Fachin. Data de Julgamento: 11 mai. 2020. STF. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur429684/false> Acesso em 07 jan. 2021.

_____. Superior Tribunal de Justiça – STJ (3ª Turma). **Recurso Especial 1758799 MG 2017/0006521-9**. Recurso Especial. Fundamento não impugnado. Súm. 283/STF. Ação de compensação de dano moral. Banco de dados. Compartilhamento de informações pessoais. Dever de informação. Violação Dano moral in re ipsa. Julgamento: CPC/15. Recorrente: PROCOB S/A. Recorrido: José Galvão da Silva. Relatora: Ministra Nancy Andrighi. Data de Julgamento: 12 nov. 2019. JusBrasil. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/859849413/recurso-especial-resp-1758799-mg-2017-0006521-9/inteiro-teor-859849423?ref=serp> Acesso em 07 jan. 2021.

_____. Superior Tribunal de Justiça – STJ (3ª Turma). **Recurso Especial 718618 RS 2005/0011060-0**. Responsabilidade civil. Dano moral. Registro no cadastro de devedores do SERASA. Existência de outros registros. Indenização. Possibilidade. Recorrente: Nilce da Silveira Leal. Recorrido: Crefisa S/A Crédito Financiamento e Investimentos. Relator: Ministro Antônio De Pádua Ribeiro. Data de Publicação: 24 mai. 2005. JusBrasil. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/84309/recurso-especial-resp-718618-rs-2005-0011060-0> Acesso em 07 jan. 2021.

_____. Superior Tribunal de Justiça – STJ . **Recurso Especial 1419697 RS 2013/0386285-0**. S2 – Segunda Seção. Recurso Especial representativo de controvérsia (art. 543-C, CPC). Tema 710/STJ. Direito do Consumidor. Arquivos de crédito. Sistema "credit scoring". Compatibilidade com o direito brasileiro. Limites. Dano moral. Recorrente: Boa Vista Serviços S/A. Recorrido: Anderson Guilherme Prado Soares. Relator: Ministro Paulo De Tarso Sanseverino. Data de Julgamento: 12 nov. 2014. JusBrasil. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-resp-1419697-rs-2013-0386285-0/relatorio-e-voto-152068681> Acesso em 07 jan. 2021.

_____. Superior Tribunal de Justiça – STJ. **Agravo em Recurso Especial 1379761 SP 2011/0004318-8**. Agravante: Banco Santander Brasil S/A. Agravado: Maria Lúcia Ribeiro Alves. Relator: Ministro Luis Felipe Salomão. Data de Publicação: 30 mar. 2011. JusBrasil.

2011. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/18697711/ag-1379761> Acesso em 07 jan. 2021.

SANTA CATARINA. Tribunal de Justiça de Santa Catarina – TJSC (1ª Turma de Recursos – Capital). **Recurso Inominado 0806692162138240023**. Recurso Inominado. SERASA. Concentre scoring. Banco de dados restritivo de crédito não autorizado pelo consumidor. Acesso à informação. Impossibilidade de retificação. Violação ao art. 5º, inciso X, da Constituição Federal. Art. 43 do CDC; e, art. 4º da Lei 12.414/11. Banco de dados obscuro e manifestamente ilegal. Falta de transparência. Fato do serviço. Recurso desprovido. Recorrente: Serasa S/A. Recorrido Rafael Ruinz Peixoto. Relator: Alexandre Morais da Rosa. Data de Julgamento: 19 set. 2013. JusBrasil. Disponível em: <https://tj-sc.jusbrasil.com.br/jurisprudencia/1102118937/recurso-inominado-ri-8066921620138240023-capital-eduardo-luz-0806692-1620138240023/inteiro-teor-1102118986> Acesso em 28 dez. 2020

NOTÍCIAS E ENTREVISTAS

NEWS, BBC. **Google searches expose racial bias, says study of names**. 2013. Disponível em: <https://www.bbc.com/news/technology-21322183> Acesso em 16 jun. 2020.

FEDERAL, Ministério Público. **Justiça atende pedido do MPF e determina que Microsoft ajuste coleta de dados pelo Windows 10**. 2018. Disponível em:<http://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/justica-atende-pedido-do-mpf-e-determina-que-microsoft-ajuste-coleta-de-dados-pelo-windows-10> Acesso em 07 jan. 2021.

GARCIA, Gabriel. **Hacker divulga dados de homem cadastrado em site de traição**. Exame. 2015. Disponível em: <https://exame.com/tecnologia/hackers-divulgam-dados-de-homem-em-site-de-traicao/> Acesso em 27 nov. 2020.

O GLOBO. **Ashley Madison Canadá tem relatos de suicídios após vazamentos do site**. 2015. Disponível em: <https://oglobo.globo.com/economia/ashley-madison-canada-tem-relatos-de-suicidios-apos-vazamentos-do-site-17282729> Acesso em 16 fev. 2020.

SENADO, Agência. **Lei Geral de Proteção de Dados entra em vigor. 2020**. 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor> Acesso em 08 jan. 2021

VENTURA, Felipe. **Procon-SP multa Google e Apple em até R$ 10 milhões por causa do FaceApp**. Tecnoblog. 2019. Disponível em: <https://tecnoblog.net/305053/procon-sp-multa-google-apple-faceapp/#:~:text=Google%20e%20Apple%20fornecem%20FaceApp,empresas%20de%20imporem%20cl%C3%A1usulas%20abusivas&text=Al%C3%A9m%20disso%2C%20o%20%C3%B3rg%C3%A3o%20diz,privacidade%20e%20termos%20de%20uso.> Acesso em 08 jan. 2021

WOODS, Tyler. **‘Mathwashing,’ Facebook and the zeitgeist of data worship**. 2016. Disponível em: <https://technical.ly/brooklyn/2016/06/08/fred-benenson-mathwashing-facebook-data-worship/> Acesso em 29 dez. 2020.

OUTROS TEXTOS EM MEIO ELETRÔNICO

WIKIPEDIA. **Accountability**. 2020c. Disponível em: <https://pt.wikipedia.org/wiki/Accountability#:~:text=Accountability%20%C3%A9%20um%20termo%20da,controladoras%20ou%20a%20seus%20representados.> Acesso em: 24 dez. 2020.

_____. **Geo-blocking**. 2020b. Disponível em: <https://en.wikipedia.org/wiki/Geo-blocking> Acesso em 27 dez. 2020.

_____. **Geographical pricing**. 2020a. Disponível em: <https://en.wikipedia.org/wiki/Geographical_pricing)> Acessado em 27 dez. 2020.