**INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP**

**ESCOLA DE DIREITO DO BRASIL – EDIRB**

MESTRADO PROFISSIONAL INTERDISCIPLINAR EM DIREITO, JUSTIÇA E DESENVOLVIMENTO

CACYONE GOMES BARBOSA GONÇALVES

# DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

A responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor

Brasília-DF

2022

**CACYONE GOMES BARBOSA GONÇALVES**

# DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

A responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor

Qualificação de Dissertação de Mestrado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito, como requisito parcial para obtenção do título de Mestre em Direito Constitucional.

Orientador Prof. Dr. Nelson Rosenvald

Brasília-DF

2022

**DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:**
A responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor

Qualificação de Dissertação de Mestrado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito, como requisito parcial para obtenção do título de Mestre em Direito Constitucional.

Brasília,_____de_____de 2022.

**BANCA EXAMINADORA**

---

Orientador Prof. Dr. Nelson Rosenvald
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP

---

Prof. Examinador 1
Filiação

---

Prof. Examinador 2
Filiação

---

Prof. Examinador 3
Filiação

Ao professor Danilo Doneda, pela inspiração, ensinamentos e trajetória na proteção de dados pessoais, toda a minha amizade, carinho e admiração.
Ao meu marido, Antônio Lavareda.
A Deus, por estar comigo sempre.

## AGRADECIMENTOS

Uma jornada de pesquisa e estudo sempre inexoravelmente, no leva a amadurecer. E não apenas na vida pessoal, mas profissional também. E em ambas, com muita intensidade. A rotina de estudos, a coleta de material, a seleção, as horas de sono, a expectativa de conseguir chegar lá com algo relevante e que contribua para o universo acadêmico, e principalmente fora dele. Toda privação, todo esforço ao final é compensado pela trajetória de descobertas e pelos desdobramentos delas.

Do lado pessoal, confesso que foi em especial doloroso pelos fatos ocorridos durante a pandemia como ter adoecido de covid-19 na reta final, por ter ao longo dos estudos perdido um paiquerido e amigos também. Por todas as privações que eu e a minha turma de mestrado passamos. Dedico a eles também. Nos vimos pouco, mas "convivemos" muito. Agradeço a Deus pela bênção por seguir diante das perdas, do medo e da sensação de incapacidade. Foram os reflexos da pandemia na saúde mental.

Ao meu amado marido, Antonio Lavareda, que me acolheu em todos os momentos angustiantes e é meu maior incentivador. A pessoa que mais quer o meu bem.

Às minhas filhas Eduarda e Maria Luísa pelo apoio e paciência quando eu não pude estar com elas porque estava escrevendo.

Ao meu orientador, Doutor Nelson Rosenvald, que, enquanto professor, é sempre brilhante e instigante, e, atualmente é um dos principais responsáveis por promover uma cultura que garanta a proteção de dados pessoais dos cidadãos brasileiros. Obrigada por ser um ser humano tão gentil e compreensivo.

Ao meu eterno mestre que se tornou um amado amigo, Danilo Doneda, que me deu todo apoio, inspiração sobre o tema proteção de dados pessoais e uma visão crítica sobre o sistema. Deus sabe como a sua partida ainda está doendo e me fez parar (justamente) por uma semana os trabalhos para orar por você e por sua saúde e tentar fazer o possível (eu queria mesmo o impossível) para você ficar bem. Os seus áudios gravados em substituição, diante da impossibilidade repentina de você não poder se fazer presente na minha qualificação, ecoarão para sempre na minha vida profissional e no meu coração. Seu exemplo de mestre e ser humano são imperativos.

Aos Professores do mestrado, gratidão e a expectativa de poder encontrá-los sempre.

Aos Professores Doutores que compõem a minha banca de defesa. Eduardo Magrani e Luciana Brasileiro pelo carinho e pelas contribuições valiosas.

A todos os Professores e Coordenadores do Instituto Brasiliense de Direito Público (IDP), em especial o Professor Gilmar Ferreira Mendes. Tão importante para os profissionais brasileiros nos proporcionando um modelo de ensino internacional e altamente qualificado.

“Muito embora a discussão acadêmica seja fundamental para identificarmos os sistemas, ela deve estar voltada às demandas que estão surgindo para nós “(DONEDA, 2022).

## RESUMO

O tratamento de dados pessoais é um dos temas mais estudados na atualidade devido à dependência da sua utilização por parte da atual economia tecnológica e globalizada, movida a dados pessoais, que são a projeção da personalidade dos indivíduos. Por isso, sua proteção como direito fundamental frente às possibilidades de uso destes dados para fins discriminatórios. O objeto desse estudo é a crescente utilização da tecnologia da informação para o processamento dos dados pessoais com propósito de atingir a máxima eficiência nos processos de diversas áreas. O objetivo central deste trabalho consiste em examinar, à luz do Direito, a natureza do *credit score* e sua relação com a inteligência artificial, com o direito do consumidor, o código civil e a Lei Geral de Proteção de dados Pessoais para o delineamento da responsabilidade civil dos atores que tratam dados pessoais tradicionais e alternativos para compor uma nota de crédito e utilizá-la para fins discriminatórios na atual sociedade tecnológica. A metodologia é pautada na concatenação entre pesquisa bibliográfica e documental, análise jurisprudencial e cotejamento entre as legislações nacional e estrangeira para investigar a responsabilidade civil no compartilhamento de dados pessoais dos consumidores com desvio de finalidade resultando em discriminações. Foi utilizado como caso concreto da Serasa Experian. Constatou-se que há influência determinante da utilização de robôs na formação do perfil, nota de crédito. Diante disto, por score de crédito ser hoje uma ferramenta que utiliza-se de big data para a conformação desse perfil, portando cuida-se de inteligência artificial. Dessa forma, harmonizando os demais ordenamentos legais do microssistema da proteção de dados pessoais e com a Constituição Federal, por uma análise sistemática, entendeu-se que a responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do score para fins discriminatórios ao consumidor é objetiva. Destaca-se a necessidade de mais observância ao devido processo legal e mais produtividade em face do grande volume de dados manuseados através do Big Data, posto que constatado o vício do consentimento na sociedade tecnológica é preciso garantir a transparência e com ênfase no direito à explicação aos titulares de dados pessoais. Pôde-se observar que os principais problemas no tratamento automatizado para formação do credit score enfrentados pelos titulares são vinculados à falta de transparência quanto aos critérios utilizados nos sistemas de classificação e avaliação. Além de prejuízos no âmbito econômico por obstruir o acesso ao crédito, a obscuridade nos processos automatizados implica, entre outros atentados à dignidade da pessoa humana, possibilidades de discriminação social, etária, étnica e de gênero. Para minorar essa condição desfavorável ao cidadão, propõe-se à Autoridade Nacional de Proteção de Dados Pessoais e aos legisladores a promoção para a adoção de melhores práticas para maior controle, previsibilidade e explicabilidade nos processos automatizados que formam o credit score, sobretudo no processo de concepção do PL 21/2020 que trata da regulação da inteligência artificial no Brasil. Posto que a proteção de Dados é um direito fundamental e a responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do score para fins discriminatórios ao consumidor precisa ser combatida.



**Palavras-chave**: Proteção de dados; Responsabilidade civil; compartilhamento; discriminação; Credit score.

## ABSTRACT

The processing of personal data is one of the most studied topics today due to the dependence on its use by the current technological and globalized economy that is driven by personal data. And, as these are the projection of the personality of individuals, their protection is necessary as a fundamental right in view of the possibilities of using these data for discriminatory purposes. In this context, this dissertation has as object of study the increasing use of information technology for the processing of personal data with the purpose of achieving maximum efficiency in the processes of several areas. The main objective of this work is to examine, in the light of law, the nature of the credit score and its relationship with artificial intelligence, with consumer law, the civil code and the General Law for the Protection of Personal Data for the outlining of responsibility civil rights of actors who process traditional and alternative personal data to compose a credit note and use it for discriminatory purposes in today's technological society. For this purpose, a methodology based on the concatenation of bibliographical and documentary research, jurisprudential analysis and comparison between national and foreign legislation is used to investigate civil liability in the sharing of personal data of consumers with misuse of purpose resulting in discrimination. For this purpose, the concrete case of Serasa Experian was also taken, for example. As a result of this research, it was found that there is a determining influence of the use of robots in the formation of the profile, credit score. In view of this, because credit scores are now a tool that uses big data to create this profile, therefore taking care of artificial intelligence. Thus, harmonizing the other legal orders of the personal data protection microsystem and with the Federal Constitution, through a systematic analysis, it was understood that civil liability for deviation from the purpose of credit protection in the use of the score for discriminatory purposes against the consumer it is objective. And from everything analysed, attention was drawn to the need for greater compliance with due legal process and more productivity in the face of the large volume of data handled through Big Data, since once the vice of consent has been verified in the technological society, it is necessary to guarantee the transparency and with an emphasis on the right to explanation for holders of personal data. It could be observed that the main problems in the automated treatment for the formation of the credit score faced by the holders are linked to the lack of transparency regarding the criteria used in the classification and evaluation systems. In addition to economic losses by obstructing access to credit, obscurity in automated processes implies, among other attacks on human dignity, possibilities of social, age, ethnic and gender discrimination. To alleviate this unfavorable condition for the citizen, it is proposed to the National Authority for the Protection of Personal Data and to legislators to promote the adoption of best practices for greater control, predictability and explainability in the automated processes that form the credit score, especially in the process of conception of PL 21/2020 that deals with the regulation of artificial intelligence in Brazil. Since data protection is a fundamental right and civil *liability* for deviation from the purpose of credit protection in the use of the score for consumer discriminatory purposes needs to be fought.



**Keywords:** Data protection; Civil *responsability*; sharing; discrimination; credit score.

## LISTA DE ILUSTRAÇÕES

## LISTA DE TABELAS

**SUMÁRIO**

# 1 INTRODUÇÃO

O presente estudo se debruça sobre um dos temas mais fecundos hoje no direito. A proteção de dados pessoais, posto que se trata de direito fundamental, inserido no contexto da coleta massiva e compartilhamento de dados de consumidores entre organizações *versus* o fomento da tecnologia e inovação. A chamada era do capitalismo de vigilância, tem suas bases, avanço e cresce em poder à medida que coleta dados pessoais e influência comportamentos. É expropriar direitos humanos críticos que podem ser mais bem compreendidos como um golpe vindo de cima: uma destituição da soberania dos indivíduos. (ZUBOFF, 2021).

Trazendo para o contexto brasileiro, titulares de dados podem ser empregados, funcionários de organizações ou consumidores. Considerando essa última categoria para fins da presente dissertação. Nessa linha, tem-se a nota de crédito de cada um, o chamado *score* de crédito como um dado pessoal.

Assim, utilizar o *score* de crédito de forma indevida, desviando a sua finalidade para fins discriminatórios e abusivos ou opacos viola os direitos fundamentais, especialmente de privacidade e proteção de dados pessoais do consumidor, e enseja que tipo de responsabilidade civil?

O *score* de crédito é criado a partir da coleta e análise de diversos dados pessoais, com a finalidade de proteção ao crédito, porém, quando utilizado para fins diversos, como a venda de dados, o compartilhamento de informações sensíveis e para negar direitos por motivos discriminatórios, torna-se um meio violador de direitos fundamentais, principalmente de privacidade e proteção de dados do consumidor.

Ainda que tenha sido criado através do cruzamento de dados coletados a respeito do consumidor, o *score* de crédito não é um banco de dados pessoais e o seu compartilhamento, assim como o do conteúdo que o compõe, não é considerado como atentatório aos direitos e garantias fundamentais, inclusive sendo desnecessário o consentimento para estas ações, como defendido pelo Superior Tribunal de Justiça através da Súmula nº 550.

A importância deste trabalho está no fato de que os titulares de dados, especialmente consumidores, que são vulneráveis na relação de consumo, encontram-se ainda mais desprotegidos quando se trata da proteção de dados pessoais, já que a legislação recente permite o tratamento de dados pessoais para fins de proteção ao crédito, não necessitando do consentimento do consumidor para formular o *score* de crédito. Além da opacidade dessa formulação, os dados pessoais podem ser compartilhados e até vendidos, dessa forma havendo

o claro desvio de finalidade e risco aos direitos fundamentais.

O presente trabalho tem como objetivo principal analisar os impactos do *score* de crédito no sistema jurídico brasileiro, em particular sua aplicabilidade frente ao sistema de proteção ao direito do consumidor e a novel lei geral de proteção aos dados que abriu perspectivas de novos caminhos para a efetividade da responsabilização civil na proteção de dados pessoais. Hoje um direito fundamental autônomo.

O presente trabalho possui como objetivos específicos: analisar a lei geral de proteção de dados no contexto europeu; estudar o surgimento da lei geral de proteção de dados no Brasil e a sua garantiaPRINCIO como direito fundamental; compreender a responsabilidade civil por danos causados ao consumidor no âmbito da Lei geral de proteção de dados; analisar qual a espéciede responsabilidade civil por compartilhamento de dados do consumidor a partir do ordenamento brasileiro. Assim, é necessário desenvolver o estudo do surgimento da lei geral de proteção de dados no Brasil e a sua garantia como direito fundamental e a compreensão acerca da responsabilidade civil por danos causados ao consumidor pelo compartilhamento de dados pessoais. Diante da ausência ou da determinação dos limites da responsabilidade civil neste tema no ordenamento brasileiro, faz-se necessário buscar subsidiariamente respostas a esta lacuna legal na Regulamento Geral de Proteção de dados pessoais Europeu.

Para responder aos questionamentos mencionados, sobretudo investigar se a principal modificação introduzida pela lei complementar nº 166/2019 na lei nº 12.414/2011- relativa à previsão da possibilidade das pessoas físicas e jurídicas serem incluídas nos bancos de dados de cadastro positivo sem sua prévia solicitação - pode de fato causar danos a sua privacidade e à proteção seus dados pessoais (elevada à categoria de direito fundamental pelo Supremo Tribunal Federal e confirmada posteriormente através de emenda constitucional), serão utilizadas basicamente três estratégias metodológicas.

1. Uma abordagem hipotético dedutiva. Partindo-se de hipóteses gerais para casos particulares. Das hipóteses teóricas de violação de direitos à privacidade e à proteção de dados aos casos específicos contidos na legislação que permitiu o *score* de dados. 2. Será realizado um estudo com referências estrangeiras. Principalmente entre a lei geral de proteção de dados e o Regulamento Geral de Proteção de dados pessoais europeu. Por esta ser considerada uma legislação subsidiária daquela no ordenamento pátrio, tal comparação se faz necessária para avaliar como é aplicada a responsabilidade civil no âmbito da proteção de dados pessoais e o *score* de crédito no âmbito europeu e americano. Este último com influência direta no Código de Defesa do Consumidor brasileiro. 3. Pretende-se ainda realizar uma pesquisa da legislação, da doutrina e da jurisprudência brasileira, cotejando-as com as de outros países, de forma

particular com as da união europeia, posto que seu regulamento geral sobre a proteção de dados (RGPD) forneceu o embasamento teórico à nossa lei geral de proteção de dados pessoais - Lei nº 13.709, de 14 de agosto de 2018. Ademais, será realizado um cotejo do novo normativo brasileiro à luz da Constituição Federal de 1988, confrontando a legislação infraconstitucional com o fundamento da dignidade da pessoa humana (art. 1º, III, da Constituição Federal de 1988) e com as garantias fundamentais (art. 5º da Constituição Federal de 1988).

Por fim a pesquisa documental será realizada, concomitantemente, com um amplo levantamento de informações, examinando-se o processo de elaboração do *score* de crédito, a alimentação da base de dados do mesmo, os algoritmos utilizados e, finalmente, os critérios envolvidos no compartilhamento.

O método hipótetico-dedutivo é uma modalidade de método científico que parte de um problema ou lacuna no conhecimento científico, para formular hipóteses através de um processo de inferência científica, que prevê a ocorrência de fenômenos abrangidos pela hipótese (PRODANOV; FREITAS, 2013). Assim, por considerar uma lacuna no ordenamento brasileiro, bem como na doutrina, formulando hipóteses a serem investigadas acerca da responsabilidade civil e inferidas através do ordenamento jurídico europeu, tal método é o mais adequado neste trabalho.

No desenvolvimento desta pesquisa, buscando atender os objetivos determinados, serão utilizados como marco teórico textos de autores como: Danilo Doneda, Laura Schertel, Nelson Rosenvald, entre outros. Como principais referências legais à lei geral de proteção de dados pessoais e o Regulamento Geral de Proteção de Dados pessoais europeu.

# 2 A LEI GERAL DE PROTEÇÃO DE DADOS E A SUA ORIGEM

## 2.1 A Lei Geral de Proteção de Dados no contexto europeu

A privacidade da informação como questão de política pública é bastante moderna, tendo surgido na década de 1970, mais ou menos na mesma época em que a "proteção de dados" (derivada do alemão, *datenschutz*) entrou no vocabulário dos especialistas europeus. A questão estava intrinsecamente ligada à ampliação da capacidade de processamento de informações dos computadores e à necessidade de construir salvaguardas de proteção em um momento em que grandes projetos nacionais de integração de dados estavam sendo contemplados pelos governos (FLAHERTY, 1989), levantando temores de um "*Big Brother*" onisciente. O Estado com poder de vigilância sem precedentes.

O termo "proteção de dados" derivou da Lei alemã no início dos anos 70. Diante da preocupação com o aumento da capacidade de processamento de dados dos computadores e a necessidade de proteger os cidadãos do poder do Estado de concentrar tantas informações dos indivíduos em suas mãos, que passava a controlar e vigiar a população sem precedentes. Até onde se tem registros, foi a Alemanha que editou a primeira Lei de Proteção de Dados pessoais do mundo, em 1970, no Estado alemão de Hesse.

> Alemanha pode ser considerada um dos países que apresenta o maior desenvolvimento doutrinário e valorização quanto à proteção de dados, sendo que o tema apresenta tamanha importância que pode até mesmo ser classificado como um instituto autônomo (Datenschutz) no universo jurídico daquele país. A primeira lei no mundo sobre o assunto foi editada em 1970 pelo estado alemão de Hessen. No ano de 1977, o Parlamento alemão aprovou lei federal de proteção de dados (Bundesdatenschutzgesetz). Todavia, o ápice do reconhecimento da proteção de dados ocorreu com a decisão do Tribunal Constitucional Federal sobre a questão do censo demográfico que se realizava na Alemanha no ano de 1983 (Volkszählungsurteil). Esta decisão estabeleceu o direito fundamental à autodeterminação informativa (Grundrecht auf informationelle Selbstbestimmung) (MENKE, 2019, p.781).

Desde então, a Alemanha é autoridade no desenvolvimento do tema e como país membro da união europeia, tem importante contribuição como fonte para a edição do Regulamento Geral de Proteção de Dados em temas que são a pedra fundamental do regulamento europeu. Direitos dos titulares de dados consagrados no Regulamento Geral de Proteção de Dados foram derivados dos princípios e regulamentos da Lei Federal de Proteção de Dados Alemã (BDSG). A título de exemplo, os relativos ao tratamento de dados pessoais, consagrados no artigo 5. do Regulamento Geral de Proteção de Dados que versam sobre

licitude, limitação de finalidade, minimização de dados, exatidão, limitação de armazenamento, integridade, confidencialidade e a responsabilidade dos agentes de tratamento de dados.

Esses princípios fundamentais operam tanto como regras legais de pleno direito, quanto como padrões orientadores para o equilíbrio dos direitos de privacidade com os interesses organizacionais legítimos (BYGRAVE, 2002, p. 57).

Durante esses primeiros debates em torno de promover a proteção de dados, se verificou que esse não era simplesmente um problema de um país isoladamente. A crescente facilidade de realizar transferência internacional de dados demandou dois acordos internacionais na década de 1980 para regular o fluxo transfronteiriço de dados pessoais: as Diretrizes de 1980 da Organização para Cooperação e Desenvolvimento Econômico (OCDE, 1980) e a Convenção de 1981 do Conselho da Europa.

A evolução regulatória histórica do princípio da privacidade no âmbito da edição do Regulamento Geral de Proteção de Dados teve início em 1948 com a Declaração Universal de Direitos Humanos, adotada pela Assembleia Geral da Organização das Nações Unidas, que estabeleceu os fundamentos de liberdade, justiça e paz no mundo, caracterizando os direitos inalienáveis. A partir disso, reconheceu-se os valores de proteção da privacidade individual e familiar (Artigo 12) e a liberdadede informação, opinião e de expressão (Artigo 19) que são inspirações de todas as leis protetivasde dados pessoais (ONU, 1948).

Já em 1950, surgiu a Convenção Europeia de Direitos Humanos, fundada nos valores da Declaração Universal dos Direitos Humanos da Organização das Nações Unidas, cujas disposições ecoaram as proteções à vida privada e familiar e à informação, bem como permitiu à autoridade pública ingerência nesses direitos, estabelecendo como limites a segurança nacional e pública, bem-estar econômico, preservação dos direitos e das liberdades de terceiros, entre outros.

Nos anos de 1973 e 1974, o Conselho de Europa editou as Resoluções 22 (1973) e 29 (1974), estabelecendo princípios de proteção de informações pessoais em bancos de dados automatizados em todos os setores.

Em 1979, os até então sete membros da Comunidade Europeia passaram a implementar leis nacionais de privacidade, além da Dinamarca, França, Alemanha, Luxemburgo e Noruega. Áustria, Espanha e Suécia incorporaram a proteção de dados ao texto constitucional ou editaram leis com status constitucional também.

Meados de 1980, foram criadas as Diretrizes da Organização Mundial de Comércio sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais. Tais diretrizes,

que são recomendações, auxiliaram na harmonização das legislações nacionais (dos membros e dos países interessados em ingressar na Organização) sobre privacidade e fluxo internacional de dados.

Já em 1981, foi realizada a Convenção 108, que tinha como objetivo consolidar as Resoluções 73/22 e 74/29. Por isso, criou o Conselho da Europa a Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais, o primeiro instrumento internacional disciplinando especificamente essa temática com força legal, aberto a membros e não membros da Comunidade Europeia.

Na década de 1990, a pretensão de harmonização foi estendida através da Diretiva de Proteção de Dados da União Europeia de 1995 (UE, 1995), cujos artigos 25 e 26 estipulavam que os dados pessoais de europeus deveriam fluir apenas para fora das fronteiras da União para países que pudessem garantir um "nível adequado de proteção". Através da Diretiva de Proteção de Dados, a harmonização da proteção de dados se estendeu geograficamente e se aprofundou em significado e conteúdo (BENNETT, 1997). Dessa forma, países foram aderindo aos novos padrões de harmonização independentemente da localização geográfica.

No final da primeira década do século 21, no entanto, a Diretiva de Proteção de Dados da União Europeia já não atendia às novas demandas tecnológicas como o advento da internet, redes sociais e a utilização do marketing direcionado (*microtargeting*). Além de aspectos legais de cumprimento pelos países e organizações.

A falta de harmonização e uniformização da interpretação da Diretiva gerou divergências em países de toda a Europa, dificultando o andar da economia. Sobre a diretiva 95/46 da Comissão Europeia:

> Convenção 108 não compreendia todos os aspectos necessários para uma ampla e densa disciplina de proteção da privacidade, o que levou a Comissão Europeia, provocada por seu Parlamento Europeu, a editar um novo documento. Essa Diretiva foi, por mais de 20 anos, o principal documento internacional sobre o assunto. (COMISSÃO EUROPEIA, 1995).

O "regime de adequação" não rendeu um número significativo de países para os quais as organizações europeias podiam transferir legalmente dados pessoais. Abordagens alternativas para a transferência legal, baseadas em princípios de "responsabilidade" organizacional (GUAGNIN et al., 2012) surgiram e se tornaram consagradas dentro de um sistema de Regras de Privacidade Transfronteiriça (CBPR) legitimado através da Cooperação Econômica Ásia-Pacífico (APEC, 2005).

Foi proposto pela primeira vez em 2012 o estabelecimento de um conjunto uniforme

de regras que proporcionariam maior proteção aos cidadãos, promoveriam a inovação no Mercado Único Europeu e tornariam a União Europeia, segundo a Comissária Jourova, “adequada à era digital”. (EUROPEAN COMMISSION, 2015).

Durante quatro anos de negociações políticas e econômicas, pois havia inúmeros interesses de grupos multinacionais em jogo, finalmente, em abril de 2016, o Regulamento Geral de Proteção de Dados foi aprovado pelo Parlamento Europeu. Contudo, só entrou em vigor em 25 de maio de 2018, com 99 capítulos. Esse período de vacância foi dado para que os setores públicos e privados pudessem atingir a conformidade com o regulamento que impunha treinamento, tecnologia, implementação de processos, prestação de contas e orçamento.

> [...] substituindo a Diretiva 95/46/CE, bem como leis e regulações nacionais nela baseadas. Diferentemente da Diretiva, a Regulação é autoaplicável e nãorequer a aprovação de leis nacionais compatíveis com suas determinações. Seu objetivo e eliminar inconsistências em leis nacionais, ampliar o escopo de proteção à privacidade e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, com aqueles decorrentes do advento da internet.(MALDONADO, 2019, p. 21).

Em dezembro de 2016, o Parlamento e o Conselho da União Europeia finalmente concordaram sobre o Regulamento Geral de Proteção de Dados, um regulamento proposto pela primeira vez em 2012, em vigor desde 25 de maio de 2018, o Regulamento Geral de Proteção de Dados oferece uma nova estrutura para proteção de dados com maior responsabilidade para as organizações e seu alcance é extraterritorial. Dado o tamanho e a abrangência da economia da União Europeia, o Regulamento Geral de Proteção de Dados se tornou rapidamente um padrão global de proteção de dados que todo profissional da privacidade em atividade deve entender em algum nível. (FOX et. al., 2019).

A estrutura do Regulamento Geral de Proteção de Dados está dividida em 173 considerandos, os quais contextualizam, direcionam e orientam a interpretação dos fundamentos, requisitos e princípios do Regulamento. A segunda parte do Regulamento Geral de Proteção de Dados é composta por 11 capítulos e 99 artigos nos quais são estabelecidos os fundamentos, requisitos e princípios que devem ser seguidos e cumpridos pelas pessoas naturais ou jurídicas que tratem de dados pessoais de pessoas naturais, de forma a garantir a proteção dos direitos e garantias fundamentais do cidadão que esteja no território europeu. (UNIÃO EUROPEIA, 2016).

O Regulamento Geral de Proteção de Dados tem um alcance territorial que envolve 28 países membros da União Europeia e outros três países que integram o espaço econômico europeu (Noruega, Islândia e Liechtenstein), sendo aplicada, independentemente, da

nacionalidade do titular dos dados pessoais ou do local de sua residência. (MALDONADO, 2019, p. 22).

Em uma visão objetiva, o Regulamento Geral de Proteção de Dados defende direitos e liberdades fundamentais dos indivíduos, nomeadamente o seu direito à proteção dos dados, estabelecendo regras para seu tratamento e ao mesmo tempo, promovendo a livre circulação desses dados de maneira segura. Do ponto de vista material, o regulamento se aplica ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em arquivos ou a eles destinados.

Mais do que instituir padrões e editar lei para regular a proteção de dados pessoais na Europa, o Regulamento Geral de Proteção de Dados justifica e impõe a adesão dos países mesmo fora da União Europeia, como o Brasil, aos padrões de privacidade. Padrão esse considerado uma condição necessária para a participação na economia internacional em rede. O Regulamento Geral de Proteção de Dados e seus desdobramentos pode ser, dessa forma, pensada como um instrumento para a globalização dos padrões de privacidade e proteção de dados.

## 2.2 O Direito fundamental à proteção de dados pessoais

Numa perspectiva histórico-normativa inicial, dá-se conta de que se passou meio século da primeira lei de proteção de dados pessoais do mundo, tendo como berço a Alemanha, no Estado de Hesse, no início da década de 1970. Merece o devido realce nesse processo, o parecer de Steinmuller solicitado pelo Ministério do Interior da Alemanha. (STEINMÜLLER et. al., 1971, p.88).

No documento, Steinmuller fundamenta as bases do direito fundamental à proteção de dados pessoais. Mesmo ainda em sede de doutrina e lei estadual, ele consegue extrair da constituição alemã um direito de autodeterminação do cidadão, que pode decidir quais informações individuais ele fornece a quem, sob que circunstâncias, e alerta para o risco do processamento automatizado desses dados. (STEINMULLER et al.,1971, p. 88).

Em continuidade em 1983, uma decisão da Suprema Corte Constitucional Alemã sobre a lei do Censo à época, lançou de fato a proteção de dados pessoais ao status de direito fundamental, ainda que não expressamente positivado, mas trazendo essa proteção de maneira indireta ao consagrar o direito fundamental à autodeterminação informativa. Que, traduzindo, seria o direito de proporcionar ao indivíduo o controle dos seus dados pessoais, o que

indiretamente lhe empodera e garante proteção a essas informações pessoais. Assim, foi fomentada a base da proteção de dados pessoais para um direito autônomo com o reconhecimento dessa autodeterminação informativa.

Na sentença referente ao recenseamento da população, o Tribunal Constitucional retomou tanto a abordagem da autodeterminação quanto a noção da limitação do comportamento por meio do processamento não transparente dos dados, a fim de conceber a partir do artigo 2, parágrafo 1 c/c artigo 1, parágrafo 1, Lei Federal (dignidade da pessoa humana), o direito fundamental à autodeterminação informativa. Esses dois elementos marcam a dogmática deste direito até hoje, embora esta vinculação seja o objeto de forte crítica no Direito. (SCHERTEL, 2020).

Da jurisprudência alemã para cá, esse risco do processamento automatizado de dados aumentou exponencialmente. Para se ter uma ideia, das cinco maiores empresas mais lucrativas do mundo na lista da revista Forbes, duas delas tratam basicamente dados pessoais como atividade principal e as outras três, vendem produtos como computadores e apetrechos que tratam dados. Apple, Google, Microsoft, Amazon e Facebook. (FORBES, 2020).

Esse crescimento do processamento automatizado de dados se revela tão alarmante, a ponto da revista The Economist, ainda em maio de 1999, anunciar em matéria de capa o fim da privacidade, tendo em vista o avanço e o desenvolvimento da internet, além de outras tecnologias que coletam e processam dados o tempo todo, transformando-os em informação e vigiando o cidadão o tempo todo. (THE ECONOMIST, 1999).

Corroborando com esse raciocínio de que a economia é movida a dados e discutindo quais os riscos disso, a professora e pesquisadora na Harvard Business School, Shoshana Zuboff, em seu livro “A Era do Capitalismo de Vigilância”, conta que todos vivem uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas. Shoshana de fato, escancara as ameaças do século XXI e vai além nas suas conceituações sobre os perigos para todas as pessoas, enquanto seres humanos. (ZUBOFF, 2020).

Para a autora, trata-se de uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos.

Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural dos séculos XIX e XX. (ZUBOFF, 2020). Mas, agora os seres humanos são o produto. Um conjunto de dados a ser explorado, manipulado, expropriado por ela, ou seja, há algumas evidências de que o direito em sentido amplo precisa

se atualizar sempre e, no caso, diante dos riscos impostos aos direitos fundamentais como privacidade e proteção de dados, face às novas tecnologias que emergem sucessiva e velozmente há décadas, mais precisamente desde o final do século XIX, como ilustrado no quadro abaixo da Maastricht University.

A Figura é um mapeamento evolutivo da tecnologia e as respostas legislativas diante do surgimento de necessidades dos indivíduos, que ameaçados em sua essência, reclamam coletivamente por novas garantias, traduzidas em direitos. Com a evolução tecnológica, o indivíduo se encontra cada vez mais cercado, vigiado, dependente, dominado e inserido, como produto no mundo globalizado, interligado pela economia movida a dados pessoais. Nesse contexto, a produção legislativa tenta acompanhar a evolução tecnológica, com a sucessiva edição de leis, acordos e normas de proteção à pessoa (Figura 1).

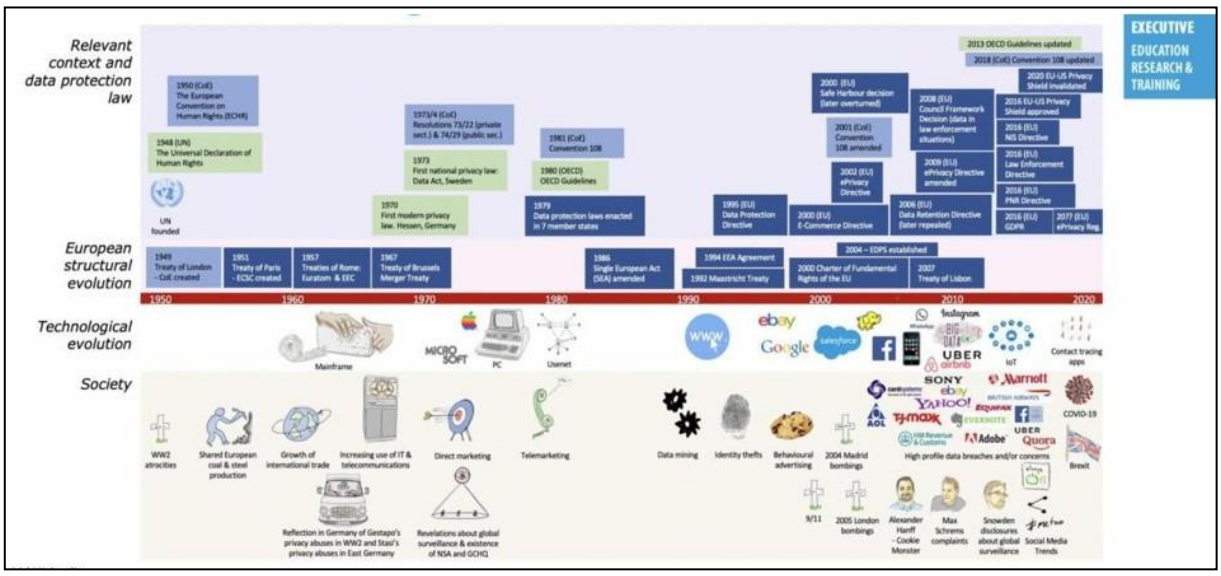


Figura 1 - The context & challenges[1]

A imagem apresentada na Figura 1 retrata, em três paralelos, a evolução da sociedade desde as atrocidades cometidas contra pelo menos oito milhões de judeus, cujos dados foram divulgados e serviram de motivo para que fossem assassinados, passando pelo desenvolvimento das telecomunicações, as estratégias de *marketing* direto, mineração de dados e propaganda comportamental. Essa tecnologia de tratamento de dados evolui exponencialmente, fomentada pelo uso da internet, redes sociais e o fenômeno do *big data* e o surgimento das *big techs*, grandes empresas de tecnologia.

[1] Fonte: Maastricht University (2022).

> Entende-se por uma ferramenta tecnológica capaz de processar os dados obtidos de diversas fontes e organizá-las. Na sequência, cataloga as informações e obtém um produto, que será usado estrategicamente por um sujeito nas tomadas de decisões (BRAGA; FERREIRA, 2019).

Em contraponto, observa-se a evolução da União Europeia que, desafiada pelas necessidades e transformações da sociedade, vem legislando proporcionalmente a cada nova ameaça a estes direitos fundamentais e humanos.

Posto que o direito fundamental à proteção de dados está na essência do direito humano e deve, portanto, receber o status de um novo direito humano.

Direitos humanos são aqueles direitos que cada ser humano deve ter e que são protegidos em virtude do direito internacional global ou regional por meio de convênios ou convenções, mas nem sempre pelos tribunais. (ARNAULD; DECKEN; SUSI, 2020). É exatamente assim que se comporta o direito à proteção de dados pessoais que é protegido internacional e globalmente, não somente no escopo normativo adotado pelo conjunto de países que compõem a União Europeia, mas também pela adesão à sua influência, em especial do Regulamento de Proteção de Dados Pessoais Europeu, o GDPR, transpõe barreiras territoriais, inspira, se impõe, e serve de guia para mais de 120 países pelo mundo, formando uma rede internacional global de proteção a esse novo direito humano: a proteção de dados pessoais.

Em reforço factual, a Figura 2 apresenta um esquema cronológico e evolutivo da proteção de dados convencionado pelos países do bloco europeu.

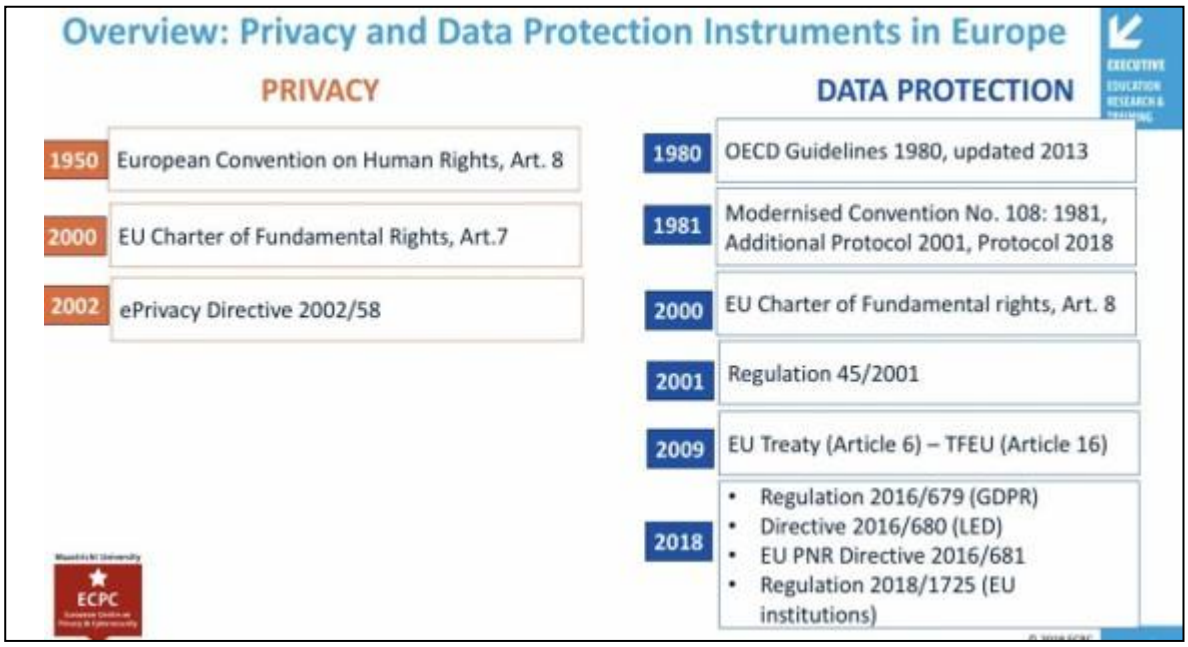


Figura 2 - Overview: privacy and data protection instruments in Europe[2]

Aproveitando o gancho do esquema legal acima exposto e as considerações sobre proteção de dados pessoais e direitos humanos, vale rememorar agora um pouco a história, um século antes, com alguns casos que se tornaram clássicos no estudo pré-proteção de dados pessoais. Ou seja, antes de ele ser objetivamente assim interpretado, extraído, positivado, para que se possa vislumbrar melhor essa transição de direitos, ou como se pode também hipotetizar, a transformação e a mutação para proteger com mais robusteza os indivíduos frente aos sucessivos desafios que se renovam. Esse caminho passou pelo direito à propriedade, transmutando-se pela privacidade, e derivando para a autodeterminação informativa de onde teria sido extraído o termo proteção de dados. Hoje ambos seguem intrinsecamente relacionados, coexistentes, porém significativamente diferentes e com conceitos sendo ainda amplamente discutidos na Alemanha (MENKE, 2020). A diferença, com base na doutrina alemã, consiste na compreensão de que a autodeterminação informativa não é a propriedade sobre os dados pessoais.

O mais adequado é que se considere os dados relacionados a uma pessoa como resultado de uma observação social ou de um processo de comunicação social multirracional (ROSSNAGEL, 2003, p. 8.) Como modelos da realidade, teriam os dados pessoais sempre um autor e um objeto. Os dados têm relação com um objeto, mas também com o autor. Não podem ser associados exclusivamente ao objeto e o direito à proteção de dados

[2] Fonte: Maastricht University (2022).

intrinsecamente relacionado à autodeterminação informativa: “consiste num ordenamento sobre a informação e a comunicação a eles relacionada, determinando quem, em qual relação, e em que situação, está autorizado a lidar com os modelos de uma determinada pessoa de uma determinada maneira”. (ROSSNAGEL, 2003, p. 8.) Na certeza dessa evolução legal e doutrinária se tem a consequente garantia da proteção de dados pessoais como um direito humano.

Concluindo o adendo sobre a coexistência e diferenças entre proteção de dados e autodeterminação informativa, será tratado a seguir sobre a evolutiva pré-proteção de dados.

Na Inglaterra em 1818, no caso Goe v. Pritchard, cartas e segredos sobre as comunicações entre a madrasta, a senhora Gee, e seu enteado, o reverendo Pritchard, viraram motivo de contenda. Depois de possíveis desentendimentos, o reverendo tentou publicar essas cartas e a madrasta dele foi à justiça, sob o argumento de que isso iria ferir seus sentimentos. Na decisão judicial, a tutela concedida foi a de propriedade, tendo em vista as leis civis vigentes entendiam até então a propriedade privada como um espaço que tinha que ser preservado, e que essa garantia decorreu sociologicamente do comportamento do homem quando deixou de ser nômade para se fixar numa porção territorial, coabitando para viver e produzir. “O primeiro sentimento do homem foi o de sua existência, sua primeira preocupação, a de sua conservação. As produções de terra forneciam-lhe todos os socorros necessários, o instinto levou-o a utilizar- se deles” (ROUSSEAU, 1991).

Dessa forma, da ideia de propriedade do território, do espaço, para o que é propriedade, de relativo à alguém, portanto, privado, já foi naquele momento se transmutando, ampliando-se dado o caso concreto que não podia ficar sem apreciação e solução legal.

> Quando a senhora Gee toma ciência do interesse do reverendo Pritchard em publicar estas cartas, ela vai ao Judiciário buscar por via de ordem judicial, restringir esta publicação, inibi-la. E consegue, mas o consegue sob o argumento do direito à propriedade. Ela argumenta que poderia ter sentimentos pessoais feridos, que teria divulgado informações que não precisam ser do conhecimento público, e isso se torna menos relevante diante do argumento da sacrossanta propriedade (CATALAN, 2021).

Mas uma possível noção de privacidade só foi mais claramente delineada, realçada e refletida até as gerações atuais, mesmo que naquele tempo ainda fora do ambiente de positivação jurídica, num manifesto pelo direito de ser deixado só, por Warren e Brandeis, na *Harvard Law Rewiew*. O episódio acontecido nos Estados Unidos, em que uma fotografia exibida em um jornal sem o consentimento dos retratados numa festa de casamento, trouxe a noção de privacidade pela primeira vez, como um direito de ser deixado só, ou *Right to be*

*alone* de Warren e Brandeis, na *Harvard Law Rewiew*, em 1890. Em defesa, clamou-se assim:

> As mais recentes invenções e modelos de negócio apontam para os próximos passos que devem ser dados para a proteção das pessoas e para garantir lhes o direito de ser deixado só. As fotografias e os jornais de ampla circulação invadiram os espaços sagrados da vida privada e doméstica. Diversos dispositivos tecnológicos ameaçam fazer com que se cumpra a profecia de que aquilo que é sussurrado nos recintos domésticos será proclamado do alto dos telhados. (HARVARD, 1980).

Na sequência cronológica, outro caso pouco divulgado na linha do tempo da evolução da privacidade, e consequente proteção de dados, é o do príncipe Otto von Bismarck, um dos maiores estadistas alemães, responsável pela unificação do país. No episódio de sua morte, jornalistas teriam subornado funcionários para ter acesso ao corpo do príncipe dentro de sua própria casa, para tirar fotos e lucrar com isso. Seriam, numa analogia, esses profissionais como são conhecidos hoje os *paparazzi*. Mas, os herdeiros de Bismarck conseguiram um mandado de injunção que impediu não apenas a divulgação das fotos, como também a apreensão do material que poderia gerar a reprodução. Mesmo assim, a decisão judicial ainda foi baseada na ideia de proteção da propriedade privada.

Apesar dessas decisões acima citadas, que abarcaram a proteção dos indivíduos mesmo sob o argumento da proteção da coisa, a propriedade privada, foi só durante o século XX que o comportamento e a codificação do direito começaram a mudar. Foi a partir dos estudos sobre direitos da personalidade que irradiaram seus reflexos diretos sobre a privacidade.

No clássico ‘Os Direitos da Personalidade’, do italiano Adriano de Cupis, com citações de Bittar:

> Assim, DE CUPIS especifica e estuda, como da personalidade, os direitos: à vida e à integridade física; às partes separadas do corpo e ao cadáver; à liberdade; à honra e respeito ao resguardo; ao segredo; à identidade pessoal; ao título; ao sinal figurativo; e o direito moral do autor (BITTAR, 1978, p. 109-110)

Dessa forma, na citação acima referida se extrai como exemplo que o segredo que está na esfera mais sensível da proteção do indivíduo, juntamente com outros direitos como respeito ao resguardo, traduzem uma nova postura do direito civil centrada no ser humano e não mais na propriedade propriamente dita.

> O reconhecimento da necessidade de tutela dos valores existenciais da pessoa humana marca o direito do final do século XX. A concepção patrimonialista é superada e o Direito passa a proteger o homem e os valores que trazem encerrados, em si; a última ratio do Direito é o homem, deixando o direito civil de ser marcado pela propriedade, pelos contratos, pela família. O núcleo do direito é a pessoa humana; assim, os institutos jurídicos só se justificam se existirem em função do homem (BERTONCELO, 2006).

De lá para cá, são múltiplas e factuais as violações a direitos fundamentais criadas pela tecnologia que precisam ser freadas para ampliar a proteção à pessoa. Dos 130 anos passados desde o "*right to be alone",* o conceito subjetivo de privacidade, de comportar o tamanho e o significado dado pela medida de cada indivíduo não permite mesmo uma conceituação objetiva, mas a possibilidade de estender, de ampliar, extrair e derivar até hoje para outros direitos a partir da noção de privacidade. Como diz Francois Rigaux, "*L´impossible définition*". Sim, é impossível definirmos o que é privacidade. (DONEDA, 2017).

Mas como doutrina Doneda, é possível ampliar o leque de outros direitos a partir da noção de privacidade. Nunca foi tão importante essa subjetividade elástica e polissêmica de como se percebe a privacidade, pois dessa forma, foi possível mudar o eixo dessa proteção diante da velocidade das transformações do mundo digital. Se antes, a ideia era de privacidade individual, de segredo, de isolamento, hoje se tem um outro cenário: o do controle, do monitoramento, da vigilância, da classificação com a perfilhação, da influência e da discriminação das pessoas, que pode chegar a alterar sua própria essência.

Assim, reafirmando, a relação da necessidade de novas garantias frente às novas tecnologias, de fato, ampliou o conceito de privacidade que teve que se "metamorfosear", se transformar e trazer consigo também o caráter de horizontalidade dessa via de reclamação do direito em pauta, não só contra o Estado, mas também entre privados.

A crescente demanda de tutela ao longo do tempo também determinou a necessidade de estruturas normativas nacionais, internacionais e regulatórias.

Antes de se adentrar nessas estruturas a exemplo das legislações, vale sintetizar, para fins didáticos deste trabalho, as gerações de direitos à proteção de dados desde a década de 70, com os bancos de dados centralizados, a segunda geração no final dos anos 70, tendo a privacidade e proteção de dados como uma liberdade negativa, e depois a terceira geração nos anos 80, com a autodeterminação informativa alemã; e atualmente, na quarta geração, tem-se essa elevação do padrão coletivo da proteção.

De acordo com Paulo Bonavides, numa outra espécie de classificação, a clássica das gerações de direitos fundamentais, a proteção de dados estaria hoje na quarta geração que se adequa tão bem ao mundo globalizado, digitalizado e de vigilância constante dos indivíduos, em que é impossível ser deixado só.

> Deles depende a concretização da sociedade aberta ao futuro, em sua dimensão de máxima universalidade, para a qual parece o mundo inclinar-se no plano de todas as

> relações de convivência. [...] Tão somente com eles será legítima e possível a globalização política (BONAVIDES, 2004, p. 563).

Após contextualizar esse cenário, é possível elencar os princípios da proteção de dados que, mesmo surgidos fora do contexto europeu, o influenciaram e fazem parte dessa evolução. Os primeiros datam de 1973, com o Código de Práticas Leais americano, o *Fair Information Practice Principles* (FPC, 2022). Nele, os bancos de dados deviam seguir um conjunto de práticas guiadas pelos princípios da transparência, livre acesso, finalidade, correção, qualidade e segurança. Princípios esses que permaneceram e foram recepcionados pelas legislações atuais mundo afora, como por exemplo no Regulamento Geral de proteção de Dados europeu. (LIMA; PEROLI, 2021, p. 48).

No artigo do Regulamento Geral de Proteção de Dados europeu fica clara essa recepção e ampliação, elencando assim os princípios basilares do tratamento de dados pessoais que devem ser:

> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»); b) Coletados para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»); d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizacionais adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»); f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidastécnicas ou organizacionais adequadas («integridade e confidencialidade») (GDPR,2016).

O Regulamento Geral de Proteção de Dados Europeu prevê que os dados pessoais são objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados, o que nos remete, ao tratarmos inicialmente do princípio da Licitude, a indicação de que dados somente podem ser tratados de acordo com o que o Regulamento em estudo expressamente dispor, com relevância maior ainda ao seu artigo 6, o qual elenca as hipóteses de “licitude de

tratamento" (BRASIL, 2018).

Dessa forma, o tratamento de dados pessoais só é lícito se o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; se o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; se o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; se o tratamento for necessário para efeito dos interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Tendo em comento o registro da trajetória do direito fundamental à proteção de dados com sua história e metamorfoseamento ao longo do tempo por causa das pressões factuais da evolução da sociedade, da tecnologia e constante inovação, gerando necessidades e provocando o direito.

## 2.3 O consentimento e o *score* de crédito no âmbito europeu

De início, neste tópico que é de suma importância para o desenvolvimento deste trabalho, será delineado o que é o consentimento no regulamento de proteção de dados europeu, sua necessidade para o tratamento de dados pessoais para fins de avaliação de crédito e se há outras bases legais que podem ser usadas para esse tipo de tratamento.

Por outro lado, também será analisado o que vem a ser *score* de crédito, como ele é formulado, qual a sua natureza (dado pessoal ou não), a finalidade e como essa pontuação de crédito é regulamentada no âmbito do escopo legal da proteção de dados pessoais europeia. Observando-se, quais as repercussões dele para o titular de dados consumidor, nos seus direitos fundamentais face à utilização de processos automatizados como o *score* de crédito, um meio que utiliza inteligência artificial para a tomada de decisões.

Pela lei de proteção de dados europeia, o processamento de dados pessoais é geralmente proibido, mas pode ser feito em alguns casos. Um deles é quando o titular de dados tenha dado seu consentimento para o processamento ou por raras exceções previstas em lei. Para melhor conceituação e caracterização do termo consentimento, o Regulamento Europeu

elenca em sete artigos as suas definições, a legalidade, as condições de processamento com base no consentimento como as decisões automatizadas, perfilhamento.

O consentimento do titular dos dados significa tomada de decisão livre, específica, informada e inequívoca dos desejos do titular dos dados pela qual, por uma declaração ou por uma ação afirmativa clara, signifique que está de acordo com o processamento de seus dados pessoais relacionados, como bem definido no artigo 4 (11) do Regulamento Europeu. (GDPR, 2016).

A Legalidade do processamento, embora seja uma das bases legais mais conhecidas para o processamento de dados pessoais, o consentimento é apenas uma das seis bases mencionadas no Regulamento Geral de Proteção de Dados (GDPR). O processamento só será legal se e na medida em que o titular dos dados deu consentimento para o processamento de seus dados pessoais para um ou mais propósitos específicos, como dispõe o artigo 6 (1, a ) (GDPR, 2016).

As outras bases legais são: contrato, obrigações legais, interesses vitais do titular dos dados, interesse público e legítimo interesse, conforme estabelecido no Artigo 6(1) GDPR. Mas, nem todas elas, além do consentimento, poderão ser utilizadas para a formulação do *score* de crédito, conforme será visto mais adiante. Abaixo segue um estudo sobre consentimento.

Os requisitos básicos para a eficácia de um consentimento legal válido são definidos no Artigo 7. Já no art. 8 estão as condições aplicáveis ao consentimento da criança em relação aos serviços da sociedade da informação. No art. 9, o processamento de categorias especiais de dados pessoais. No art. 22, tomada de decisão individual automatizada, incluindo criação de perfil e por fim, no art. 49 as derrogações para situações específicas. (GDPR, 2016).

Somado a isso, os chamados Considerandos complementam a lei guiando e detalhando especificidades, condições e algumas situações especiais para a operabilidade adequada dessa base legal: (32) Condições de Consentimento (33) Consentimento para Certas Áreas de Pesquisa Científica (38) Proteção Especial de Dados Pessoais de Crianças (40) Legalidade do Processamento de Dados (42) Ônus da Prova e Requisitos de Consentimento (43) Consentimento Livre (50) Processamento Adicional de Dados Pessoais (51) Proteção de Dados Pessoais Sensíveis (54) Processamento de Dados Sensíveis no Setor de Saúde Pública (71). (GDPR, 2016).

Os requisitos para a eficácia de um consentimento legal válido no Artigo 7 do Regulamento Geral de Proteção de Dados Europeu, que reza: o consentimento deve ser dado livremente, específico, informado e inequívoco. Para ser livre, o consentimento deve ser dado

voluntariamente. De acordo com o Regulamento Geral de Proteção de Dados Europeu, "livre" implica uma escolha real pelo titular dos dados. Qualquer elemento de pressão ou influência inadequada, que possa afetar o resultado dessa escolha, torna o consentimento inválido. A ideia que se pode extrair daqui é entender que existem pontos de desequilíbrio numa relação titular/consumidor. Por isso importa que a proteção do consentimento livre almeje equilibrar a relação.

Para que o consentimento seja informado e específico, o titular dos dados deve pelo menos ser notificado sobre quem está de posse dos seus dados, que tipo de dados serão processados, como serão usados e a finalidade das operações de processamento. Lembrando que ainda há outras orientações no considerando 32 do Regulamento Geral de Proteção de Dados Europeu.

Por último, mas não menos importante, o consentimento deve ser inequívoco, o que significa que requer uma declaração ou um ato afirmativo claro. O consentimento não pode ser implícito e deve sempre ser dado por meio de um *opt-in*, uma declaração ou uma conduta ativa, para que não haja mal-entendidos de que o titular dos dados tenha consentido com o processamento específico, artigo 7 (GDPR, 2016).

O titular dos dados também deve ser informado sobre seus direitos (capítulo 3, artigos 12 ao 23 do Regulamento Geral de Proteção de Dados Europeu) como o de retirar o consentimento a qualquer momento, de maneira tão fácil e rápida quanto foi dá-lo. Dessa forma o titular de dados passa a gerir seu consentimento, dando-lhe autonomia em consonância com o princípio da autodeterminação informativa. Nas lições de Danilo Doneda (2006, p. 372): “a transferência da responsabilidade para o titular dos dados traz consigo a terceira geração de proteção de dados, na qual passa a ter papel central o consentimento do indivíduo para coleta e processamento de seus dados”, uma vez que diversos serviços como bancários e afins coletavam dados sensíveis de seus clientes, sem informar ao titular precisamente de qual forma se daria seu processamento e utilização.

Relevante no contexto deste tópico da dissertação é que, o controlador passou a ter o dever de, diante do consentimento, também informar o titular sobre o uso dos dados, seu processamento, os possíveis riscos de transferências de dados devido à ausência de uma decisão de adequação ou outras salvaguardas apropriadas, como passou a garantir a lei.

Nessa linha de estudo, o Regulamento Geral de Proteção de Dados Europeu diante das inovações tecnológicas e os riscos ao cidadão com o processamento de dados automatizado, colocou uma trava na barra de proteção, reforçando e valorizando a importância do consentimento para tal tratamento. A lei europeia também vislumbra mais duas possibilidades

para o processamento automatizado de dados vinculando-o ao surgimento de uma necessidade, que é a celebração ou execução de contrato, e a segunda, com base na Lei da União ou do Estado-Membro, que pode autorizar o processamento automatizado, incluindo a perfilização. Porém impõe precauções, a fim de proteger e deixar fora de perigo o indivíduo. "Art. 22 GDPR: O titular dos dados tem o direito de não estar sujeito a uma decisão baseada apenas no processamento automatizado, incluindo a criação de perfis, que produza efeitos legais sobre ele ou que o afete significativamente." (GDPR, 2016).

Contudo, o parágrafo 1º não se aplica se a decisão for necessária para celebrar ou executar um contrato entre o titular dos dados e um controlador de dados; for autorizada pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito e que também estabelece medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados; ou baseia-se no consentimento explícito do titular dos dados.

Nos casos de consentimento explicito do titular de dados e quando o tratamento automatizado é necessário para celebração ou execução de contrato, o controlador de dados deve implementar medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados, inclusive o direito de obter intervenção humana por parte do controlador, para expressar seu ponto de vista e contestar a decisão automatizada. O que de fato, considerando o vício de consentimento, é o que garantirá a devida transparência para o exercício da autodeterminação informativa.

Outro ponto importante, como restrições ao tratamento automatizado dos dados, é que as decisões referidas apoiadas no consentimento, na necessidade de celebração ou realização de contrato, e onde a lei de um dos países membros ou da União permitirem, mesmo assim, esse tratamento automatizado não deve se basear em categorias especiais de dados pessoais. Essas categorias especiais são dados de origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e o processamento de dados genéticos, dados biométricos com o objetivo de identificar exclusivamente uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física, pois esses dados são passiveis de discriminação, exposição, violação de direitos, vieses algorítmicos e danos imensuráveis ao titular de dados.

Este trecho chama a atenção para os riscos de usar o ser humano como um conjunto de dados a ser explorado:

> Alguns artigos também definiram os alvos potenciais das tecnologias de mineração de dados discutiram o aumento da exploração dos vulneráveis como uma das sequências mais preocupantes da mineração de dados; eles alegaram que os algoritmos podem identificar aqueles que são menos capazes, como indivíduos mais velhos com hábitos de jogo, e prendê-los com anúncios de alcatrão ou persuadindo Leese afirmou que a discriminação é um dos danos que deriva da enorme escala do perfil da sociedade e que o risco é ainda maior para populações vulneráveis. (BIG DATA, 2019).

O tratamento automatizado desses dados com seus vieses causa danos que podem ser irreversíveis ao ser humano. A formação do perfil automatizado, uma modalidade de tratamento automatizado, além de violar a proteção de dados, produz uma falsa identidade do indivíduo e esta ganha legitimidade para circular em seu lugar e representá-lo num mundo cada vez mais digitalizado. Desde sua própria casa com a internet das coisas, seu trabalho, lazer e entretenimento, compras, até o acesso à justiça e a direitos. Com o falso "eu'' produzido pelos algoritmos perpassando no lugar do indivíduo em todos os espaços, o verdadeiro 'eu' vai deixando de existir, isolado, excluído e discriminado.

Não há mais espaço para ele no mundo *on-life*, onde não existe mais a possibilidade de viver desconectado. A consequência disso poderá ser uma geração de indivíduos adoecidos, e especialmente esquizofrênicos obrigados, pelo capitalismo tecnológico, a viver uma outra personalidade (a virtual). "São adolescentes que sofrem crises de ansiedade por estarem sem sinal de internet, estudantes que perdem a capacidade de se concentrar e até programador que começou a desenvolver esquizofrenia por viver isolado, interagindo só via *web*." (SILVA, 2017).

Mais preocupante ainda é que esses indivíduos que terminam por ser moldados pela vigilância constante da tecnologia e influenciados pelos algoritmos de predição, podem nem se dar conta que foram adoecidos e expropriados de si, despersonalizados, perdendo sua essência. (ROSENVALD, 2021).

Dessa forma, há o risco do ser humano se tornar uma massa de dados ambulante e defeituosa produzida pelas falhas da tecnologia que erra já no *input*, na coleta dos dados pessoais, que falha na receita desse processamento, a que tecnicamente damos o nome de algoritmo. Ele produz um resultado que, interpretado, traduz-se na sequência do erro sobre o erro (input) sobre o erro (processamento) sobre o erro (resultado). Daí é razoável hipotetizar que esse processo automatizado pode tornar a humanidade inservível e desvirtuada em sua essência em nome do capitalismo que a explora como principal produto.

Os vieses da máquina são uma das questões mais relevantes no perfil automatizado: o processamento automatizado de tomada de decisão pode produzir saídas que representam uma realidade distorcida, incompleta ou enganosa. Tem sido argumentado por estudiosos que distorções e erros podem se manifestar em julgamentos de máquinas de três maneiras: “nos dados, no *design* do algoritmo e no resultado”. (BAROCAS; SELBST, 2016).

Visando uma proteção legal mais robusta do ser humano, diante dos riscos da tecnologia, a categoria de dados pessoais sensíveis anteriormente citadas, só poderá ser utilizada em processos automatizados, de acordo com o artigo 9 e 2, alíneas, com acopladas medidas de precaução:

> a) O titular dos dados deu consentimento explícito para o processamento desses dados pessoais para um ou mais fins específicos, exceto quando a legislação da União ou dos Estados-Membros prevê que a proibição referida no artigo 9, n. 1 não pode ser levantada pelo titular dos dados; ou g) O processamento é necessário por razões de interesse público substancial, com base no direito da União ou dos Estados-Membros, que devem ser proporcionais ao objetivo perseguido, respeitar a essência do direito à proteção de dados e prever medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados (GDPR, 2016).

Em ambas as situações, desde que estejam em vigor medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados. Para sistematizar, recapitulando rapidamente as ideias na lógica do tópico consentimento e *score* de crédito: consentimento é base legal para tratamento de dados pessoais especialmente em processos automatizados, outra base é a necessidade de celebração ou execução de contrato; ou quando a lei da União ou países membros assim permitir. No caso de dados pessoais sensíveis, o titular dos dados tenha dado seu consentimento explícito para o processamento, ou ele é necessário por razões de interesse público substancial. Condições substanciais de interesse público estão estabelecidas no Anexo 1, Parte 2 do DPA 2018 (GDPR, 2016).

Dessa forma, fica claro que o *score* de crédito não é base legal para tratamento de dados pessoais no Regulamento Europeu, pois não está no rol do artigo 6 (1) da GDPR e excluída essa hipótese, o *score* de crédito ou pontuação de crédito passa aqui a ser conceituado a partir e conforme interpretação do Regulamento Europeu como perfilização, ou seja, formação de perfil conforme o Considerando 71 do Regulamento Geral de Proteção de Dados Europeu.

De acordo com o Regulamento Geral de Proteção de Dados, perfil ou perfilização é qualquer forma de processamento automatizado de dados pessoais utilizando-se de procedimentos matemáticos ou estatísticos que avalie informações pessoais relacionadas a

uma pessoa física, em particular para analisar ou prever aspectos em relação à confiabilidade, situação econômica, ao desempenho do titular dos dados no trabalho, saúde, preferências ou interesses pessoais ou comportamento, localização ou movimentos, produzindo efeitos legais sobre ele ou afetando-lhe significativamente. Assim, *score* de crédito é um tipo de perfil, portanto, forma de processamento automatizado de dados pessoais usado para tomada de decisão como demonstrado.

Já a palavra *score* vem do inglês antigo *scora*; relacionado ao nórdico antigo *skor notch*, quer dizer contagem de acordo com o dicionário Collins (COLLINS, 2022). Já a palavra crédito, essa vem do Latim *creditum*, originada de *credere*, que significa confiança. Numa tradução livre conjugada das duas palavras, é possível extrair o sentido de uma contagem de confiança. E por óbvio, para saber o quantum uma pessoa é confiável, é necessário utilizar nessa avaliação características pessoais e informações de e/ou relativas à alguém e que denotam o quão confiante ela pode ser, dessa forma individualizando-a, diferenciando-a e podendo identificá-la entre as demais. O que já aponta que independentemente do método para avaliar essas informações, o resultado será uma informação, um dado pessoal. (CREDITUM, 2022).

No entanto, por oferecer riscos elevados, a tomada de decisão com base nesse processamento, só deve ser permitida quando expressamente autorizada pela legislação da União ou do Estado-Membro responsável pelo tratamento, inclusive para fins de monitoramento e prevenção de fraude e evasão fiscal realizados de acordo com os regulamentos, normas e recomendações de instituições da União ou órgãos nacionais de supervisão. Em qualquer caso, esse processamento deve estar sob salvaguardas adequadas, que devem incluir informações específicas ao titular dos dados e o direito de obter intervenção humana, expressar seu ponto de vista, obter uma explicação da decisão tomada após essa avaliação e contestar a decisão. Decisões apoiadas em processamento automatizado medida não devem ser aplicadas a uma criança. (GDPR, 2016).

Corroborando nessa mesma linha de raciocínio temos: o Grupo de Trabalho do Art 29.º (2007) enfatizou que as informações se referem a um indivíduo quando tratarem da identidade, das características, dos comportamentos de uma pessoa ou quando essas informações forem usadas para determinar ou influenciar a maneira como essa pessoa é tratada ou avaliada. Sendo assim, uma pessoa natural é considerada “identificada” dentro de um determinado grupo de pessoas porque se distingue de todos os outros membros do grupo. (NEGRI; GIOVANINI, 2020).

Diante do exposto, numa lógica sistematizada, se o *score* de crédito é obtido a partir

da avaliação de dados pessoais formando um perfil individual referente a um indivíduo, a uma única pessoa, logo ele é dado pessoal. Essa interpretação se encaixa perfeitamente no conceito adotado pelo Regulamento Europeu de Proteção de Dados que de acordo com Bruno Bioni, aplica o modelo expansionista de dado pessoal no vocabulário utilizado na conceituação expandindo assim a moldura normativa de uma lei de proteção de dados pessoais. (BIONI, 2019).

De fato, a definição de dado pessoal segundo o art. 4 (1) da Regulamento Geral de Proteção de Dados Europeu, diz que dados pessoais são qualquer informação relacionada a uma pessoa física identificada ou identificável. Logo, assim que a Regulamento Geral de Proteção de Dados Europeu incluiu o termo "qualquer informação", deve-se supor que "dados pessoais" deve ser interpretado da maneira mais ampla possível. (CONSULTING, 2022).

Dessa mesma ideia também comunga o Tribunal de Justiça Europeu. A jurisprudência do referido Tribunal considera dados pessoais informações menos explícitas, como registros de horários de trabalho que incluem o horário em que um funcionário começa e termina seu dia de trabalho, bem como intervalos ou horários que não se enquadram no tempo de trabalho. Além disso, deve-se observar que os dados pessoais não precisam ser objetivos.

Informações subjetivas, como opiniões, avaliações ou estimativas, podem ser dados pessoais. Assim, isso inclui uma avaliação da credibilidade de uma pessoa ou uma estimativa do desempenho no trabalho por um empregador. (GDPR, 2016).

Nesse sentido de que o dado pessoal pode ser subjetivo demonstra claramente que na União Europeia ele é realmente interpretado de maneira extensiva:

> The European Union’s expansionist approach to PII is more in tune with technology than is the United States’ reductionist approach. It also has exercised significant international influence. In 1980, the Privacy Guidelines of the Organization for Economic Cooperation and Development (OECD) followed the recently enacted first federal data protection law of Germany. These guidelines define personal data as “any information relating to an identified or identifiable indi- vidual (data subject).” The OECD Guidelines apply eight privacy principles to all PII, and, in doing so, demonstrate the European Union’s expansionist approach. Once there is PII, the OECD principles are to be applied in full force. Like the OECD Guidelines, the Privacy Framework of the Asia-Pacific Economic Cooperation of 2004 defines PII as “any information about an identified or identifiable individual.” (SCHWARTZ; SOLOVE, 2011).

Esta aplicação da interpretação extensiva do dado pessoal explica que fatores devem ser analisados, levados em conta para ter certeza que se trata de dados pessoais: Identificabilidade e fatores relacionados; Se alguém é diretamente identificável; Se alguém é indiretamente identificável; O significado de "relaciona-se a"; E quando organizações

diferentes estão usando os mesmos dados para propósitos diferentes. (ICO, 2022).

Numa rápida análise diante do exposto, é possível constatar por todos os requisitos e definições que *score* de crédito é dado pessoal. Pois as informações se relacionam a alguém, que pode ser diretamente identificada ou indiretamente identificável, ou seja, há identificabilidade e fatores relacionados. Além do mais, organizações utilizam os mesmos dados para propósitos diferentes, como por exemplo, uma venda de um carro ou um financiamento imobiliário.

No que diz respeito à classificação de *score* de crédito como dado pessoal, a partir da definição do termo "dados pessoais", com base no estudo da conceituação, é de extrema importância, pois a partir do conceito adotado são definidos os limites da tutela jurídica (NEGRI; GIOVANINI, 2020)

Por falar em conceituação, vale ressaltar que para efeito deste estudo, a diferença entre relatório de crédito e *score* de crédito, para evitar errôneas interpretações. De acordo o *Consumer Financial Protection Bureau* (CFPB), uma agência do governo dos EUA que garante que bancos, credores e outras empresas financeiras tratem o consumidor de forma justa, são duas coisas diferentes. Um relatório de crédito é um extrato que contém informações sobre sua atividade de crédito e a situação atual de crédito, como histórico de pagamento de empréstimos e o status de suas contas de crédito. Já o *score* de crédito ou pontuação de crédito, objeto do nosso estudo neste tópico, é calculado com base nas informações do relatório de crédito. (CFPB, 2020).

Num estudo concluído em abril de 2021 para apoiar uma avaliação de impacto dos requisitos regulatórios para inteligência artificial na Europa, concluído para a Comissão Europeia, foram identificados os impactos negativos desse tipo de tecnologia em todos os direitos fundamentais da União Europeia, incluindo o consumidor.

> […] o estudo encontra fortes evidências de que certos usos dos sistemas de IA podem afetar significativamente todos os direitos fundamentais reconhecidos na Carta dos Direitos Fundamentais da União Europeia. Tais riscos podem ocorrer em uma variedade de contextos, incluindo situações de coleta de dados empreendimentos do tipo empresa para empresa, de empresa para consumidor e também na relação de governo para cidadão. Examinamos vários casos que ficaram sob o escrutínio do Tribunal de Justiça da União Europeia, do Relator Especial da ONU sobre liberdade de opinião e expressão, do Grupo de Especialistas de Alto Nível da União Europeia em inteligência artificial de muitos tribunais nacionais e agências de proteção de dados da UE, bem como de vários cientistas e organizações da sociedade civil. (ONU, 2022).

Além de todo o estudo, ao final, foi produzido uma tabela nessa sequência, incluídos os tipos de caso analisados, o risco a longo prazo, as entidades que coletam os dados, a origem e uso dos dados e o grau de intervenção.

A categoria *score* de e crédito, foi considerada uma ameaça aos Direitos Humanos de Liberdade, de acordo com os artigos 6-19 da Carta dos Direitos Fundamentais da União Europeia, em particular aos direitos à liberdade. Tal direito é gênero dos: Direito à liberdade e segurança, respeito pela vida privada e familiar, Proteção de dados pessoais, Liberdade de pensamento, consciência e religião, Liberdade de expressão e informação, Direito à educação, Direito de asilo.

Dessa forma, *score* de crédito foi avaliado como um tratamento automatizado de alto impacto que compromete a longo prazo os padrões de vida das gerações futuras. No caso do *score* de crédito, a origem e o uso dos dados provêm de G2C (do governo para o cidadão, numa relação comumente pela internet para, por exemplo, pagar impostos, multas e tarifas públicas), e sobretudo, na relação B2C *business to consumer* (do comércio efetuado diretamente entre a empresa produtora, vendedora ou prestador e o consumidor final), e os dados podem ser fornecidos voluntária e involuntariamente pelo consumidor. E sobre a possibilidade de intervenção, esta foi considerada baixa ou mesmo nenhuma possibilidade de intervenção se a pontuação de crédito for automatizada.

Pelo estudo, fica evidente que as empresas são as que mais coletam dados do consumidor, que a baixa ou nenhuma possibilidade de intervenção quando a pontuação de crédito for automatizada, viola frontalmente não só direitos humanos, mas também o direito do consumidor e o Regulamento Geral de Proteção de Dados Pessoais.

O estudo também apontou que vários princípios processuais são quebrados com o uso de dados e elementos que não foram objeto de um debate contraditório, explorando conclusões que não foram obtidas pelo raciocínio do juiz, falta de transparência do processo, pois não se sabe o que deve ser atribuído ao juiz ou a uma máquina, falta de condições de igualdade (paridade de armas), quebra do princípio da imparcialidade devido à impossibilidade de neutralizar e conhecer os vieses dos *designers* desse sistema.

> O viés potencial nos conjuntos de dados usados para treinar um modelo de IA afeta claramente a justiça de um julgamento. Muitos sistemas de IA funcionam em correlações estatísticas sem qualquer compreensão humana dos contextos sociais. Os dados de entrada são o único contexto em que os sistemas de IA operam e se os dados fornecidos para treinar um modelo de IA ou como sua entrada estão incompletas ou incluem viés problemático (mesmo não intencional), então pode-se esperar que a saída da IA também seja incompleta e tendenciosa. Os sistemas de IA ainda carecem de transparência e "explicabilidade" (a capacidade de explicar tanto os processos técnicos de um sistema de IA quanto os resultados relacionados). O viés pode ser inofensivo na maioria das situações, mas também pode ser prejudicial, especialmente quando os sistemas de IA são usados perante um tribunal de que as conclusões baseadas neles podem ser insuficientemente fundamentadas para garantir a equidade do processo. (ICF, 2021)

Ainda sobre o tratamento automatizado, não é de se surpreender com os riscos aos direitos fundamentais tão bem categorizados no estudo ora apontado, quando os professores Citron e Pasquale, muito antes também já alertavam para o uso de inteligência artificial no *score* de crédito do ponto de vista de que dados imprecisos ou incorretos, sem transparência e sem intervenção humana não podem gerar resultados justos.

> A pontuação tem sido realizada há anos para dar nota ao consumidor. Os professores Citron e Pasquale se referem ao uso de pontuações de crédito para alocar empréstimos […] Em um nível analítico, a natureza dessas preocupações pode estar ligada à maneira como o processo depende de conjuntos de dados tendenciosos e imprecisos, sua opacidade inerente, ou à falta de revisão humana suficiente. (ZARSHY, 2014).

Uma das respostas ao estudo de impacto da inteligência artificial aos direitos humanos realizado pela *European Commission*, quatro meses depois, em agosto de 2021, e a Autoridade Supervisora Europeia para a Proteção de Dados (EDPS), uma autoridade independente da União Europeia e responsável por garantir o respeito ao tratamento de dados pessoais, direitos e liberdades fundamentais sejam respeitados pelas instituições e órgãos da União, foi a *opinion*. A Autoridade Supervisora Europeia para a Proteção de Dados tem o poder de elaborar, por sua própria iniciativa ou a pedido, pareceres às instituições e órgãos da União e ao público sobre qualquer questão relacionada à proteção de dados pessoais.

O documento chamado de *opinion* demonstra clara interação da Regulamento Geral sobre a Proteção de Dados com a lei de defesa do consumidor e a proposta de lei de inteligência artificial em andamento na União Europeia. E mais detidamente os procedimentosque devem ser realizados para a avaliação de crédito, considerando o alto impacto desse tipode avaliação na vida das pessoas.

Especialmente em relação à publicidade e marketing envolvendo contratos de crédito, Autoridade Supervisora Europeia para a Proteção de Dados recomenda especificar na proposta que o uso de dados coletados e processados no contexto da avaliação de credibilidade para fins de publicidade ou marketing não deve ser permitido. Essa atitude por si só já é uma medida de precaução de danos ao consumidor e que impacta diretamente também na aferição da responsabilidade dos controladores.

A respeito da precaução e responsabilidade, o alemão Hans Jonas em sua obra princípio da responsabilidade, ensaio de uma ética para a civilização tecnológica, alertou sobre a necessidade de conter o progresso da tecnologia uma vez que as teorias éticas tradicionais

já não dão conta de regular as relações sociais. Pois o utópico virou real. Mas se deve encarar isso como uma precaução inteligente que envolve a atitude decente para com as próximas gerações. Pois do contrário, a natureza o fará, de um jeito terrível. (JONAS, 2006).

O documento de recomendação robusta sobre avaliação de crédito produzido pela EDPS estabelece mais de cinquenta pontos importantes sobre esse tratamento de dados pessoais do consumidor. Para o propósito deste trabalho, foi selecionado alguns deles que detalham melhor o proceder da atividade e que põem um ponto final em várias dúvidas que havia até então, a respeito do tema. A primeira delas é sobre os direitos do consumidor e a proposta de regulamentação de Inteligência Artificial.

> 25. O artigo 18., n. 6, estabelece que, quando a avaliação de credibilidade envolver o uso de perfis ou outro processamento automatizado de dados pessoais, os Estados-Membros devem garantir que o consumidor tenha o direito de: (A) solicitar e obter intervenção humana por parte do credor ou do provedor de serviços de crédito de crowdfunding para revisar a decisão;(B) solicitar e obter do credor ou do provedor de serviços de crédito de crowdfunding uma explicação clara da avaliação da credibilidade, inclusive sobre a lógica e os riscos envolvidos no processamento automatizado de dados pessoais, bem como seu significado e efeitos na decisão;(C) expressar seu ponto de vista e contestar a avaliação da credibilidade e da decisão. (GDPR, 2016).

O consentimento vai perdendo seu protagonismo diante da crescente importância da transparência para o controle dos dados pessoais. Dessa forma a intervenção humana é usada no sentido de revisão e avaliação humana. Devendo inclusive, o termo “intervenção” ser substituído por “avaliação” para evitar risco de dano pela exclusão financeira oriunda da decisão automatizada.

A Autoridade Supervisora Europeia para a Proteção de Dados recomenda a substituição do termo "intervenção" por "avaliação", nos termos do artigo 18, n. 6, e do considerando 48. De fato, dado o alto risco para os consumidores, bem como o aumento do viés de automação, a Autoridade Supervisora Europeia para a Proteção de Dados considera que o termo "avaliação", implicando uma revisão humana completa no momento em que a decisão automatizada é proferida (acompanhado de cronograma e ponto de contato nomeado para consultas pelos consumidores), é mais adequado para abordar ou mitigar o risco de exclusão financeira desencadeado pela decisão sobre a elegibilidade do requerente para o empréstimo. (GDPR, 2016).

Também temos aqui o detalhamento de como deve ser especificamente exercido o direito à explicação que vai além do sentido de transparência. Na letra (C), o direito de se opor

está na possibilidade de o consumidor expressar seu ponto de vista e contestar essa avaliação, tendo em conta que ela é de alto risco para o titular dos dados pessoais.

> 25. O considerando 48 da Proposta lembra que a Proposta de Regulamento que estabelece regras harmonizadas sobre inteligência artificial (Lei de Inteligência Artificial), especifica que os sistemas de inteligência artificial usados para avaliar a pontuação de crédito ou a credibilidade de pessoas físicas deve ser classificada como sistemas de inteligência artificial de alto risco, uma vez que determinam o acesso dessas pessoas a recursos financeiros ou serviços essenciais, como habitação, eletricidade e serviços de telecomunicações. O considerando 48 afirma ainda que […] sempre que a avaliação de credibilidade envolver processamento automatizado, o consumidor deve ter o direito de obter intervenção humana por parte do credor ou prestadores de serviços de crédito de crowdfunding. O consumidor também deve ter o direito de obter uma explicação significativa da avaliação feita e do funcionamento do processamento automatizado usado, incluindo, entre outras, as principais variáveis, a lógica e os riscos envolvidos, bem como o direito de expressar seu ponto de vista e contestar a avaliação da credibilidade e da decisão. (GDPR, 2016).

A este respeito, a Autoridade Supervisora Europeia para a Proteção de Dados lembra que o titular dos dados (neste caso, o consumidor/mutuário) deve ser informado sobre a criação de perfis e a tomada de decisões automatizadas sobre ele ou ela e receber informações significativas sobre a lógica envolvida, o significado e as consequências do processamento, de acordo com os artigos 13 e 14 do GDPR, em todos os casos de decisões que afetam significativamente ou preço "injusto" (GDPR, 2016).

Sobre o período de retenção dos dados do consumidor, a Autoridade Supervisora Europeia para a Proteção de Dados recomenda o que deve ser feito, já que a proposta de regulação de inteligência artificial, à luz do regulamento geral de proteção de dados, tem de ter prazo definido e caso o pedido de empréstimo seja rejeitado, esse prazo deve ser ainda menor.

A Autoridade Supervisora Europeia para a Proteção de Dados também observa que o artigo 18, n 3, da Proposta não fornece nenhuma indicação de quanto tempo os dados podem ou devem ser retidos. Também não diferencia entre a situação em que o pedido de crédito foi concedido ou rejeitado. De acordo com o princípio da limitação de armazenamento, os dados pessoais devem ser mantidos de uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para os fins para os quais os dados pessoais são processados (artigo 5, n.1, alínea e, do regulamento geral de proteção de dados). Para aumentar a segurança jurídica e promover a harmonização, a Autoridade Europeia para a Proteção de Dados recomenda especificar o período máximo durante o qual os dados podem ser retidos pelo credor ou provedor, levando em conta se o pedido de crédito foi concedido ou rejeitado. Em caso de rejeição, os dados sobre o requerente do empréstimo devem, em princípio, ser

mantidos por menos tempo do que no caso de o empréstimo ser concedido, de acordo com um período máximo de retenção a partir da rejeição do pedido ao empréstimo (tendo em conta também o direito do requerente de contestar a decisão).

Tratando-se de tratamento de alto risco sob vários pontos de vista, o controlador terá de realizar uma avaliação de impacto antes de usar o sistema automatizado para fins de pontuação de crédito. Assim, a Autoridade Supervisora Europeia para a Proteção de Dados é explícita na recomendação de avaliação de impacto para *score* de crédito para não restar dúvidas da necessidade de fazê-lo, bem como tomar medidas para evitar a discriminação oriunda de viés algorítmico.

A Autoridade Supervisora Europeia para a Proteção de Dados também lembra o Parecer Conjunto EDPB-EDPS sobre a Lei de Inteligência Artificial, afirmando que a classificação de um sistema de Inteligência Artificial como de alto risco desencadeia uma presunção de alto risco sob o regulamento geral de proteção de dados, na medida em que os dados pessoais são processados. O usuário do sistema de Inteligência Artificial deve, portanto, realizar uma avaliação de impacto na proteção de dados de acordo com o Artigo 35 do regulamento geral de proteção de dados antes que o sistema seja usado.

Finalmente, a Autoridade Supervisora Europeia para a Proteção de Dados lembra o risco de viés inerente à tomada de decisão algorítmica. A fim de evitar discriminação com base em viés, o credor deve, também com base em uma avaliação de impacto na proteção de dados, tomar medidas organizacionais e técnicas adequadas para lidar com esse risco.

Com base no direito à informação e transparência, independente do acesso ao crédito com base em decisão automatizada for rejeitado ou não, não basta informar o consumidor. Isso tem que ser feito de forma explícita e na hora que a aprovação ou desaprovação deste acontecer.

Por uma questão de clareza e segurança jurídica, a Autoridade Supervisora Europeia para a Proteção de Dados recomenda a alteração do n. 7 do artigo 18 da proposta para esclarecer que as informações devem ser fornecidas independentemente de o pedido ser rejeitado ou concedido. Para melhorar a proteção do consumidor, a Autoridade Supervisora Europeia para a Proteção de Dados também recomenda especificar que os indivíduos sejam explicitamente informados dos seus direitos nos termos do artigo 18, n. 6, da proposta, no momento em que o pedido for rejeitado ou concedido. (GDPR, 2016).

Sobre as ofertas personalizadas de crédito, baseadas em perfis ou outro tipo de decisões automatizadas, o consumidor deve ser informado a respeito para que ele possa avaliar os riscos de sua escolha e deve ser utilizada uma base legal válida para esse tipo de oferta. Além disso,

também deve ser informado para determinação do preço personalizado, a regulamentação do seu uso e os quais categorias de dados pessoais podem ser usados. Isso revela uma análise detida sobre a proposta preocupada também em diminuir a assimetria nesse tipo de relação de consumo.

O artigo 13 prevê que os Estados-Membros devem exigir que credores, intermediários de crédito e prestadores de serviços de crédito de *crowdfunding*, ou financiamento coletivo, informem aos consumidores quando receberem uma oferta personalizada baseada na criação de perfis ou em outros tipos de processamento automatizado de dados pessoais. O considerando 40 afirma ainda que credores, intermediários de crédito e provedores de serviços de crédito de *crowdfunding* devem ser autorizados a personalizar o preço de suas ofertas para consumidores específicos ou categorias específicas de consumidores com base na tomada de decisões automatizadas e no perfil do comportamento do consumidor, permitindo que eles avaliem o poder de compra do consumidor. Portanto, os consumidores devem ser claramente informados quando o preço que lhes é apresentado for personalizado com base no processamento automatizado, para que possam levar em conta os riscos potenciais em sua decisão de compra. O artigo 10, n. 3, alínea t e artigo 11, n. 2, alínea m, também se referem à obrigação do credor de fornecer ao consumidor "quando aplicável, uma indicação de que o preço foi personalizado com base no processamento automatizado, incluindo a criação de perfis". (GDPR, 2016).

Como resultado, qualquer preço personalizado de crédito ao consumidor ainda requer uma base legal válida de acordo com o Artigo 6 do regulamento geral de proteção de dados, bem como a conformidade com outros princípios de proteção de dados, incluindo os princípios de justiça e limitação de finalidade.

A Autoridade Supervisora Europeia para a Proteção de Dados recomenda revisar o considerando 40, regulando ainda mais o uso de ofertas personalizadas em acordos de crédito ao consumidor e delineando claramente as categorias de dados pessoais que podem ser usadas como parâmetros para elaborar uma oferta personalizada. Além disso, a Autoridade Supervisora Europeia para a Proteção de Dados recomenda a expansão da obrigação de informação contida no artigo 13 da Proposta, que deve exigir o fornecimento pelo credor de informações claras, significativas e uniformes sobre a lógica e os parâmetros usados para determinar o preço.

A EDPB ressalta a necessidade integração entre a lei de defesa do consumidor, o regulamento geral de proteção de dados e a proposta de lei de inteligência artificial em andamento na União Europeia para que as leis sejam cumpridas de maneira coerente e

harmônica, os consumidores protegidos diante do alto risco da atividade e sejam imponderados diminuindo sua condição de vulnerabilidade.

Na ausência da referida integração (que poderia ser alcançada, por exemplo, introduzindo uma referência cruzada à Proposta no referido Capítulo 2 do Título III), a avaliação da conformidade dos sistemas de inteligência artificial que avaliam a credibilidade não levaria em conta as regras estabelecidas pela proposta para melhorar a proteção do consumidor e dos dados (por exemplo, restrições relativas ao uso de dados de mídias sociais ou dados de saúde).

A Autoridade Supervisora Europeia para a Proteção de Dados também lembra que o Parecer Conjunto EDPB-EDPS recomendou que a Lei de Inteligência Artificial proíba qualquer tipo de pontuação social. Tal proibição "horizontal" de pontuação social na Lei de Inteligência Artificial seria benéfica não apenas tendo em conta exemplos de decisões sobre elegibilidade para hipotecas ou produtos de seguros (possivelmente confiando em tal "partitura social"), mas também tendo em conta a avaliação da solvabilidade. A Autoridade Supervisora Europeia de Proteção de Dados recomenda incluir na Proposta uma referência cruzada à proposta de Lei de Inteligência Artificial no que diz respeito à proibição de pontuação social, de acordo com as recomendações fornecidas no Parecer Conjunto EDPB-EDPS, o que de fato todas as sugestões foram incorporadas na devida proposta.

Finalmente, a Autoridade Europeia para a Proteção de Dados lembra a necessidade de integração dos requisitos da lei de proteção de dados (por exemplo, minimização de dados, privacidade por design e por padrão) nos requisitos da Lei de Inteligência Artificial, em particular no contexto da certificação do sistema de credibilidade de inteligência artificial. A integração deste requisito seria crucialmente benéfica para os direitos dos indivíduos, tanto como titular dos dados quanto como consumidor. (BIONI, 2019).

# 3 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

## 3.1 A criação da lei geral de proteção de dados no Brasil

Para entender como foi criada a atual Lei Geral de Proteção de Dados Pessoais no Brasil (Lei n.13.709/2018 ou LGPD) é necessário compreender seus antecedentes, a elaboração, e o contexto histórico somados aos quase dez anos de debates no executivo e no legislativo, nas universidades e na sociedade civil. A trajetória da Lei Geral de Proteção de Dados Pessoais no Brasil é permeada por discussões, polêmicas e comemorada pelos defensores dos consumidores.

O projeto de lei de Proteção de Dados Pessoais (PL 53/2018) foi aprovado por unanimidade no Congresso Nacional depois de muita pressão da sociedade e vista como uma vitória da democracia e importante instrumento de defesa de milhares de consumidores: a aprovação é o resultado de um longo trabalho feito por amplos setores da sociedade. São mais de nove anos de debate, duas consultas públicas, onze audiências públicas realizadas somente na comissão especial da Câmara e oito meses da campanha “Seus dados são você”, da coalizão direitos na rede (IDEC, 2018). Conduto, rejeitada desde sempre pelo empresariado.

Em 2016, a Confederação Nacional da Indústria (CNI) através do Portal da Indústria sentiu ameaças ao setor, pois a Lei Geral de Proteção de Dados Pessoais não poderia impedir a inovação “o excesso de proteção das informações pessoais por meio da privacidade pode levar a efeitos indesejados, como a criação de obstáculos ao desenvolvimento econômico e tecnológico, à livre iniciativa e à livre concorrência" (CNI, 2016).

Finalmente foi a Lei Geral de Proteção de Dados Pessoais sancionada em 14 de agosto de 2018 e mesmo assim, ainda neste mesmo ano, após sua sanção, a *Mobile Marketing Association* (MMA) considerou a Lei um empecilho que poderia causar prejuízos e desestimular a inovação, pois "regular esse mercado era mesmo necessário. Só que, ao fixar as mesmas exigências para companhias de diferentes portes, a lei levantou o sarrafo a uma altura que startups e empresas menores dificilmente conseguirão alcançar. Corre-se o risco de desestimular a inovação e prejudicar o desenvolvimento da economia digital" (MMA, 2022). Pois bem, voltamos aqui aos antecedentes da Lei Geral de Proteção de Dados Pessoais, quando surgiram os primeiros clamores de um novo direito que emergia diante da inovação, da tecnologia e já tinha reflexos na vida do cidadão titular de dados pessoais, na garantia dademocracia, da liberdade de expressão e na economia.

A ausência de um quadro normativo específico não implicava, em absoluto, que a matéria não fosse relevante, posto que diversas situações relacionadas ao uso de dados pessoais geravam efeitos jurídicos que, por vezes, chegavam aos tribunais. No Brasil, portanto, e como não poderia ser diferente, os problemas relacionados ao tratamento de dados pessoais surgiram e foram, em boa parte, encaminhados, a despeito da existência de uma legislação geral a respeito (DONEDA, 2020, p. 245). A demanda crescente relacionada à utilização de dados pessoais não satisfazia a contento o problema em causa indo parar nas instâncias superiores já que não havia um regramento geral sobre o tema proteção de dados.

Para Doneda (2020, p. 246), nem a tão invocada formação da proteção da privacidade, como um dos direitos da personalidade até sua consolidação no artigo 5, X e XII, com menção no Código Civil, artigo 21, foi capaz de proteger os indivíduos diante das novas tecnologias e suas questões.

Dessa forma o perigo da demora em se reconhecer esse novo direito foi tamanho, pois ele ameaçava a sobrevivência de garantias preexistentes. Sua ausência também se traduzia em afronta ao Estado-Nação. A notícia do portal Nic.br, que faz parte do Comitê Gestor da Internet no Brasil, denunciou que robôs influenciaram eleições no Brasil, inclusive manipulando algoritmicamente pessoas reais:

> Engana-se quem pensa que isso é coisa de eleição americana e treta EUA x russos. Se você é um desses, uma notícia desagradável: Somos influenciados pelos *bots* há pelo menos 2 eleições e até então ainda não havíamos nos dado conta. Quem garante isso é Dan Aranudo, professor brasileiro e pesquisador da Universidade de Washington, autor de um estudo que analisou como a propaganda computacional pode assumir a forma de contas automatizadas (*bots*), disseminar informações, manipular algoritmicamente pessoas reais e disseminar notícias falsas para moldar a opinião pública e influenciar na escolha de representantes (NIC.BR, 2014).

Ou seja, desde pelo menos 2006 já se havia dado conta do tamanho do perigo pela falta de uma regulação geral da proteção de dados pessoais no Brasil que ia na contramão de mais 140 países onde essa garantia já era uma realidade há muitos anos. (GRAHAM; GREENLEAF; COTTIER, 2020)**,** em alguns desses países, há pelo menos cinco, seis décadas, como já referenciado o caso da Alemanha no capítulo exordial. Mas, mesmo assim, o direito à proteção de dados pessoais percorreu um longo caminho legislativo a fim de garantir um mínimo legiferante até sua entrada em vigor em 18 setembro 2020 que ainda teve o risco de ser postergado por manobras parlamentares que pretendia que a vigência da Lei Geral de Proteção de dados Pessoais fosse adiada. O que de fato ainda aconteceu com parte do seu texto, no que diz respeito à vigência das sanções e o ao estabelecimento do seu correspondente

Órgão Administrativo Regulamentador, A Autoridade Nacional de Proteção de dados (ANPD).

> A entrada em vigor da LGPD nesta sexta-feira (18) ocorreu devido à aprovação pelo Senado da MP 959/2020 (PLV 34/2020) no final de agosto. O texto original da medida previa o adiamento da vigência da LGPD para o fim do período de calamidade pública, conforme estabelecido no artigo 4º do PLV. Contudo, em atendimento à questão de ordem e a solicitações de lideranças partidárias, o presidente do Senado, Davi Alcolumbre, declarou a prejudicialidade desse dispositivo, que passou a ser considerado "não escrito" no projeto, transformado na Lei 14.058, de 2020. Davi lembrou que, em maio, o Senado aprovou destaque do PDT e do MDB que mantinha a vigência da LGPD para agosto de 2020. Não há previsão de nenhuma penalidade a empresas e pessoas quanto à entrada em vigor da LGPD. A Lei 14.010, de 2020 adiou de 1º de janeiro de 2021 para 1º de agosto de 2021 a vigência das sanções que a Autoridade Nacional de Proteção de Dados (ANPD), ainda pendente de instalação, pode aplicar nos órgãos, entidades e empresas que lidam com o tratamento de dados (BRASIL, 2020).

Nessa análise de contextualização do nascimento da Lei Geral de Proteção de Dados é preciso também olhar para alguns dos principais acontecimentos e marcos com normas nacionais e internacionais (no caso, o Regulamento Geral Europeu de Proteção de dados) que antecederam e influenciaram o novo diploma no Brasil. No artigo "a Lei Geral de Proteção de Dados como elemento estruturante do modelo brasileiro de proteção de dados", de Danilo Doneda é possível ir além, de modo a elencar de maneira didática e robustamente contextualizada a trajetória da proteção de dados pessoais no Brasil, mesmo quando no dizer do próprio autor, existiam apenas centelhas que inspiraram uma sistemática própria. E essa retrospectiva é muito valiosa, pois desmistifica a ideia corrente de que o debate público brasileiro sobre o tema é recente, quando ele pode ser identificado desde 1970 (DONEDA, 2020, p. 247).

No projeto, o Registro Nacional de Pessoas Naturais (RENAPE) seria um órgão de abrangência nacional, integrando o Registro Civil de Pessoas Naturais e a Identificação Civil e uma base de dados, que foi arquivado (VIANNA, 2014).

Em 1978, também foi arquivado o projeto de Lei nº 4.365 de 1977, de autoria do deputado Faria Lima que criava um Registro Nacional de Bancos de Dados e normas de proteção da intimidade pelo uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados. (BRASIL, 1977).

Já em 1980, surgiu o projeto de Lei nº 2.796 de 1980, da Deputada Cristina Tavares que assegurava aos cidadãos acesso às suas informações constantes de bancos de dados e dava outras providências. (BRASIL, 1980). Apesar de arquivado este projeto merece grande destaque, pois no caminho da luta pela redemocratização do país, a deputada Cristina Tavares

deu corpo, materializava princípios e direitos de cidadãos titulares de dados frente ao Estado no tratamento automatizado de dados pessoais e seu uso em bancos de dados públicos e privados, demonstrando as bases para a lei de proteção de dados. Embora não tivesse à época esse nome, era exatamente o que ela representava, um projeto de lei de proteção de dados pessoais extremamente bem contextualizado, justificado e aprovado com emendas sobretudo em relação ao seu parágrafo segundo que buscava garantir que as informações ali constantes fossem verídicas. Mas, estranhamente, após uma nova Comissão Especial destinada a dar parecer ao Projeto de Lei 364, do Poder Executivo, que dispunha sobre o Código Civil, requisitou esse e outros projetos de lei em tramitação. Em seguida a própria Cristina Tavares, em agosto de 1984, pediu desistência do Projeto de Lei e ele foi retirado de plenário e arquivado em 30 de maio de 1985, sem apresentação dos motivos no único requerimento que conta dos autos do processo digital de tramitação (às folhas 40) do mesmo. Oito anos depois, o Habeas Data foi introduzido na Constituição Federal de 1988 em reação ao processo ditatorial no Brasil para que os cidadãos tivessem acesso às suas informações pessoais frente ao Estado e às injustiças que vinham sendo perpetradas:

> O habeas data foi introduzido, no Direito brasileiro, com a Constituição Federal de 1988. Conforme a definição constitucional, no inciso LXXII do art. 5o da Carta Magna, trata-se de um meio posto à disposição das pessoas para que conheçam as informações a seu respeito constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, permitindo ainda que seja feita a retificação dos dados eventualmente inexatos. (WALD, 1997)

Dessa forma, mais que uma ação constitucional, o Habeas Data tem caráter de direito material quando garante aos cidadãos acesso às suas informações pessoais e o direito de corrigir retificando ou apagando o que eventualmente esteja incorreto ou por uma interpretação extensiva, o que consta incompleto.

Em 1984 no Rio de Janeiro, a Lei Estadual 824, de 28 de dezembro de 1984, que "Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no Estado do Rio de Janeiro e dá outras providências"; e, em São Paulo, a Lei Estadual 5.702, de 5 de junho de 1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa" que surgiram inspirados no projeto de lei anterior.

> Faço saber que a Assembleia Legislativa do Estado do Rio de Janeiro decreta e eu sanciono a seguinte Lei: Art. 1º - A toda pessoa física ou jurídica é assegurado, livre de qualquer ônus, o direito de conhecer as suas informações pessoais contidas em bancos de dados, públicos-estaduais e municipais - ou privados, operando no Estado do Rio de Janeiro, bem como de saber a procedência e o uso dessas informações e de completá-las ou corrigi-las, no caso de falhas ou inexatidões. Parágrafo único - Qualquer informação pessoal só poderá ser registrada com a identificação da fonte

> onde foi obtida. Art. 2º - Os bancos referidos no artigo anterior devem ter a existência divulgada, juntamente com sua finalidade, abrangência e categorias de informações arquivadas, bem como o nome do responsável pela sua administração. Art. 3º - O uso de informações pessoais para fins diversos daqueles para os quais foram obtidas depende do consentimento expresso da parte diretamente interessada, que poderá, ainda, contestar a relevância das informações a seu respeito para as finalidades declaradas do banco. Art. 4º - É vedada a transferência de dados pessoais de um banco de dados para outro cujas finalidades não sejam as mesmas, salvo prévio e expresso consentimento da pessoa envolvida. Art. 5º - Esta Lei entrará em vigor na data de sua publicação, revogadas as disposições em contrário (RIO DE JANEIRO, 1984).

O que chama a atenção dessa Lei Estadual de 1984, é que seu conteúdo reflete quase na totalidade, o núcleo duro do Projeto de Lei 2.796 de 1980, da Deputada Cristina Tavares, que assegurava aos cidadãos acesso às suas informações constantes de bancos de dados e dava outras providências, tocando no assunto do compartilhamento de dados para outros com finalidade diversa da coleta e a necessidade de consentimento expresso. Outra coincidência é que a Lei Estadual do Rio de Janeiro entra em vigor em dezembro de 1984, quatro meses depois que a Deputada Cristina Tavares, pede desistência do Projeto de Lei nº 2.796 de 1980, o que pode indicar uma clara influência desse Projeto de Lei que embora não prosperando inspirou não só a criação do Habeas data, mas também da Lei Estadual do Rio de Janeiro e, em 05 de junho de 1987, a Lei Estadual 5.702, no estado de São Paulo, concedendo ao cidadão o direito de acesso às informações nominais sobre sua pessoa.

No ano de 1988, na Constituição Federal, houve o estabelecimento da defesa do consumidor. Passa-se a receber as demandas relacionadas a dados pessoais e anos depois, em 1990, o Código de Defesa do Consumidor, que foi inspirado, de acordo com o resposável pela elaboração do anteprojeto, na normativa norte-americana de proteção ao crédito estabelecida pelo National Consumer Act e pelo Fair Credit Reporting Act – FCRA (DONEDA, 2021).

Podendo-se nele observar princípios e extrair os direitos do consumidor sobre seus dados pessoais:

> SEÇÃO VI - Dos Bancos de Dados e Cadastros de Consumidores. Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados

> entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores (BRASIL, 1990).

No ano de 1991, a lei dos Arquivos Públicos (Lei 88159/91) seria uma das primeiras leis ordinárias sobre proteção de dados. Ela consagra o direito do cidadão de acesso à informação de seu interesse particular ou de interesse público, assim como a proteção do sigilo, da intimidade e da vida privada.

No ano de 2002, o Código Civil (Lei 10.406/2002), em seus artigos 12 e 21, considerando a proteção de dados como um dos aspectos da privacidade, e a privacidade sendo um direito da personalidade, esses artigos surgem como uma proteção da vida privada e de se fazer imediatamente cessar lesão à ameaça, e tendo entre as medidas, a responsabilidade de reparar perdas e danos causados. (OLIVEIRA; LOPES, 2020, p. 66).

Em 2003, conforme elencado por Doneda (2020, p. 250), o Governo brasileiro assinou a Declaração de Santa Cruz de La Sierra reconhecendo ter consciência de que a proteção de dados pessoais é um direito fundamental:

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade (BRASIL, 2003).

Somente em 2004 foi promulgado o Acordo de Santa Cruz de La Sierra Constitutivo da Secretaria Geral Ibero-Americana, assinado pelo Brasil em 12 de julho de 2004, pelo decreto nº 6.659, de 20 de novembro de 2008, que determina em seu artigo 1º "O Acordo de Santa Cruz de La Sierra Constitutivo da Secretaria Geral Ibero-Americana, apenso por cópia ao presente Decreto, será executado e cumprido tão inteiramente como nele se contém" (BRASIL, 2008). Apesar de o Governo brasileiro ratificar que tem consciência desse direito fundamental à proteção de dados pessoais, esse acordo à época, mesmo tendo conteúdo genérico não se evidenciou internamente nem tão pouco gerou repercussões para que se reconhecesse esse direito como fundamental por vários anos.

No ano de 2011 foi sancionada a Lei do Cadastro Positivo, lei nº 12.414, de 9 de junho de 2011. Que veio disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, apontada por Doneda (2020, p. 251), como a primeira norma brasileira que foi concebida a partir de conceitos e sistemática de proteção de dados já consolidada em outros

países, mas frustrou a expectativa por não demonstrar de fato sua importância para cultura de formação de uma cultura jurídica de proteção de dados. De fato, como veremos posteriormente, essa lei não se demonstrou tão positiva assim aos olhos do consumidor e nem seu sistema de proteção. Também em 2011, foi sancionada a Lei de Acesso à informação (lei 12.527/2011) que de fato contribuiu para as bases da futura Lei Geral de Proteção de dados.

> A Lei de Acesso à Informação (Lei 12.527/2011), que regulamenta o princípio constitucional da transparência, além de definir o que é informação pessoal de forma análoga à que posteriormente estaria presente na própria LGPD, possui, em seu artigo 31, um regramento específico para a proteção de dados pessoais em poder do poder público, pelo qual tais informações estariam disponíveis, a princípio, somente ao interessado até um período de cem anos de sua produção, salvo na verificação de algumas das exceções previstas no mesmo artigo (DONEDA, 2020, p. 251)

Embora depois de sancionada a Lei Geral de Proteção de Dados, esta passou a ser analisada por parte da doutrina como incompatível ou até divergente da Lei de Acesso à Informação, servindo inclusive para negar solicitações dos titulares o que tem causado embate entre as leis (CÂMARA DOS DEPUTADOS, 2021).

O próprio caso da decretação do sigilo de cem anos dos filhos do presidente Jair Bolsonaro é exemplo disso, de acordo com Bruno Bioni, que defende que as leis são harmônicas entre si, e o que acontece é um equívoco de interpretação. Nesse sentido, nota-se um padrão de violação das regras da Lei de Acesso à Informação relativas ao direito de acesso em razão do argumento de sigilo baseado na Lei Geral de Proteção de Dados, afastando do público informações de evidente interesse público. A má interpretação da Lei Geral de Proteção de Dados foi utilizada para embasar o sigilo de 100 anos, por exemplo, dos dados dos crachás de acesso dos filhos do presidente da república, Jair Bolsonaro, por serem dados pessoais; do cartão de vacinação do presidente e para não informar o salário do policial acusado de matar Marielle Franco, todos os casos embasados no fato de esses dados serem pessoais. (BIONI, 2022).

Em 2012, mesmo insuficiente, podemos citar a Lei12.737/12 (Lei Carolina Dickmann) sobre a invasão de dispositivos, comentada pelo professor Tomasevicius Filho. (TOMASEVINICIUS, 2014).

A atriz teve fotos íntimas obtidas de seu computador pessoal e divulgadas na Internet pelo fato de ela não se ter submetido à chantagem da pessoa que teve acesso a esse material. Tipificou-se o crime de interrupção ou perturbação de serviço telemático ou de informação de utilidade pública, como também o de “clonagem” de cartões de crédito e de débito, equiparando-se ao crime de falsificação de documento particular. Merece destaque a inserção

do art. 154- A no Código Penal brasileiro, para estabelecer como crime a violação da privacidade por meio da invasão de dispositivo informático alheio:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 1942)

Para Tomasevicius (2014), essa lei foi meramente simbólica, porque as penas imputadas são muito brandas e não dissuadirão as pessoas que sentem compulsão a invasão de privacidade a deixarem de praticar essas condutas. (TOMASEVICIUS FILHO, 2014).

Em 2014, o Marco Civil da Internet (Lei 12.965/2014) foi a legislação que mais se aproximou da Lei Geral de Proteção de Dados que estava por vir. Inclusive, na obra proteção de dados contexto, narrativas e elementos fundantes, organizado por Bruno Bioni, até a plataforma criada para as discussões sobre o Marco Civil da Internet, foi utilizada para a primeira consulta pública sobre o Anteprojeto de Lei de Proteção de Dados.

> O processo de materialização desse interesse na criação de uma lei geral teve início na Secretaria de Assuntos Legislativos, em parceria com o Departamento de Proteção e Defesa do Consumidor, ambos do Ministério da Justiça, que, sob a coordenação de Laura Schertel Mendes e com a colaboração do então consultor Danilo Doneda, elaborou uma minuta de Anteprojeto de Lei de Proteção de Dados e, em dezembro de 2010, submeteu o texto a consulta pública, seguindo os moldes da elaboração da Lei n.° 12.975/2014 (Marco Civil da Internet). (BIONI, 2022, p. 19).

Por outro lado, o Marco Civil da Internet vinha numa necessidade crescente de proteção de dados pessoais posto que a lei foi sancionada pós revelações feitas por Edward Snowden sobre o esquema de vigilância em massa orquestrado pelo Governo Americano depois dos atentados das torres gêmeas, no histórico 11 de setembro. Francisco Brito Cruz descreve como o efeito "Snowden" influenciou diretamente o texto do Marco Civil da Internet quanto à privacidade e à proteção de dados.

> Por fim, o Projeto de Lei nº 2.126/2011 ganhou atenção especial quando o governo brasileiro tornou sua aprovação ponto de honra após o ex-funcionário da Agência Nacional de Segurança dos Estados Unidos da América, Edward Snowden, protagonizar um amplo vazamento de informações que abarcava, dentre outras denúncias, a espionagem da Petrobras e a interceptação do telefone pessoal da Presidenta Dilma Rousseff. De um lado ou de outro o tema do Marco Civil não passou batido no debate político, ao menos dentro de uma comunidade de usuários de Internet interessados no tema e de setores políticos, acadêmicos, econômicos e governamentais especializados (CRUZ, 2015)

Nos anos de 2015, o parágrafo 6, acrescentado no Código de Defesa do Consumidor, pela Lei 13.146/2015 - Estatuto da Pessoa com Deficiência – passou a tratar de modo mais específico do acesso dos portadores de necessidades especiais. Da leitura desse artigo, a doutrina extrai: “i) o direito de acesso; ii) o princípio da qualidade dos dados; iii) o princípio da transparência; iv) o direito de retificação e cancelamento, e v) o princípio do esquecimento”. (SHERTEL, 2011).

No mesmo ano, o projeto de Lei nº 3.541/2015, entre outras medidas, propõe acrescentar os direitos básicos do consumidor: i) a privacidade e a segurança de informações e de seus dados pessoais coletados, inclusive, no meio eletrônico; e ii) a liberdade de escolha, vedados a discriminação e o assédio do consumo. (BRASIL, 2015).

Em 2016 foi aprovado em âmbito internacional aquela que seria a maior influência sobre a Lei Geral de Proteção de dados Pessoais: o Regulamento Geral de Proteção de Dados Europeu. “Em âmbito internacional, foi no intervalo de 2012 a 2016 que foi discutido e aprovado, em diferentes níveis, o Regulamento Geral de Proteção de Dados (RGPD) europeu, reconhecido como a maior influência da Lei Geral de Proteção de Dados.”. (BIONI, 2022, p. 21).

| | |
|---|---|
| **Estrutura** | A Lei 13.709, de 2018, tem 65 artigos, distribuídos em 10 Capítulos. O texto foi inspirado fortemente em linhas específicas da regulação europeia, o Regulamento Geral de Proteção de Dados (GDPR, em sua sigla em inglês) |
| **Hipóteses para o tratamento de dados** | Com o consentimento do titular; Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento; Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; Para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa; Para a proteção da vida ou da incolumidade física do titular ou de terceiros; Para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; Para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular quando a seu pedido; Para pleitos em processos judicial, administrativo ou arbitral; |

| | |
|---|---|
| **Abrangência** | Quaisquer dados, como nome, endereço, e-mail, idade, estado civil e situação patrimonial, obtido em qualquer tipo de suporte (papel, eletrônico, informático, som e imagem, etc). |
| **Contratos de adesão** | Nos casos de contratos de adesão, quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, o titular deverá ser informado com destaque sobre isso. |
| **Dados sensíveis** | O texto traz o conceito de dados sensíveis, que recebem tratamento diferenciado: sobre origem racial ou étnica; convicções religiosas; opiniões políticas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; dados referentes à saúde ou à vida sexual; e dados genéticos ou biométricos vinculados a uma pessoa natural |
| **Sanções administrativas** | Quem infringir a nova lei fica sujeito a advertência, multa simples, multa diária, suspensão parcial ou total de funcionamento, além de outras sanções. |
| **Responsabilidade civil** | O responsável que, em razão do exercício de atividade de tratamento de dados, causar a dano patrimonial, moral, individual ou coletivo, é obrigado a reparar. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa |

Tabela 1 - Entenda o marco legal de proteção de dados[3]

Depois de elencar as normas que influenciaram e estimularam a elaboração da Lei Geral de Proteção de Dados, é importante ressaltar que no Brasil, a referida lei, como já se percebe pelo exposto, percorreu um cenário de ameaças, resultando na sua lentidão. Foi um processo que se arrastou por mais de dez longos anos (CAITLIN, 2020, p. 7), deixando os brasileiros expostos às vulnerabilidades tecnológicas, ou melhor dizendo, vulnerabilidades digitais.

Para Doneda (2020, p. 21-25) os debates para uma futura Lei Geral de Proteção de Dados no Brasil, começaram ainda em 2005, no "I Seminário Internacional de Proteção de Dados Pessoais", promovido pelo Ministério do Desenvolvimento, Indústria e Comércio

[3] Fonte: Agência Senado Federal (2020).

Exterior, que dele derivou um documento chamado de “Medidas para a Proteção de dados pessoais e sua livre circulação”, incorporado em 2010 ao Mercosul e a matéria teria sido discutida, segundo Doneda, pela primeira vez pelo Poder Executivo Brasileiro. O texto que serviu de base a partir do debate público, com devidas contribuições posteriores, serviu para a consolidação de texto base para o Anteprojeto de Lei de Proteção de Dados pelo Ministério da Justiça. Até 2015 o texto que serviu de base foi revisado e aperfeiçoado várias vezes quando sua nova versão foi tornada pública pela Secretaria Nacional do Consumidor (SENACON) ligada ao Ministério da Justiça, que levou o Anteprojeto a um debate público que resultou em cerca de 1200 contribuições para enfim ser consolidado o texto em 2016 e enviado ao Congresso Nacional (Projeto de Lei 5.726/2016. Aprovado unanimemente no Congresso, a Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018).

Apesar disso, sua elaboração e sanção não foram suficientes para sua pronta entrada em vigor que foi adiada por forças políticas e econômicas. E havia a necessidade do Brasil integrar a Organização para a Coordenação e desenvolvimento Econômico (OCDE), que tinha como requisito que o país candidato tivesse um regramento de proteção de dados pessoais. (BIONI, 2022, p. 27). Considerando a questão da Organização para a Coordenação e desenvolvimento Econômico e da entrada em vigor do Regulamento Geral Europeu de Proteção de Dados, fatos complementares tornaram o cenário mais ideal ainda para a aprovação da Lei Geral de Proteção de Dados, como um verdadeiro ultimato:

> Foram eles: i) o escândalo *Cambridge Analytica*, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados (RGPD) europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; ili) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão super-visor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, queenvolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável (BIONI, 2022, p. 27)

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) foi então aprovada em 2018 e entraria em vigor a partir de 14 de agosto de 2020. Um pedido de adiamento da vigência da lei para maio de 2021, rejeitado pelo Congresso, fez com que a legislação entrasse em vigor em 18 de setembro de 2018, três anos depois da sua sanção, mesmo contrariando alguns setores da economia. “O lobby favorável ao adiamento era vocalizado por muitas entidades, como as dos ramos de telecomunicações e fármacos, com base na incapacidade de as empresas - ou mesmo de o Estado - conseguirem cumprir com a

LGPD a tempo". (GIMENEZ, 2020).

A pressão contra a entrada em vigor da Lei Geral de Proteção de Dados Pessoais era tanta que Felipe Palhares dedicou-se a escrever sobre esse período na obra Temas Atuais de proteção de Dados o capítulo 21, sob o título: "As falácias do amanhã. A saga da entrada em vigor da Lei geral de proteção de dados pessoais". (PALHARES, 2020).

Se por um lado, fatores a princípio podiam levar ao adiamento da vigência da Lei Geral de Proteção de Dados Pessoais, forçaram a sua aprovação. A pandemia da COVID -19, tornou sua entrada em vigor urgente em 2020, ante o surto, metaforicamente falando, do uso indiscriminado de dados pessoais e suas decorrentes violações a direitos humanos, fundamentais, do consumidor, da personalidade, e direitos da livre concorrência sob o argumento de que a pandemia global justificava a emergência e calamidade pública. (DATAPRIVACY, 2020).

Era preciso traçar critérios e limites para o tratamento de dados pessoais durante a pandemia da COVID-19 que desencadeou – ou reforçou, para alguns países – o uso da tecnologia como meio de monitoramento da população. Em Taiwan e Israel, smartphones foram programados para notificar as autoridades públicas caso os pacientes não observassem a quarentena, em um sistema de autoridades. Na Coreia do Sul, foram divulgados os dados de viagens de 29 pacientes confirmados, compilados por meio de bases de celulares, cartões de crédito e câmeras de segurança. Nessa breve digressão, é possível perceber que o tratamento dos dados pessoais está sendo utilizado para geolocalização, identificação e rastreamento de pacientes, gerenciamento do risco de contágio, entre outras atividades, com a finalidade de melhorar os instrumentos de combate à pandemia. (SILVA; MODESTO, JUNIOR, 2022, p. 167).

Pela urgência da situação, as normas tenderam a ser flexibilizadas e as decisões governamentais sendo, muitas vezes, tomadas sem as devidas reflexões acerca do impacto na vida em sociedade. O tratamento de dados deve obedecer a uma série de regras para que se garanta a tutela dos direitos à privacidade, à liberdade e à proteção dos dados pessoais, ao contrário do que se observa: a violação dos direitos dos cidadãos sob a justificativa de uma necessária escolha entre o direito à saúde ou o direito à proteção de dados pessoais. (GUIMARÃES, 2021)

De fato, a entrada em vigor da Lei Geral de Proteção de Dados no Brasil não significou sua plena eficácia. Ou seja, até os idos de 2022 a Lei Geral de Proteção de Dados Pessoais não se tornou completa realidade, mas continua a ser um grande desafio no tocante à regulamentação, aplicação e interpretação sobretudo. (BRASIL, 2022).

Sob o olhar hermenêutico, que configura mais um obstáculo, a Lei Geral de Proteção de Dados Pessoais não é uma certeza também pelas barreiras impostas para a sua devida interpretação, pela sua integração ao ordenamento jurídico, pela aplicação e julgamento razoável por parte dos magistrados, e pelo uso da ética e da conformidade por parte das organizações.

Além disso, a busca pela fiscalização e regulamentação por órgãos administrativos, atualização e retificação oriunda do legislativo, e respeito ao cumprimento da lei pelo Poder Executivo são outros *fronts* atuais. Nessa lista, pela eficácia da norma, não se deve esquecer da imprescindibilidade da educação e conscientização da população, pois como bem rememorado, o direito não socorre aos que dormem. Esses múltiplos fatores tornam a Lei Geral de Proteção de Dados Pessoais ainda uma legislação em aberto, no sentido de vaga e em certos casos, de difícil implementação que carece do olhar de múltiplos atores. Em especial os três Poderes, executivo, legislativo e judiciário, dada a forte legitimidade destes para agir em prol da coletividade. Pois, a inovação e a tecnologia, como a própria etimologia das palavras sugere, com seu poder de predição do comportamento humano e mapeamento de tendências, tem alma bandeirante. É liberal e capitalista que tem seu maior ativo extraído do ser humano. Este em condição variável, crescente e permanente de vulnerabilidade na relação assimétrica de consumo. Citam-se as relações de consumo, pois além de terem ligação direta com os objetivos desse trabalho, elas preponderam na Lei Geral de Proteção de Dados Pessoais. Estima-se que cerca de 80% por cento dos dados pessoais são de forma direta ou indireta, tratados em situações consumeristas.

Posto que este trabalho se dedica a chamar a atenção e levantar hipóteses e possíveis caminhos para um problema decorrente da soma de divergências de cunho hermenêutico, de um diálogo de fontes e um confuso, moroso, e em determinadas situações, vazio regulamentador. Este último expõe as chamadas áreas cinzentas da lei. Sem deixar de lado a falta de consenso factualizada pelas múltiplas aplicações e julgamentos proferidos citando a Lei Geral de Proteção de dados Pessoais que não necessariamente, traduzem-se na busca do melhor direito, mas revelam a falha de eficácia da novel em todas as camadas de poder e da sociedade.

No estudo em comento será focado adiante na análise da responsabilidade civil no compartilhamento de dados pessoais dos consumidores. Estes que no contexto de avanço da tecnologia e da inovação, são na essência, a alma da Lei Geral de Proteção de Dados Pessoais. Pois até na relação estado - cidadão, analogicamente discorrendo, segundo o relatório de inteligência artificial da União Europeia, no cenário de pagamento de taxas e impostos, o

cidadão também pode ser visto numa relação de consumo. Nesse caso, o que seria também o Estado, senão um grande concentrador de dados pessoais. E esse mesmo Estado por sua vez, apesar da Lei Geral de Proteção de Dados Pessoais, pode em determinadas situações, compartilhar dados dos consumidores com a iniciativa privada.

O eixo guia dessa dissertação pretende apontar caminhos para a responsabilidade civil no compartilhamento de dados dos consumidores, protagonistas- alvo da Lei Geral deProteção de Dados Pessoais.

## 3.2 O novo direito fundamental: a proteção de dados pessoais

Antes de se falar em um novo direito fundamental, vale aqui relembrar o que é um direito fundamental, como surgiu, para que serve a sua proteção e quando ele deve ser protegido, por quem, para enfim, trazer à baila esse novo direito fundamental e autônomo da Carta Magna à proteção de dados pessoais no Brasil.

Diante disso, como aplicá-lo, ou melhor, como compreendê-lo e protegê-lo no âmbito da Lei Geral de Proteção de Dados Pessoais conectando-o na prática ao desafio do mundo globalizado com suas facetas, os métodos e as denominações que são utilizadas para o tratamento de dados pessoais. Ou seja, como proteger pessoas da dominação e manipulação algorítmica que pode avançar sem controle de si própria ou de seu inventor. Como melhor proteger seres e sua essência diante de um caminho ladrilhado pela tecnologia e inteligência artificial quando não é possível saber exatamente para onde ela levará a humanidade. Há estudos recorrentes a apontar que esse caminho independentemente de onde vá, varia de baixo a altíssimo risco ao indivíduo e a sua coletividade.

Inauguramos este tópico que trata da proteção de dados como um direito fundamental com uma primeira análise em que contexto está inserido o tema proposto. Isso numa breve análise histórica e normativa para em seguida apresentar o conceito e os fundamentos da Lei Geral de Proteção de Dados Pessoais. Na sequência dos acontecidos, a proposta de Emenda Constitucional e a Jurisprudência do Supremo Tribunal Federal que corroboraram para sedimentar o entendimento e o reconhecimento de que a proteção de dados é um direito fundamental brasileiro e autônomo.

Esse direito foi contextualmente invocado pelas inúmeras mudanças aconteceram no cenário tecnológico de captura de dados pessoais em afronta aos direitos fundamentais. Pois as empresas privadas demonstraram ao longo do tempo serem potencialmente ainda mais danosas que o Estado na coleta de dados pessoais. Elas desenvolveram o método de

comoditificação de dados. Perceberam que através disso conseguem maior concentração econômica e controle político. Nos elementos que fazem parte da autofagia do capitalismo de plataforma (uma expressão cunhada em 2017, pelo canadense Nick Srnicek, radicado em Londres Artigo em 17 de agosto de 2020), depende da colossal captura diária de dados, hoje na casa de quintilhões. Dados que se transformaram em mercadoria única (em grandes volumes, sendo, portanto, uma *commodity*). Dados capturados, armazenados e movimentados demandam uma infraestrutura (plataformas) e outras condições que viabilizam o mundo digital e sua importância no capitalismo contemporâneo. (MORAES, 2020).

Sendo assim, temos aqui algumas das evidências de um direito novo e necessário diante dos riscos impostos aos direitos fundamentais até então positivados, face às novas tecnologias se crescendo há décadas.

E às vezes avivar alguns fatos parecem obviedades, mas eles são fundantes e fortes argumentos baseados em necessidades crescentes da transformação das sociedades quesempre estão a clamar soluções. No caso da privacidade foi preciso se ampliar essa proteção de alguma forma, ao ponto de chegar-se a um novo direito. Pois, a constitucional tutela da privacidade já não satisfazia sozinha, a proteção de dados pessoais. Reafirmando, pois, segundo Doneda, “tal operação, se bastaria para abarcar a disciplina sob a égide constitucionalacaba por simplificar demasiadamente os fundamentos da tutela de dados pessoais, o que podeeventualmente limitar o seu alcance”. (DONEDA, 2021, p. 269).

Corroborando, o que se quer dizer é que várias liberdades individuais não são albergadas pelo direito à privacidade. Afastando-as assim do direito à privacidade. Nesse caso, autonomizando a proteção de dados pessoais.

A privacidade, fundamentada na divisão entre os domínios público e privado, consiste em uma liberdade negativa pela qual o indivíduo resguarda-se da interferência alheia. Em contrapartida, a proteção de dados apresenta uma característica dinâmica, proporcionando uma liberdade positiva, por meio da qual o indivíduo detém o controle das suas informações, ainda que disponibilizadas em ambiente público. (BIONI, 2019, p. 96 -97).

Assim, claramente, mesmo que deixando de lado outros aspectos, este argumento já se mostra suficiente para que a proteção de dados pessoais se tornasse um novo direito e autônomo, apartado da tutela da privacidade. Pois, o surgimento, as identificações de novos direitos fundamentais estão diretamente ligadas às novas demandas da sociedade à sua época. Como afirma José Afonso da Silva, a historicidade dos direitos fundamentais "é precisamente o que lhes enriquece o conteúdo e os deve pôr em consonância com as relações econômicas e sociais de cada momento histórico". (SILVA, 2013, p. 181).

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) também já implicitamente reclamava esse novo direito em seus sete fundamentos do seu seu artigo 2. o respeito à privacidade, à liberdade de expressão, à autodeterminação informativa, liberdade de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Citar tais fundamentos da Lei Geral de Proteção de Dados é relacionar direitos essenciais que reforçam os motivos pelos quais o ordenamento jurídico pátrio reuniu esforços para inserir na Constituição Federal de maneira expressa, o direito fundamental à proteção de dados pessoais através de uma Proposta de Emenda Constitucional analisada a seguir antes de sua aprovação.

O projeto de emenda a constituição 17/19 (aprovada na Câmara dos Deputados em agosto de 2021, em segundo turno, por maioria de 436 votos a 4) incluindo expressamente a proteção de dados pessoais na Constituição Federal do Brasil. Dessa forma, a ideia à epoca, era a de que fosse competência da União a função de legislar sobre o tema. Ou seja, pelo projeto de emenda a constituição caberia à União fiscalizar e organizar essa proteção. Mas, a proposta em sua tramitação teve que retornar ao Senado para pequenas alterações em relação à inclusão de uma Autoridade Nacional Independente de Proteção de Dados expressa na Constituição.

E sobre essa Proposta de Emenda Constitucional, defendeu o Deputado Orlando Silva, relator. “Todos nós aqui utilizamos sistematicamente aplicativos na internet, e o manejo desses aplicativos se dá a partir da oferta de dados pessoais, que, muitas vezes, é objeto de manipulação sem que cada um de nós saiba os riscos à nossa privacidade”, afirmou Orlando Silva. (BRASIL, 2021).

A Ementa do projeto de emenda a constituição 17/19 formalmente na tramitação acrescentava dois incisos em dois artigos: o inciso XII-A, ao art. 5º que trata dos direitos fundamentais, e o inciso XXX, ao art. 22, estabelecendo as competências privativas da União na Constituição Federal. (SENADO FEDERAL, 2019).

Pois veja-se: com esses precedentes legislativos e num cenário de transformações históricas e sociais, evidenciou- se cada vez mais o que era inescapável: a tutela constitucional da proteção de dados. O acelerador determinante e em paralelo à tramitação arrastada do projeto de emenda a constituição 17/19, estava no Supremo Tribunal Federal através da Ação Direta de Inconstitucionalidade 6.387 (SUPREMO TRIBUNAL FEDERAL, 2019). A ADI

analisava a Medida Provisória nº 954/2020. E, se antecipando ao projeto de emenda a constituição 17/19, promoveu uma decisão histórica. Na resolução do caso, a Corte proclamou o direito à proteção de dados como um fundamental autônomo. Como um dos efeitos, essa decisão da Suprema Corte acabou por determinar urgência à tramitação da anteriormente ao projeto de emenda a constituição 17/19. Esse julgamento influenciou decisões de casos no próprio Supremo Tribunal Federal.

Rememorando os fatos do conteúdo da citada Ação Direta de Inconstitucionalidade, em abril de 2020, o governo editou a Medida Provisória n.954/2020 determinando que empresas de telecomunicação do STF e do SMP deveriam disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoais físicas ou jurídicas a fim de realizar pesquisa estatística não presencial diante do isolamento populacional imposto pela pandemia. (BRASIL, 2020).

Os ministros em seus votos, manifestaram -se pelos mais diversos motivos. Entre eles ausência de proporcionalidade, de regulação quanto aos mecanismos de segurança da informação, desnecessidade da coleta de dados milhares de brasileiros, tendo em vistarealizar-se de pesquisa que precisaria apenas de amostra; além da falta de transparência paracom os titulares de dados e a falta de um relatório de impacto, sendo flagrante a violação de privacidade no compartilhamento desses dados entre as empresas e o IBGE. Posto que os dados utilizados continham uma capacidade infinita de processamento. Assim, pondo em risco direitos, como se lê no trecho do voto da Ministra do Supremo, Cármen Lúcia:

> Mais do que isso, a partir de técnicas de agregação e de tratamentos, sua utilização pode-se dar para fins muito distintos dos expostos na coleta inicial, ainda sendo capazes de identificar seu titular por outras maneiras, formando, no plano virtual, perfis informacionais sobre sua personalidade. Muita vez, porém, isso se dá sem sua participação ou anuência. (SUPREMO TRIBUNAL FEDERAL, 2020).

O voto da ministra entra em consonância com a pós-modernidade, em que a economia é baseada em dados pessoais, projeção da personalidade de cada um, sob o abrigo de garantias fundamentais. Pois este, é um recurso natural finito, ao contrário dos dados que são potencialmente infinitos, porque podem ser processados, cruzados e minerados, assim como acontece no atual fenômeno do *Big Data*.

> Entende-se por uma ferramenta tecnológica capaz de processar os dados obtidos de diversas fontes e organizá-las. Na sequência, cataloga as informações e obtém um produto, que será usado estrategicamente por um sujeito nas tomadas de decisões. (BRAGA; FERREIRA, 2019).

O que também foi levado em conta na decisão foi a recomendação da Organização Mundial de Saúde. O Regulamento Sanitário Internacional da OMS foi incorporado ao ordenamento brasileiro pelo Decreto n. 10.212, de 30 de janeiro de 2020. Tal norma determina que não devem existir "processamentos de dados desnecessários e incompatíveis" com o propósito de "avaliação e manejo de um risco para a saúde pública" (art. 45, 2, "a"). (SCHERTEL; JÚNIOR; FONSECA, 2021, p. 63).

E embora não citada, mas que possivelmente também pode ter influenciado a decisão da Corte, foi a Convenção Interamericana de Direitos Humanos na declaração n. 01/2020, em abril de 2020, que considerou condenável no contexto da pandemia da Covid-19 a invasão desmedida da privacidade e do uso indevido de dados pessoais. Ou seja, posicionou-se a favor da proteção de dados e do princípio geral da não-discriminação.

> O acesso à informação verdadeira e confiável, assim como à internet, é essencial. Medidas adequadas devem ser tomadas para garantir que o uso da tecnologia de vigilância, para monitorar e rastrear a disseminação do coronavírus (Covid-19), seja limitado e proporcional às necessidades de saúde, e não envolva uma interferência desmedida e lesiva à privacidade, à proteção de dados pessoais e à observância ao princípio geral de não discriminação. (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2020).

Dentre os efeitos gerados pela proteção advinda da declaração de inconstitucionalidade da Medida Provisória n. 954/2020, conhecida como caso IBGE no contexto da pandemia da Covid-19 talvez o maior deles foi propiciar uma dupla proteção: como liberdade negativa do cidadão perante o Estado e ao mesmo tempo o dever de agir do Estado para garantir mecanismo de exercer esse direito. (BRASIL, 2019). De um lado, (a) essa proteção se desdobra como liberdade negativa do cidadão, oponível diante do Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro lado, (b) ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).

Dito de outra maneira, segundo o Ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita àquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados. Ao contrário, refere-se a qualquer dado que identifique ou possa identificar um indivíduo. Esse direito fundamental autônomo e com contornos próprios, seria extraído de uma "compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5.º, inciso X, da

CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa" .(SCHERTEL; JÚNIOR; FONSECA, 2021, p. 67).

Mas, independentemente da decisão da Corte supra comentada, a doutrina em peso já defendia neste mesmo sentido. No de que, mesmo implicitamente, da constituição já poderia se extrair um direito fundamental à proteção de dados pessoais. Porém, o Supremo Tribunal Federal surpreendeu mais. Foi para melhor delineamento desse direito lhe dando caráter autônomo em relação aos outros direitos fundamentais. Mesmo assim não é demais expor o posicionamento de Sarlet (2020), reforçando o caráter de direito fundamental da proteção de dados pessoais anterior ao reconhecido *status* constitucional positivado:

> Já mediante uma simples leitura do catálogo que segue, enunciado nos arts. 17 e 18 da LGPD, é possível perceber que em grande medida as posições jurídicas subjetivas (direitos) atribuídas ao titular dos dados pessoais objeto da proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados, coincidem com o rol de posições jurídico-constitucionais diretamente e habitualmente associadas à dupla função de tal direito como direito negativo (defesa) e positivo (a prestações). [...] A inserção de um direito à proteção de dados pessoais no texto da CF, a condição de direito fundamental autônomo não depende, em si, de tal expediente, porquanto sobejamente demonstrado que se trata de um direito implicitamente positivado, o que é objeto de amplo consenso doutrinário e mesmo acolhido na esfera jurisprudencial. um direito fundamental à proteção de dados pessoais daria maior sustentação ao marco regulatório infraconstitucional, bem como a sua aplicação pelos órgãos do Poder Judiciário, entre outras vantagens apontadas. Particularmente relevante é o fato de que a condição de direito fundamental vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional. Nesse contexto, nunca é demais lembrar que levar à sério a proteção de dados pessoais é sempre também render homenagem à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à liberdade pessoal como autodeterminação. (SARLET, 2020).

Nesse percurso, assim, após 30 anos, desde a Constituição de 1988, em 10 de fevereiro de 2022, foi promulgada pelo Congresso Nacional a Emenda Constitucional 115/2022 que inseriu expressamente a proteção de dados pessoais no rol dos direitos fundamentais do art. 5 da Constituição Federal através do inciso LXXIX, nos seguintes termos: "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais". A Emenda Constitucional ainda adicionou o inciso XXVI ao art. 21 e o inciso XXX ao art. 22 da Constituição de 1988. O que estabeleceu a competência privativa da União para legislar sobre

o tema da proteção e tratamento de dados pessoais, organizar e fiscalizar a proteção e o tratamento de dados pessoais. (BRASIL, 1988)

Dessa forma, o reconhecimento desse direito foi o início de um novo horizonte de garantias e delineamento desse novo direito que já vinha sendo acolhido pela doutrina, ocorrendo outras proteções constitucionais como o direito à privacidade, à intimidade e ao sigilo das comunicações, do habeas data e do princípio da dignidade humana. (TEIXEIRA, 2022, p. 246).

> Como todo direito fundamental, também o direito à proteção de dados tem um âmbito de proteção que, embora dialogue com o de outros direitos, cobre um espaço próprio e autônomo de incidência, o que se pode ilustrar mediante a referência ao fato de que a proteção de dados pessoais e o direito à privacidade e intimidade, embora zonas de convergência, são direitos fundamentais distintos. Tal âmbito de proteção é também sempre (em maior ou menor medida) - como igualmente já referido - delimitado e definido em conjunto com outros direitos e bens/interesses de hierarquia constitucional, mas também concretizado pelo legislador infraconstitucional e mesmo por decisões judiciais [...] considerando que a definição corrente e legalmente consagrada de dados pessoais - cuja consistência constitucional não tem sido objeto de relevante contestação - seja a de "informação relacionada a pessoa natural identificada ou identificável" (art. 5.°, I, da LGPD), conceito praticado também pelo RGPDE (art. 4.°, n.° 1), eventual distinção entre dados e informações parece não ser relevante do ponto de vista de sua proteção jurídico-constitucional, o que importa, ao fim e ao cabo, seria a configuração dos requisitos legais referidos, e não a forma mediante a qual se corporifica determinada informação. (SARLET, 2021, p. 39-40)

O reconhecimento do direito fundamental à proteção de dados pessoais, assim como a sua aplicação na experiência jurídica brasileira, constitui um passo necessário para a concretização da nossa Constituição. Também a aplicação dos princípios da proteção de dados, em consonância com os modernos princípios firmados internacionalmente, representa a consolidação desse direito entre nós. Trata-se de um desenvolvimento natural do direito à privacidade, que ocorre invariavelmente a partir de novas demandas sociais originadas na sociedade da informação (MENDES, 2014, p. 235-236). Consagrado o novo direito, cabem à Doutrina e à Jurisprudência encontrar formas de fortalecê-lo, protegê-lo e delimitá-lo no que ainda não foi possível.

No que concerne a sua extensão, aplicabilidade e interpretação no caso concreto, tendo em vista, que há inúmeras ações em trâmite envolvendo o tema, a exemplo as ações de controle concentrado de constitucionalidade que tramitam no Supremo Tribunal Federal: a Ação Direta de Inconstitucionalidade (ADI) 6649/DF, ajuizada pelo Conselho Federal da OAB contra o Decreto 10.046/2019 da Presidência da República, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro

Base do Cidadão e o Comitê Central de Governança de Dados; a Ação Direta de Inconstitucionalidade 6.529/DF, com requerimento de medida cautelar, ajuizada pela Rede Sustentabilidade e pelo Partido Socialista Brasileiro contra o parágrafo único, do art. 4 da Lei 9.883/1999, que institui o Sistema Brasileiro de Inteligência, criando a Agencia Brasileira de Inteligência - ABIN; e a Ação de Descumprimento de Preceito Fundamental (ADPF) 695/DE interposta pelo Partido Socialista Brasileiro (PSB), que questiona o compartilhamento de dados no âmbito da administração pública federal, em que se estima que dados de 76 milhões de brasileiros chegariam a ABIN (Agência Brasileira de Inteligência), incluindo informações como nome, filiação, endereço, telefone, dados dos veículos e fotos de todo portador de carteira de motorista no país, depende de solução a partir da decisão da Corte.

Depois de todo o exposto, constata-se que o reconhecimento do direito fundamental autônomo à Proteção de Dados e seu contexto, são de suma importância também porque esse reconhecimento após a vigência da Lei Geral de Proteção de dados e da nova lei do Cadastro Positivo, e, por conseguinte, depois do *score* de crédito, traz toda uma expectativa de alterações e interpretações benéficas no cenário da rede de proteção do consumidor titular de dados pessoais.

### 3.3 Score de crédito

Inicia-se esse tópico com a citação de Frederike Kaltheuner.

> O mundo está sendo reconstruído por empresas e governos para que possam explorar os dados. Sem uma ação urgente e contínua, os dados serão usados de maneiras que as pessoas nem podem imaginar agora, para definir e manipular nossas vidas sem que possamos entender o porquê ou sermos capazes de contra-atacar efetivamente. Pedimos às autoridades de proteção de dados que investiguem essas empresas e protejam os indivíduos da exploração em massa de seus dados, e incentivamos jornalistas, acadêmicos, organizações de consumidores e a sociedadecivil em geral a responsabilizar ainda mais essas indústrias (CARRIERE- SWALLON; HAKSAR, 2019).

Segundo Carriere-Swallon e Haksar (2019), esse texto ilustra o dilema e a preocupação da sociedade diante dos riscos do modelo de capitalismo que se alimenta de dados pessoais para produzir riqueza. Frederike pediu a uma empresa de publicidade chamada *Quantcast* todos os dados que ela tinha sobre ele e ficou horrorizado com a quantidade de informações pessoais.

A empresa com sede em São Francisco coleta informações em tempo real sobre as características do público na Internet e afirma que pode fazê-lo em mais de 100 milhões de

sites e coleta informações de mais de 700 milhões de pessoas em todo o mundo.

A Quantcast é apenas uma das muitas empresas que fazem parte de um complexo sistema de back-end usado para direcionar publicidade a indivíduos e públicos-alvo específicos. O termo back-end foi criado em 2015 por Phil Calçado, então colaborador da SoundCloud (plataforma alemã de distribuição de áudio e música). A ideia era que através do design era possível prover experiências mais ricas, mas isso requerem dados ricos, e isso significa agregar informações de várias fontes. Na prática, o back-end é onde estão em detalhes e em tempo real, todos os dados pessoais coletados de várias fontes. É a "tela" por trás "tela" de qualquer site, aplicativo que o indivíduo não tem acesso. É como se numa loja física, o estoque fosse o back-end e a vitrine, a tela, o front-end. Mas é no estoque que está todos os produtos (dados), fornecedores (fontes), porém o consumidor só tem acesso ao pouco que está em exposição pela loja, depois de passar por um filtro de seleção.

A captura de tela (deliberadamente) feita pelo Frederike (borrada abaixo) mostra como isso sobre para uma única pessoa. Ele verificou que ao longo de uma única semana, o Quantcast acumulou de informações pessoais sobre ele mais de 5.300 linhas e mais de 46 colunas de dados, incluindo URLs, carimbos de data/hora, endereços IP, IDs de cookies, informações do navegador e muito mais.

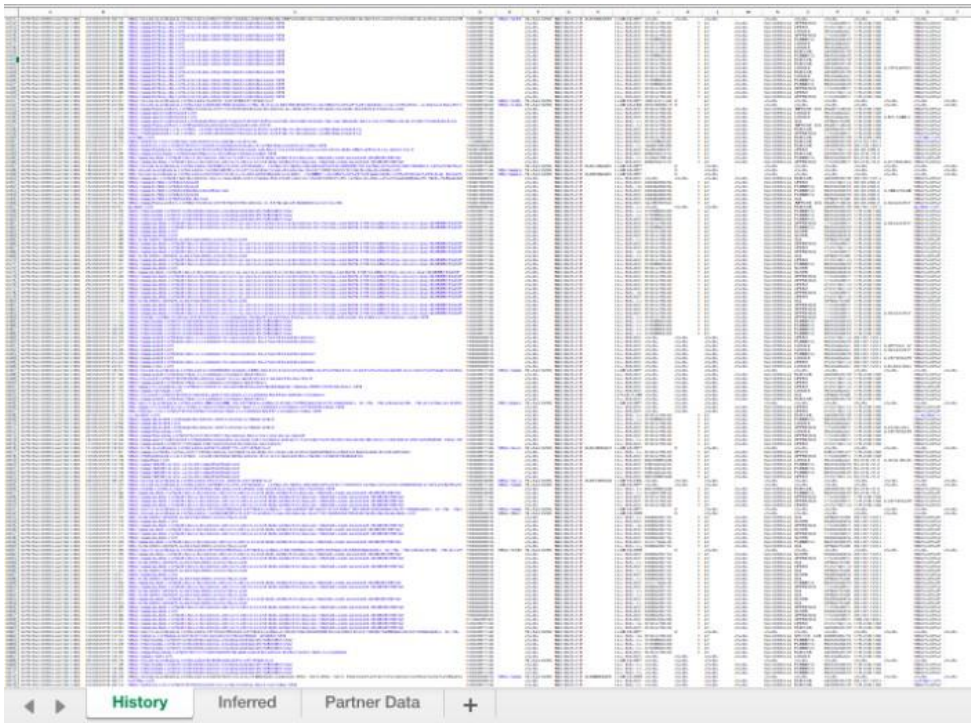


Figura 3 - Uma captura de tela do PI de solicitação de acesso do titular dos dados[4]

[4] Fonte: (QUANTCAST, 2018).

Ver que a empresa tem uma visão tão granular sobre meus hábitos online é bastante enervante. No entanto, os sites, onde a Quantcast rastreou minha visita, são apenas uma pequena fração do que a empresa sabe sobre mim. O Quantcast também previu meu gênero, idade, a presença de crianças em casa (em número de crianças e suas idades), o nível educacional e a renda familiar bruta anual em dólares americanos e libras esterlinas. O Quantcast também colocou em categorias muito mais refinadas cujos nomes sugerem que os dados foram obtidos por corretores de dados como Acxiom e Oracle, mas também MasterCard e agências de referência de crédito como Experian. Algumas das categorias são estranhamente específicas. Os interesses de compras no MasterCard UK, por exemplo, incluem viagens e lazer para o Canadá (na verdade, estive no Canadá recentemente a trabalho) e transações frequentes em restaurantes Bagel (lembro-me de uma noite em que comprei alguns bagels). A Experian UK o classifica de acordo com a suposta situação financeira (por algum motivo inexplicável, é classificado como "Prosperidade da cidade: riqueza de classe mundial", o corretor de dados Acxiom até colocou em uma categoria chamada "Álcool em casa gasta muito", talvez por ele ter ido fazer compras para uma festa de aniversário em sua casa, e uma empresa chamada Affinity Answers acha que ele tem uma afinidade social com o perfil de consumidor "Baby Fraldas & Wipes" (muito, muito errado). (ASKED, 2018). A situação relatada demonstra um caso concreto de como a coleta de dados pessoais em rede é onipresente pelo fluxo contínuo e foram desenvolvidos algoritmos que podem conectar conjuntos de dados para permitir análises muito mais amplas e profundas do que antes. (PROVOST, 2016, p. 2).

A partir de dispositivos tecnológicos conectados à internet denominados de "IOT" pode-se vigiar um indivíduo. A IOT ou Internet das Coisas (Internet of Things - IoT) é a expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e de armazenamento de dados. O que todas as definições de IOT têm em comum é que elas se concentram em como computadores, sensores e objetos (artefactos como refrigeradores inteligentes, relógios, aparelhos celulares) interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade. O atual cenário de hiperconectividade é, portanto, baseado na estreita relação entre: seres humanos, objetos físicos, sensores, algoritmos - conjuntos de regras que os computadores seguem para resolver problemas e tomar decisões sobre um determinado curso de ação. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas

para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa; Big Data- um volume massivo de dados sendo processado, na escala de bilhões de dados diariamente, permitindo que seja possível conhecer cada vez mais os indivíduos em seus hábitos, preferências, desejos e tentando, assim, direcionar suas escolhas; Inteligência Artificial, entre outros elementos. (MAGRANI, 2019, p. 19-30).

Entende-se por Inteligência Artificial um mundo em que as decisões serão tomadas de três formas básicas: por humanos, por máquinas, e por genuína colaboração entre humanos e máquinas. A Inteligência Artificial também está em vias de transformar as máquinas - que, até hoje, eram ferramentas - em parceiras. A Inteligência Artificial receberá cada vez menos instruções específicas sobre como atingir os objetivos que lhe são estabelecidos. (KISSINGER; LLC; HUTTENLOCHER, 2021, p. 26).

Com seu poder de aprendizagem automática por exemplo, a Inteligência Artificial tem uma gama de aplicações. “Nas finanças, a Inteligência Artificial tem os meios para tornar mais expeditos processos de grande volume: aprovação (ou recusa) de empréstimos, aquisições, fusões, declarações de falência e outras convenções.” (KISSINGER; LLC; HUTTENLOCHER, 2021, p. 73).

Depois da conceituação acima que se faz necessária, retomamos que a coleta, processamento e compartilhamento de dados acontece sem que se tenha noção do alcance desse monitoramento. Um outro exemplo é o sistema do Amazon Echo que monitora o que está sendo dito no ambiente o tempo inteiro sob o argumento de identificar comando de voz podendo levar a uma violação direta da privacidade e segurança de dados pessoais, posto que esse dispositivo armazena informações ininterruptamente. (MAGRANI, 2019, p. 69).

> Há aí uma reflexão também sobre quem são as organizações responsáveis, quantos e que dados são coletados, os tipos de dados, para quais finalidades, onde eles estão localizados, quem está lucrando com isso. Provavelmente, a maior aplicação de técnicas de mineração de dados está no marketing. para tarefas como marketing direcionado, publicidade online e recomendações para venda cruzada. A mineração de dados é usada para gestão de relacionamento com o cliente para analisar seu comportamento a fim de gerenciar o desgaste e maximizar o valor esperado do cliente. A indústria financeira utiliza a mineração de dados para classificação e negociação de crédito e em operações via detecção de fraude e gerenciamento de força de trabalho. Os principais varejistas, do Walmart à Amazon, aplicam a mineração de dados em seus negócios, do marketing ao gerenciamento da cadeia de fornecimento. Muitas empresas têm se diferenciado estrategicamente com data science, às vezes, ao ponto de evoluírem para empresas de mineração de dados. (PROVOST, 2016, p. 2).

E mais: como esses dados estão sendo tratados e até que ponto eles são usados para discriminar alguém a partir da criação de perfis automatizados, com base na utilização de

algoritmos. “Muitos métodos de criação de perfil [...] em sua essência, são simplesmente instâncias do conceito fundamental [...]: definir uma função numérica com alguns parâmetros, definir uma meta ou objetivo e encontrar os parâmetros que melhor atendam ao objetivo.” (PROVOST, 2016, p. 298).

No caso do Score de Crédito, pode-se compará-lo com um método de formação de perfil, posto que é uma função estatística matemática (algorítmica) que atende à variáveis (parâmetros) com a meta para atender o objetivo de formular uma nota de pontuação de crédito relativa à alguém com base em informações pessoais a partir de fontes de dados. “A utilização de escore de crédito, método estatístico de avaliação de risco [...] sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.” (STJ, 2009)

Dessa forma, é possível hipotetizar também que o score de crédito é um algoritmo de inteligência artificial utilizado para minerar dados no sentido de que minerar também é: “a busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos.” (DONEDA, 2006, p. 176)

Não podendo ficar submisso a esses dilemas do consumidor na era da tecnologia, que se utiliza de inteligência artificial para tentar extrair ao máximo o valor dos dados pessoais, de maneira discriminatória a regular o que também vem sendo chamado de “colonialismo de dados”. O que é um novo tipo de dependência surgida neste capitalismo da era digital. (NICK; MEJIAS; ULISES, 2018).

Na compreensão de Couldry e Mejias:

> O uso da palavra colonialismo, nesse caso, não é mera metáfora, mas realmente uma nova forma de colonialismo diferente da que vimos nos séculos anteriores. O colonialismo de dados combinaria as mesmas práticas predatórias do colonialismo histórico com a quantificação abstrata de métodos computacionais. Trata-se de um novo tipo de apropriação no qual as pessoas ou as coisas passam a fazer parte de infraestruturas de conexão informacionais. A apropriação da vida humana (por meio da captura em massa de dados) passa a ser central. Nada deve ser excluído nem apagado. Nenhum dado pode ser perdido. Couldry e Mejías chamam de *data relations* (algo como relações baseadas em dados) os novos tipos de relações humanas que permitem a extração de informações pessoais para exploração lucrativa. Nossa vida social tornou-se um recurso que pode ser extraído e utilizado pelo capital como forma de acumulação de riquezas. Tanto populações do Norte Global quanto do Sul passaram a ser fontes de informações que alicerçam o capitalismo. Não importam a cultura, a religião, a ideologia. Tudo gera dados capturáveis, que são armazenados e utilizados para formatação de perfis. As pessoas passam a considerar a captura de suas informações como algo normal, natural. As relações sociais mudam e tornam-se mecanismos dos modos de extração.Um dos efeitos mais marcantes sobre os novos sujeitos colonizados é o fato de que eles passam a ficar atados a julgamentos alicerçados em seus próprios dados. Não sabem quais de seus dados são coletados, como são usados nem mesmo quais as fontes coletoras, em um processo completamente opaco e obscuro. As informações pessoais capturadas são a chave para as novas formas de geração de valor. O novo eu-colonizado vê as práticas das empresas de dados invadirem seus espaços mais íntimos, tornando o rastreamento uma característica permanente da vida, delimitando inclusive o que cada ser humano pode explorar em relação aos seus semelhantes. Adicionalmente, o processo de alteração comportamental é majoritariamente conduzido por meio de sistemas de inteligência artificial, que utilizam da coleta e do processamento de dados junto a sistemas algorítmicos para modular tomadas de decisão. Trata-se de uma modulação algorítmica baseada na coleta das informações que nós mesmos fornecemos espontaneamente às grandes empresas de tecnologia. (CASSINO, 2021, p. 2012).

Por isso, o Direito precisa buscar formas de reagir para regular de forma ética o avanço da tecnologia e da inovação frente aos desafios impostos aos direitos fundamentais.

Se o Direito é um dos mais importantes instrumentos de controle social e, portanto, de preservação da própria democracia, não há como se manter alheio aos impactos tecnológicos de nítido caráter universal. Na concorrência entre o virtual e o real, caberia ao Direito se colocar como mais um relevante protagonista, principalmente quando se observa uma gigantesca interconexão entre pessoas, propiciada por ferramentas digitais. Quanto mais contato, maior é a tendência de conflitos e, consequentemente, a necessidade de prevenção e solução destes. (LACERDA; ZAMPIER, 2022, p. 2).

Do ponto de vista de Harari, a autoridade mudou mais uma vez na humanidade. Antes Deus, passando pelo antropocentrismo com as pessoas como centro das leis, passando para os algoritmos por eles desenvolvidos. (HARARI, 2018).

Em outras palavras, essa nova autoridade suplantaria a regulação Estatal que vem sendo tragada pela Tecnorregulação. O conceito se refere a uma prática bem estabelecida e vem sendo utilizada para atender exclusivamente a propósitos comerciais, sem qualquer preocupação em observar direitos constitucionais ou regulações específicas da internet no Brasil como o Marco Civil da Internet, que declara enfaticamente a importância de se garantir a liberdade de expressão no ciberespaço. (MAGRANI, 2019, p .250)

O termo ciberespaço surgiu em 1984 no romance Neuromancer do escritor américo-canadense de ficção. Willian Gibson utilizou o termo ciberespaço em seu livro como sendo um conjunto de rede de computadores na quais todo o tipo de informação circula sem a necessidade de interação física do ser humano. (GIBSON, 1984).

Para garantir liberdades se estabelece um clamor para uma regulação mais efetiva das tecnologias, no que vem a se convencionar como uma visão metatecnológica do Direito que consiste numa metaregulação para atacar o impacto da tecnologia no Estado de Direito. (STANFORD, 2016)

Da relação clara entre direito e tecnologia e a necessidade de uma metaregulação, que se sobreponha à tecnorregulação, o score de crédito como uma tecnologia apoiada no uso de algoritmos de inteligência artificial, tem merecido atenção da sociedade para regulação e governança.

A inteligência artificial que se utiliza de algoritmos alimentados por bases de dados pessoais. Esses dados são coletados de inúmeras fontes conhecidas e desconhecidas no grande mundo interconectado do ciberespaço: Internet das coisas, redes sociais, sites, cookies (rastreamento on-line) o que torna isso um problema. Uma forma de governança de algoritmos

está na regulação dos dados que o alimentam e o direito à revisão humana dessas decisões para evitar um “looping” eterno de decisões por máquina como acontece na Lei Geral de Proteção de Dados. (DONEDA, 2016, p. 60).

Dados pessoais podem ser minerados, explorados para obter informações, conhecimento e valor. “Datamining and the handling of extremely large data sets seems to be an essential for almost every empirical discipline in the 21st century." (STANFORD BUSINESS, 2022).

Quanto mais dados são coletados, mais a capacidade de formar perfis com maior granularidade, de detalhamento de conhecer a fundo os hábitos de consumo, prever comportamentos e influenciar pessoas.

> There is however a crucial difference between the legal debate on automation from the 1890s and current discussions on automated processing. The technological leap concerns the "logic involved" in such automated processing. The latter increasingly regards a par-ticular class of algorithms that either augment or replace analysisand decisionmaking by humans, as occurs with the discipline of ma-chine learning, .e. algorithms capable to define or modify decisionmaking rules autonomously. The second step of our phenomenology has thus to do with the field of AI and more particularly, with the crucial shift from automation to artificial autonomy. (PAGALLO, 2013, p. 11)

Ou seja, numa tradução livre do teórico italiano, há, no entanto, uma diferença crucial entre o debate jurídico sobre automação da década de 1890 e as discussões atuais sobre automação em processamento. O salto tecnológico diz respeito à "lógica envolvida" em tal processamento automatizado. Este último considera cada vez mais uma classe especial de algoritmos que aumentam ou substituem a análise e tomada de decisões por humanos, como ocorre com a disciplina de aprendizagem por máquinas, assim algoritmos capazes de definir ou modificar decisões fazendo regras de forma autônoma. O segundo passo de nossa fenomenologia tem, portanto, a ver com o campo da Inteligência Artificial e, mais particularmente, com a mudança crucial da automação para a autonomia artificial.

Essa “lógica envolvida”, refere-se ao problema da opacidade algorítmica de decodificar o resultado gerado pelo algoritmo o que reclama transparência principalmente quando eles são usados para tomar decisões importantes como a de concessão de empréstimo através da pontuação de crédito. A opacidade algorítmica também chamada de caixa-preta (PASQUALE, 2015) por utilizar maneiras ocultas, complexas, difusas e tecnológicas, possui semelhança com os pilares do colonialismo digital que planejou um novo sistema de dominação impondo controle sobre a produção do conhecimento e o Estado, do trabalho e da população mundial. Sendo a colonialidade a “pedra angular desse padrão de poder que opera

em cada um dos planos, meios, e dimensões, materiais e subjetivos, da existência social quotidiana e da escala societal.” (QUIJANO, 2009, p.73)

E se esse tratamento de dados para formação de perfis é automatizado como exemplo, e considerando para efeito deste trabalho, o score de crédito oferece riscos aos direitos fundamentais. Resguarda a dignidade da pessoa humana, a proteção de dados pessoais, do consumidor, privacidade, autodeterminação informativa, livre desenvolvimento da personalidade. Além do princípio da não discriminação. Pois a Constituição Federal de 1988 proíbe a discriminação. Constituição Federal de 1988, Art. 3° "Constituem objetivos fundamentais da República Federativa do Brasil: [..] IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". "Art. 5° [..] XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais". (BRASIL, 1988). Cabendo ao Direito regular e promover a responsabilização.

Se não considerarmos a internet como um espaço "constitucional", rico de garantias adequadas, podem prevalecer apenas as razões da segurança e do controle, conforme corre o risco de acontecer neste período. E, de toda forma, prevaleceriam as lógicas de mercado, que já estão impondo regras, visto que a maioria das atividades on-line são de tipo comercial e que a Web é considerada como uma gigantesca mina de dados pessoais, fatores graças aos quais nasceu uma sociedade da vigilância e da classificação. (RODOTA, 2003).

A insistência sobre a necessidade de considerar estes problemas de um ponto de vista "constitucional" indica com clareza quais são as direções que o Direito deve tomar se quiser respostas adequadas à maneira pela qual as tecnologias estão dando nova forma às nossas sociedades. (RODOTA, 2003).

O direito atento às transformações não pode se eximir de regular e proteger tais garantias e ao mesmo tempo, precisa equacionar o dilema de não impedir o desenvolvimento tecnológico, a inovação e o proteger o segredo de negócio protegido na Lei Geral de Proteção de Dados: o art. 6º, VI, da Lei Geral de Proteção de Dados Pessoais o define como “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.” Embora Ruha Benjamim centre de outra forma o “lado subjacente do desenvolvimento tecnocientífico – quem e o que é fixado no mesmo lugar – classificado, encurralado e/ou coagido, para permitir a inovação.” (RUAH, 2020, p.18).

Apesar de regulações da internet, como o Marco Civil, e da privacidade, como a Lei Geral de Proteção de Dados Pessoais no Brasil, tentarem valorizar o potencial da internet regular práticas que busquem proteger direitos constitucionais, a autorregulação tecnológica

baseada no design do código a simplesmente se sobrepõe à regulação pelo Direito, subvertendo a tradicional lógica do "dever ser" típica do Estado de Direito, que salvaguarda o livre-arbítrio dos indivíduos, e estabelece uma lógica de "pode/não pode", sem deixar nenhuma alternativa de ação para cidadãos ou governos. (FRAZÃO, 2021, p. 429).

### 3.4 O score de crédito no contexto da LGPD: desafios e caminhos à efetividade da lei

Dissertar sobre riscos aos direitos fundamentais, aos direitos da personalidade, observados na seara do direito brasileiro, inevitavelmente, é tocar em algum momento, no tratamento de dados pessoais e na positivação de uma de suas bases legais mais controversas e preocupantes do ponto de vista da defesa do consumidor qual seja, a de proteção ao crédito (MARQUES, 2022, p. 9). Uma permissão legal que de maneira polêmica e potencialmente causídica foi efetivada na Lei Geral de Proteção de Dados Pessoais e pode ser usada sem o consentimento do consumidor e através daquela base legal, sob essa justificativa, o mercado pode lançar mão do uso do *score* de crédito em nome de uma suposta proteção ao crédito e benefício do cidadão na concessão de juros mais baixos e inclusão social, o que é oposto a todo argumento científico, como atesta o IDEC- Instituto de Defesa do Consumidor (RODRIGUES; BRITO, 2022, p .18-19). Pois, a Lei Geral de Proteção de dados Pessoais vem exatamente para o contrário que é proteger o consumidor de práticas que podem ser abusivas na utilização dos seus dados pessoais acrescentando-lhe direitos. Dessa forma, fica evidente que a base legal de proteção ao crédito como permissão para o tratamento dos dados dos consumidores, antagoniza com a própria Lei Geral de Proteção de Dados que garante textualmente que a defesa do consumidor é fundamento da proteção de dados (Art.2).

> Art. 2° A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2021)

O uso abrangente de informações de crédito por organizações e empresas de todos os setores da cadeia produtiva e que não são abarcados pela Lei do Cadastro Positivo dificulta a fiscalização, sanção e exercício dos direitos por parte dos titulares. Além de risco de dano e discriminação, posto que a base legal de proteção ao crédito na Lei Geral de Proteção de Dados Pessoais refere-se exclusivamente a dados coletados através do cadastro positivo.

> Segundo a pesquisa TIC Empresas 2021, que analisou práticas de privacidade e proteção de dados de pequenas, médias e grandes empresas brasileiras, dentre as categorias de dados de clientes e usuários que as empresas tratam, dados "para checagem de crédito dos clientes" são a segunda categoria mais comum. O uso de dados para checagem de crédito está bastante presente em todas as categorias de empresas analisadas, indo além do comércio e serviço (em que análises creditícias são esperadas) para indústria, construção, transporte, alojamento e alimentação, informação e comunicação e atividades profissionais. Este uso tão abrangente de informações creditícias, por atores não previstos pela Lei do Cadastro Positivo, provavelmente é justificado pela genérica base legal de proteção ao crédito da LGPD- ou pelo acesso indiscriminado à pontuação de crédito para propósitos que não a relação creditícia - e pode indicar diversos riscos ao titular, como tratamentos com finalidades abusivas e discriminatórias. Pode-se dizer que a base legal se refere exclusivamente a dados coletados no âmbito do cadastro positivo, porém isso não está expressamente previsto. Tampouco, há previsão de deveres ou responsabilidades adicionais para agentes de tratamento que adotem essa base legal, como ocorre no caso do legítimo interesse ou do uso de informações para tutela da saúde (SIMÃO; OMS, 2022, p. 103-104)

A base legal de proteção ao crédito na Lei Geral de Proteção de Dados Pessoais é ampla e não informa que atividades podem ser consideradas e isso também não está definido por qualquer outra legislação. O que implica na falta de positivação de deveres para os agentes de tratamento que utilizam essa base para o *score* de crédito.

Por oportuno, se faz necessário diferenciar score de crédito (pontuação de crédito) e cadastro positivo, feita pelo Recurso Especial nº 1.419.697 (REsp. n° 1.419.697). O *credit score* é um método - ou fórmula matemática - desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, que, considerando diversas variáveis de decisão, atribuindo uma nota ao consumidor avaliado. Vale dizer ainda que a pontuação de crédito é a metodologia que utiliza apenas informações negativas ou publicamente disponíveis. Já o cadastro positivo é um banco de dados de informações financeiras "positivas" de pagamento, regulamentado pela Lei do Cadastro Positivo, e que pode, ou não, dar subsídio à pontuação de crédito (SIMÃO; OMS, 2022, p. 91). Contudo, não há limites especificados de que forma ou não se pode formar a pontuação de crédito.

> O Min. Relator exemplifica o que seriam as "variáveis de decisão", mas não traz uma definição clara: "Consideram-se informações acerca do adimplemento das obrigações (histórico de crédito), assim como dados pessoais do consumidor avaliado (idade, sexo, estado civil, profissão, renda, número de dependentes, endereço)" (p. 11). Deixa principalmente para as empresas a determinação do que constituem as variáveis, por serem "fatores que a experiência empresarial denotou como relevantes (para avaliação do risco de retorno do crédito concedido". (SIMÃO; OMS, 2022, p. 89)

Além disso, o cadastro positivo tem regulamentações por Decreto e atende às normas do Banco Central (Decreto 9.936/2019, que regulamenta a Lei n° 12.414/2011 e a Resolução 4.737/2019 do Banco Central), mas, a pontuação de crédito possui não possui regulamentação neste sentido.

> O Banco Central do Brasil fica apenas a cargo de regulamentar o uso e compartilhamento de informações financeiras entre gestores de bancos de dados, uma assimetria regulatória é criada. Assim, o *enforcemens* da lei recairá principalmente sobre uma categoria específica de birôs de crédito: aqueles que declarem utilizar informações provenientes de instituições financeiras. O problema está no que fica as margens disso, já que, como já mencionado, a avaliação de risco de crédito pode ir muito além da análise restrita sobre informações de pagamento. (SIMÃO; OMS, 2022, p. 99).

Também da leitura do artigo 11, da Lei Geral de Proteção de Dados Pessoais que normatiza sobre o tratamento de dados sensíveis fica claro que a base legal de proteção ao crédito (artigo 7. Inciso X), foi deixada de fora não podendo esses dados serem utilizados com essa finalidade. Ou seja, seja sob o argumento da proteção ao crédito, e consequentemente, para formular nota de crédito do consumidor ou qualquer outra avaliação, ficha, cadastro, coleta em rede social, o que for, reafirma-se: as organizações não podem utilizar esse tipo de dado pessoal para fins de score de crédito.

Ademais, assim como no Regulamento Geral de Proteção de Dados Europeu (artigo 9), segundo o art. 5, inciso II, da Lei Geral de Proteção de Dados Pessoais, dados sensíveis são dados que revelam informações sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São igualmente sensíveis aqueles referentes à saúde ou à vida sexual e dados genéticos ou biométricos. O termo “revelam” na lei já demonstra que esse rol não é taxativo, posto que ali está exemplificada e didaticamente se informando apenas que: qualquer dado que venha a revelar informações a respeito dessas categorias, será considerado sensível para fins da Lei Geral de Proteção de Dados Pessoais. Dessa leitura do artigo se extrai também que pelo caráter expansionista de dado pessoal adotado pela Lei Geral de Proteção de Dados Pessoais, podem inclusive surgir adiante subcategorias de dados pessoais sensíveis alertando-se para os riscos na utilização desses dados. A título de exemplo sobre como dados podem se demonstrar “sensíveis” um único medicamento para tratamento da AIDS comprado numa farmácia pelo consumidor. Esse dado associado à pessoa através do simples número do Cadastro de Pessoa Física (mesmo que para fins únicos emissão de nota fiscal, pois ele está sendo tratado. Coleta é tratamento, mesmo que não ficasse armazenado o dado) poderá ele ser utilizado com

potencial discriminatório. Não é irrazoável dizer que comumente o Cadastro de Pessoa Física em farmácias é coletado do consumidor também para fins cadastro para suposto oferecimento de desconto, vulnerabilizando-o ainda mais diante do seu desconhecimento e condição financeira precária. Fica patente que, sendo assim utilizados esses dados, estão ausentes por parte do controlador a boa-fé, a transparência e o direito à informação clara e precisa em relação ao consumidor. Pois na prática esse dado somado a outro(s) é utilizado comumente não só para formação de perfil, mas para compartilhamento com outras empresas e para compor nota de score de crédito. Cada vez mais recorrente até a venda desses dados, incentivando modelos negócios exclusivos para isso e escancarando que outras grandes empresas já fazem isso faz tempo. Inclusive, André Vellozo, fundador da DrumWave afirma que tem a chancela (parceria) do governo brasileiro através do SERPRO (Serviço Federal de Processamento de Dados), o maior servidor de dados do Brasil, e de início, também com outras três grandes redes (hipotetizamos aqui SERASA EXPERIAN e Boa Vista por exemplo), que servirão de "pontapé inicial para que a 'carteira de dados' seja massificada no país." (VELLOZO, 2022).

Ou seja, para que o consumidor venda seus dados. O que não tem previsão legal a respeito no ordenamento proibindo expressamente a prática nem permitindo. Mas, numa análise e interpretação mais detalhadas, esse tipo de negócio pode ferir direitos e garantias constitucionais, como já se manifesta a doutrina. (QUINTILIANO, 2022). Nesse sentido por exemplo, pode-se vulnerabilizar ainda mais os pobres que por certo, venderão seus dados para ter uma renda extra. Pois o consumidor já faz parecido quando dá suas informações pessoais numa farmácia em troca de desconto num medicamento que não pode pagar ou obter por direito, do Governo.

Mas, já antes dessa notícia acima de 20 de novembro de 2022, a Serasa Experian, como é demonstrado nesse trabalho vendia dados do consumidor, só que em desconhecimento total deste. E sem o consentimento válido do consumidor e ausente a legitimidade para o uso da base de proteção ao crédito, obviamente torna-se uma prática ilegal. Contextualizando a situação com a pontuação de crédito, além da venda dos dados dos consumidores (desvio de finalidade) pela Serasa Experian, a nota do score de crédito por exemplo, poderá ou não ser usada para fins de fornecimento de crédito (sua real finalidade legal juntamente com a oferta de juros mais baixos). Isso deixa claro que mesmo que o tratamento desses dados, sensíveis ou não, fossem permitidos, são eles desnecessários para a proteção ao crédito, ou composição de score, já que esse dado pode não ser considerado para fornecimento do crédito. Por consequência, com amparo nos princípios da necessidade e da minimização na Lei Geral de

Proteção de Dados Pessoais, dados pessoais não devem ser tratados para esse fim de obtenção de nota de crédito.

Neste mesmo sentido, Luz, Neto e Sérgio (2009), afirmam que a análise de crédito compreende a aplicação de técnicas subjetivas, financeiras e estatísticas para avaliar a capacidade de pagamento do tomador de recursos, que é o proponente ao crédito. O sistema utiliza um método de notas, onde está varia de 0 a 1000 para saber em que grau de comprometimento a capacidade de concessão de crédito poderia ser feita ou em qual nível de risco está concessão estaria sendo efetivada. Sendo que, quanto mais próximo esta nota se aproximar de 1000, maior será a possibilidade da liberação de crédito por parte da concedente (SERASA, 2020).

Ou seja, aqui não se fala em garantia, mas em possibilidade de liberação de crédito. E de maneira mais contundente a Serasa ressalta que o *Credit Scoring* é uma ferramenta que não influi na decisão de aprovar o crédito. A aprovação é discricionária da concedente. De acordo com a Serasa, o *scoring* é apenas um instrumento que pode ser consultado antes de concessão de crédito (SERASA, 2020).

Em outras palavras, devido à grande vulnerabilidade do consumidor da qual é subespécie, a vulnerabilidade informacional deste no mercado de consumo digital (MIRAGEM, 2021), permitir o tratamento dos dados deles a partir de uma base legal muito ampla da Lei Geral de Proteção de Dados, é como jogar uma serpente no berço de um bebê. A base legal de proteção ao crédito e por abrangência o uso do *credit score*, no dizer da professora (MARQUES, 2022, p. 9,) é um dos temas que mais preocupam o movimento consumerista brasileiro, pois a possibilidade de discriminação de consumidores e violação de seus direitos fundamentais é muito grande contrariando princípios como da não-discriminação, da autodeterminação informativa e o da finalidade da Lei Geral de Proteção de Dados Pessoais.

> Os temas tratados são muitos e abordados por importantes autores nacionais, desde o impacto do *credit scoring* na economia e o endividamento do consumidor, o uso de informações excessivas nos sistemas de pontuação de crédito e a importância de critérios para aferir discriminação abusiva, se o cadastro positivo é mesmo "positivo" para o consumidor, a privacidade e os limites constitucionais para a utilização da pontuação de crédito; a base legal de análise de crédito na Lei Geral de Proteção de Dados Pessoais (LGPD); os direitos básicos do consumidor na pontuação de crédito e no cadastro positivo, o acesso a produtos e serviços, a responsabilidade civil pelo tratamento dados do consumidor na pontuação de crédito, a compatibilização dos regimes jurídicos da pontuação de crédito e do cadastro positivo, considerando suas regulações e a jurisprudência do Superior Tribunal de Justiça, o desafio da transparência e do direito à informação na pontuação de crédito, o uso de dados alternativos e dados excessivos na composição da pontuação de crédito, a compreensão engajamento da sociedade sobre os escores

> de crédito e seus algoritmos, as discriminações no sistema de pontuação de crédito, sob uma perspectiva de gênero e raça e aprendizagem de máquina e os riscos de alocar recursos predizendo o passado. (MARQUES, 2022, p. 9-10).

Nessa linha, a Súmula 550 do Superior Tribunal de Justiça, só reforça a vulnerabilidade do consumidor na medida em que tem origem no compartilhamento de dados pessoais que o alimentam para fins da nota de crédito; tem potencial violador de direitos da personalidade (nome e intimidade), desfavorece o consumidor perante o mercado. A proteção ao crédito já é efetivada por meio da negativação do nome, dos protestos, da exigência de garantias reais, sendo desnecessário pôr em risco direitos da personalidade do consumidor; fomenta desigualdade nos polos: consumidor x empresa; O risco de analisar unilateralmente contraria direito do consumidor que não tem conhecimento sobre o cadastro e como é o processo de *scoring*. Sobre o acesso à informação, Nunes (2010) diz que o direito de se informar é uma prerrogativa concedida às pessoas e decorre do fato da existência da informação.

A realidade mostra que, de modo geral, nas atividades bancárias, securitárias, de financiamento e de crédito, abusos de toda ordem são cometidos, com graves lesões aos consumidores, decorrentes, sobretudo, da desigualdade de poder entre estes e as instituições financeiras e equiparadas. (CAVALIERI, 2019, p. 104).

Como entendimento de Sousa (2020) a súmula 550 do Superior Tribunal Justiça, deu carta branca para as empresas utilizarem os dados colhidos na internet como fonte para as suas avaliações, sem qualquer tratamento de veracidade e sem o consentimento do consumidor, o qual é o principal (ou deveria ser), interessado para confrontar tais informações. Mas, apesar disso, o consumidor, conforme a súmula sequer tem ciência que o seu nome está inserido em um cadastro, e que ele se encontra disponível para todos aqueles que desejarem saber de sua situação financeira e/ou em qual perfil de pagadores este presumidamente está inserido, acessem tais informações de maneira livre.

> A legislação também gera dúvidas a respeito de quem pode acessar a nota de crédito de um cidadão e com quais propósitos. Os artigos 15 da CP e 9 do Decreto n° 9.936/2019 afirmam que as informações sobre o cadastrado constantes nos bancos de dados somente poderão ser acessadas por consulentes que com ele mantiverem ou pretenderem manter relação comercial ou creditícia. A regra, no entanto, restringe-se às "informações constantes nos bancos de dados" do cadastro positivo. Não há a mesma vedação colocada de maneira abrangente para a nota de crédito, algo a parte das informações que compõem o cadastro. Não há, assim, vedação expressa a0 acesso à pontuação por qualquer pessoa jurídica que pague pelo serviço. O que abre portas para abusos. (SIMÃO; OMS, 2022, p. 100-101).

Assim estas empresas constroem seus próprios bancos de dados e cadastros, e analisa-os somente com base em fontes primárias ou outros bancos similares ao seu, não esclarecendo aos cadastrados sobre a oportunidade prevista em lei para aquele que se sentir prejudicado provar, rebater e retificar as informações errôneas a respeito de sua pessoa. (SOUSA, 2020).

O Ramon Vilarino Pesquisador e doutorando na *University of California Berkeley* em Ciência da Computação, onde se preocupa em usar computação para desenhar políticas públicas que construam justiça social, trabalhou construindo modelos de inteligência artificial na Serasa e no Nubank. (RAMON VILARINO, 2022).

Pois bem, assim ele testemunhou que para explorar as possibilidades de produzir aplicações acessíveis aos consumidores a partir dos *SHAP values*, técnica de predição que utilizou no tempo em que trabalhou no Serasa Experian para construir o primeiro sistema do Brasil e da Experian em todo o mundo, que oferecesse explicações individuais aos consumidores sobre suas pontuações de crédito. Essas explicações segundo Vilarino, integraram o sistema de pontuação de crédito lançado pela SERASA EXPERIAN para o novo cadastro positivo. Vilarino relata que foram construídos alguns sistemas experimentais de pontuação de crédito. Um desses sistemas experimentais utilizava 10 informações para atribuir uma probabilidade de inadimplência a cada consumidor. Entre essas informações constavam os três primeiros dígitos do CEP (CEP-3) de cada consumidor, que delimita regiões maiores que bairros específicos e menores que estados inteiros, a depender da granularidade postal da região. Entendia-se que essa informação era abrangente e agregadora o suficiente para não resultar em discriminações imorais. Porém, um estudo aprofundado do impacto dessa variável nas predições do sistema resultou na primeira documentação pública de um caso de racismo algorítmico no sistema brasileiro de crédito de que temos notícia, sendo o Brasil o segundo maior país em população negra do mundo. Ou seja, imagine-se aí o tamanho da afronta a direitos fundamentais, de personalidade e do consumidor. Pois utilizado o modelo com parte das informações do Censo do IBGE, e simplificadamente demonstrando, através do cruzamento do endereço (Código Postal), raça (cor) dos indivíduos, demonstrou que os cidadãos do sul e sudeste do país, onde há maioria branca, historicamente descendente de europeus, o *score* de crédito foi mais alto, e em contrapartida, no norte e nordeste do país, onde predominantemente, a população é afrodescendente, esses consumidores receberam os *scores* mais baixos do país. Conforme gráficos demonstram abaixo.

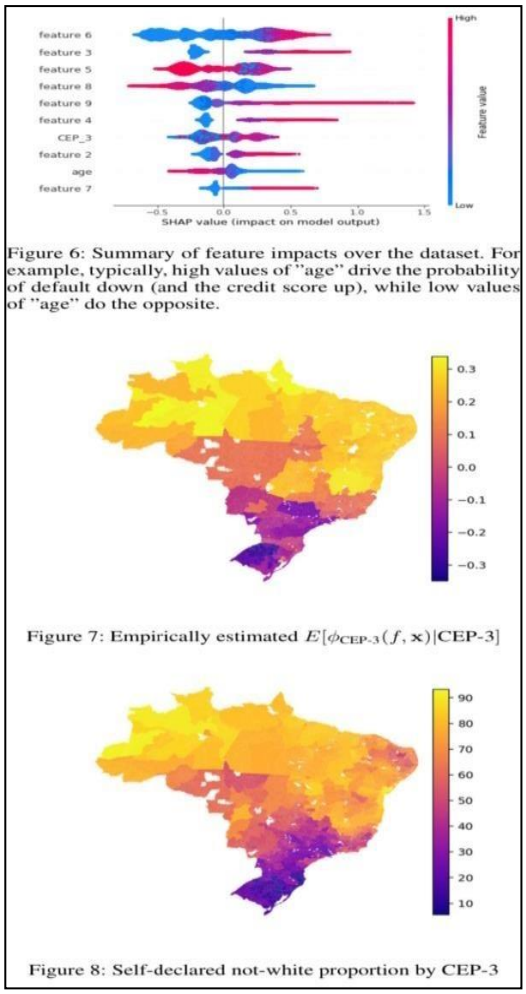


Figura 4 - Mapa de modelo que resultou em discriminação algorítmica no Brasil[5]

Corroborando com o acontecido relatado por Vilarino (2022), e no dizer de Frazão (2021) "quanto mais arraigado for um preconceito na vida real, mais os algoritmos tenderão a vê-lo como um padrão e mais tenderão a replicá-lo se não houver nenhum cuidado para conter esse processo".

Do lido acima, utilizando-se de dados de geolocalização, de raça, cor, origem social se enquadram contrariamente não só à Lei Geral de Proteção de Dados Pessoais, mas também à Lei do Cadastro Positivo praticando discriminação através do uso dos dados pessoais (WINEGAR; SUNSTEIN, 2019. p. 3-5.). Assim a Lei do Cadastro Positivo prevê:

> Art. 3o Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. § 3o Ficam proibidas as anotações de: I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao

[5] Fonte: Ramon Vilarino (2022).

> consumidor; e II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. (BRASIL, 2019).

Em 1995, mesmo antes da Lei do Cadastro Positivo, já decidia o ministro Ruy Rosado no caso em que o Clube de Diretores Lojistas de Passo Fundo confrontava com o art. 43 do Código de Defesa do Consumidor. Constatou-se na situação risco à privacidade e de discriminação. O ministro pronunciou-se no sentido de que:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado e ao particular, para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica. (STJ, 1995).

Em outro julgamento posterior sobre proteção ao crédito do Superior Tribunal de Justiça, do qual dele derivou a súmula 550 da Corte, o ministro revela que a questão do ponto de vista do consumidor não está em diferenciar o *score* de crédito dos bancos de dados e dos cadastros de consumidores, pois se estipulou que o instituto não se confunde com o cadastro de consumidores ou o banco de dados.

Mas, acontece que o *score* de crédito está intrinsecamente ligado à progressão e maior articulação dos agentes concedentes de crédito, e por diversos princípios presentes nas legislações consumeristas que a ele se aplicam. Vê-se que o problema é que a decisão do Superior Tribunal de Justiça ignorou o que realmente importa: embora tenha sido criado como um método para a avaliação do risco de concessão de crédito, o *score* atribuído aos cidadãos pode transpor o cenário de fornecimento de crédito e passar a ser indicador de "bom caráter", de modo a influenciar outras relações jurídicas dos cidadãos. Além disso, os algoritmos usados na formulação do score de crédito se alimentam de dados pessoais e, portanto, é necessário que exista algum tipo de proteção especial a esses dados e que tipos de dados. (STJ, 2011).

Afora o risco de discriminação, a promessa de redução na taxa de juros através do cadastro positivo "compulsório" aumentou o volume da base de dados do cadastro positivo de 5,5 milhões para 100 milhões de cadastrados (STEINWASCHER, 2020). Mas, os estudos

mostram que essa promessa não foi cumprida. Pois, atualmente a taxa média de todas as modalidades de crédito ao consumidor no Brasil é de 104,20% ao ano. O Brasil, historicamente e atualmente, é o país que tem as maiores taxas de juros do mundo, segundo a ANEFAC-Associação Nacional dos Executivos de Finanças, Administração e Contabilidade. (ANEFAC, 2021).

Trajetoriamente o país ostenta as maiores taxas de juros do mundo, uma posição vergonhosa e indutora de endividamento das famílias, pois amparada numa política de crédito injusta, abusiva e que explora a desigualdade social por meio da redução do poder de compra das famílias com transferência de renda na forma de juros para o sistema financeiro. (SOUZA, 2022, p.65).

A nova lei do cadastro positivo que ancora o *score* de crédito, passou por 4 governos, sendo vetada nos governos Lula e Dilma, e em 2017, passou no governo Michel Temer, a ter Projeto de lei aprovado com dispensa da necessidade de autorização do consumidor para a inclusão no cadastro positivo. Em outubro**,** a proposta aprovada e passou à Câmara. Em bril de 2019 **–** Aprovado pela Câmara. Em março**,** o projeto foi sancionado pelo presidente Jair Bolsonaro (VEJA, 2019).

Não é de hoje a atividade de concessão de crédito no Brasil. Mas, houve a fase que não havia regulação alguma, em seguida, a introdução do CDC, do Cadastro Positivo, e por último, a Lei geral de Proteção de Dados (com o reconhecimento do direito fundamental autônomo à proteção de dados pessoais.

Analisando antecedentes, curioso é que no Projeto de Lei 40/60 de 2012 da Lei Geral de Proteção de Dados, do Deputado Milton Monti, não se incluía ou se falava em bases legais (proteção ao crédito) ou sequer, em lei do Cadastro Positivo, base do sistema score de crédito. (BRASIL, 2012).

O Projeto de Lei n. 5.276/16 recebeu 11 Emendas de Plenário. Numa delas, do Deputado Paes Landim, a Emenda Parlamentar 8 acrescia a hipótese de os dados pessoais poderem ser tratados também para fins de proteção de crédito (Art. 7, X) que, naquele momento, foi acolhida pelo relator Orlando Silva no encaminhamento das orientações sugeridas ao Projeto de Lei:

> [Art. 7o] – Hipóteses de tratamento Cotejando os Projetos de Lei em análise propomos dez hipóteses para o tratamento de dados pessoais, sendo, a principal delas, mediante a obtenção de consentimento livre, informado e inequívoco. Prevemos o tratamento no cumprimento de obrigação legal, regulatória, contratual, estudos, processos judiciais, entre outros. Ademais, julgamos pertinente incluir (inciso X) recepção expressa à possibilidade de abertura de cadastro de

> consumidores para proteção do crédito, tal como consagrada no art. 43 do Código de Defesa do Consumidor. Porém, com as seguintes ressalvas, já compreendendo que havia riscos aos titulares de dados: Devido à popularidade e ubiquidade das novas mídias digitais, percebemos que há casos em que o próprio titular torna parte de seus dados manifestamente públicos. Para esses casos, incluímos um novo §4o, em que fica dispensada a obtenção do consentimento, resguardados os direitos do titular e demais princípios desta Lei, por exemplo, a solicitação de exclusão de dados ou suspensão do tratamento. A profusão de aplicações para os dados pessoais, assim como de empresas do mesmo e de outros grupos empresariais que realizam o compartilhamento de dados coletados de titulares, evidenciou, em vários casos, a perda do controle do titular sobre seus próprios dados. Como forma de permitir um maior domínio, assim como facilitar a revogação de consentimentos porventura concedidos, prevemos um novo §5o, dispondo que na transferência de dados para outros responsáveis será necessária a obtenção de consentimento específico para esse fim. Ressalte-se que essa autorização pode ser obtida ao mesmo tempo em que se obtêm os demais consentimentos. Apenas deverá ser destacado dos demais. (BRASIL, 2012).

Mas, ao final, o relator rejeitou a Emenda Parlamentar que pretendia a inserção da base legal de proteção ao crédito na Lei Geral de Proteção de Dados por considerá-la por demais ampla. A esse respeito, EMP no 8, Dep. Paes Landim: somos pela rejeição, por entendermos que a expressão “proteção ao crédito” é por demais ampla, podendo ensejar interpretações extensivas e fragilizando o direito ao sigilo financeiro dos titulares cuja proteção à privacidade é o objetivo principal dessa Lei.

Porém, a base legal da proteção ao crédito foi aprovada no apagar das luzes e incorporou-se à Lei Geral de Proteção de Dados Pessoais, sancionada em setembro de 2020.

Essa base legal por demais ampla na interpretação para a utilização dos dados pessoais, abriu portas para a perfilização. "O processo de 'descobrir' correlações entre dados em bancos de dados que podem ser usados para identificar e representar um sujeito humano ou não humano (indivíduo ou grupo) e/ou a aplicação de perfis (conjuntos de dados correlacionados) para individualizar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria". (HILDEBRANDT, 2022).

É isso que fazem os birôs de crédito, corretores de dados, como destacado pelo relatório da *Cracked Labs*, “os corretores de dados também calculam pontuações que preveem o possível comportamento futuro de um indivíduo, em relação, por exemplo, à estabilidade econômica de alguém ou aos planos de ter um filho ou de mudar de emprego” (CHRISTL, 2022).

A exemplo da Serasa Experian, que desde 2007 faz parte do Grupo Experian, uma das maiores agências de crédito do mundo, deixa clara a hipótese de utilização dessa base legal de proteção ao crédito em sua página de perguntas frequentes, ao responder o questionamento

“Por que a Serasa Experian pode tratar os meus dados se eu não forneci o consentimento?” (SERASA, 2022).

O consentimento, ou seja, a autorização expressa do titular, é uma das hipóteses que legitimam o tratamento de dados pessoais, mas não é a única. Existem outras nove hipóteses que podem ser utilizadas como base legal para justificar o tratamento conforme a finalidade e a utilização dos dados, como a proteção do crédito ou o legítimo interesse, por exemplo. Nesses casos, desde que o tratamento seja feito conforme determina a Lei Geral de Proteção de Dados Pessoais, principalmente quanto ao cumprimento dos princípios e dos direitos do titular, não há necessidade de autorização expressa do titular”. (BIONI, 2020).

As hipóteses de tratamento de dados também são resultado do direito que legisla de maneira a correr contra o tempo refletindo, deixando escapar nas normas o que nelas não deveria conter: potenciais violações. Mas esse embate tempo e direito não é de hoje. Em 1942, pelo economista Joseph Schumpeter, em sua obra Capitalismo, socialismo e democracia, apresenta o conceito de destruição criativa, que reflete até hoje as discussões sobre os desafios que a inovação tecnológica representa ao direito. (BAPTISTA; KELLER, 2016).

Na obra Direito do Consumidor e Novas Tecnologias, Arthur Pinheiro Bassan e Tales Calaza discorrem sobre a necessária atualização do Código de Defesa do Consumidor. Os referidos autores reforçam a necessidade da inclusão de alguns artigos previstos no Projeto de Lei n.3.514/15. Ele altera a Lei n° 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor) para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9° do Decreto-Lei n° 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais.

Nesse sentido, é necessário o acréscimo do inciso XI ao artigo 6 do CDC, proposto no Projeto de Lei n° 3.514/15, que se encontra pendente de apreciação, consolidando como direito básico do consumidor à proteção de dados, nos seguintes termos: "XI-a autodeterminação, a privacidade e a segurança das informações e dados pessoais prestados ou coletados, por qualquer meio, inclusive o eletrônico". (BRASIL, 1990).

Logo em seguida, propõe o Projeto o acréscimo do Inciso XII, que proíbe expressamente o assédio de consumo e a discriminação, isto é, "XII - a liberdade de escolha, em especial frente às novas tecnologias e redes de dados, vedada qualquer forma de discriminação e assédio de consumo". (BASSAN; CALAZA, 2021, p. 103).

No caso do Código Civil, já se reclama e discute novas leituras e parâmetros pra a definição e positivação atualizada dos conceitos de domicílio e responsabilidade civil objetiva e subjetiva na era da informação.

No caso da Lei do Cadastro Positivo, o confronto com a Lei Geral de Proteção de Dados Pessoais de acordo com especialistas, envolve também a questão da privacidade, bem como e em especial a transparência dos critérios dos cadastros e a autorização dos bancos de dados de compartilharem as informações – neste caso, portas escancaradas para os vendedores de serviços, produtos e ações de marketing.

Nesse raciocínio é possível aventar a possibilidade de que essas leis seriam em parte, uma fonte de inspiração ultrapassada e/ou colidente com direitos nos novos tempos representada pela Lei Geral de Proteção de Dados Pessoais.

E tal base legal como consta do artigo 7, inciso X, da Lei Geral de Proteção de Dados Pessoais, foi supostamente harmonizada com suas normas antecessoras: a lei do cadastro positivo e o código de defesa do consumidor e o código civil. O Instituto de Defesa do Consumidor sempre considerou que a inclusão automática dos consumidores no cadastro positivo, o sistema *opt out*, viola princípios fundamentais constitucionais e direitos básicos do consumidor. Além da autodeterminação informativa (BRITO, 2022, p. 8). O que interessa aqui para fins desse estudo, não é a ideia da proteção *latu sensu*, que está no espírito e declaradamente evidenciada nessas leis às suas épocas vigoradas (BRASIL, 1990; 2002; 2019), mas como elas foram positivadas, descritas nas suas normatizações, a ponto de no cenário atual de vulnerabilidades digitais insurgentes, onde são imprevisíveis todas as frentes e formas de violação de dados pessoais, põe essas normas fundantes em cheque. Nesse raciocínio é possível aventar a possibilidade de que essas leis seriam em parte, uma fonte de inspiração incompleta para os novos tempos e a codificação mais atual que o representa no ordenamento jurídico brasileiro, qual seja, a Lei Geral de Proteção de Dados Pessoais. E sendo mais detalhista, se a inspiração nelas para de certa forma, lastrear a Lei Geral de Proteção de Dados Pessoais, seria então nesses pontos cruciais da proteção do consumidor, uma arriscada iniciativa. Pois fundar um diploma de proteção de dados sob um solo defasado e potencialmente causador de insegurança jurídica para os titulares de dados pessoais não condiz com o espírito de qualquer lei.

Corroborando, de acordo com Zanatta (2009), as obrigações informacionais e antidiscriminatórias já estavam relativamente consolidadas no Brasil, em termos jurídicos, por meio do Código de Defesa do Consumidor (Lei 8.078/1990) e da Lei do Cadastro Positivo (Lei 12.414/2011). A Lei de Proteção de Dados Pessoais, na esteira da General Data Protection

Regulation (GDPR), trouxe um elemento adicional ao adotar uma espécie de "direito à explicação" em decisões automatizadas de perfilização. Chamarei essa obrigação como de "natureza dialógica", inspirada em teorias pedagógicas contemporâneas, pois há nela um elemento de comunicação que não é unidirecional, mas uma obrigação que implica em um engajamento interrelacional que tem um certo caráter pedagógico, de explicar como um determinado processo técnico (uma decisão automatizada baseada em perfilização) funciona. Sustento, enfim, que esse ato de explicação – chamado por doutrinadores contemporâneos de "*right to explanation*" tem um caráter pedagógico imposto pela própria lei. A opção, por parte do controlador, de realizar a perfilização implica, também, em assumir obrigações de níveis informacionais, antidiscriminatórias e dialógicas.

Mas, voltando à inserção da base legal de proteção ao crédito positivada a Lei Geral de Proteção de Dados Pessoais, no sentido da proteção ao consumidor, é torná-la empecilho para que se estabeleça uma compreensão extensiva e eficaz para a aplicação da rede de proteção, desobedecendo inclusive, a maior de todas as fontes, o pilar central de onde emana a defesa do consumidor. A Carta Magna em seu artigo 1, estabelece que normas de proteção e defesa do consumidor são de ordem pública e interesse social. "Art. 1° O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5°, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitórias" (BRASIL, 1988).

Continuando, no seu artigo 4, incisos I e II, o Estado reconhece a vulnerabilidade do consumidor e que suas ações serão no sentido de proteger "efetivamente" o consumidor, inciso III: fala em harmonização de interesses da relação de consumo, compatibilização com interesses econômicos de maneira a promover o equilíbrio na relação. Ainda no inciso X, a prevenção e tratamento do superendividamento como forma de evitar a exclusão social do consumidor é mandamento constitucional.

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo; II - ação governamental no sentido de proteger efetivamente o consumidor: III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores; X - prevenção e tratamento do superendividamento como forma de evitar a exclusão social do consumidor. (BRASIL, 1988).

Fere o princípio fundamental da privacidade conforme (repetindo) o voto do relator Orlando Silva na tramitação da própria do Projeto de Lei da própria Lei Geral de Proteção de Dados Pessoais: EMP no 8, Dep. Paes Landim: somos pela rejeição, por entendermos que a expressão "proteção ao crédito" é por demais ampla, podendo ensejar interpretações extensivas e fragilizando o direito ao sigilo financeiro dos titulares cuja proteção à privacidade é o objetivo principal dessa Lei. (BRASIL, 2012).

Trata-se, no caso em tela, de inequívoca violação de garantias pétreas como a proteção à intimidade e à privacidade.

No entanto, as pressões econômicas viabilizaram posteriormente de forma pouco ética e carente de boa-fé, sua inclusão legislativa. (UOL, 2019).

Desta feita, base legal de proteção ao crédito (recepcionando a lei do Cadastro positivo com seu modelo *Opt-out*) inserida na Lei Geral de Proteção de Dados Pessoais já encontra indícios de motivos suficientemente plausíveis na Constituição Federal para a alegação de sua inconstitucionalidade. Carecendo de vício na sua origem: ter inserido o cadastro positivo é ato temerário e grave por parte do estado e de agentes do setor econômico terem exposto, automaticamente, a condição econômica, a situação financeira e a vida pessoal de mais de 100 milhões de brasileiros desrespeitando regras e fundamentos básicos do Estado de Direito.

Material, pois fere o conteúdo, princípios, direitos e garantias assegurados pela Constituição como demonstrado acima e formal, que se refere ao procedimento ou forma de elaboração da norma.

> Ao falar-se do valor normativo da constituição aludiu-se à constituição como lex superior, quer porque ela é fonte de produção normativa (norma *normarum*) quer porque lhe é reconhecido um valor normativo hierarquicamente superior (superlegalidade material) que faz dela um parâmetro obrigatório de todos os atos estatais. A idéia de superlegalidade formal (a constituição como norma primária da produção jurídica) justifica a tendencial rigidez das leis fundamentais, traduzida na consagração, para as leis de revisão, de exigências processuais, formais e materiais, 'agravadas' ou 'reforçadas' relativamente às leis ordinárias. Por sua vez, a parametricidade material das normas constitucionais conduz à exigência da conformidade substancial de todos os actos do Estado e dos poderes públicos com as normas e princípios hierarquicamente superiores da constituição. Da conjunção destas duas dimensões — superlegalidade material e superlegalidade formal da constituição— deriva o princípio fundamental da constitucionalidade dos actos normativos: os actos normativos só estarão conformes com a constituição quando não violem o sistema formal, constitucionalmente estabelecido, da produção desses actos, e quando não contrariem, positiva ou negativamente, os parâmetros materiais plasmados nas regras ou princípios constitucionais". (CANOTILHO, 1999, p. 826).

Sobretudo quando o assunto, considerando aqui o consumidor como protagonista da Lei Geral de Proteção de Dados Pessoais, e o aumento exponencial da assimetria na relação consumerista tornando-se mercadoria. Afinal, "tornar-se e continuar sendo uma mercadoria vendável é o mais poderoso motivo de preocupação do consumidor, mesmo que em geral latente e quase nunca consciente" (BAUMAN, 2008), que avança a cada milésimo de segundo, num clique ou até mesmo sem interação direta com as novas tecnologias; esse mesmo consumidor sem saber ou ter clareza, está ali sendo ao mesmo tempo, um dos polos e o verdadeiro objeto contratual daquela relação de consumo. Ou melhor, está sem entender as finalidades de uma vigilância, sua extensão, o tamanho do risco pela exposição, as consequências desse risco real, com quem esses dados são compartilhados, a vantagem financeira sobre isso, e eventual lucro continuado dessa relação que não foi objeto dessa suposta relação contratual e o pior, à revelia do consumidor. Vale ressaltar que o risco zero não existe, mas diante de cada hipótese de tratamento de dados pessoais, em especial com relação a dados sensíveis, mostra-se necessária a implementação de mecanismos efetivos para prevenção de incidentes de segurança e dados aos titulares de dados pessoais (INPD, 2021).

Somado a essa falta de transparência e boa-fé por parte dos agentes de tratamento de dados, que viola direitos dos titulares, há ainda o trinômio: base legal de proteção ao crédito positivada na Lei Geral de Proteção de Dados Pessoais, o chamado *score* de crédito e o uso de inteligência artificial, que juntos podem ter efeito demolidor passando por cima de direitos fundamentais, humanos, de personalidade, de titulares de dados.

A base legal de proteção ao crédito no Brasil foi uma imposição do sistema econômico-financeiro para proteger o sistema, colocado numa lei que visa exatamente o oposto: proteger o consumidor na sua faceta predominante como titular de dados. (OMS, 2022, p.18).

O *score* de crédito que só pode hoje ser analisado numa interpretação extensiva, *lato sensu*, ampla pois se alimenta, se desenvolve, aumenta e se multiplica a partir de fontes legais e de inúmeras alheias e não declaradas, extrapolando sua conceituação, finalidade, limitada à conexões previstas na Lei do Cadastro Positivo necessitando assim de atualização da referida Lei n. 12.414/11 que não abrangeu um tema necessário os chamados “dados alternativos” aqueles que não são tradicionalmente usados pra análise do *score* de crédito e o potencial discriminatório no seu uso. Eles vão desde o pagamento de serviços públicos, pagamento de aluguel de imóvel, e segundo o pesquisador Victor Doering da Silveira (2022, p. 279-278)

Dados alternativos não-financeiros, por outro lado, não têm relação direta com a vida financeira do consumidor, mas podem ter, considerados a partir de cruzamento com outras informações e em determinados contextos, na análise preditiva e consideração da concessão

de crédito e dos seus termos. Exemplos desse tipo de informação são dados sobre a educação formal e histórico profissional de pessoas naturais, atividades em mídias sociais e até mesmo históricos de navegadores da Internet - informações geralmente definidas como Big Data.

Um exemplo relevante de uso desse tipo de informação é o nível de educação formal, a área de especialização e o histórico profissional do cadastrado: embora esse tipo de dado não tenha sentido financeiro inerente, é possível inferir a partir dele a probabilidade de que o titular dos dados venha a ocupar um cargo com maior ou menor remuneração no curto ou médio prazo - o que, por sua vez, afeta a probabilidade de que venha a ocorrer inadimplência. Empréstimos considerados como de maior risco, portanto, tendem a ser negados ou concedidos em proporções menores ou mediante condições menos generosas (e.g. taxas de juros mais altas, menores oportunidades de refinanciamento, cláusulas penais com multas moratórias mais elevadas etc.), a fim de compensar o risco assumido pelo credor pela fixação de um prêmio maior. Há ainda concedentes de crédito que colhem outros tipos de dados não-financeiros, como endereços de e-mail ou informações do histórico de navegação, para filtrar possíveis fraudes.

As fintechs, empresas que oferecem serviços financeiros através da tecnologia, coletam dados de celular, geolocalização e redes sociais para avaliação de crédito, tendo acesso inclusive a dados sensíveis. (GLOBO, 2021).

Em 2016, já se demonstrava o risco da coleta, do tratamento, do controle e transmissão de dados pessoais por terceiros: o grande desafio que se coloca à frente dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos governos. Há possibilidade de verificação, por meio de um monitoramento online, de preferências artísticas, musicais, hábitos de vida, de viagens, operações financeiras, orientação sexual, crenças religiosas, entre outros (RAMINELLI; RODEGHERI, 2016 p. 92).

Com o aumento do volume de dados disponíveis, a quantidade de dispositivos que coletam dados com o avanço tecnológico da internet das coisas, esses riscos são cada vez maiores à privacidade e segurança dos usuários. São televisores inteligentes, assistentes eletrônicas, geladeiras conectadas, câmeras de circuito interno, além dos celulares, coletam dados estritamente particulares e íntimos, que são armazenados e compartilhados ininterruptamente, até mesmo quando estão desligados, alimentando a massa de dados dessas empresas. (MAGRANI, 2012, p. 24).

De acordo com o Instituto Tecnologia e Sociedade, os birôs de crédito hoje fornecem dados pessoais também para o setor público não só para o setor financeiro. O que deixa claro essa mudança inclusive na finalidade dessas organizações. E durante a pandemia da COVID

- 19, ampliaram a coleta de dados para seu indicador de vulnerabilidade sob o argumento de que precisava-se tomar decisões mais acuradas no contexto de uma pandemia. O que de acordo com Bianca Kremer, acentuou a discriminação racial na concessão de crédito para pessoas negras (KREMER, 2022 p. 232).

Toda a Manipulação desses dados sem a ciência ou conhecimento em prejuízo do direito à informação do consumidor, da sua autodeterminação informativa, segundo o pesquisador (DOERING, 2022, p. 278), promovem discriminação, riscos de transparência e auditabilidade pela maneira que são coletados, prejuízo à consequente possibilidade de revisão diante de decisões desfavoráveis, prejuízo no acesso ao credito, risco na confiabilidade dos dados (acurácia) e à segurança da informação posto que com um volume maior de informações de perfis para a avaliação desses birôs de crédito o dano seria muito maior em caso de vazamento.

Reforçando de outra forma o argumento, os métodos usados no Score nos últimos anos ultrapassaram as técnicas estatísticas tradicionais e passaram a envolver métodos inovadores, como inteligência artificial, incluindo algoritmos de aprendizado de máquina. Em alguns casos, a adoção de soluções inovadoras e técnicas também ampliou a gama de dados e fontes de dados que podem ser considerados relevantes para pontuação de crédito, modelos e decisões. (PÁDUA, 2015). Mesmo com a vigência da Lei Geral de Proteção de Dados Pessoais, a *Serasa Experian* através de site solicitava na área em que era possível acessar o *score* de crédito, estranhamente, a senha de banco dos consumidores, o que chamou atenção do Procon por violação do CDC e da Lei Geral de Proteção de Dados Pessoais:

> A opção para a pesquisa online constava na parte da ‘área do cliente’ do site da empresa espaço fechado que, para ter acesso, é preciso fazer um cadastro prévio. Nessa área é possível ver o *score* de crédito, se o nome do consumidor está ‘limpo’ (sem nenhuma pendência financeira), verificar a situação do CPF junto à Receita Federal, entre outras funcionalidades. (UOL, 2021).

Tais condutas levam o *score* de crédito a não funcionar e subverter o fim a que ora se deveria se destinar. Gerando inclusive, enriquecimento ilícito através da venda dos dados pessoais. (SANTANA, 2020).

Também se comprovam tais fundamentos na seguinte ação civil pública promovida contra a Serasa Experian:

Na prática a Serasa está vendendo os dados pessoais de mais de 150 milhões de brasileiros para empresas interessadas em prospectar novos clientes, sem que exista qualquer tipo de conhecimento por parte dos titulares das informações. Venda de dados para fins

publicitários das empresas contratantes, sem que o titular do CPF tenha qualquer tipo de relação contratual com a compradora de seus dados. (OUL, 2020).

Somado a isso, ainda pairam riscos decorrentes de vazamentos de dados pessoais como em Ação civil pública com pedido de liminar, ajuizada pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, *Compliance* e Segurança da Informação - SIGILO em face da União e Serasa Experian S.A., por suposto vazamento de dados de cerca de 223,74 milhões de consumidores, em janeiro de 2021. (JUSBRASIL, 2021). O que o levaria a não funcionar e a desviar do fim a que ora se deveria se destinar.

Ademais, o uso de inteligência artificial para confecção de perfil do consumidor protegida pela Lei do Cadastro Positivo e pela súmula 550 do Superior Tribunal de Justiça, sob o argumento de que "é segredo de negócio" e, portanto, sigiloso, só dá margem para que se cometam abusos por meio desse "método estatístico de avaliação de risco". Decisão feita por meios automatizados, envolvendo sistemas complexos de inteligência artificial, ocorre na formulação da própria pontuação de crédito - o que é gerido pelos birôs de crédito. Será essa pontuação que, examinada pelo consulente, poderá gerar uma concessão de crédito a juros mais ou menos baixos. Causa estranheza, dessa forma, que o legislador tenha conferido este direito perante o consulente que, de maneira geral, é contratante do serviço oferecido pelos birôs de crédito. (SIMÃO; OMS, 2022, p. 101). Pois perfil a partir do *score* do consumidor é dessa forma a representação de sua personalidade manipulada ao bel prazer do sistema financeiro. Pois como foi aprovado por Emenda Parlamentar que antecedeu a Lei Geral de Proteção de Dados Pessoais e na própria Lei, ficou limitado o princípio da transparência pela incógnita e ampla interpretação parcial do que venha a ser considerado segredo industrial e comercial. (PASQUALE, 2015, p. 86).

> EMP no 9, Dep. Paes Landim: somos pela APROVAÇÃO, pois entendemos que todos os casos de informação ao titular e ao órgão competente devam respeitar e observar os eventuais segredos comercial e industrial. Art. 6o As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (BRASIL, 2012).

Sobre tratamento desses dados o que vem se tornando pacífico na doutrina é se que leva à manipulação de comportamentos, entrincheirando o livre desenvolvimento da personalidade e consequente e hipotético desmonte do ser humano em sua essência. E isso demonstra visível a desordem caótica para que se consiga viabilizar a proteção de dados do

indivíduo, sobretudo no Brasil onde cultura de proteção de dados engatinha. E sempre relacionando a outro problema que nasce da inteligência artificial que é o uso de algoritmos.

> Algoritmos não estão imunes ao problema do fundamental da discriminação em que suposições negativas e infundadas cristalizam-se em preconceitos. Eles são programados por seres humanos, cujos valores estão incorporados em seu software. E eles muitas vezes usarão dados presos ao mais humano dos preconceitos. (PASQUALE, 2015, p. 38).

Assim, essa caixa preta do *score*, onde é elaborado o perfil do consumidor, abriga alegadamente pelos birôs de crédito, a zona dos segredos comerciais e industriais. E é lá onde está o cerne da questão da discriminação algorítmica (não só no *input*) posto que o direito de acesso, da transparência, de informação, e a possibilidade de mitigação ficam prejudicados já que as organizações podem se utilizar desse argumento para negar direito ao consumidor.

O *profiling*, ou perfilização automatizada, segundo Hildebrandt se estabelece quando máquinas são pré-programadas para recuperar correlações inesperadas em massas de dados agregados em grandes bancos de dados. (CLARKE, 1993, p. 403).

*Profiling* no mesmo sentindo, está definido na Lei Geral de Proteção de Dados no artigo 20 quando o legislador fala de "[...] decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". (BRASIL, 2021). Sobre formação de perfis, discriminação e direitos, Zanatta (2008) deixa claro através do estudo de obras referenciais sobre proteção de dados pessoais que o caráter aparentemente técnico dos debates sobre algoritmos e *profiling* – traduzido como "perfilização", expressão utilizada por Marta Kanashiro e outros pesquisadores brasileiros –, evidencia na verdade, uma a profunda conexão com questões éticas e de justiça.

Se a escolha desses fatores, ou de quaisquer outros fatores, assentada numa relação de pertinência lógica, justifica a discriminação realizada é questão que somente poderá ser aferida a partir do perfeito conhecimento de quais exatamente foram os critérios eleitos e qual foi o tratamento concretamente dispensado. (CALABRICH, 2018, p. 8).

Por conseguinte, transparência como também se verá adiante, as explicabilidades se fazem extremamente importantes, visto que não se tendo conhecimento de como foi tomada a decisão, não há como afirmar se ela foi lícita ou ilicitamente discriminatória. Logo, no que tange ao princípio da (VI) transparência, tem-se a "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." (CALABRICH, 2018, p. 8).

Para mais, a própria Lei Geral de Proteção de Dados nos parágrafos 1§ e 2§ do artigo 20, estabelece que o controlador deve fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo sistema para a tomada da decisão, e ainda disciplina que na ausência dessa transparência, a Autoridade Nacional de Proteção de Dados poderá auditar o sistema com o intuito único de verificação de aspectos discriminatórios. Em sentido semelhante, afirma Maria Cristina Lindoso (2019, p. 100) quando declara que as auditorias são uma forma de controle das estruturas automatizadas: "Há, portanto, um reconhecimento legal de que esse mecanismo pode mapear o mal ferimento das estruturas aos princípios que devem nortear toda a automatização na leitura de dados pessoais".

A Lei Geral de Proteção de Dados dispõe das garantias do titular dos dados no Capítulo III, denominado "Dos Direitos do Titular". Por ser uma legislação que trata sobre o direito à informação, ela possui diversos dispositivos que buscam informar ao titular dos dados o que efetivamente ocorre no tratamento dos seus dados pessoais. Portanto, tem-se o direito à transparência, o direito a ser informado sobre a existência do tratamento, positivado no artigo 19: "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular". Também no direito de acesso entendido assim o inciso II do mesmo artigo, "[...] por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial". (BRASIL, 2020).

Ademais, a Lei Geral de Proteção de Dados Pessoais possui dois instrumentos relevantes de proteção ao titular dos dados pessoais quando se trata de decisões automatizadas: o direito à explicação e o direito à revisão. Importante, contudo, ressaltar que o primeiro não está expressamente positivado na legislação brasileira, nem na legislação europeia.

Mas Julia Powles e Andrew Selbst (2017) afirmam que embora não exista uma disposição legal com os dizeres textuais "direito à explicação" no Regulamento Geral de Proteção de Dados Europeu, esse direito não é ilusório. A legislação fornece direitos a informações significativas sobre a lógica envolvida em decisões automatizadas, portanto, concluem:

Achamos que faz sentido chamar isso de direito à explicação, mas esse ponto é menos importante do que a substância do direito em si. Acreditamos que o direito à explicação deve ser interpretado de forma funcional, flexível e deve, no mínimo, permitir que o titular dos dados exerça seus direitos de acordo com o Regulamento Geral de Proteção de Dados Europeu e a legislação de direitos humanos. (SELBST; POWLES, 2017, p. 10).

Em sentido semelhante, pode-se entender o direito à explicação na legislação

brasileira. Quando o legislador estabelece no parágrafo 1o do artigo 20 da Lei no 13.709/2018, “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”, entende-se como um direito que tem como objetivo que o titular dos dados possa obter informações inteligíveis sobre a forma como os seus dados estão sendo tratados em sistemas automatizados. (BRASIL, 2018).

Além do direito a conhecer os critérios e procedimentos de processamento da decisão automatizada, a legislação ainda possibilita ao titular solicitar a revisão dessa decisão no caso de ela estar incorreta, chamado de direito à revisão, previsto no *caput* do artigo 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.

Percebe-se que o legislador se preocupou em estabelecer explicitamente a possibilidade de questionar a decisão desses sistemas algorítmicos de inteligência artificial, além disso solicitar a revisão dessa tomada de decisão caso tenha tomado por base critérios e procedimentos que impactam direitos e liberdades fundamentais de forma abusiva e desproporcional.

O artigo 20, que como observado traz o direito à revisão, em primeiro momento continha um trecho que estipulava que essa revisão deveria ser realizada por uma pessoa natural. No entanto, esse parágrafo foi vetado pelo Projeto de Lei de Conversão no 7, de 2019 (MP no 869/2018) por contrariar interesse público e inviabilizar modelos de negócios. (BRASIL, 2018).

Isso abriu margem para as revisões das decisões automatizadas serem também realizadas por outros algoritmos. Em suma, todo o processo de tomada de decisão por algoritmos de inteligência artificial poderá ser realizado pelos mesmos, sem nenhuma intervenção e juízo de valor de um ser humano, nem mesmo quando solicitada a revisão dessas decisões. (CALABRICH, 2019).

Faz-se necessária uma observação no que diz respeito ao *profiling* dos algoritmos de decisão autônoma, que diferencia indivíduos com base em características prováveis de um grupo. (RIBEIRO, 2021). Ou seja, o indivíduo não é julgado pelo que é, mas por uma probabilidade e sem direito à revisão humana, em tese.

Para explicitar minimamente melhor essas ideias sem denotar radicalismo hermenêutico e/ou doutrinário, ou como alguns poderiam reclamar, sem a demonização da

tecnologia e da inovação, é necessário traçar uma linha do tempo mundo real (acontecimentos) e esforços legislativos. Ou seja, numa contextualização de datas em que as leis foram criadas, as necessidades emergentes da sociedade e os acontecimentos, e a devida e proporcional previsão e eficácia para conter comportamentos ilegais. Quais sejam: Código Civil, Código de Defesa do Consumidor, Lei do Cadastro Positivo, súmula 550 do *score* de crédito, a proteção ao crédito no pré-projeto da Lei Geral de Proteção de Dados, bem como seus polêmicos desdobramentos econômicos, sociais e normativos até a sanção e entrada em vigor da lei em comento. Na sequência, a positivação da proteção ao crédito como base legal para tratamento de dados pessoais na Lei Geral de Proteção de Dados, e por último, o reconhecimento do Direito Fundamental à proteção de dados pessoais como direito fundamental autônomo na Constituição Federal, juntos formam em parte, um sistema incompatível e incompleto para a proteção do indivíduo pelo que já foi explicitado.

Mas, em quais leis e códigos nomeadamente há de haver no mínimo novas interpretações ou mesmo novas leis que sejam consonantes à disciplina da proteção de dados pessoais e dos direitos fundamentais, e/ ou alterações legislativas e regulamentares para que se possa identificar de forma mais efetiva e segura, como o consumidor estará mais protegido em seus direitos.

Como prevenção, que tipo de responsabilidade civil há de ser invocada no compartilhamento dos dados dos consumidores. O que há de largada a ser considerado é que em qualquer responsabilidade civil que venha a ser pacificamente adotada, da mais clássica como as que decorrem das teorias objetiva ou subjetiva, até as mais digamos, disruptivas como são classificadas: de especial ou especial qualificada pelo ilícito, esta última defendida pelo professor Nelson Rosenvald, deverá incorporar o devido respeito ao princípio da precaução. Este objetiva inclusive inibir atividades potencialmente danosas já que há a certeza de riscos e danos inclusive desconhecidos, inimagináveis e irrastreáveis até então, em virtude do tratamento de dados pessoais com o uso de inteligência artificial. (BECK, 2002, p. 237).

A precaução como princípio extraído da Constituição Federal em seu art. 225 e 925 do Código Civil, e da Lei Geral de Proteção de Dados Pessoais com o princípio da *accoutability* e os relatórios de impacto à proteção de dados pessoais (BIONI, 2018) será melhor estudada adiante. Em seus objetivos: o de evitar o *laissez faire* (deixar fazer do liberalismo econômico) em situações de incerteza legítima e produzir o conhecimento sobre o risco em causa, seja para dar origem à ação preventiva, seja para liberar a atividade afastando a possibilidade de risco. (ARAGÃO, 2008).

Adiantando, fala-se na doutrina em princípio da precaução quando as informações que

se têm sobre os riscos são precárias, não se podendo determinar com segurança um juízo de avaliação razoavelmente correto. (AYALA; LEITE, 2004, p. 75). Sob uma abordagem proativa dos processos de decisão sobre os riscos, explica-se a relevância do princípio porque atua de forma prática como instrumento de controle e gestão da informação, uma vez que o efetivo problema proposto pela precaução é o de como se decidir em contextos de elevado grau de imprevisão e insegurança científica, impondo obrigações de originar decisões mesmo perante bases cognitivas precárias (AYALA; LEITE, 2004, p. 76).

Segundo Cristiane Derani (2001), precaução tem um sentido de cuidado e, dessa forma, se relaciona aos conceitos de "afastamento de perigo" e "segurança das gerações futuras". Na verdade, esse princípio remete à própria ideia de proteção da existência humana. Proteger o meio ambiente importa garantir a própria dignidade da vida humana.

Precaução se relaciona com a ciência. É uma questão técnica, visto que se procura evitar um dano mesmo antes de se ter certeza sobre a existência de um risco (DALLARI, 2002, p. 59).

A precaução se mostra como um caminho que precisa ser mais estudado, explicado e explicitamente positivado a fim de se proteger os direitos do consumidor, a privacidade e a proteção de dados pessoais.

No caso de dados pessoais e precaução, de certa forma, já se encontram levantes na sociedade que estão refletindo no legislativo para alterar a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, Lei Geral de Proteção de Dados Pessoais) e a Lei nº 12.414, de 9 de junho de 2011, para restringir o acesso, tratamento de compartilhamento de dados de consumidores por empresas de proteção ao crédito. (BRASIL, 2018). O que pode ser encarada como precaução que visa nesse caso, evitar o risco.

Conforme o Projeto de Lei de 27/08/2020 de autoria do à época deputado federal Wolney Queiroz, visando, segundo ele, impedir "verdadeira investigação particular na vida do consumidor [...] serviços de proteção ao crédito existentes no Brasil, na atualidade, são empresas privadas e, portanto, realizam profundas investigações sobre a vida financeira dos consumidores para atender aos interesses de seus clientes, os bancos", explica o deputado Wolney Queiroz (PDT-PE) (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020).

Analisando a justificativa de tal projeto, é possível observar que ele toca em questões sensíveis e necessárias por representarem queixas da população e colisões entre leis que precisam ser harmonizadas com a atual e mais moderna em consonância em maior parte, com os tempos atuais, a Lei Geral de Proteção de Dados Pessoais.

O objetivo deste Projeto de Lei é impedir os serviços de proteção ao crédito de

promoverem verdadeira investigação particular da vida do consumidor, em afronta ao direito constitucional à privacidade (BRASIL, 1988).

De acordo com ele, a base legal de Proteção ao crédito na Lei Geral de Proteção de dados é ampla e genérica, necessitando de delimitação. Ele também entende que as informações coletadas e tratadas pelas empresas privadas fogem do mínimo necessário. Posto que não são mais utilizadas hoje em dia para a composição do score de crédito apenas informações permitidas antes pela lei do cadastro positivo, pelo código de defesa do consumidor. E a própria Lei Geral de Proteção de Dados Pessoais não consegue ainda conter essa atividade com detalhes.

A Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, Lei Geral de Proteção de Dados Pessoais), em seu Art. 7o, inciso X, autoriza a coleta e tratamento de dados de consumidores para fins de proteção ao crédito, mas não especifica quais dados podem ser utilizados. (BRASIL, 2021). Sublinha-se que os serviços de proteção ao crédito existentes no Brasil, na atualidade, são empresas privadas e portanto, realizam profundas investigações sobre a vida financeira dos consumidores para atender aos interesses de seus clientes, os bancos.

O referido Projeto de Lei sugere alteração na Lei do Cadastro Positivo vedando o uso de informações pessoais com potencial de revelarem dados sensíveis através da utilização do que a doutrina vem chamando de dados críticos como os bancários que merecem tratamento diferenciado. (CASTRO, 2021).

Esses dados são normalmente utilizados hoje pelas empresas através do monitoramento do comportamento dos consumidores em aplicativos bancários, sistema *open-banking*, cookies de navegação, e tantas outras formas de que a tecnologia possui na atualidade para rastrear e vigiar os consumidores. Ou seja, o cadastro positivo de hoje faz parte do sistema de score de crédito, sendo este último, mais invasivo. Pois há novas fontes de dados agregados que servem para deixá-lo mais robusto e exponencialmente mais potente.

No referido Projeto de Lei buscou-se também conter a excessiva permissividade para coleta, tratamento e compartilhamento de informações de clientes praticados por empresas de proteção ao crédito, através de alterações na Lei 12.414/2011, a Lei do Cadastro Positivo. Introduziu-se a vedação ao uso de informações que possam caracterizar “espionagem” do consumidor pelas empresas de proteção ao crédito, tais como o histórico de compras, seu patrimônio e sua movimentação bancária (ou seja, seus extratos de conta corrente, quantias investidas e tomadas em empréstimo. (BRASIL, 2011).

A restrição ao compartilhamento dos dados dos consumidores também é atacada dando

nova redação ao correspondente artigo da Lei 12.414/2011 e visa impedir a obrigatoriedade do compartilhamento de todas as informações contidas nos bancos de dados, o que fere o princípio da segurança e o da minimização.

> A nova redação dada ao inciso VI e ao parágrafo único do Art. 8o da Lei 12.414/2011 visa reverter a permissividade da redação vigente da Lei. A redação vigente permite que serviços de proteção ao crédito forneçam livremente todos os dados de que dispõem sobre os consumidores. Mais do que isso, é alarmante que a redação vigente do parágrafo único proíbe que as fontes de informação criem regras que limitem o acesso dos bancos (os consulentes) aos dados dos consumidores (cadastrados):Art. 8o São obrigações das fontes: VI - fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados. Parágrafo único. É vedado às fontes estabelecer políticas ou realizar operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados. Ressalta-se que essa redação contraria frontalmente os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), ao obrigar o compartilhamento de todas as informações contidas nos bancos de dados. O parágrafo único impede o estabelecimento de regras que limitem a transmissão de informações de cadastrados. Os dispositivos destacados invertem o princípio da segurança dos dados prevista na LGPD (da Lei no 13.709/2019, Art. 6o, VII), pois ao invés de se protegerem os dados pessoais, os gestores de banco de dados são obrigados a difundi-los. Em outras palavras, esses dispositivos criam o "princípio da insegurança" dos dados dos consumidores. (BRASIL, 2021).

O Projeto de Lei ainda proíbe que dados dos consumidores sejam compartilhados com a finalidade de publicidade e propaganda direcionada sem o consentimento dos titulares de dados, aproximando-se de orientações recentes de autoridades europeias de proteção de dados. A nova redação dada a esses dispositivos no presente Projeto de Lei proíbe o compartilhamento de dados que possam ser usados para os incômodos contatos de bancos por meio de telemarketing, marketing digital e por meio de impressos enviados sem solicitação aos endereços dos consumidores. Dada a notória relevância da proteção das informações dos consumidores contra o mau uso por empresas de proteção ao crédito, rogo aos pares o apoio para a aprovação deste Projeto de Lei.

E ainda, embora não citado no Projeto de Lei, dados pessoais são vendidos às empresas pelos bureaus de crédito ilegalmente. O que fere o direito à privacidade das pessoas, bem como os direitos à intimidade, privacidade e honra dos titulares dos dados. Como no caso do Serasa, que vem por vezes citado, por ser objeto de a Ação Civil Pública proposta pelo MPDFT, sob o argumento de que a venda dos dados fere a Lei Geral de Proteção de Dados Pessoais – LGPD, uma vez que a norma impõe a necessidade de manifestação específica para cada uma das finalidades de tratamento dos dados.

Em 17 dezembro de 2020, o mencionado Projeto foi apensado ao Projeto de Lei nº 4963/2019, que trata de alterar a Lei nº 13.709, de 14 de agosto de 2018, para regulamentar o

compartilhamento voluntário de dados bancários, de investimentos e de seguros dos correntistas com outras pessoas físicas ou jurídicas do então Deputado Federa Otto Alencar Filho. É certo que o Projeto de Lei em comento precisa de revisão na redação e possíveis emendas. Mas não se tire dele o mérito da coragem e a legitimidade de, por essa via, tentar sanar dores pelas violações aos direitos do consumidor, da privacidade, da personalidade e fundamental à proteção de dados.

Além do já citado Projeto de Lei n. 3.514/15, sobre comércio eletrônico, de outra forma, é preciso relembrar que invocar o art.170 da Constituição Federal, é estender os braços para a defesa do consumidor também como um dos fundamentos da Lei Geral de Proteção de Dados Pessoais. O texto constitucional (art. 5., inciso XXXII) eleva a defesa do consumidor não só como direito fundamental através do qual o Estado precisa atender às novas demandas em nome da vedação da proteção insuficiente (SILVA, 2015. p. 585.). Mas também como princípio da ordem econômica e financeira, previsto no artigo 170 da Constituição Federal, ao estabelecer que a ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, terá por fim assegurar a todos existências dignas, conforme os ditames da justiça social, observados os princípios da defesa do consumidor. "Art.170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existências dignas, conforme os ditames da justiça social, observados os seguintes princípios: V - defesa do consumidor;" (BRASIL, 1980).

Continuando a invocar aqui o *enforcement* de toda a potencialidade do ordenamento jurídico para demonstrar a necessidade de ampliação e empenho na proteção de dados pessoais, sobretudo do consumidor, vale citar também o Projeto de Lei n. 786, de 2019, que altera o Código de Defesa do Consumidor para tratar do armazenamento, pelo fornecedor, de dados referentes aos instrumentos de pagamento utilizados pelo consumidor. O projeto inclui um artigo 43-A, no Código de Defesa do Consumidor, para exigir o consentimento prévio do consumidor para o armazenamento de dados de cartão de crédito ou débito, também a cada nova utilização dos dados de pagamento, e, por fim, para repasse a terceiros. A autoria justifica a necessidade do projeto nos relatos de consumidores que tiveram seus cartões clonados e sofreram prejuízos financeiros e morais em razão das mais diversas fraudes. E menciona haver prática de condutas abusivas por parte de certos fornecedores no sentido de reutilizar os dados de pagamentos, sem solicitação do consumidor, efetuando negociações não autorizadas ou renovando automaticamente serviços contratados sem que haja solicitação do consumidor.

O Relator da matéria, Dep. Jorge Braz (PRB/RJ), apresentou substitutivo propondo mudar o texto inicial para criar dispositivo no Código de Defesa do Consumidor apenas referenciando a Lei Geral de Proteção de Dados Pessoais, no que couber.

Outra iniciativa é o Projeto de Lei n. 1805/2021 de atualização do Código de Defesa do Consumidor sobre crédito responsável, prevenção e tratamento do superendividamento dos consumidores. Reclama a atuação responsável dos bancos de dados, negativos e positivos, que incluam o tratamento de dados sobre (in)adimplemento ou superendividamento. Realmente, o PL n° 1805/2021 prevê a inclusão de dois novos capítulos no Código de Defesa do Consumidor e cria um direito básico dos consumidores, qual seja "a garantia de práticas de crédito responsável". O projeto, aprovado pelo Parlamento em junho e que foi sancionado em 02 de julho de 2021, combate a prática de assédio de consumo (Art. 54-C, IV), prevê um reforço nas informações dos consumidores, mas impõe o dever do fornecedor "avaliar, de forma responsável, as condições de crédito do consumidor, mediante análise das informações disponíveis em bancos de dados de proteção do crédito, observado o disposto neste Código e na legislação sobre proteção de dados" (Art. 54-D, II). Ainda, no capítulo referente ao tratamento do superendividamento com uma conciliação em bloco e um plano de pagamento, este plano deve prever a "data a partir da qual será providenciada a exclusão do consumidor de bancos de dados e de cadastros de inadimplentes" (Art. 104-A, s 4°, II). Esperamos que esta atualização do Código de Defesa do Consumidor possa colaborar para melhorar as práticas, inclusive o uso dos bancos de dados. (MARQUES, 2022, p. 15).

O (PL 3101/21) inclui como fundamento da Lei Geral de Proteção de Dados Pessoais “a garantia de acesso a informações públicas, em especial sobre agentes públicos no exercício de suas funções”. (BRASIL, 2021). Ele explica que a proposta tem como objetivo evitar que a Lei de Proteção de Dados Pessoais sirva para não dar a transparência que devem ter as ações públicas e seus agentes no exercício do cargo.

De acordo com o autor do Projeto de Lei, “A lei não pode servir de escudo para dados importantes que a população tem o direito de saber. São os dados dos agentes públicos referentes à sua função, dados de agentes privados que também recebem ou gerenciam recursos públicos” (BRASIL, 20211).

O projeto já foi aprovado pela Comissão de Trabalho, Administração e Serviço Público e aguarda votação na Comissão de Constituição e Justiça e de Cidadania.

Diante de todo o exposto é possível questionar se o Código de Defesa do Consumidor (LGL\1990\40) e a Lei do Cadastro Positivo não fracassaram. Um dos motivos foi não conseguir entregar ao titular dos dados acesso às informações que são usadas no procedimento

de concessão de crédito, apesar de o art. 4o, IV, "a", da Lei 12.414/2011 (LGL\2011\1883) prever que o gestor deve disponibilizar a nota ou pontuação de crédito do consumidor. As instituições financeiras, além de não revelarem o método empregado no cálculo do score de crédito, também não informam quais dados foram efetivamente considerados para esse cálculo, aproveitando-se claramente da proteção do segredo empresarial (art. 5º, § 4º, da Lei 12.414/2011 (LGL\2011\1883) para impedir qualquer forma de averiguação da licitude desses *scores*.

Por tudo elencado, fica claro que a Súmula 550 do Superior Tribunal de Justiça sobre pontuação de crédito só tem servido para perpetuar desigualdades e discriminações em detrimento do consumidor, e ampliar exponencialmente os poderes dos birôs de crédito e financeiras que são ilimitados para tratamento de dados excessivos, massivos dos titulares. Demonstrando inclusive, textual e legalmente, à que lado a súmula 550 do Superior Tribunal de Justiça serve e protege:

> Todo modelo de análise de crédito utilizado deve proporcionar a instituição (financiador) uma segurança de que o cliente (tomador) tenha as condições pré-estabelecidas para honrar com os seus compromissos assumidos, ou seja, tem por objetivo verificar a compatibilidade do crédito solicitado com a capacidade financeira do cliente de pagamento, dentro do prazo preestabelecido, e com o menor risco possível de inadimplência. (SANCHES et al, 2018).

A Súmula 550 do Superior Tribunal de Justiça por vários motivos contraria a Lei Geral de Proteção de Dados Pessoais, o Código de Defesa do Consumidor, o Código Civil e a Constituição Federal, sendo imperativo que esta seja, como uma das medidas de proteção ao consumidor, declarada inconstitucional.

Até lá, a Lei Geral de Proteção de Dados Pessoais tem a difícil missão de impor limites jurídicos à coleta e tratamento de dados excessivos ou sensíveis e, ainda, a garantir que a pontuação dos consumidores e o seu enquadramento como "bons ou maus pagadores" se vincule estritamente à finalidade financeira. Pois é fundamental impedir a sua consideração para fins diversos daqueles pelos quais foram originalmente coletados e tratados, como, por exemplo, serem considerados para traçar o perfil pessoal dos cidadãos, de modo a inferir aspectos sobre a sua personalidade e credibilidade. (STJ, 2011).

Em última análise, mesmo que o argumento de que o score de crédito continue a ser determinante na jurisprudência que afirma não se tratar de banco de dados pessoais, ainda assim, não há de haver empecilho para a proteção do consumidor frente as suas potenciais discriminações: "o foco não está no dado, mas no seu uso – para a formação de perfis

comportamentais – e sua consequente repercussão na esfera do indivíduo". (ZANATTA, 2019). Por exemplo, até no caso mais seguro, quando os dados são anonimizados, mesmo estes podem ser considerados dados pessoais caso sejam utilizados para a formação de perfis comportamentais, na linha do art. 12, § 2, que dirá na hipótese de pontuação de crédito. Visto que o foco está nas "consequências das atividades de tratamento de dados", havendo proteção jurídica mesmo nas situações de perfilização por *grouping*.

> Muitas vezes, processos de decisões automatizadas valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo – grouping. É pelo fato de ela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem individualizá- la diretamente. [...] As expressões "determinada pessoa" ou "identificada" [...] devem ser compreendidas com relação aos desdobramentos que o tratamento de dados pode ter sobre um indivíduo, ao contrário de significá-los com os olhos voltados para a base de dados em si, especificamente se o perfil comportamental pode ser ou não atribuído a uma pessoa em específico. (BIONI, 2019, p. 80).

Em qualquer das hipóteses, o cidadão titular de dados poderá se socorrer do direito à explicação que pode até hoje ser extraído da Lei do Cadastro Positivo, e mesmo antes da Lei Geral de Proteção de Dados Pessoais. Mas a Lei Geral de Proteção de Dados Pessoais consagrou o direito à revisão de decisões exclusivamente automatizadas e de formação de perfil, como está em seu artigo 5., inciso VI: "solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados;" (BRASIL, 2019). De acordo com Zanatta, a Lei do Cadastro Positivo seria a inspiração da Lei Geral de Proteção de Dados Pessoais a respeito das regras sobre decisões automatizadas e perfilização com base em autores como Renato Leite Monteiro, Maria Cecília Gomes e Bruno Bioni, e também fazendo um paralelo do Regulamento Europeu de Proteção de Dados com a Lei do Cadastro Positivo e o artigo 20 da posterior Lei Geral de Proteção de dados. Sendo o direito à explicação um instrumento para o exercício de um direito negativo que é o da não discriminação.

> O direito de uma revisão por uma pessoa natural de tomada de decisão automatizada que impacta os titulares de dados (Art. 22) não é novo para o sistema legal brasileiro. Ele foi fornecido em relação aos modelos de credit scoring pela Lei do Cadastro Positivo juntamente com o direito à explicação, que incluiria não apenas os dados usados pelo algoritmo, mas também os critérios usados para processamento, limitados ao sigilo comercial e levando em consideração direito de propriedade intelectual. Essa estrutura foi totalmente copiada pela LGPD, mas aplicável para processamento de dados para qualquer finalidade. No entanto, comparado com o GDPR, o impacto sobre o titular dos dados é presumido quando a tomada de decisão automatizada se baseia na criação de perfis (profiling), e não há limitação para situações em que os dados foram fornecidos por consentimento. (BIONI; MONTEIRO; OLIVEIR, 2018).

Como reforço para que não haja limites à explicabilidade sobre decisões automatizadas (em questão aqui o score de crédito) seja reafirmada a necessidade crucial, conforme redação legal, da ANPD, como órgão administrativo regulamentador, com sua capacidade de supervisionar os setores que envolvam o tratamento de dados pessoais, reprima supostos limites. E um ponto sensível para isso, mais especificamente no tocante ao art. 20, § 2, da Lei Geral de Proteção de Dados Pessoais. Para que 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 realize auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. Agir assim é evitar que a lei não vire letra morta.

Outra forma, é a Autoridade Nacional de Proteção de Dados atentar que empresas que façam avaliação de risco de crédito sem informações do cadastro positivo, por outro lado, não têm obrigação de registro perante nenhuma autoridade. Sendo assim, não há penalidades ou sanções para não cumprimento das obrigações legais especificamente nesse caso, a não ser aquelas previstas pelo Código de Defesa do Consumidor e pela Lei Geral de Proteção de Dados. Nesses casos, a Autoridade Nacional de Proteção de Dados (ANPD) e a Secretaria Nacional de Defesa de Consumidores (SENACON) ficariam responsáveis pela fiscalização e *enforcement* das leis diante de birôs de crédito.

Mesmo na hipótese remota de que se consiga usar de maneira eficaz o aparato legal da Lei Geral de Proteção de Dados Pessoais, ainda assim, o tratamento de dados pessoais para fins de proteção ao crédito é como já demonstrado, de alto risco. Pois se utiliza de uma vasta base de dados pessoais de diversas origens e é que compartilhada constantemente entre inúmeros atores. E esses dados servem de base para o perfilhamento através de score de crédito, que por sua vez, não tem tipos de dados delimitados nem fontes definidas e é manchado pela opacidade. Desta feita, é inescapável diante do risco de dano aos consumidores titulares de dados identificar que tipo de responsabilidade civil há de ser invocada e a extensão de sua proteção/reparação, bem como seu novo sentido diante das inseguranças jurídicas que ora se apresentam.

# 4 UM NOVO SENTIDO PARA A RESPONSABILIDADE CIVIL

## 4.1 A responsabilidade civil no Código Civil

A Lei Geral de Proteção de Dados Pessoais, o Código de Defesa do Consumidor, fazem parte de um microssistema de responsabilidade Civil estabelecido no Código Civil de 2002 que tem por objetivo a proteção da personalidade humana em consonância e em decorrência dos mandamentos constitucionais da dignidade da pessoa humana, princípios e direitos fundamentais frente aos desafios de toda ordem. Sobretudo aqueles impostos pela economia em seus desdobramentos. Entre eles a tecnologia e a inovação que nas últimas décadas andam em ritmos diferentes, num descompasso desafiando as leis e aumentando riscos e desigualdades e discriminações. A inteligência artificial dependente de dados pessoais para funcionalizar-se é exemplo disso. No caso em estudo, refletido no Score de crédito como já demonstrado caracterizando-se em grande medida danos extrapatrimoniais.

Entre os desafios hoje no ordenamento jurídico brasileiro para a proteção da pessoa no uso de algoritmo de inteligência artificial para formulação do score de crédito, está o de encontrar que tipo de responsabilização civil seria a mais adequada pelo compartilhamento de dados dos consumidores com parceiros e terceiros dessa nota de crédito com finalidades ilegais, redundando em discriminação.

O que se propõe é um estudo do ordenamento atual e as possibilidades de se extrair conceitos e interpretações legais e extensivas a respeito sobretudo, da responsabilidade civil a fim de que possam socorrer a sociedade antes de criar novos institutos a partir do Código Civil. Assim ganha-se tempo, tão valioso para a eficácia do direito no que realmente importa que é a proteção da pessoa humana de maneira ética e satisfatória a reestabecer o “status quo” para os novos tempos. A era da chamada 4 Revolução industrial que se socorre da instrumentalização do ser humano e exposição a riscos indetectáveis em sua totalidade através do uso de seus dados pessoais (projeção da personalidade) ininterruptamente e de maneira onipresente para ampliar o lucro.

Dessa forma, antes de criar institutos ou copiar tal e qual os de outros países, é razoável considerar uma revisão do atual ordenamento para regular na atualidade partindo do há posto para em um segundo momento, sendo necessário, buscar a regulação complementar.

Como diz Felipe Medon: “Necessário se faz, portanto, adotar a cautela de não importar descuidadamente institutos que, apesar de serem recomendados fora do Brasil, não se adéquem à nossa realidade. Deve-se considerar que são sistemas diferentes, com realidades

jurídico-culturais distintas e que a falta de normas que justifica a criação de certos institutos para a Inteligência Artificial alhures, talvez não seria necessária aqui. Um desses exemplos é a cláusula geral de responsabilidade civil objetiva do parágrafo único do artigo 927, que não existe em diversos ordenamentos ao redor do mundo. (MEDON, 2022, p. 522).

A regra geral supramencionada reza que: "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haveráobrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ouquando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza,risco para os direitos de outrem." (BRASIL, 2002).

Considerando que a Constituição Federal de 1988 em seu artigo 1, inciso III, tem no princípio da dignidade da pessoa humana um fundamento para tutela da pessoa como cláusula geral e embasando todos os direitos fundamentais no ordenamento; que recebe o Código Civil a incidência imediata e direta dos direitos fundamentais sobre as relações privadas, hoje prevalece:

> e tende a expandir sua aplicabilidade a campos ainda inexplorados e incessantemente renovados (por força da própria atipicidade dos direitos essenciais), parece evidentemente que o direito civil-e, dentro dele, o instituto da responsabilidade civil- deve apresentar-se operativo e útil aos objetivos constitucional e civilmente vinculantes, no que se refere à concretização dos direitos. (VENTURI, 2014, p. 96).

Assim, proteger a pessoa humana deve passar da "responsabilidade da pessoa à responsabilidade para com a pessoa." (MONIER, 1996).

Como aponta Nelson Rosenvald, a interpretação de uma responsabilidade civil como repositório das disfunções nas relações humanas e econômicas no sentido de apenas reparar o dano concebendo-a apenas como "direito de danos", que só sanciona o efeito deixando de lado a conduta, visando apenas a compensação do dano é cada vez mais insuficiente reclamando sua essência cambiante sensível a mudanças numa trajetória que não é linear exigindo-se mais uma vez sua reelaboração. O curso da civilização redefine as extremas da propriedade e dos contratos que se transmudou em apropriação unilateral de direitos. Ressalte-se aqui, quando há contrato. Em muitas hipóteses como score de crédito, não há sequer o consentimento do titular de dados.

O sentido de responsabilidade numa realidade de mercado de dados pessoais transformados no capital mais lucrativo da atualidade, utilizando-se do humano como matéria prima, é arrastado para outra compreensão. Mais ampla e potencialmente capaz de satisfazer

não só o dano resultado. É preciso que haja o pleno desenvolvimento onde a responsabilidade civil pode e deve operar. É ter que responder à emergência de novos danos para que a responsabilidade jurídica possa abranger a totalidade do termo “responsabilidade”. “Nosso direito de responsabilidade já mostrou suas capacidades de evolução e de adaptação à emergência de novos riscos. A avaliação dessa evolução pode nos ajudar a percorrer essa nova etapa sem muita resistência à necessária mudança. Para tanto, a “responsabilidade”, ela própria, no sentido etimológico e filosófico, nos traz um precioso desafio.” (THIBIERGE, 1999, p. 3).

Dito de outra forma, palavras muitas vezes servem como redomas de compreensão do sentido, sendo que a polissemia da responsabilidade nos auxilia a escapar do monopólio da função compensatória da responsabilidade civil (*liability)*, como se ela se resumisse ao pagamento de uma quantia apta a repor o ofendido na situação pré-danosa. Ao lado dela, colocam-se três outros vocábulos: *"responsibility", "accountability" e "answerability*". Os três podem ser traduzidos em nossa língua de maneira direta com o significado de responsabilidade, mas na verdade diferem do sentido monopolístico que as jurisdições da *Civil Law* conferem a *liability,* como palco iluminado da responsabilidade civil (artigos 927 a 954 do Código Civil). Em comum, os três vocábulos transcendem a função judicial de desfazimento de prejuízos, conferindo novas camadas à responsabilidade, capazes de responder à complexidade e velocidade dos arranjos sociais. (ROSENVALD, 2021).

*Liability* seria apenas a epiderme da responsabilidade civil. Após o dano. Não sendo suficiente para a tutela das relações existenciais resumindo-se a uma compensação, mas buscando novas bases da coesão social e dos fundamentos de racionalidade do direito adaptando instituições e modelos jurídicos para tempos de incerteza. Um direito que venha a ser mais princípio que regra, de cláusulas gerais que rejuvenesçam constantemente o sistema. E a própria realidade tratou disso, como exemplifica Rosenvald com propriedade nas seguintes observações a partir do Código Civil:

> a) a cláusula geral da imputação objetiva de danos, situada no parágrafo único do art. 927 do Código Civil, se conecta com o princípio da solidariedade, impondo obrigação de reparação como impositivo de segurança social em face do risco intrínseco de determinadas atividades; b) o simples exercício de um comportamento antijurídico poderá ser sancionado pela via da tutela inibitória quando as circunstâncias apontem a ameaça a situações existenciais e patrimoniais de terceiros (art. 12, parágrafo único, CC). Cuida-se de atuação preventiva, como reação do ordenamento jurídico ao ilícito propriamente dito, independente da consumação do dano; c) pela função precaucional da responsabilidade civil uma atividade ou produto potencialmente lesivo sofrerá restrições se a ponderação de bens indicar a necessidade de antecipação de riscos; d) o nexo causal deixa de estar circunscrito a uma causalidade natural e, em situações merecedoras de tutelas, assume-se como

> uma causalidade puramente jurídica e diluída, permitindo a responsabilização em hipóteses de vinculação entre um fato e um risco hipotético, ou entre um dano e uma atividade exercida indistintamente por um grupo de agentes, sem que se saiba de onde partiu a lesão; e) o direito civil reputa novos danos como dignos de proteção: para além da aceitação da dicotomia danos patrimoniais/morais, considera a legitimidade de figuras jurídicas mais refinadas – entre eles o dano estético, dano existencial, perda de uma chance –, cada qual com os seus limites perfeitamente destacados. (ROSENVALD, 2021).

E dessas situações se extrai novas interpretações, funções para a responsabilidade civil:

> Cremos que no direito brasileiro do alvorecer do século XXI, a conjunção aponta para o estabelecimento de três funções para a responsabilidade civil: (1) Função reparatória: a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) Função punitiva: sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de comportamentos reprováveis; (3) Função precaucional: possui o objetivo de inibir atividades potencialmente danosas. O sistema de responsabilidade civil não pode manter uma neutralidade perante valores juridicamente relevantes em um dado momento histórico e social. Vale dizer, todas as perspectivas de proteção efetiva de direitos merecem destaque, seja pela via material como pela processual, em um sincretismo jurídico capaz de realizar um balanceamento de interesses, através da combinação das funções basilares da responsabilidade civil: punição, precaução e compensação. (ROSENVALD, 2021).

E numa sociedade de riscos, porque não além da punição, compensação e desestímulo às vantagens porventura indevidas auferidas pelo dano (art.884 CC), invocar o princípio da prevenção dos ilícitos, amparado na Constituição Federal de 1988, no princípio da solidariedade social, da dignidade da pessoa humana, de ser responsável pelo outro e como consequência das três referidas funções. Pois:

> [...] a proteção da dignidade se dá em uma dimensão intersubjetiva -que implica a imposição de limites à ação dos sujeitos, com vistas a evitar que os demais tenham ofendido sua dignidade; pode, e deve, o Direito, através da responsabilidade civil, buscar a prevenção de danos à pessoa (RAMOS, 2002, p. 135).

E tendo em conta que os direitos fundamentais possuem uma categoria específica de direitos que dizem respeito aos valores essenciais da pessoa humana que são os direitos da personalidade frontalmente atingidos na sociedade de risco, há uma enorme relevância de refundar a responsabilidade civil com base na prevenção para melhor tutelar os direitos de personalidade:

> Na tutela jurídica dos direitos de personalidade, a que se contrapõe um dever geral de abstenção ou obrigação geral de respeito, é de grande relevo a cominação feita a quem ameaça violar o direito para que se abstenha de consumar a ameaça, como o é a intimação feita a quem já ofendeu o direito para que cesse essa ofensa. E porque os direitos da personalidade são direitos pessoais, de conteúdo e função não patrimonial, a sua adequada e eficaz tutela passapela prevenção do acto ilícito lesivo, e não pela repressão e remedeio da violação. (SILVA, 1995, p. 466).

Feitas essas argumentações, passa-se aos conceitos e conexões das funções (punição, precaução e compensação) olhando para o ordenamento civil sem a intenção de esgotá-las nesse primeiro momento.

A *responsability* é o sentido moral da responsabilidade. Independe de convenções ou lei. Há a aceitação voluntária como um guia pessoal para vida de tomar atitudes frente ao outro. Enquanto a *liability* se situa no passado - sempre atrelada a uma função compensatória de danos - a responsibility é perene, transitando entre o passado, o presente e o futuro. Sempre seremos responsáveis, não apenas perante um certo demandante, mas por toda a humanidade e pelas gerações futuras. (ROSENVALD, 2021).

A accountability, para Bruno Bioni na percepção legislativa há a ideia de uma responsabilidade afirmativa com mecanismos de exteriorização, a exemplo de boas práticas, documentação, no que viria a se traduzir numa governança e conformidade com a lei. (BIONE, 2022, p. 26). Isso reforça a compreensão de que a accountability amplia o espectro da responsabilidade civil, mediante a inclusão de parâmetros regulatórios preventivos, que promovem uma interação entre a *liability* do Código Civil com uma regulamentação voltada ao compliance (governança apoiada no art.944) de dados pessoais, seja em caráter ex ante tendo como objetivo a inviolabilidade dos direitos e a prevenção do dano, a exemplo dos artigos 6, 50,52,53, da Lei Geral de Proteção de Dados Pessoais (responsabilidade e prestação de contas) ou ex post, na atribuição do juiz ao sopesar a *liability* com as condutas preventivas e comprováveis para minimizar ou mitigar o dano diante dos riscos (BRASIL, 2002).

É importante observar a *accoutability*, constata-se uma mudança na racionalidade do regime da responsabilidade civil responsável por moldar a moldura normativa da Lei Geral de Proteção de Dados Pessoais que passa a representar prestação de contas e responsabilização como precaução. O grau de responsabilidade de uma atividade de tratamento de dados é correspondente à ao nível de demonstração das medidas adotadas para o cumprimento das normas. (BIONE, 2002, p. 77)

Também na inteligência do artigo 944, do Código Civil reflete-se outra conexão com a accountability. Ela possui uma relação de casualidade com a *liability*. Quanto mais accountable se estiver, menor a expectativa do dano ou de seu tamanho. E a indenização se mede pela extensão do dano. “Conforme o parágrafo único, do art. 944, Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização". A mensagem é clara: O valor da indenização não pode ultrapassar a extensão do dano, preservando-se a função de teto do princípio da reparação integral, porém pode ficar aquém, indenizando-se menos do que o montante

total dos prejuízos sofridos pelo lesado. Isto se dá quando o agente, agindo com uma mínima negligência causa danos vultosos." (ROSENVALD, 2021).

Esse raciocínio reabre uma discussão mais adiante sobre a culpa e danos na responsabilidade civil frente às atividades de risco, sendo este presumido. Posto que no tratamento de dados não há a possibilidade de risco zero. Assim, o gerenciamento da variável risco será sempre uma medida de segurança a determinar o montante a ser indenizado. Ficando a culpa de lado sobretudo frente às possíveis lesões de cunho existencial.

Em complementação à accountability, a *answerability* viabiliza o direito à explicabilidade que é inerente no ato da responsabilidade de prestar contas. De comunicar e demonstrar de maneira inteligível as razões das tomadas de decisões, o porquê, para quê, detalhamento de processos, indo além da transparência. Atinge a explicabilidade antes, durante e depois da atividade. Proporcionando assim inclusive a possibilidade de se viabilizar outros direitos como o de acesso. Sobretudo nos processos de tomada de decisão automatizada através de perfilização, como o score de crédito posto que algoritmos são fórmulas ou modelos matemáticos que fogem da compreensão do homem médio.

Assim a nova leitura da responsabilização civil, integra à *liability*, o princípio da prevenção, a *responsability* associada ao dever moral, a accountability e a *answerability* ante os novos desafios da tecnologia e da inovação a fim de minimizar riscos e prevenir danos de maneira precaucional, utilizando-se de boas práticas imbuídas de ética e boa-fé refletidas no espírito da Lei Geral de Proteção de Dados Pessoais.

## 4.2 A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais

A necessidade do Estado regular diante de um novo modelo de sociedade denominada pós industrial, de vigilância física, psicológica e de dados - esses últimos extremamente valiosos pra economia que deles hoje depende- , os riscos na manipulação dessas informações em todas as áreas seja saúde, educação, entretenimento, gerou a expectativa na sociedade de um regramento geral de proteção de dados pessoais.

> *There was of course no way of knowing whether you were being watched atany given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time, but at any rate they could plug in your wire whenever they wanted to. You have to live - did live, from habit that became instinct- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized. (ORWELL, 1984, p. 3)*

Pela imprescindibilidade de uma normatividade geral e com caráter de transversalidade em

relação a todos os setores de ramos do direito foi preciso lançar mão de um grande debate público entre Estado e Sociedade como sugere Habermas, para a conceber a Lei Geral de Proteção de Dados Pessoais. “Sistema de alarme com sensores que, apesar de não especializados, funcionam por toda a sociedade.” (HABERMAS, 1992, p. 359)

A esfera pública enquanto um sistema de detecção de problemas sociais, segundo Habermas tem uma concepção de que a esfera pública é igualmente capaz de problematizar estes problemas por si detectados e identificados. Mas para que se desempenhe corretamente esta função, a esfera pública deverá tematizá-los, apresentar possíveis soluções e dramatizá-los de modo a que os complexos parlamentares os encarem como tópicos de discussão. Aqui, a esfera pública assume a capacidade de tematização ou problematização dos problemas sociais por si detectados. A sua capacidade de resolução destes problemas é reduzida. Estes deverão ser encaminhados, de acordo com a proposta de Habermas, através de canais comunicativos parlamentares e judiciais, para o sistema político, o único domínio com capacidade de formação de vontade ou tomada de decisão. De qualquer forma, a função da esfera pública não termina aqui: deverá ainda supervisionar o tratamento que o sistema político aplica a estes problemas. (SILVA, 2001).

E assim foi feito no Brasil. A Lei Geral de Proteção de Dados Pessoais foi pré-concebida com o desafio de ser harmônica a todo o ordenamento pré-existente amplo e segmentado, e ao mesmo tempo, para trazer em seu bojo uma abertura para alcançar novas situações trazidas pela sociedade de riscos atual vulnerabilizada pela tecnologia e inovação. Com a missão tendo que proteger direitos fundamentais e ao mesmo tempo não obstaculizar essas atividades econômicas. E ainda, ter a capacidade de abrir caminhos para uma responsabilização civil dinâmica que atendesse a todo esse cenário e demanda. A tarefa não foi fácil no que transparece até pela duração do seu processo legislativo que durou longos anos. E ainda assim, a Lei Geral de Proteção de Dados Pessoais é a legislação que, apesar de depois de sancionada e em vigor, mais suscita debates e produção doutrinária em várias áreas do direito, não só na específica e pura matéria de proteção de dados pessoais. Isso ora por causa de pontos pendentes de regulamentação por parte da Autoridade Nacional de Proteção de Dados, ora em torno das “incertezas” e reflexões a respeito do seu regime de responsabilidade civil. Nesse tema, uma das discussões mais fecundas e com variadas interpretações é devida à prescrição estabelecida em seus dispositivos que deixaram uma reflexão posterior se a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais é subjetiva ou objetiva.

> A tensão também ficou clara em dois textos de posição produzidos por entidades distintas: de um lado, o Manifesto sobre a Futura Lei de Proteção de Dados Pessoais, coordenada por Brasscom, Abranet e outras associações; de outro, a Carta Aberta à Comissão Especial de Tratamento e Proteção de Dados Pessoais produzida pelo Idec. Observando-se as contribuições do setor privado à Comissão Especial de

> Tratamento e Proteção de Dados Pessoais - em especial, BSA, Facebook, Brasscom, Febraban, ABMED e ANBC -, nota-se, também, um posicionamento massivo contra as regras de responsabilidade [...]. (ZANATTA, 2019, p. 250 )

A doutrina segue e se divide principalmente nessa classificação binária que põe em cheque a questão da culpabilidade e sua relevância ou não, para fins de responsabilização. E o papel do risco da atividade no tratamento de dados pessoais. Relevante nessa discussão é também seguir o espírito da lei como norte orientador.

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para a governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou passa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis. (PECK, 2018)

Bruno Bioni tenta trazer a racionalidade jurídica na concepção da referida lei para trazer luz ao debate. Ele analisou desde a primeira versão do anteprojeto de lei passando por quatro textos até a redação final. Na primeira 1conforme quadro abaixo, a responsabilidade é objetiva; na segunda do anteprojeto, diz que os agentes da cadeia responderiam "independentemente da existência de culpa", pela reparação dos danos; a partir de então, a responsabilidade civil subjetiva ganhou força apesar das críticas no processo de consulta pública e em audiência pública na Camara dos Deputados. E na redação final da Lei Geral de Proteção de Dados Pessoais eliminou-se os termos "independentemente de culpa" ou "atividade de risco" que descartaria a culpa como pressuposto da responsabilidade civil. (BIONI, 2022, p. 312-313). Essa evolução na concepção da Lei Geral de Proteção de Dados Pessoais pode ser visualizada através dos quadros 1 e 2 a seguir:

| 1º versão do anteprojeto | 2º versão do anteprojeto | PLC 53/2018 | LGPD |
|---|---|---|---|
| Art. 6º. O tratamento de dados pessoais é atividade de risco e todo aquele que , por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei. | Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa. | Art. 42. O responsável ou o operador que, em razão do exercício da atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral invidual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. §1º A fim de assegurar a efetiva indenização | 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.§ 1º A fim de assegurar a efetiva indenização |

| | | | |
|---|---|---|---|
| | | ao titular de dados: I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável, hipótese em que o operador equipara-se a responsável, salvo nos casos de exclusão previstos no art. 43 desta lei; II – os responsáveis que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. | ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. |

Tabela 2 - Comparativo entre os textos que deram origem a LGPD[6]

| 1º versão do anteprojeto | 2º versão do anteprojeto | PLC 53/2018 | LGPD |
|---|---|---|---|
| Art. 6º. O tratamento de dados pessoais é atividade de risco e todo aquele que , por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a | Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa. | 43 desta lei. § 2º. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a | § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova |

[6] Fonte: (Bione, 2022).

| | | | |
|---|---|---|---|
| ressarci-lo, nos termos da lei. | | produção de prova pelo titular resultar-lhe excessivamente onerosa. §3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observando o disposto no Título III da Lei nº 8.078, de 11 de setembro de 1990 (Código de defesa do consumidor). §4º. Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. | pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. |

Tabela 3 - Comparativo entre os textos que deram origem a LGPD[7]

Analisando os quadros, o que isso pode significar com a retirada desses elementos textuais é que o legislador preferiu deixar a lei com possibilidades de interpretação da responsabilidade civil considerando as transformações socias como as advindas da internet por exemplo, e seus riscos de danos digitais. O que demonstra uma prudência legislativa. Pois, "o estágio atual da responsabilidade civil pode justamente ser descrito como um momento de crosão dos filtros tradicionais da reparação, isto é, da relativa perda de importância da prova da culpa e da prova do nexo causal". (SCHREIBER, 2015, p. 11-12).

"Erosão" e "relativa perda de importância" podem significar exatamente uma fase transição em que se há que ter a devida cautela, precaução, diante dos riscos atuais da sociedade "a consciência proporcionada pela ciência e pela tecnologia a respeito das dimensões das ameaças que pairam sobre

[7] Fonte: (Bioni, 2022).

a humanidade e a consciência de que essas ameaças foram potencializadas pelo próprio processo de modernização." (SANTOS, 2018, p. 164)

Esses riscos soaram o alarme para uma realidade em que é preciso ampliar a compreensão semântica do signo culpa buscando despi-lo do subjetivismo e apresentá-lo ao mundo como comportamento lesivo. A esse respeito, as correntes normativas permitiram aflorar a incompatibilidade entre o viés psicológico na aferição da culpa e a reparação de danos atados à industrialização e ao aumento da complexidade da vida em sociedade. (MORAES, 2007. p. 12)

Assim compreendido, a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais passa a ser percebida através de seus fundamentos eleitos como essenciais no artigo 2.: o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o direito ao livre desenvolvimento da personalidade, o desenvolvimento econômico e tecnológico, à livre iniciativa, à livre concorrência e a defesa do consumidor. Os fundamentos são uma maneira a conferir uma proteção integral à pessoa com base na Constituição de 1988, no Código Civil (através dos direitos da personalidade), nas relações de consumo e, ao mesmo tempo, não obstaculizar o desenvolvimento. Busca-se estimular comportamentos mais seguros baseados na prevenção de riscos, mitigação de danos e boas práticas dentro do contexto da realidade brasileira.

A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais também encontra conexões no Regulamento Geral de Proteção de Dados europeu como países que subsidiam o amplo desenvolvimento da tecnologia e há muito lidam com a questão da proteção de direitos frente à tecnologia e que têm ressignificado o conceito de responsabilidade civil. Utilizando-se dele para prevenir e reparar o dano (art.82). (CORDEIRO, 2021, p. 494).

As funções identificadas na responsabilidade civil servem de parâmetro de condução. A responsability é um norte ex ante para a Lei Geral de Proteção de Dados na medida em que expressa os valores morais individuais refletidos no comportamento humano com o outro, no sentido de cuidado. É uma atitude individual que termina por caracterizar costumes morais que inspiram e orientam a criação de leis para a harmonização destas com ética que traz na sua essência a abstenção de comportamentos negativos e o estímulo ao que é positivo visando o bem do ser humano como um todo.

> But before whom is someone responsible? There may be many replies. I think the Kantian idea of moral responsibility based on the dignity and the highest value of humankind and the integrity of humanity is an acceptable and unique frame of moral orientation. But Kant's perspective doesn't mean that mankind would somehow be a real judge entitled to legally produce judgments and sanctions, but rather a kind of ideal court. [Kant's moral system specified that one should act as if one's actions

> defined laws for humanity as a whole, thereby making humanity itself a sort of judge - Ed.] In this case then, 'responsibility' is an idealized concept of attribution. This Kantian notion at least circumscribes the five- and six-place relational concept. We can say that moral responsibility is a special form of responsibility. (LENK, 1991).

A *accountability* traduz a união da responsabilidade e da prestação de contas. É uma palavra que surgiu no contexto da proteção de dados no mundo para a prevenção de danos através das próprias medidas personificadas pelos dispositivos normativos positivados. (BIONI, 2022). *Accountability* está intrinsecamente ligada ao principio da precaução tão importante no processo de regulação das tecnologias de Inteligência Artificial que envolvem o tratamento de dados pessoais. Tal princípio é como uma porta de entrada para a precaução que é o alicerce da deliberação sobre a adoção ou não de Inteligência Artificial, através da definição do tipo de risco desta. É com base na precaução que se decide correr ou não um risco potencial causador de dano. Haja vista que "O dano é um mal social e, por isso, antes de combatido, deve ser evitado." (CATALAN, 2019, p. 119).

Nunca é demais lembrar que o risco assumiu proporções inimagináveis na contemporaneidade, disseminando-se globalmente. Por isso, qualquer oportunidade de evitá-lo há de ser valorada. (CATALAN, 2019, p. 114).

A *accountability* também tem uma relação direta com estar de acordo, estar conforme as normas. Do inglês "*to comply*". (ARNAUD, 2014, p. 10-12). Surge o compliance de dados. Na Lei Geral de Proteção de Dados Pessoais a accountability está presente como princípio a orientar essa conformidade com a lei. Através da 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 da eficácia dessas medidas. (Art. 6, X, Lei Geral de Proteção de Dados Pessoais) num sistema de gestão que exige a abstenção de condutas, o estímulo de outras positivas, a documentação dessas condutas de maneira ética a fim de se obter uma rastreabilidade probatória para minimizar riscos na expectativa de prevenção e medidas de mitigação que vão atacar as consequências, o dano, caso os riscos se concretizem nos arts. 50 e 51 da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018).

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. $ 1° Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a

> gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. § 2° Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6° desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: 1-implementar programa de governança em privacidade que, no mínimo a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejamsob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; 1) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.§ 3° As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.(BRASIL, 2021).

O termo *accountability* permeia toda a Lei Geral de Proteção de Dados Pessoais. Além de prescritivo de como se deve proceder, da conduta aos mecanismos a lançar mão, para cumprir a lei. O princípio ainda carrega consigo uma alta carga retórica, especialmente quando ele é significado como sinônimo de virtude. O termo funciona semanticamente como um adjetivo, a qualidade de um comportamento responsável (*accountatable*). E, como se notou, não diferiu historicamente no campo da proteção de dados no qual o termo é recorrentemente empregado para denotar um ponto de chegada - a virtude de estar em conformidade com a lei. Em vez de enxergar accountability apenas como um fim em si mesmo, deve-se encará-la como um mecanismo para se alcançar tal virtuosidade. (BIONI, 2022, p. 75).

A *accoutability* se incorpora ao dever de transparência desse processo de prestação de contas em todos os mecanismos do ciclo de vida do dado desde a coleta dos dados ao seu apagamento, à informação clara e precisa:

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, de acordo com o art.6, inciso VI, Lei Geral de Proteção de Dados Pessoais. (BRASIL, 2021).

A *answerability* aplicada às leis de proteção de dados pessoais vem a ser uma faceta da transparência que transpassa todo o tratamento de dados com uma característica que é

típica frente às peculiaridades do processamento das informações na era da tecnologia com o uso de algoritmo de inteligência artificial.

> *Transparency and accountability are related because the transparency of a decision-making process or system is necessary (but not sufficient) for making that process or system accountable.This includes accountability as to compliance with other rule of law principles, such as equality before the law. (ZALNIERIUTE; MOSES; WILLIAMS, 2019)*

Em tradução livre, a transparência e a responsabilidade estão relacionadas porque a transparência num processo ou sistema de tomada de decisão é necessária (mas não suficiente) para tornar esse processo ou sistema responsável. Isso inclui a responsabilidade quanto ao cumprimento de outros princípios do estado de direito, como a igualdade perante a lei.

É através do direito à explicabilidade que o indivíduo tem a expectativa de acessar e compreender de maneira clara e adequada toda a linguagem tecnológica (técnica) utilizada durante todo o processo de tomada de decisão automatizada.

A *liability* é a camada, a função da responsabilidade civil de na sociedade de risco, aferir a extensão do dano residual posto que no modelo de responsabilidade preventiva presume-se que medidas de precaução ao menos mínimas, foram tomadas durante a atividade. Em havendo ainda dano, a *liability* ou a indenização, o "quantum" a ser aferido será resultado de uma equação: desconta-se o que foi feito pelo agente para prevenir e/ ou mitigar o dano e o que sobre, seria o dano residual. Na extensão do que não se conseguiu evitar. *Liability* é a responsabilidade de uma pessoa, empresa ou organização de pagar ou abrir mão de algo de valor. (CAMBRIDGE DICTIONARY, 2022).

Dessa forma, não importando a culpa como determinante da responsabilização. Pois tendo culpa ou não, sempre haverá o risco no tratamento de dados (ISO/IEC 27002, 2013) e a possibilidade da sua materialização, impendentemente da classificação binária da responsabilidade subjetiva ou objetiva. Pois, é a extensão do dano e o quanto se concorreu para esse resultado é o que vai definir o tamanho da reparação. Observa-se aí de logo, a preponderância então do regime objetivo de responsabilização civil na Lei Geral de Proteção de Dados Pessoais. Pois nesse regime a culpa não importa em sentido algum. Por outro lado, a variável risco para mais ou para menos, será a régua, o parâmetro da indenização não podendo ultrapassar o teto do dano, mas podendo considerar uma avaliação do julgador que premie o agente de tratamento pelo cumprimento de regras de governança (compliance). Lidar com um caso de responsabilização por tratamento inadequado de dados pressuporá o equacionamento do enfrentamento das ações adotadas pelos envolvidos ou o reequilíbrio de

tensões nessa condução.

> In these circumstances there can only be different specific kinds of duty, with each kind representing the particular policies or the particular balance among policies that are recognized as decisive in situations of that sort. Moreover, the conception of duty is inwardly fragmented into the various policies that favor one party or the other. The duty issue is therefore seen as the locus not for defining the wrong identically from the standpoint of both parties, but for forwarding or balancing policies that rest on considerations that apply differently to each of them. (WEINRIB, 2005, p.177-178).

Dessa forma, o objetivo da responsabilidade civil vai sendo atingido a curto, médio e longo prazo numa perspectiva crescente de proteção de dados e consequentemente, de seus titulares, com o fomento através do incentivo de uma cadeia forte e desenvolvida atuando na prevenção e precaução de danos.

Conjugados os elementos funcionais da responsabilização civil identificados na Lei Geral de Proteção de Dados Pessoais, eles devem ser conectados com os artigos que tratam especificamente da responsabilidade civil a fim de compreender mais detalhadamente o regime jurídico desta a partir do seu artigo basilar e seguintes que tratam da responsabilidade e do ressarcimento de danos na seção III, do capítulo VI.

Da responsabilidade e do ressarcimento de danos:

> 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).

A priori, o legislador enfatiza quais tipos de agentes do rol do art.5 incisos VI e VII, da Lei Geral de Proteção de Dados Pessoais, são destinatários: controlador e operador e as espécies de danos que podem ser cumulativos pois se tratam de espécies diferentes. E sendo a Lei Geral de Proteção de Dados Pessoais uma norma em que os danos extrapatrimoniais são os de maior risco, a lei não mexeu na caracterização de dano moral (art.186, Código Civil), que decorre da violação de um direito de personalidade. Também no caput já se evidencia a solidariedade "controlador ou operador" que "causar dano". O elemento culpa não foi considerado o que chama a atenção pra a não caracterização da responsabilidade subjetiva, parametrando-se ao art. 927 do Código Civil. "§ 1º A fim de assegurar a efetiva indenização ao titular dos dados" (BRASIL, 2018).

A "efetiva indenização" reforça o caráter polissêmico e amplo da responsabilidade civil na reparação estabelecida no caput. Deve ser a mais ampla e completa possível até o teto do dano. Pode ser considerada nascente a partir de qualquer fase do tratamento dos dados

para aferição. Ou seja, ela abarca o caráter preventivo da Lei Geral de Proteção de Dados Pessoais no equacionamento do dano (CHINELLATO; MORATO, .2021).

> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. (BRASIL, 2018).

A possibilidade de inversão do ônus da prova deixa clara a intenção do legislador de que o titular de dados mediante o desconhecimento técnico do processamento de dados na era da tecnologia, a gama de tratamentos e a opacidade algorítmica, além da trava da barreira da propriedade intelectual e do sigilo e segredo de negócio, resulta de uma assimetria de conhecimento que pode tornar a pessoa híper vulnerável (BIONI, 2019, p. 165).

No mais, no microssistema da Lei Geral de Proteção de Dados, com normas previstas em diversas leis, esse dispositivo só revela a harmonia com o ordenamento pátrio (art. 373, parágrafo 3.) do Código Civil e art. 6. VIII, do Código de Defesa do Consumidor), e em termos de "legislação tributária", o art. 96 do CTN "Art. 96. A expressão "legislação tributária" compreende as leis, os tratados e as convenções internacionais, os decretos e as normas complementares que versem, no todo ou em parte, sobre tributos e relações jurídicas a eles pertinentes". Assim, o Código Tributário Nacional inclui não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades (CAPANEMA, 2020).

A noção de risco- proveito também se extrai do parágrafo 2, do artigo 42, quando cita o ônus da prova em eventos decorrentes do mau-tratamento dos dados pessoais e chama a atenção que a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais não só decorre da violação de normas derivadas do microssistema de proteção de dados, mas também de normas técnicas que tratam da segurança para a proteção dos dados pessoais, conforme artigo 46, Lei Geral de Proteção de Dados Pessoais. (BRASIL, 2018).

A noção de risco, aproveito também deixa pistas aqui da responsabilidade invocada, qual seja, a objetiva:

> A assunção de um risco – classificado como "risco- proveito", risco profissional e

> risco criado, de um risco qualquer atado ao exercício de liberdades positivas aptas a suscitarem a atenção e a confiança do outro, do alter, - ocupa o lugar outrora reservado à culpa. É oportuno salientar, ainda, que, apesar de os estudos sobre a culpa na guarda e preocupação com a tutela dos menos favorecidos terem cooperado com a objetivação do dever de reparar, as ancoragens mais importantes do fenômeno se prendem à (a) inconteste mutação social havida nos últimos séculos, (b) ampliação dos deveres impostos àqueles que exercem atividades perigosas ou não tanto, (c) necessidade de promover, de adequadamente tutelar, os direitos da personalidade e, ainda, (d) ao pulular dos deveres gerais de conduta no curso de cada processo obrigacional (CATALAN, 2019, 117-118).

Outra pista de que a culpa é irrelevante a partir da leitura desse dispositivo da Lei Geral de Proteção de Dados Pessoais, é que o pressuposto ou elemento do dever de reparar com a inversão do ônus da prova que rompe os diques do modelo subjetivo. Algumas leis podendo ser lembradas: o Decreto 24.637/34, reformado pelo Decreto-Lei 036/44, o Decreto-Lei 483/38, substituído pela Lei 7565/86 e as Leis 6.938/81, 8078190 e 8.884/94, instituindo, respectivamente, a lei de política nacional do meio ambiente, o código de defesa do consumidor e lei antitruste (CATALAN, 2019, p. 114) e todas elas em harmonia com a Lei Geral de Proteção de Dados Pessoais.

> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (BRASIL, 2018).

O paragrafo terceiro prevê que as ações de reparação por danos coletivos que tenham por objeto a responsabilização dos agentes de tratamento podem ser exercidas coletivamente em juízo deve ser lida em conjunto com o art. 6°, inciso VI do Código de Defesa do Consumidor, pois a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos são direito básicos do consumidor. (MARTINS; ROZATTI; 2022, p.485-486). Os parágrafos 3 e 4, demonstram os efeitos da solidariedade dos agentes de tratamento e a atenção perante os danos coletivos que podem ser exercidos coletivamente em juízo, diante da natureza do tratamento massivo de dados pessoais.

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018).

O caput e parágrafos I e II do art.43 demonstram a necessidade dos agentes de registrarem todo o processamento de dados a fim de demonstrar tais excludentes caso sejam

demandados. Para isso tendo de cumprir os artigos 50 e 51 da Lei Geral de Proteção de Dados Pessoais. Utilizando-se os agentes do exercício regular de direito (art.188, inciso I, do Código Civil) e do artigo 37, da própria Lei Geral de Proteção de Dados Pessoais no caso do Inciso I, que requer a inversão do ônus da prova. Há duas excludentes, fato exclusivo do titular dos dados (vítima) e de terceiro. Sendo está última situação abarcando qualquer terceiro que podem ser clientes, colaboradores, fornecedores, prestadores de serviço que porventura tenha acesso (art.5, inciso XVI, Lei Geral de Proteção de Dados Pessoais) aos dados não sendo estes os agentes (controlador e operador) na relação. Nesta categoria se inclui o encarregado de dados (art.5, inciso VIII, e 41 da Lei Geral de Proteção de Dados Pessoais). Nesse caso, o regime de responsabilidade civil do encarregado, posto que ele não está fora da cadeia de reparação civil, sendo ele pessoa física ou jurídica. (ANPD, 2021). Dessa forma, o terceiro sendo ele o encarregado de dados ou não, em consonância da Lei Geral de Proteção de Dados Pessoais (art.6, inciso VI, e 46 com o artigo 14, caput, do Código de Defesa do Consumidor, sendo caracterizado o defeito na prestação do serviço, pois fere a expectativa de segurança que se pode esperar.

> 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. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas desegurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018).

Assim, responderão objetivamente os terceiros na Lei Geral de Proteção de Dados Pessoais. Pois em ambas as situações, o que é central é o risco quando se refere ao tratamento de dados pessoais.

O artigo 45 só vem reafirmar toda a prescrição normativa interpretada na Lei Geral de Proteção de Dados Pessoais de que a responsabilidade civil, seja dos agentes de tratamento de dados pessoais. “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).

Em uma interpretação sistemática do Artigo 42, I deve ser afirmada como regra geral na Lei Geral de Proteção de Dados a responsabilidade objetiva dos agentes de tratamento, ou seja, o controlador e o operador, tendo em vista o risco da atividade. Tal conclusão decorre do Artigo 927, parágrafo único, do Código Civil, em cujos termos haverá obrigação de indenizar

o dano, independentemente de culpa, nos casos especificados em lei, ou, como é a hipótese da proteção de dados pessoais, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. Tal norma se aplica aos danos ocorridos em qualquer fase do processamento de dados pessoais seja de terceiros, devem ser aplicados os comandos da responsabilidade civil objetiva reforçada por boa parte da doutrina (MARTINS; LONGHI, 2022, p. 482).

> O legislador, ciente dos percalços enfrentados para a efetivação de direitos devidamente regulamentados, adotou a governança como parâmetro expresso - embora não obrigatório - para a delimitação dos contornos do nexo de causalidade em eventos de mau tratamento de dados, abrindo espaço para a discussão acerca da criação de um novo regime de responsabilidade que, ao fim e ao cabo, se realmente existir, não surge atrelado a uma nova dogmática, mas à condensação de aspectos inter-relacionais para a formatação do elemento nuclear da teoria objetiva. Tem-se, em essência, um dever geral de cautela desdobrado da consagração de um regime de imputação baseado na verificação e demonstração do defeito na prestação de serviço relacionado aos processos de coleta, tratamento e armazenagem de dados. Eventual violação, por causar a ruptura de legítimas expectativas do titular dos dados, conduzirá à responsabilização do agente. Superam-se as barreiras da culpa, suplantam-se as escusas técnicas e a ampla incidência de causas excludentes decorrentes do domínio da técnica pelo controle da arquitetura de software e se impõe a cooperação como modal de controle e aferição dos limites da responsabilidade civil" (DRESCH; MOURA JÚNIOR, 2019, p. 85).

## 4.3 A responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor

Foi analisado no decorrer do trabalho o contexto jurídico, social e econômico da proteção de dados pessoais no Brasil e na Europa principalmente. Dentro do ordenamento pátrio procurou-se demonstrar sua relação com o Código Civil, com a Constituição Federal, e preliminarmente, com o Código de defesa do consumidor.

Também se discorreu sobre o score de crédito e seus riscos discriminatórios com pontos sensíveis dessa atual problemática na sua formulação, como a falta de consentimento, transparência e de controle por parte dos cidadãos frente à opacidade algorítmica a respeito dos seus dados pessoais, bem como a conexão as diferenças em relação à Lei do Cadastro Positivo e a necessidade de efetividade legal com a vigência da Lei Geral de Proteção de Dados Pessoais e a possibilidade de maior regulação.

A partir de então, serão analisados mais alguns pontos do score de crédito para ratificar o direcionamento do estudo e trazer mais elementos argumentativos a fim de conectá-lo ainda

mais com o ordenamento e com a sua caracterização dentro do conceito de inteligência artificial. E, de maneira conjugada e harmonicamente, contribuir para a responsabilidade civil no compartilhamento de dados dos consumidores por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor.

O score de crédito é um método baseado em modelos de predição que se utiliza de algoritmos alimentados por dados pessoais para produzir o perfil de um indivíduo. Ou em outra palavras:

O escore de crédito é a manifestação quantitativamente sumarizada de resultados de modelos de análises preditivas quanto ao comportamento financeiro do consumidor. O resumo numérico em escore serve como artefato de mediação entre consumidores, organizações que contratam o serviço preditivo-classificatório e as empresas de análise que oferecem os serviços. Entretanto, as pessoas jurídicas nesta relação possuem um rol de dados e informações desproporcionais em relação ao consumidor. Incluem nessa relação não só os escores, mas também comensuração e cruzamento com perfis demográficos e variáveis de categorização quanti-qualitativa que consideram categorizações de personas e perfis de consumo, de maturidade financeira e inferências sobre comportamento de segmentos criados a partir de pesquisa psico-demográfica. (PEREIRA; SILVA, 2022, p. 194).

Pereira e Silva (2022, p. 196) enriquecem ainda mais o conceito ao dizer que “o modelo credit scoring envolve ainda a dinâmica dos algoritmos no mundo dataficado e o consumo de informações produzidas por birôs, veículos, organizações e pessoas comuns”.

O que se chama de perfilização: No dicionário de língua inglesa, *profiling* (expressão inglesa de perfilização) significa "o ato ou processo de extrapolar informação sobre uma pessoa baseado em traços ou tendências conhecidas". Na tradição da ciência da informação anglo-saxônica, a perfilização se refere ao processo de construção e aplicação de um perfil de usuário (user profile) gerado por análises de dados computadorizadas. (ZANATTA, 2019, p. 4-5).

O perfil pode ser considerado um registro sobre uma pessoa que expressa uma completa e abrangente imagem sobre a sua personalidade. Assim, a construção de perfis compreende a reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor (MENDES, 2014, p. 111).

Com base nos ensinamentos de Danilo Doneda, Falheiros e Medon, concluem sobre

perfilização que se aplica ao contexto do score de crédito: perfilização (profiling) permite que grandes acervos de dados sejam utilizados por sociedades empresárias que se dedicam a obter uma

> Metainformação, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa", sendo que o resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo" Com efeito, pode-se afirmar que esta técnica, em essência, proporciona o aumento do poder contratual do fornecedor, por lhe permitir antecipar as preferências do consumidor a ponto de, até mesmo, predizer seu comportamento negocial, que pode trazer diversos riscos, sobretudo para a liberdade de contratar, acentuando ainda mais a disparidade de poder inerente às relações de consumo (DONEDA; FALHEIROS; MEDON, 2022, p. 374).

Score de crédito como perfilização algorítmica automatizada, é um sistema de inteligência artificial. E segundo a lei europeia no *Artificial Inteligent Act* , a definição de sistema de inteligência artificial deve basear-se nas principais características funcionais do software, em particular a capacidade, tendo em vista um determinado conjunto de objetivos definidos pelos seres humanos, de criar resultados, tais como conteúdos, previsões, recomendações ou decisões que influenciam o ambiente com o qual o sistema interage, quer numa dimensão física, quer digital. Os sistemas de inteligência artificial podem ser concebidos para operar com diferentes níveis de autonomia e ser utilizados autonomamente ou como componente de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem estar incorporado nele (não integrado). (EUR, 2021).

Dessa forma, a definição se encaixa exatamente ao sistema de inteligência artificial posto que, o score tem os objetivos definidos por seres humanos a fim de criar resultados (nota de crédito) para previsão de comportamentos, recomendação ou decisões (de concessão e oferecimento de crédito) que vão influenciar o ambiente com o qual o sistema interage (on-line ou off-line). Sendo as decisões automatizadas.

O score de crédito se utiliza da coleta de informações que vão para além do cadastro positivo e das informações internas sobre o credor. O comportamento do consumidor no mercado externo como um todo é mais utilizado a formulação dos modelos de score, em virtude de que se um cliente tomador causa problemas no mercado, ele poderá acabar trazendo problemas também ao credor isoladamente. (SICSÚ, 2010).

Sobre as considerações acima em conceituação e contexto semelhantes aos de score de crédito no Brasil, a jurisprudência já se debruçou sobre o tema. Assim o Superior Tribunal de Justiça, em decisão paradigmática, no julgamento do Recurso Especial 1.457.199-RS, verificou os riscos do escore de crédito praticado pelas instituições financeiras, levando à

delimitação de perfis ser qualquer filtro ético, nas mãos do controlador e operador do tratamento de dados, levando a situações extremamente deletérias ao corpo eletrônico. (MARTINS, 2021, p. 83).

Em uma linguagem mais técnica, os modelos de Credit Scoring são sistemas que atribuem pontuações às variáveis de decisão de crédito de um proponente, mediante a aplicação de técnicas estatísticas. Esses modelos visam a segregação de características que permitam distinguir os bons dos maus créditos (LEWIS, 1992)

Para a legislação alemã, no dizer de Laura Schertel, a condição para a legitimidade do scoring é que ele se baseie em um critério matemático-estatístico reconhecido e passível de comprovação, conforme se extrai da Lei federal de proteção de dados alemã (BUCHINER, 2014, p. 123). Ou seja, não basta ser apenas um critério matemático-estatístico, precisa ser possível de comprovação e a lei alemã, a princípio, não impõe alguns limites que a jurisprudência brasileira impôs, como por exemplo, o sigilo e segredo de empresa.

Para fins de ratificar a diferença básica e prática entre cadastro positivo e score de crédito, pontua-se: cadastro positivo é aquele que leva em conta o histórico de crédito dos consumidores, ou seja, suas dívidas adimplidas. Paralelo aos cadastros negativo e positivo, surge o controverso sistema *credit score* ou *credit scoring*, que utiliza os dados dos consumidores para traçar perfis de consumo, bem como o risco de crédito, atribuindo notas que variam do "bom" ao "mau" pagador. (CORTAZIO, 2018).

Em relação à metodologia utilizada na construção de modelos Credit Scoring, Thomas (2000), afirma que ela era, originalmente, julgamental. Nos modelos julgamentais, as variáveis que compõem os escores e seus respectivos pesos são determinados pelos gestores de crédito da instituição, com base em critérios subjetivos. Como ressalta Andrade (2004), embora algumas instituições ainda utilizem modelos de Credit Scoring julgamentais, atualmente, a vasta maioria desses modelos são construídos a partir de técnicas de análise estatística multivariada, como análise discriminante e regressão logística, ou em modelos de inteligência artificial, como redes neurais. (IPEA, 2006). O IPEA, Instituto de Pesquisas Econômicas Aplicadas no estudo "Risco de Crédito: desenvolvimento do modelo credit scoring para a gestão da inadimplência de uma instituição de microcrédito" ainda expõe:

> Os modelos de Credit Scoring são sistemas que atribuem pontuações às variáveis de decisão de crédito de um proponente, mediante a aplicação de técnicas estatísticas. Esses modelos visam a segregação de características que permitam distinguir os bons dos maus créditos. [...] A partir de uma equação gerada através de variáveis referentes ao proponente de crédito e/ou à operação de crédito, os sistemas de Credit Scoring geram uma pontuação que representa o risco de perda.

> O escore que resulta da equação de Credit Scoring pode ser interpretado como probabilidade de inadimplência ao se comparar a pontuação de um crédito qualquer com determinada pontuação estabelecida como ponto de corte ou pontuação mínima aceitável. [...] Os modelos de Credit Scoring são divididos em duas categorias: modelos de aprovação de crédito e modelos de escoragem comportamental, também conhecidos por Behavioural Scoring. [...] Os modelos de Credit Scoring propriamente ditos são ferramentas que dão suporte à tomada de decisão sobre a concessão de crédito para novas aplicações ou novos clientes. Já os modelos Behavioural Scoring auxiliam na administração dos créditos já existentes, ou seja, aqueles clientes que já possuem uma relação creditícia com a instituição. (IPEA, 2006).

No julgamento do Recurso Especial 1.457.199-RS, além de definido o que é o score de crédito, a jurisprudência define a natureza de relação de consumo do score de crédito que é baseada no risco:

> I - 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). II - 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). III - 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 (STJ, 2014).

Vale ressaltar que a prática de score, considerando o comportamento do consumidor, tende a ser banida pela proposta do Regulamento do Parlamento Europeu e do Conselho Europeu. Ela estabelece regras harmonizadas em matéria de Inteligência artificial recomendando pela sua proibição devido ao altíssimo risco aos direitos fundamentais:

> Artigo 5.º 1. Estão proibidas as seguintes práticas de inteligência artificial: [...]c)A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA por autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a uma das seguintes situações ou a ambas: i)tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos, ii)tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é injustificado e desproporcionado face ao seu comportamento social ou à gravidade do mesmo; (UNIÃO EUROPEIA, 2021).

A proposta da União Europeia que pode vir a ser aprovada. Nesse caso, o score baseado em coleta de dados comportamentais para classificação de credibilidade pelas autoridades publicas ou por organizações em seu nome (concessão de crédito como política pública), tende a ser expressamente proibida. No Brasil, ainda está pendente de regulamentação o Marco Regulatório da Inteligência artificial. O Projeto de Lei está em fase de discussão e entrega de

relatório final. O PL 21/2020 estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências trazendo em seu projeto inicial fundamentos, princípios e diretrizes e conceito de inteligência artificial que também se aplica ao score de crédito.

> O CONGRESSO NACIONAL decreta: Art. 1º Esta Lei estabelece fundamentos e princípios para o desenvolvimento e a aplicação da inteligência artificial no Brasil e diretrizes para o fomento e a atuação do poder público nessa área. Art. 2º Para os fins desta Lei, considera-se sistema de inteligência artificial o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões, e que utiliza, sem a elas se limitar, técnicas como: I – sistemas de aprendizagem de máquina (*machine learning*), incluída aprendizagem supervisionada, não supervisionada e por reforço; II – sistemas baseados em conhecimento ou em lógica; III – abordagens estatísticas, inferência bayesiana, métodos de pesquisa e de otimização (BRASIL, 2020).

Mas apesar disso, o Projeto de Lei 21/2020 não prevê nada explicitamente ou especificamente no texto disponível no endereço eletrônico do senado sobre o tema score de crédito. Porém a interconexão da Lei do Cadastro Positivo, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados Pessoais. De logo, em seu art. 1º , caput, a Lei de Cadastro Positivo traz disposição expressa no sentido de se aplicar conjuntamente, de forma coordenada e harmônica, as disposições trazidas pela nova lei com o Código de Defesa do Consumidor sobre score, art. 1 da Lei n. 12.414/2011: “Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito (do qual o score está vinculado), sem prejuízo do disposto na Lei no 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor”. (MARQUES, 2016, p. 136). Ou seja, a lei reforça a ideia de diálogo de fontes.

Conjunta dos diversos diplomas legais incidentes sobre o mesmo suporte fático. A exemplo desse constante diálogo, o próprio artigo 7 do Código de Defesa do Consumidor traz a previsão de que os direitos previstos no código não excluem outros decorrentes de outras fontes, o que se mostra muito importante para a conjugação do Código de Defesa do Consumidor, da Lei de Cadastro Positivo e a Lei Geral de Proteção de Dados Pessoais. (CORTAZIO, 2018).

Dada a harmonia entre as leis consumeristas que fazem parte microssistema da Lei Geral de Proteção de Dados Pessoais e a relação consumerista e passível do escopo de normatização do score de crédito pela Lei Geral de Proteção de Dados Pessoais, a partir de

então passa-se a analisar o sistema de responsabilidade civil no código de defesa do consumidor, e relacioná-lo com a Lei Geral de Proteção de Dados no caso do score de crédito como sistema de Inteligência artificial. Aliás, esse diálogo das fontes observado entre a lei geral de proteção de dados pessoais e a lei brasileira encontra correspondência nas propostas normativas da união europeia, como o regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial (incluindo-se score de crédito - perfilização algorítmica automatizada), regulamento europeu de proteção de dados, normas de direito do consumidor e direitos humanos a fim de proteger os indivíduos de discriminação e impedir a desigualdade de gênero.

É igualmente garantida coerência com a Carta dos Direitos Fundamentais da União Europeia e a legislação derivada da União em vigor em matéria de proteção de dados, defesa dos consumidores, não discriminação e igualdade de género. A proposta não prejudica e completa o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679] e a Diretiva sobre a Proteção de Dados na Aplicação da Lei [Diretiva (UE) 2016/680] com um conjunto de regras harmonizadas aplicáveis à conceção, ao desenvolvimento e à utilização de determinados sistemas de Inteligência Artificial de risco elevado e restrições a determinadas utilizações de sistemas de identificação biométrica à distância. Além disso, a proposta completa o direito da União em vigor em matéria de não discriminação com requisitos específicos que visam minimizar o risco de discriminação algorítmica, em particular no que diz respeito à conceção e à qualidade dos conjuntos de dados utilizados no desenvolvimento de sistemas de Inteligência Artificial, complementados com obrigações de testagem, gestão de riscos, documentação e supervisão humana ao longo do ciclo de vida dos sistemas de Inteligência Artificial. A proposta não prejudica a aplicação do direito da concorrência da União. (EUR, 2021)

No campo da responsabilidade civil, a Corte brasileira definiu que a inobservância dos limites normativos no tratamento de dados pelo sistema de credit scoring configura abuso de direito, o que enseja indenização por danos morais e materiais:

> 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. 3°, 830, I e Il, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados (SIMÃO et. al., 202, p. 354).

O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando

abuso no exercício desse direito (art. 187 do Código Civil), 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. (STJ, 2022).

Buscando a responsabilidade civil do credit scoring na Lei Geral de Proteção de Dados Pessoais, embora o Superior Tribunal de Justiça já tenha reconhecido que o credit scoring não constitua tecnicamente um banco de dados (diferentemente da União Europeia) ainda assim é sedimentado e cristalino que todos os dados estatísticos utilizados para a sua finalidade, depende de dados pessoais. "Desta feita, importa perquirir, à luz da Lei Geral de Proteção de Dados Pessoais, a origem e a qualidade dos dados que alimentam a fórmula, de modo a aferir eventual emprego de dados cujo tratamento, a princípio, dependeria de consentimento do titular, por não se enquadrar nas hipóteses previstas no art. 7º, incisos II a X, e § 4º, da Lei Geral de Proteção de Dados Pessoais" (OLIVA; VIÉGAS, 2019, p. 591). E pelo resultado do score de crédito ser um "dado resumo" referente a uma pessoa e que pode representá-la virtualmente por corresponder ao seu perfil individual. Logo, a nota, a origem e a qualidade dos dados que alimentam o score também estão sob a abrangência do escopo da Lei Geral de Proteção de Dados Pessoais.

Reafirmado pelo que dispõe o artigo 20 da Lei Geral de Proteção de Dados Pessoais que "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). O desenvolvimento das técnicas de IA tem ocorrido com incrível velocidade nos últimos anos, de modo que esses modelos passam a ser cada vez mais atraentes para o interesse econômico na pontuação de crédito. No Brasil, tem crescido o número de empresas ofertando serviços de pontuação com pelo menos algum elemento de Inteligência Artificial desde a reforma da LCP, a exemplo das empresas Serasa e Neoway. (MATTIUZZO; FÉLIZ, 2022, p. 35).

Sendo a natureza do score de crédito de consumo, logo, o artigo 45 da Lei Geral de Proteção de Dados Pessoais, deixa claro como já explicitado que a responsabilidade civil também será textualmente objetiva: "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). Considerando o score de crédito como um sistema de inteligência artificial já categorizado, possui relação consumerista e utiliza dados pessoais, o Projeto de Lei 21/2020 também prevê explicitamente o regime de responsabilidade civil nesse caso Art.6, inciso VI, da responsabilidade:

> § 3º Quando a utilização do sistema de inteligência artificial envolver relações de consumo, o agente responderá independentemente de culpa pela reparação dos danos causados aos consumidores, no limite de sua participação efetiva no evento danoso, observada a Lei nº 8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor). (BRASIL, 2018).

Do artigo 6., inciso VI, do Projeto de Lei referido projeto de lei, como diz Gustavo Tepedino, “percebeu-se a insuficiência da técnica subjetivista, também chamada aquiliana, para atender a todas as hipóteses em que os danos deveriam ser reparados” (TEPEDINO, 1999, p. 175).

Dessa forma, conclui-se que a responsabilidade civil pelo uso de score de crédito é objetiva conforme o Projeto de Lei 21/2020 que estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil, nas relações de consumo, com todos os elementos objetivos que a conceituam no Código Civil pátrio.

> 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).

Ratificadas as hipóteses a respeito da responsabilidade civil objetiva e solidária a respeito dos agentes de tratamento e dos terceiros, comungada pelo microssistema de proteção de dados no caso do score de crédito, verifica-se que o desvio de finalidade da proteção ao crédito no uso do score para fins discriminatórios ao consumidor, a relação de consumo permanece. Dessa forma, permanecendo o mesmo tipo de responsabilidade atribuída a todos os atores. O que difere é a forma de dar eficácia a essa responsabilização de maneira preventiva e precaucional no caso específico do score de crédito a fim de inibir, minimizar, mitigar o dano discriminação que se coaduna ao objetivo de se interpretar a responsabilidade civil num sentido polissêmico. A partir da *responsability*, *accoutability*, *anwerability* e como última racio, a *liability* a fim de se alcançar uma responsabilidade civil mais lastreada na ética, na prevenção do que no dano em si. (EUR, 2021).

A Lei Geral de Proteção de Dados Pessoais em seus fundamentos protege a pessoa em seis dos seus sete incisos do artigo 2. São o reflexo dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural objetivados pela lei em seu artigo primeiro.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Uma das formas de proteção é o agir de boa-fé (uma manifestação moral, *responsability* que precede a lei), impedindo a discriminação atendo o tratamento de dados pessoais a uma finalidade espelhada em seus princípios no Art. 6º que já demonstram o caráter ético na prevenção do dano delimitando o tratamento.

> 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; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018).

Logo, será ilícito ou abusivo o tratamento de dados que não respeitar tais princípios. Posto que o perfil de crédito utilizado para finalidade outra que não seja a composição da referida nota para proteção ao crédito, concessão ou negativa de crédito (art.7, X, Lei Geral de Proteção de Dados Pessoais). Bem como a utilização de dados coletados para compor a nota desrespeitando critérios lícitos nos procedimentos de tratamento dos dados, desde a coleta ao compartilhamento e descarte desses dados, em decorrência da falta de transparência, negativa de acesso, opacidade das decisões automatizadas, coleta de dados sensíveis, falta de qualidade dos dados, resultando em práticas discriminatórias que expressam clara falta de conformidade (*compliance*) com a Lei Geral de Proteção de Dados Pessoais.

Reportando ao caso da venda de base de dados dos consumidores pela Serasa *Experian* em que o ministério público investigou o uso dos dados para criação de perfis discriminatórios em listas que eram compartilhadas e vendidas no mercado livremente.

A ação civil pública, proposta pelo ministério público do distrito federal busca o fim da comercialização de dados pessoais de consumidores por meio dos produtos “Lista Online” e “Prospecção de clientes”. Em suma, o MPDFT argumenta que a requerida, ao comercializar dados pessoais dos cadastrados, ultrapassa o limite permitido pela legislação e fere os direitos

de privacidade e intimidade, por realizar tratamento de dados de forma irregular. Considera violadas disposições constantes no Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet e na Lei Geral de Proteção de Dados. (TJDF, 2020).

O Tribunal de Justiça do Distrito Federal negou a apelação da Serasa, reconhecendo o desvio de finalidade no uso da base legal de proteção ao crédito, que as informações coletadas pela Serasa são coletadas de outras fontes por se encontrarem ali milhares de informações pessoais sensíveis e não permitidas pela Lei do Cadastro Positivo, nem pelo Código de Defesa do consumidor, nem pela Lei Geral de Proteção de Dados Pessoais para a finalidade de score. Que a base do legítimo interesse também não seria a via adequada pois não permite o tratamento de dados sensíveis e tal base requer necessariamente transparência no tratamento dos dados. O recurso da Serasa Experian foi improvido. Em suma:

> É estranho que as ferramentas e seus produtos sejam apresentados no site da empresa como serviços de elevada especialização e aprofundamento sobre segmentos sociais e hábitos de consumo e, nestes autos, sejam reduzidos a mera sintetização de informações cadastrais facilmente obtidas por qualquer sujeito. É de se indagar como a requerida poderia alcançar complexa segmentação de mercado e apontar inclusive padrões de consumo servindo-se tão somente de "dados meramente cadastrais" (disponibilizados às empresas no produto final). (TJDF, 2020).

Acerca da inteligência trazida pela decisão magistral sobre a massiva base de dados do Serasa Experian, a doutrina conclui que os dados pessoais que utilizados em decisões automatizadas acabam sendo coletados, em grande parte, de manifestações voluntárias por parte dos usuários, que os cedem muitas vezes como contrapartida para a participação em espaços de lazer, como ocorre com as redes sociais, ou, até mesmo, da busca pela saúde, a exemplo da coleta de dados sensíveis das tecnologias vestíveis voltadas para o monitoramento corporal. (MEDON, 2020, p. 245).

Continuando com a decisão:

> ademais, ao contrário do que pretende fazer crer a recorrente, a legislação pertinente à matéria não busca resguardar apenas informações sigilosas, confidenciais ou sensíveis. As regras de tratamento de dados incidem sobre quaisquer informações relacionadas a pessoas naturais identificadas ou identificáveis (art. 5º, inciso I, Lei nº 13.709/2018). Salienta-se, ainda, que os produtos ora impugnados estão precipuamente vinculados ao *marketing service*, o que afasta a hipótese de tratamento de dados para fins de proteção ao crédito (artigo 7º, inciso X, Lei nº 13.709/2018). A propósito, confira-se o teor do parecer colacionado aos autos pela recorrente, na parte em que trata dos objetivos da comercialização das ferramentas em questão (TJDF, 2020).

Sobre a impossibilidade de aplicação do legítimo interesse pela falta de transparência, de conformidade, pela afronta ao princípio da *accoutabilitty*. Além da utilização de dados pessoais de natureza meramente cadastral por conter no banco de dados informações

socioeconômicas e comportamentais dos consumidores: “Ocorre que, como bem pontuado pelo eminente parecerista (Professor Doutor Tércio Sampaio Ferraz Júnior – ID 29804815):

> a própria lei, ao estabelecer que o legítimo interesse é base legal admissível, exige, porém, uma série de cuidados e medidas especiais, antes e durante o curso do tratamento de dados pessoais. O legítimo interesse conecta-se, assim, com os princípios da transparência, responsabilização e prestação de contas, previstos nos incisos VI e X do art. 6° da LGPD, aí encontrando especial ressonância quando da sua utilização para o tratamento de dados [...] Em arremate, parece claro que o direito de exclusão do banco de dados – garantido pela requerida ao consumidor – mais interessaria em caso de demandas individuais. Ainda, constitui argumento incapaz de confrontar a ausência de transparência dos procedimentos de coleta e processamento de informações que, sob o pretexto de prestar serviços benéficos ao consumidor, invade a esfera da privacidade e avança sobre liberdades individuais, ultrapassando a legítima expectativa do titular das informações tratadas com tal propósito. Mesmo que o produto final dos serviços impugnados garanta ao contratante um apanhado de informações de natureza meramente cadastral, é inafastável a conclusão de que a segmentação e o direcionamento de mercado – prometidos pela requerida – depende de tratamento de informações outras, de natureza socioeconômica e comportamental, não havendo transparência sobre os trâmites de coleta e tratamento. IV. Dispositivo Ante o exposto, NEGO PROVIMENTO ao apelo. É o voto. (TJDF, 2020).

Cumpre ressaltar da decisão acima vai evidenciando que os dados utilizados para escoragem de crédito são coletados de diversas fontes sem transparência e essa base de dados também é vendida e compartilhada fomentando algoritmos de predição que sob o segredo de negócio embutido nos modelos algoritmos perpetuando discriminações carecendo de explicabilidade.

Outra situação a requerer atenção, é a da empresa “Decolar.com” que teve uma decisão paradigmática contestando os limites da predição algorítmica de comportamentos discriminação dos consumidores através de práticas que consideram dados de localização geográfica e precificação algorítmica, conhecidas por *“geo pricing*” e “*geo blocking*. A ação foi proposta pelo Ministério Público do Estado do Rio de Janeiro Martins, à época da 5ª Promotoria de Tutela Coletiva do Consumidor da Capital, com a instauração de inquérito civil (347/2016) e a propositura de ação civil pública (0111117- 27.2019.8.19.0001) em face da empresa "Decolar.com". Ela teve grande repercussão ao pôr em xeque os limites da perfilização do consumidor. Pois é a partir dela que são operadas discriminações por algoritmos de inteligência artificial. A decisão serviu de paradigma ao abrir a caixa-preta do algoritmo (PASQUALE, 2015, p. 09).

É extremamente difícil investigar abusos cometidos e escondidos em algoritmos complexos e robustecidos por técnicas de predição com base em aprendizado de máquina (*machine learning*). E a auditoria de algoritmo é outra barreira, pois os sistemas de inteligência artificial gozam de proteção ao segredo industrial como barreira. (art.20 Lei Geral de Proteção

de Dados Pessoais). Dessa forma, ponderando o segredo de negócio com direitos fundamentais, resultou na decisão do Superior Tribunal de Justiça que permitiu mediante sigilo, ato pericial para avaliar o código-fonte do algoritmo. Abriu-se a caixa-preta. E sem violar o sigilo de negócio posto que este ficou protegido pela justiça.

A decisão encontra paralelo com a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial. permitindo a abertura da caixa-preta algorítmica combatendo sua opacidade.

> A proposta impõe algumas restrições à liberdade de empresa (artigo 16.º) e à liberdade das artes e das ciências (artigo 13.º), a fim de assegurar o cumprimento de razões imperativas de reconhecido interesse público, como a saúde, a segurança, a defesa dos consumidores e a proteção de outros direitos fundamentais («inovação responsável») em caso de desenvolvimento e utilização de tecnologia de IA de risco elevado. Essas restrições são proporcionadas e limitadas ao mínimo necessário para prevenir e atenuar riscos de segurança graves e possíveis violações dos direitos fundamentais. O aumento das obrigações de transparência também não afetará desproporcionadamente o direito à proteção da propriedade intelectual (artigo 17.º, n.º 2), uma vez que estarão limitadas às informações mínimas necessárias para as pessoas singulares exercerem o seu direito à ação e à transparência necessária perante as autoridades de supervisão e execução, em conformidade com os mandatos destas. Qualquer divulgação de informações será realizada de acordo com a legislação aplicável, incluindo a Diretiva (UE) 2016/943 relativa à proteçãode know-how e de informações comerciais confidenciais (segredos comerciais)contra a sua aquisição, utilização e divulgação ilegais. Quando precisam de obter acesso a informações confidenciais ou a código-fonte para analisarem ocumprimento das obrigações substanciais, as autoridades públicas e os organismos notificados ficam sujeitos a obrigações de confidencialidade vinculativas. (EUR, 2021)

A decisão abre um precedente que se coaduna com as expectativas do titular de dados, com direito à transparência e explicação como solução, mas também como forma a inibir atos discriminatórios no uso de algoritmos e por outro lado, pode fomentar o caminho para uma inteligência artificial mais ética. O direito à explicação decorre do princípio da transparência, previsto na maioria das leis de proteção de dados do mundo (MONTEIRO; 2018)

O Regulamento Geral de Proteção de Dados Europeu, por exemplo, prevê o direito à informação qualificada *(meaningful*) sobre a lógica dos processos de decisões automatizadas (SELBST; POWLES, 2017, p. 233-242). A explicação surge, assim, como uma ferramenta à *accountability* de Inteligência artificial ao expor a lógica da decisão, devendo permitir ao observador determinar a extensão em que um input particular foi determinante ou influenciou um resultado. (DOSHI-VELEZ; KORTZ, 2017).

Ademais, espaços deliberativos com a participação de diversos atores podem ajudar a mitigar os custos envolvidos em sistemas de explicação - que, de outra forma, poderiam afetar desproporcionalmente empresas menores - bem como os desafios tecnológicos de se pensar

esse tipo de sistema. (BIONI, 2022, p. 23). Mas para essa problemática, apesar do Projeto de Lei 21/2020 de regulamentação de Inteligência artificial brasileiro ainda não prever como seria solucionada essa situação, ainda cabe discussão posto que poderá ser emendado. De outraforma, há previsão a esse respeito na doutrina prevendo uma espécie de seguro: para a ampliação de coberturas para os seguros atuais a cobrir expressamente os riscos causados pelaIA, a criação e comercialização de seguros facultativos específicos para o uso de Inteligência artificial (contratados por produtores e/ou proprietários) e seguros obrigatórios para produtores e/ou proprietários. Outra categoria seria o seguro dos chamados fundos de compensação. (JUNQUEIRA, 2022).

Na já citada proposta de regulação de inteligência artificial da União Europeia também há a previsão do estabelecimento de seguros a fim de não prejudicar a cadeia econômica nem deixar de responsabilizá-la pelo risco da materialização de danos.

Sob outro aspecto, a partir da decisão paradigmática em face da decolar.com, a barreira da revisão automatizada por revisão automatizada a pedido do titular de dados, encontra uma solução alternativa, posto que a Lei Geral de Proteção de Dados Pessoais veda a revisão por humano, impedindo um resultado justo. Assim, a perícia judicial não deixa de ser uma forma de revisão humana. Seria uma solução enquanto a Lei Geral de Proteção de Dados Pessoais não passa por regulamentação da Autoridade Nacional de Proteção de Dados ou, seja proposto um projeto de lei visando suas alterações. A revisão humana é prevista no regulamento geral de proteção de dados europeu e ratificada na proposta do projeto de inteligência artificial do bloco em seu artigo 14, que trata da supervisão humana. O termo "supervisão" é proposital e pretende que se vá além da revisão, posto que a interferência humana não deve estar apenas no resultado, a fim de garantir um processo ético em inteligência artificial apto a mitigar, mas a prevenir:

> 1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA. 2.A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos neste capítulo. 3.A supervisão humana deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas: a) Medidas identificadas e integradas, quando tecnicamente viável, pelo fornecedor no sistema de IA de risco elevado antes de este ser colocado no mercado ou colocado em serviço; b) Medidas identificadas pelo fornecedor antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que sejam adequadas para implantação por parte do utilizador. 4.As medidas a que se refere o n.º 3 devem permitir que as pessoas responsáveis pela supervisão humana façam o seguinte, em função das

> circunstâncias: a) Compreendam completamente as capacidades e limitações do sistema de IA de risco elevado e sejam capazes de controlar devidamente o seu funcionamento, de modo que os sinais de anomalias, disfuncionalidades e desempenho inesperado possam ser detetados e resolvidos o mais rapidamente possível; b) Estejam conscientes da possível tendência para confiar automaticamente ou confiar excessivamente no resultado produzido pelo sistema de IA de risco elevado («enviesamento da automatização»), em especial relativamente aos sistemas de IA de risco elevado usados para fornecer informações ou recomendações com vista à tomada de decisões por pessoas singulares; c)Sejam capazes de interpretar corretamente o resultado do sistema de IA de risco elevado, tendo em conta, nomeadamente, as características do sistema e as ferramentas e os métodos de interpretação disponíveis; d)Sejam capazes de decidir, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter o resultado do sistema de IA de risco elevado; e)Serem capazes de intervir no funcionamento do sistema de IA de risco elevado ou interromper o sistema por meio de um botão de «paragem» ou procedimento similar. 5.Em relação aossistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as medidas referidas no n.º 3 devem, além disso, permitir assegurar que nenhuma açãoou decisão seja tomada pelo utilizador com base na identificação resultante do sistema, salvo se ela tiver sido verificada e confirmada por, pelo menos, duas pessoas singulares. (EUR, 2021).

Essa estratégia da avaliação humana também socorre de um risco no input dos dados. Com a avaliação e intervenção humana em várias fases há a presunção melhora na qualidade dos dados coletados para serem utilizados nos sistemas de inteligência artificial para a formação de perfis. Outra sugestão é a efetividade da pátria da regulação que veda a utilização de informações sensíveis para score de crédito em seu art. 7-A, incisos I a III, da Lei 12.414/2011, com a redação que lhe determinou a Lei Complementar 166/2019:

> Art. 7°-A Nos elementos e critérios considerados para composição da nota ou pontuação de crédito de pessoa cadastrada em banco de dados de que trata esta Lei, não podem ser utilizadas informações. I - que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e as convicções políticas, religiosas e filosóficas; II - de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica; e II - relacionadas ao exercício regular de direito pelo cadastrado, previsto no inciso II do caput do art. 5° desta Lei. (BRASIL, 2019).

A disciplina dos sistemas de pontuação de crédito, como de resto, dos bancos de dados de proteção ao crédito, embora submetidos à legislação específica, não afasta as normas sobre tratamento de dados pessoais (em especial a Lei Geral de Proteção de Dados Pessoais) e de proteção do consumidor (Código de Defesa do Consumidor). Em especial, para prevenir a discriminação de consumidores, um dos aspectos de maior repercussão no tocante ao tratamento de dados pessoais no âmbito das relações de consumo.

Os limites fixados na norma, claramente relacionam-se com princípios que informam o tratamento de dados pessoais, a saber, da finalidade, necessidade e adequação, bem como para evitar eventual discriminação injusta. Mas não tem caráter exaustivo, uma vez incidir

sobre este tratamento de dados para fins de proteção e crédito não apenas a norma específica, mas também a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. O art.7-A, 1, da Lei 12.414/2011, deste modo, tem sua interpretação associada aos arts. 2, IV, e 6, I, II, III e IX, da Lei Geral de Proteção de Dados Pessoais. Tratam-se, ademais, de dados pessoais sensíveis, segundo definição do art. 5°, II, da IGPD, cujo tratamento observa hipóteses restritas no art. 11 da IGPD. (BIONI, 2022, p. 304- 306)

Mas a vedação das leis não tem resolvido o problema da coleta e uso dos dados pessoais sensíveis e de comportamento social pelos birôs de crédito que tem usado os chamados dados alternativos diante da insuficiência dos dados tradicionais (para as atividades de escoragem de crédito. (HURLEY; ADEBAYO, 2016, p. 53-54).

Segundo Victor Silveira (2017), são alternativos todos os dados que não são tradicionalmente empregados para análise de crédito. Em um primeiro momento, dados alternativos podem ainda ser classificados em duas subcategorias: dados alternativos financeiros e não-financeiros. (SILVEIRA, 2022, p. 279)

A primeira subcategoria se refere a dados que são financeiros, mas que, por qualquer razão, não são costumeiramente utilizados na composição de escores de crédito. Por exemplo, tanto informações sobre o adimplemento de dívida garantida por hipoteca como sobre pagamento de aluguel de imóveis têm natureza financeira, mas, nos Estados Unidos, apenas as primeiras fatoram como dados tradicionais em análises de crédito; por essa razão, as segundas são consideradas dados alternativos financeiros. Outras informações que se encaixam nessa categoria, no contexto norte-americano, são as que se referem ao pagamento de serviços públicos, demonstrações de fluxo de caixa de pessoas jurídicas, dentre outras. (SILVEIRA, 2022, p. 279)

Dados alternativos não-financeiros, por outro lado, não têm relação direta com a vida financeira do consumidor, mas podem ter, considerados a partir de cruzamento com outras informações e em determinados contextos, na análise preditiva e consideração da concessão de crédito e dos seus termos. Exemplos desse tipo de informação são dados sobre a educação formal e histórico profissional de pessoas naturais, atividades em mídias sociais e até mesmo históricos de navegadores da Internet - informações geralmente definidas como Big Data. Um exemplo relevante de uso desse tipo de informação é o nível de educação formal, a área de especialização e o histórico profissional do cadastrado. (SILVEIRA, 2022, p. 279)

Apesar desses dados oferecerem riscos de discriminação quebra de equidade no tratamento de consumidores pertencentes a grupos desprotegidos pela descontextualização de determinadas informações, como “moradores de áreas subvalorizadas” (carentes). Há também

riscos de transparência, pois o consumidor não sabe como essa informação foi compor a base de dados, gerando prejuízos de acesso ao crédito e ao direito da personalidade; A falta de confiabilidade dos dados alternativos pela sua incapacidade de validar fontes; e o risco à segurança da informação pois os birôs de crédito tendem a possuir uma base mais robusta e maior para perfis diversificados, o que aumenta a hipótese de vazamentos (SILVEIRA, 2022, p. 280)

Assim os quatro maiores birôs de crédito que atuam no país – Serasa Experian, Boa Vista, SPC brasil e Quod, estão reunidos pela Associação Nacional de Birôs de Crédito (ANBC, 2022), passam a sofrer a incidência da atuação da Autoridade Nacional de Proteção de Dados Pessoais para fiscalizar e regulamentar o uso dos dados alternativos pelo disposto nos artigos 7. , inciso, e pelo artigo 55-J, inciso I, devendo a Autoridade Nacional da Proteção de Dados em sua função, zelar pela proteção de dados pessoais nos termos da legislação. Assim além da regulamentação da avaliação humana, pode a Autoridade Nacional da Proteção de Dados, regular o uso dos dados alternativos pelos birôs de crédito. O que caracteriza uma medida lastreada na *liability*.

Na proposta de regulamento de inteligência artificial da União europeia, o sistema de cumprimento para a qualidade dos dados proposto reside num ambiente de treinamento dos dados para diminuir os riscos de enviesamento e discriminação:

> A disponibilidade de dados de elevada qualidade é um fator essencial para o desempenho de vários sistemas de IA, sobretudo quando são utilizadas técnicas que envolvem o treino de modelos, com vista a assegurar que o sistema de IA de risco elevado funcione como pretendido e de modo seguro e não se torne a fonte de uma discriminação proibida pelo direito da União. Para garantir conjuntos de dados de treino, validação e teste de elevada qualidade é necessário aplicar práticas adequadas de governação e gestão de dados. Os conjuntos de dados de treino, validação e teste devem ser suficientemente relevantes, representativos, livres de erros e completos, tendo em vista a finalidade prevista do sistema. Também devem ter as propriedades estatísticas adequadas, nomeadamente no que respeita às pessoas ou aos grupos de pessoas nos quais o sistema de IA de risco elevado será utilizado. Em particular, os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do exigido face à sua finalidade prevista, as características, as funcionalidades ou os elementos que são específicos do ambiente ou do contexto geográfico, comportamental ou funcional no qual o sistema de IA será utilizado. A fim de proteger os direitos de outras pessoas da discriminação que possa resultar do enviesamento dos sistemas de IA, os fornecedores devem poder efetuar também o tratamento de categorias especiais de dados pessoais por motivos de interesse público importante, para assegurar o controlo, a detecção e a correção de enviesamentos em sistemas de IA de risco elevado. (EUR, 2021)

Os relatórios de impacto à proteção de dados pessoais (RIPDP), diante da dificuldade da gestão de consentimento, cada vez mais são uma saída nas leis de proteção de dados pessoais para gerir riscos. Em linhas gerais, tais relatórios seriam a documentação pela qual o

controlador - quem tem poder de tomada decisão na cadeia de tratamento de dados - registraria seus processos de tratamento de dados com as respectivas medidas adotadas para mitigar riscos gerados aos direitos dos titulares dos dados.

No cenário europeu, o controlador é obrigado a executar um RIPDP sempre que houver um alto risco em jogo. Há uma lista exemplificativa das hipóteses em que o tratamento de dados seria de alto risco, destacando-se a situação de perfilhamento como ponto de apoio para tomada de decisões. Por meio dessa definição, o emprego de Inteligência Artificial para automatização de processos de concessão de crédito, precificação de planos e seguro de saúde, seleção ou recrutamento de candidatos, elegibilidade a programas de assistências social, dentre uma outra série de situações do nosso cotidiano, deveria ser antecedida pela elaboração de um RIPDP. Além disso, quando o controlador não encontrar meios para mitigar os prováveis malefícios da sua respectiva atividade, deve, nesse caso, aguardar "luz verde" do regulador para seguir em frente. (BIONI, 2022, p. 232-233)

Como estratégia para minimizar e mitigar danos, a risquificação é utilizada no bloco europeu e no AI Act., projeto de inteligência artificial do bloco, há uma proposta de classificação ainda mais detalhada de risco de tecnologias. O risco varia de altíssimo baixo risco estabelecendo para cada tipo de tecnologia, medidas de governança e prestação de contas (*accountability*). No caso de score de crédito por ser sistema de inteligência artificial classificado como de risco elevado, há a obrigatoriedade, de acordo com o capítulo III, item 6, de realizar relatório de impacto.

> Os utilizadores de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º para cumprirem a sua obrigação de realizar uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, conforme aplicável. (EUR, 2021).

Pela Lei Geral de Proteção de Dados Pessoais, o relatório de impacto está previsto no artigo 5., inciso XVII – "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;" A regulamentação impondo obrigatoriedade de relatório de impacto ainda não tem correspondência no brasil, mas encontra parâmetros na Lei Geral de Proteção de Dados Pessoais de que poderá ser feito, mas a legislação não deixa claro, apesar do guia orientativo da ANPD (BRASIL, 2020) se, e quando ele será obrigatório. Mas como a governança de dados prevista na Lei Geral de Proteção de Dados Pessoais é baseada na gestão de riscos, as organizações são incentivadas a

realizar o relatório de impacto como exercício de boa -prática, o que por certo, impactará positivamente na indenização caso venha a ocorrer danos pelo tratamento de dados.

Para Bioni, no cenário brasileiro, a lei geral de proteção de dados pessoais não procedimentalizou minimamente o RIPDP. Muito embora haja algumas menções a tal instrumento, não há um capítulo próprio para tratar da matéria. Dessa forma, o RIPDP estaria condicionado à regulação posterior por parte de órgãos reguladores que precisariam quando seria obrigatório, bem como quais elementos e o tipo de análise que se espera encontrar em tal documentação. (BIONI, 2022, p. 232-233).

No cenário americano, há um projeto de lei, de autoria dos senadores Cory Booker e Ron Wyden, que obriga a elaboração de relatórios de impacto à proteção de dados, bem como de um relatório de impacto mais genérico, nas hipóteses em que não há o tratamento de dados pessoais, toda vez que houver o emprego de Inteligência Artificial para automatização de processos de tomada decisão: o Algorithmic Accountability, diferentemente da racionalidade regulatória europeia, não há a previsão da necessidade de iniciar uma conversa com o regulador quando se deparar com uma situação de alto risco e na qual não se encontrou medidas para controlá-lo.

De acordo com a definição adotada no RGPD:

> ‘profiling' means 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, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (WYDEN, 2022).

Outra forma de demonstrar responsabilidade e prestação de contas está também na proposta de regulamentação de inteligência artificial europeia. São as certificações e declarações de conformidade dos sistemas de inteligência artificial usado no score de crédito, por exemplo. A primeira demonstra o cumprimento das normas e a segunda, a chancela da conformidade com elas, com data de validade, ficando o fornecedor responsável por informar qualquer alteração nos sistemas. Essas informações que devem abastecer uma plataforma de consulta pública na internet, de maneira transparente.

> Artigo 48.º Declaração de conformidade UE 1.O fornecedor deve elaborar uma declaração de conformidade UE escrita para cada sistema de IA e mantê-la à disposição das autoridades nacionais competentes por um período de dez anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA. A declaração de conformidade UE deve especificar o sistema de IA para o qual foi elaborada. Deve ser fornecida uma cópia da declaração de conformidade UE às autoridades nacionais competentes, mediante pedido. 2.A declaração de conformidade UE deve mencionar que o sistema de IA de risco elevado em questão

> cumpre os requisitos estabelecidos no capítulo 2 do presente título. A declaração de conformidade UE deve conter as informações indicadas no anexo V e ser traduzida para uma ou várias línguas oficiais da União exigidas pelos Estados-Membros em que o sistema de IA de risco elevado é disponibilizado. 3.Se os sistemas de IA de risco elevado estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração de conformidade UE, deve ser elaborada uma única declaração de conformidade UE respeitante a todos os atos jurídicos da UE aplicáveis ao sistema de IA de risco elevado. A declaração deve incluir todas as informações necessárias para identificar a legislação de harmonização da União a que diz respeito. 4.Ao elaborar a declaração de conformidade UE, o fornecedor deve assumir a responsabilidade pelo cumprimento dos requisitos estabelecidos no capítulo 2 do presente título. O fornecedor deve manter a declaração de conformidade UE atualizada, consoante necessário. 5.A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar o conteúdo da declaração de conformidade UE preconizado no anexo V, a fim de introduzir elementos que se tornem necessários à luz da evolução técnica. Artigo 49.º Marcação de conformidade CE 1.A marcação CE deve ser aposta de modo visível, legível e indelével em sistemas de IA de risco elevado. Caso a natureza do sistema de IA de risco elevado não permita ou não garanta essas características da marcação, esta deve ser aposta na embalagem ou na documentação que acompanha o sistema, conforme mais adequado. 2.A marcação CE a que se refere o n.º 1 está sujeita aos princípios gerais estabelecidos no artigo 30.º do Regulamento (CE) n.º 765/2008. 3.Quando aplicável, a marcação CE deve ser seguida pelo número de identificação do organismo notificado responsável pelos procedimentos de avaliação da conformidade estabelecidos no artigo 43.º. O número de identificação deve ser igualmente indicado em qualquer material promocional que mencione que o sistema de IA de risco elevado cumpre os requisitos aplicáveis à marcação CE. (GDPR, 2016).

Esse tipo de incentivo e regulamentação de gestão dos dados e registro pode ser regulado pela Autoridade Nacional de Proteção de Dados e compor o Projeto de Lei 21/2020, em trâmite, que trata da regulação de inteligência artificial no Brasil.

Por fim, através da *responsability*, há formas de conceber uma abordagem ética e de boa fé que contamine todo o sistema de gestão de dados. Laudelina Pereira e Tarcizio silva, demonstram através de pesquisa feita no site reclame aqui e na rede social twitter, como a falta de transparência e opacidade algorítmica refletida através de reclamações nesses ambientes por parte dos consumidores revelam os sentimentos de discriminação e injustiça diante da falta de ensinamentos, de discussões que possam promover a consciência social sobre informações referentes ao score de crédito, e como hábitos financeiros interferem diretamente na pontuação a longo prazo. Por isso é preciso investir em informação e conscientização para preparar cidadãos aptos a exercerem seus direitos. (PEREIRA; SILVA, 2022, p. 193-209)

O Idec, Instituto Brasileiro de Defesa do Consumidor, desenvolve iniciativas nesse sentido que podem ser ampliadas com parcerias junto ao Governo e à sociedade civil. Instituto Brasileiro de Defesa do Consumidor, Guia de Educação Financeira. (IDEC, 2015).

Dessa maneira, sem a expectativa de exaurir o conteúdo, mas de contribuir para o debate, e encarando a responsabilidade civil de maneira ampla, na perspectiva de se agir preventivamente e com precaução para evitar o dano, essa é a proposta que mais se mostrou adequada ao cenário de riscos e ao que as leis nacionais já vêm positivando.

## 5 CONSIDERAÇÕES FINAIS

A crescente e onipresente utilização de dados pessoais somada ao argumento da necessidade destes para desenvolvimento tecnológico, para a inovação e proteção ao crédito – através da diminuição de riscos para o negócio das empresas – trouxe o problema da potencial discriminação dos consumidores.

Tal desvio na sua finalidade no tratamento desses dados através do compartilhamento entre as empresas, configura flagrante desrespeito aos direitos da personalidade, aos do consumidor, e aos direitos fundamentais como é pacífico na doutrina sobre proteção de dados pessoais globalmente.

Ademais a crescente digitalização dos serviços, as decisões automatizadas são a base da estratégia para o desenvolvimento econômico mundial. Como demonstrado no presente trabalho através de casos concretos e da bibliografia visitada, é que a utilização dessa tecnologia de inteligência artificial vem sendo incorporada pelos setores econômicos, utilizando dados pessoais tradicionais e alternativos coletando em tempo real detalhes dos comportamentos humanos nas áreas da educação, da saúde, profissional, de consumo para uso financeiro, como apontado nos sistemas de perfilização de crédito.

O uso de dados alternativos pode ensejar em inferências discriminatórias, equivocadas ou desatualizadas que afetem o acesso ao crédito. O uso do *score* de credito, numa relação de causa - consequência trouxe à baila das discussões legais e reivindicações da sociedade principalmente acerca da natureza do score de crédito, o vício do consentimento como ferramenta ineficaz diante da incapacidade de gerir apenas através dele a autodeterminação informativa, carecendo o consumidor de ter o direito de tratamentos mais transparentes com respeito aos dados utilizados nos novos métodos de avaliação do crédito, que se utiliza de perfilização dos consumidores para diminuir o risco de concessão de crédito para o mercado.

O presente trabalho então valeu-se de questionar, a fim de garantir segurança jurídica sobre o assunto, o entendimento jurisprudencial brasileiro estabilizou no sentido de que o *credit score* é um método legal de avaliação de risco financeiro. Posto que este tem como barra de trava o respeito aos direitos fundamentais e ao sistema jurídico de proteção aos dados pessoais e o atual desafio de se interpretar o score de crédito como um tratamento de dados automatizado na modalidade perfil de crédito. Ou seja, há o uso de algoritmo que se alimenta de dados pessoais. Somado a isso, há os riscos inerentes dessa atividade que necessita do tratamento de dados de comportamento dos consumidores, o que não é permito em lei.

Logo, o desafio de efetividade e regulação são flagrantes, bem como os riscos aos direitos fundamentais que podem gerar danos aos titulares. Então, refletir sob esse contexto que envolve a reclamação do consumidor e os possíveis danos é, naturalmente, desaguar no território da responsabilidade civil. Pois, sob essa perspectiva, o Direito tem um papel fundamental na estabilização de ambientes tecnológicos mais justos e previsíveis.

Entretanto, a complexidade da modelagem preditiva torna a condução do senso de justiça um encargo extremamente complexo sobre se é justo prever o comportamento humano e a confiança com base em algoritmos.

O desafio desta dissertação foi estabelecer uma relação lógica e sistemática para, com fins de minimizar e mitigar esses problemas, buscar no microssistema do ordenamento jurídico brasileiro com pontuais recortes da literatura e legislação e internacional que são referência no tema, um sentido amplo e ressignificado de responsabilidade civil que abarque a prevenção do dano. Não apenas o resultado dele. E verificou-se clara identificação da possibilidade dessa interpretação à luz da Constituição Federal, do Código Civil, Código de Defesa do Consumidor, da Lei Geral de Proteção de Dados Pessoais e do projeto de lei 21/2020, que versa sobre a regulação da inteligência artificial de onde harmônica e sistematicamente, extraem-se elementos que caracterizam essa responsabilidade civil preventiva baseada no risco. Entre eles funções como *Responsability, accoutability, liability e answerability.*

Juntos e separadamente, esses elementos dão uma função à responsabilidade civil que empoderam os direitos fundamentais frente à responsabilização civil que requer mais transparência no tratamento de dados pessoais.

Dessa leitura foi possível encontrar caminhos que apontam à Lei Geral de Proteção de Dados Pessoais a chave que estrutura o modelo brasileiro de proteção de dados com elementos para a instrumentalização desse sistema protetivo que, associados a outros recursos como regulação e aplicação eficaz da Autoridade Nacional de Proteção de Dados, do Poder Legislativo e do Poder Judiciário. Posto que a falta de transparência pode influenciar significativamente a capacidade de compreensão da metodologia utilizada nestes sistemas, reforçando o modelo de sociedade “caixa preta” que reproduz decisões algorítmicas em um ambiente opaco.

Assim, a prática é que pontuação de crédito deve respeitar a autodeterminação informativa, os direitos dos titulares de dados e demais direitos fundamentais e assumir as responsabilidades pelo compartilhamento de dados dos consumidores e desvio de finalidade no tratamento desses dados. O direito à explicação se coaduna com todos os outros direitos

do titular e está por trás de todas as sugestões elencadas neste trabalho – a exemplo da intervenção humana – para que a Lei Geral de Proteção de Dados Pessoais possa de fato, garantir ao indivíduo, o direito de exigir a eficaz transparência e autocontrole no processo de perfilização de crédito.

Assim, será possível chegar-se a uma responsabilidade civil preventiva como sugere a ampla doutrina e que demonstra o caráter dessa responsabilidade, não só pelas funções delineadas como a *accoutability* e a *liability*, mas também por outro elemento que deve permear todo ordenamento jurídico ético: a transparência ou *answerability* como parâmetro resolução numa sociedade de riscos.

Chegou-se à conclusão que pela harmonia do ordenamento jurídico antes e pós Lei Geral de Proteção de Dados Pessoais, que a responsabilidade civil pelo descumprimento é objetiva, cabendo ao julgador em caso de dano, responsabilizar o fornecedor ou operador do *credit score*, bem como terceiros, não na medida da culpa, mas na medida proporcional em que esses atores tiveram uma conduta a prevenir o dano.

Como tema fervilhante na doutrina e jurisprudência, não houve nesta pesquisa e reflexão, qualquer interesse em reduzir a amplitude do tema do Direito ou resolver a questão de maneira puramente objetivo.

Conclui-se que é necessário o aprofundamento dos estudos para além do agora e em paralelo ao desenvolvimento da tecnologia e ao célere movimento de inovação que tende, por sua natureza, a tornar mais complexo ainda mais o assunto com os problemas emergentes e a particularidade de cada caso.

Por outro lado, pesquisas acadêmicas como esta servem para manter o tema proteção de dados pessoais na evidência que reclama e com a possibilidade de contribuir para o desenvolvimento da disciplina e apoiar estudos empíricos que pretendem identificar as falhas dos novos riscos de inferências ocasionadas pelo score de crédito em processos de perfilização de crédito automatizado.

Portanto, a fim de que a presente dissertação seja um convite a novos estudos sobre a matéria e, assim contribua para que o necessário avanço tecnológico, apesar de inevitável, não atropele os direitos fundamentais e humanos, despersonalizando-os de sua essência, que nos cumpre enquanto agentes do Direito buscar sua devida proteção.

## REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Brasília, 31 ago. 2005. Disponível em: https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf. Acesso em: 03 nov. 2022.

ABRAFI. **Carta aberta às Autoridades:** Pela imediata segurança jurídica no tratamento de dados pessoais. Brasília, 2018Disponível em: http://www.abrafi.org.br/js/ckeditor/foto_internas/CartaabertaasautoridadesLGPDeSeguranc aJuridica_VF15.pdf. Acesso em: 09 abr.2022.

ACESSO à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas. Agência Câmara de Notícias, Brasília, 2021. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de--protecao-de-dados-dizem-especialistas. Acesso em: 5 set. 2022

ACESSO à informação não pode ser prejudicado por conta de Lei de Proteção de Dados. Brasília, 2021. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado- por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/#:~:text=Autoridades%20ouvidas%20pela%20Comiss%C3%A3o%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(LGPD). Acesso em: 19 abr. 2022.

ACN. **Lei Geral de Proteção de Dados Pessoais completa quatro anos com avanços e desafios**. Brasília, 2022. Disponível em: https://www.camara.leg.br/noticias/904176-lei-geral-de-protecao-de-dados- pessoais-completa-quatro-anos-com-avancos-e-desafios/. Acesso em: 5 out. 2022

ANDRADE, Robson Braga de. Os danos da insegurança jurídica para o Brasil: Falta de nitidez sobre direitos e deveres e alterações em leis atrapalham a competitividade. **Veja**, São Paulo, 14 set. 2018. Disponível em: https://veja.abril.com.br/economia/os-danos-da-inseguranca-juridica-para-o- brasil. Acesso em: 10 set. 2022

ANEFAC - Associação Nacional dos Executivos de Finanças, Administração e Contabilidade. Brasília, 2021. Disponível em: https://www.anefac.org/pesquisa-de-juros setembro/2021 https//819885de-e57a- 4397-b034-8bc82d0102a.filesusr.com/ugd/bed087_ddfd9d-d91271401ba5ce510cac93f881.pdf>. Acesso em: 06 set. 2022

ANGWIN, Julia et al. **Breaking the black box**: When machines learn by experimenting on US. ProPublica. New York, 12 out. 2016. Disponível em: https://www.propublica.org/article/breaking-the-black-box-when-machines-learn- by-experime nting-on-us. Acesso em: 03 mar. 2021.

ANPD. **Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília/DF. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 9 dez. 2022

ARNAUD, André-Jean. **La gouvernance**: un outil de participation. Paris: LGDJ, 2014.

ARNAULD, Andreas Von; DECKEN, Kerstin Von; SUSI, Mart. **The Cambridge Handbook of new human rigths**. Cambridge: Cambridge University Press, 2022.

ARNAULD, Andreas Von; DECKEN, Kerstin Von; SUSI, Mart. **The Cambridge Handbook of new human rigths**. Cambridge: 2020.

ASIA-PACIFIC ECONOMIC COOPERATION (APEC). **Privacy Framework**. 2005. Disponível: https://www.apec.org/ Publications/2005/12/APEC-Privacy-Framework. Acesso em: 20 mar. 2022

ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO. **Sobre ANBC**. 2022. Disponível em: https://anbc.org.br/sobre-a-anbc. Acesso em: 9 dez. 2022

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias: Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 273, p. 123-163, set./dez. 2016.

BARRETO, A. Menezes Cordeiro. **Comentário ao regulamento geral de proteção de dados e à lei n.° 58/2019**. Coimbra: Almedina, 2021.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BELLI, Luca; DONEDA, Danilo. **Proteção de Dados na américa Latina**. Porto Alegre: Aquipélogo, 2021

BENJAMIN, Ruha. Retomando nosso fôlego: estudos de ciência e tecnologia, teoria racial crítica e a imaginação carcerária. *In*: SILVA, Tarcizio (Org.). **Comunidades, algoritmos e ativismos digitais**: olhares afrodiaspóricos. São Paulo: LiteraRUA, 2020.

BENJAMIN, Ruha. Retomando nosso fôlego: estudos de ciência e tecnologia, teoria racial crítica e a imaginação carcerária. *In*: Silva, Tarcizio (Org.). **Comunidades, algoritmos e ativismos digitais**: olhares afrodiaspóricos. São Paulo: LiteraRUA, 2020.

BENNET, Colin. The european general data protection regulation: an instrument for the globalizatin of privacy standards? **Policy Review**,v. 23, 2018. Disponível em:https://web.archive.org/web/20180720050914id_/https://content.iospress.com/download/ i nformation-polity/ip180002?id=information-polity%2Fip180002. Acesso em: 01 abr. 2022

BENNETT, C.J. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, *In*: AGRE, Philip. E.; ROTENBERG, Marc. **Agre and M. Rotenberg, Technology and Privacy.** The New Landscape. Cambridge: The MIT Press, 1997.

BENNETT, C.J. **Regulating Privacy**: Data Protection and Public Policy in Europe and the United States. Ithaca, NY: Cornell University Press, 1992.

BENNETT, C.J.; RAAB, C. **Revisiting the Governance of Privacy**. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086. Acesso em: 2 abr. 2022,

BENNETT, C.J.; RAAB, C. **The Governance of Privacy**: Policy Instruments *in*: Global Perspective. Cambridge: MIT Press. Bennett, C.J. 2016. Is Canada still 'Adequate' under the New European General Data Protection Regulation? Disponível em: http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-newgeneraldata-protection-regulation/. Acesso em: 6 abr. 2022.

BESSA, Leonardo Roscoe. Banco de dados e cadastros de consumo. *In*: BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2016.

BIONE, Bruno Ricardo. **Regulação e proteção de dados pessoais, o principio da accoutability**. Rio de Janeiro: Forense, 2022.

BIONI, B. R. **Proteção de Dados pessoais**: a função e os limites do consentimento. Rio de Janeiro. Forense, 2019.

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

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

BIONI, Bruno Ricardo. **Proteção de dados**: contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. (Direito e constituição).

BIONI, Bruno Ricardo**. Regulação e proteção de dados pessoais, o princípio da accoutability**. Rio de Janeiro: Forense, 2022.

BIONI, Bruno **Ricardo. Regulação e proteção de dados pessoais: o princípio da *accountability*.** Rio de Janeiro: Forense, 2022.

BIONI, Bruno. **Proteção de dados pessoais**: as funções e os limites do consentimento. Rio de Janeiro: Gen, 2019.

BIONI, Bruno; MONTEIRO, Renato Leite; OLIVEIRA, Maria Cecília. **GDPR Matchup**: Brazil's General Data Protection Law. 2018. Disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (original em inglês). Acesso em: 09 nov. 2022

BIONI, Bruno; SILVA, Paula; MARTINS, Pedro**.** Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso.**Coletânea de Artigos da Pós-Graduação em Ouvidoria Pública**. 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504/284. Acesso em: 16 nov. 2022.

BITTAR, Carlos Alberto. Os direitos da personalidade e o projeto de Código Civil brasileiro. **Revista de Informação Legislativa,** Brasília, n. 60, out/dez 1978.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 15. ed. São Paulo: Malheiros, 2004.

BRAGA, Jeffeson Oliveira; FERREIRA, Rafael Freire. **Direito, economia e tecnologia:**

ensaios interdisciplinares. Goiânia: Editora Espaço Acadêmico, 2019.

BRASIL, 2005. ABNT: ISO/IEC27002. 2005. Disponível Em: https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf Acesso em: 9 dez. 2022

BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 02 out. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei n° 3514/2015**. Altera a Lei n° 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9° do Decreto-Lei n° 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao-2052488.Acesso em: 21mar.2021

BRASIL. Camara dos Deputados. **Projeto de Lei nº l4.060, de 2012**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01d4l9hv9v o6ho4zbue0qsw2ck844430.node0?codteor=1663305&filename=Tramitacao-PL+4060/2012 Acesso em: 14 maio. 2021

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

BRASIL. **Decreto nº 6659**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6659.htm Acesso em: 14 maio 2021

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 set. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 ago. 2020

BRASIL. **Lei nº 824, de 28 de dezembro de 1984**. Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no estado do rio de janeiro e dá outras providências. Brasília: 1984. Disponível em: https://gov-rj.jusbrasil.com.br/legislacao/149858/lei-824-84. Acesso em: 10 ago. 2022

BRASIL. **O PL 3.514/2015** teve origem no PLS 281/2012, de autoria do Senador José Sarney PMDB/AP. 2015. Disponível em: [www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=D89C4075A7213370D943E25F33D5904C.proposicoesWebExterno2?-codteor=1408274&filename=PL+3514/2015]..Acesso em: 1 ago. 2022

BRASIL. **Projeto de Lei nº 4.365, de 1977**. Brasília: Diário do Congresso Nacional, 1977. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD55 7906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 10 nov. 2020

BRASIL. **Projeto de Lei nº 4.374, de 2020**. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) e a Lei nº 12.414, de 9 de junho de 2011 para restringir o acesso, tratamento de compartilhamento de dados de consumidores por empresas de proteção ao crédito. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2261130 Acesso em: 3 set. 2022

BRASIL. **Proposta de Emenda à Constituição nº 17 de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 20 set. 2021.

BRASIL. Superior Tribunal de Justiça. **Ação Direta de Inconstitucionalidade nº 6.387**. Brasília, DF: Congresso Nacional, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 20 ago. 2021

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 22.337-8/RS**, Relator Ministro Ruy Rosado Aguiar, Recorrente Clube de Diretores Lojistas de Passo Fundo, Recorrido José Orivaldo Branco, Quarta Turma do Superior Tribunal de Justiça, 13 de fevereiro de 1995. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/157578?mode=full. Acesso em: 10 ago. 2022.

BRASIL. Superior Tribunal de Justiça. Segunda Seção. **Súmula nº 550.** Brasília, 14 de outubro de 2015. DJe 19/10/2015. Disponível em: https://scon.stj.jus.br/SCON/sumstj/toc.jsp. Acesso em: 30 nov. 2022.

BUCHINER, Benedikt. Informationelle Selbstbestimmung im Prioatrecht. *in*: MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

BYGRAVE, L. **Data Protection Law**: Approaching its Rationale, Logic and Limits. Toronto: Information and Privacy Commission, 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Acesso em: 1 abr. 2022.

CALABRICH, Bruno Freire de Carvalho. Discriminação Algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. **Revista de Direito e as Novas Tecnologias**, v. 8, jul-set/2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38411/1/Bruno%20Freire%20de%20Carvalho%2 0Calabrich.pdf. Acesso em: 1 mar. 2021.

CAMBRIDGE DICTIONARY. ***Liability***. 2022. Disponível em:

https://dictionary.cambridge.org/pt/dicionario/ingles/liability. Acesso em: 9 dez. 2022

CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da constituição**. Coimbra: Almedina, 2000.

CAOUETTE, J. ; ALTMAN, E; NARAYANAM, P. **Gestão do Risco de Crédito**: o Próximo Grande Desafio Financeiro. Rio de Janeiro: Qualitymark, 1999

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, jan./mar. 2020.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção Dados. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 163-170, Jan.-Mar./2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 9 dez. 2022

CARRIERE-SWALLON, Yan; HAKSAR, Vikram. **The economics and implications of data**: an integrated perspective. Washington, DC: International Monetary Fund, 2019.

Cassino, João Francisco. **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021.

CASSINO, João Francisco. *In:* SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO, João Francisco (orgs.). **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo, SP: Autonomia Literária, 2021.

CASTRO, Dayane. **Dados pessoais bancários e financeiros são considerados dados sensíveis para a LGPD?** 2021. Disponível em: https://www.migalhas.com.br/depeso/350335/dados-pessoais-bancarios-sao-considerados-dados-sensiveis-para-a-lgpd. Acesso em: 15 out. 2022.

CATALAN, Marcos. **Morte da culpa na responsabilidade contratual.** 2. ed. Indaiatuba, SP: Editora Foco, 2019.

CATALAN, Marcos. **Morte da culpa na responsabilidade contratual**. 2. ed. Indaiatuba, SP: Editora Foco, 2019.

CATALAN, Marcos. **Morte da culpa na responsabilidade contratual**. 2. ed. Indaiatuba, SP: Editora Foco, 2019.

CATALAN, Marcos. **Os sistemas de responsabilidade civil e a proteção de dados**. CIDP. 2022. Disponível em: https://4u-tenant.s3.sa-east-1.amazonaws.com/fmp/aulas/x7D4cqWMr1wmJPJbwCxHiP4EdrHswP9yE4b2lPmQ.pdf. Acesso em 16 ago. 2022.

CFPB. **Qual é a diferença entre um relatório de crédito e uma pontuação de crédito. Consumer Financial protecyion beureau**. Brasília, 2020. Disponível em: https://www.consumerfinance.gov/ask-cfpb/what-is-the-difference-between-a-credit-report-and-a-credit-score-en-2069/ . Acesso em: 12 ago. 2022.

CHINELLATO, Silmara Juny de Abreu; MORATO, Antonio Carlos. Direitos básicos de proteção de dados pessoais, o princípio da transparência e a proteção dos direitos intelectuais. In: In: DONEDA, Danilo *et al.* **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 644-667.

CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, v. 4, p. 403, 1993.

COLLINS, 2022. **Score**. Disponível em: https://www.collinsdictionary.com/pt/dictionary/english/score . Acesso em: 2 abr. 2022.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Sistemas de Petições e Casos**. OEA, 2010. Disponível em: https://www.oas.org/es/cidh/docs/folleto/CIDHFolleto_port.pdf. Acesso em: 02 out. 2021.

CONSUMER FINANCIAL PROTECTION BUREAU. **Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process**. Federal Register. Notices, v. 82, n. 33, 2017.

CORDEIRO, A. Barreto Menezes (coord.). **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Coimbra: Almedina, 2021.

CORTAZIO, Renan Soares**. Bancos de dados no Brasil**: uma análise do sistema credit scoring à luz da LEI N. 13.709/2018 (LGPD). v. 2, n. 3, 2019. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/99. Acesso em: 9 dez. 2022

COSIC, COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO. **Importância da LGPD**. 2022. Disponível em: https://lgpd.tcero.tc.br/importancia-da-lgpdc/. Acesso em: 9 dez. 2022

COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: rethinking big datas relation to the contemporary subject. **Sage Jourhals**, [s.l.], Sep. 2018. Disponível em: https://journals.sagepub.com/doi/10.1177/1527476418796632. Acesso em: 29 jul. 2021.

COULDRY, Nick; MEJIAS, Ulises. Colonialismo de dados: repensando a relação da big data com o sujeito contemporâneo. **SAGE**. ed. 4, v.20. 2018. Disponível em: https://journals.sagepub.com/doi/10.1177/1527476418796632. Acesso em: 9 dez. 2022

CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital**: A experiência de elaboração legislativa do Marco Civil da Internet. 138f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 3 ago. 2022

DATA PRIVACY, 2020. **Dados e o vírus**. 2020. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/04/Os-dados-e-o-vi%CC%81rus.pdf Acesso em: 14 maio 2021.

DATA PROTECTION WORKING PARTY . **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. Disponível em: https://www.dataprotection.ro/servlet/ViewDocument?id=1086. Acesso em: 19 maio. 2021.

DI PIETRO, Maria Sylvia. **O STJ e o princípio da segurança jurídica**. 2019. Disponível em: https://www.migalhas.com.br/depeso/302189/o-stj-e-o-principio-da-seguranca-juridica. Acesso em: 19 abr. 2022.

DIAS, Daniel. Implementação de seguro obrigatório de responsabilidade civil no contexto da inteligência artificial. In: **O Direito Civil na era da Inteligência Artificial**. TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coords). São Paulo: Revista dos Tribunais, 2020

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Revista Espaço Jurídico**. v. 12, n. 2, jul./dez. Joaçaba: 2001. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4972/0. Acesso em: 2 ago. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: Elementos da formação da Lei Geral de Proteção de Dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade a proteção de dados**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Lei geral de proteção de dados (Lei n° 13.709/2018) a caminho da efetividade:** contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo. **Privacy in the digital age**. 2017. Disponível em: https://www.itu.int/en/ITU-D/Capacity-Building/Documents/events/2017/Internet-Governance/AMS/Presentations/Session%209_1%20Danilo%20Doneda.pdf. Acesso em: 8 ago. 2021.

DONEDA, Danilo; ALMEIDA, Virgilio A. F. What is algorithm governance? **IEEE Internet Computing**, v. 20, p. 60, 2016.

DONEDA, Danilo; ALMEIDA, Virgilio A. F. **What is algorithm governance?** IEEE Internet Computing: 2016.

DONEDA, Danilo; MENDES, Laura Shertel. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DOSHI-VELEZ, KORTZ. **Accountability of AI Under the Law.** The Role of Explanation, 2017.

DRESCH, Rafael de Freitas Valle; MOURA JÚNIOR, José Falheiros. *In:* **Responsabilidade civil**: novos riscos / PASQUALOTTO, Adalberto et al. Indaiatuba, SP: Editora Foco, 2019.

ECONOMIST. **leaders**. 1999. Disponível em: https://www.economist.com/leaders/1999/04/29/the-end-of-privacy. Acesso em: 2 ago. 2020

EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (Coord.). **Direito Civil e Tecnologia.** Belo Horizonte: Fórum, 2021.

EUR-LEX. Proposta de regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas sobre a inteligência artificial (lei da inteligência artificial) e que altera certos legislativos da união. 2021. Disponível em: EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu). Acesso em: 9 dez. 2022

EUROPEAN COMMISSION. **Data Protection Rules Fit for a digital and globalized age, Press Statement**. 2015. Disponível em: www.europa.eu/rapid/press-release_IP-15-6321_en.htm. Acesso em: 06 mar. 2022.

EUROPEAN COMMISSION. **Quais dados pessoais são considerados confidenciais**?. Europa: UC, 2021.

EUROPEAN COURT OF JUSTICE. **Maximilian Schrems v. Data Protection Commissioner Case**.2015. Disponível em: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ0362. Acesso em: 12 mar. de 2022.

EUROPEAN UNION, Article 29 Working Party. **Adequacy Referential**. 2017. Disponível em: http://ec. europa.eu/newsroom/article29/itemdetail.cfm?item_id=614108. Acesso em: 05 abr. 2022

EUROPEAN UNION. **Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data**. 1995. Disponível em: http:// eur-lex.europa.eu/eli/dir/1995/46/oj. Acesso em: 09 abr. 2022

FAVARETTO, Maddalena. Big data and driscrimination: perils, promises and solutions. **Journal of big data**. 2019. Disponível em: https://d-nb.info/1180279247/34. Acesso em: 4 ago. 2022

FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados**: o direito à privacidade e os limites a função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. São Paulo: Revista dos Tribunais, 1992.

FERREIRA, Tamires. **LGPD**: ainda faltam muitos pontos para regulamentação, diz presidente da ANPD. Olhar digital. 2021. Disponível em: https://olhardigital.com.br/2021/06/28/pro/lgpd-ainda-faltam-muitos-pontos-para-regulamentacao-diz-presidente-da-anpd/. Acesso em: 09 abr. 2022.

FLAHERTY, D.H. **Protecting Privacy in Surveillance Societies**. Chapel Hill: University of North Carolina Press. Guagnin, D, Hempel L, Ilten C, Kroener I, Neyland D and Postigo H. 2012. Managing Privacy through Accountability. London: Palgrave Macmillan, 2012.

FORBES. **As marcas mais valiosas do mundo**. 2020. Disponível em: https://forbes.com.br/listas/2020/07/as-marcas-mais-valiosas-do-mundo-em-2020/. Acesso em: 1 ago. 2020.

FPC. **Princípios de Prática de Informação Justa (FIPPs**). 2022. Disponível em: https://www.fpc.gov/resources/fipps/. Acesso em: 9 dez. 2022.

FRAZÃO, Ana. **Discriminação algoritmica**: por que os algoritmos preocupam quando acertam e quando erram? Parte VIII. Disponível em: http://www.professo-manafrazao.com.br/files/publicacoes/2021-08-04-1Discriminacao_algoritmica_por_que_os_algoritmos_preocupam_quando_acertam_e_quando_erram_Mapeando_algumas_das_principais_discriminacoes_algoritmicas_ja_identificadas_Parte_VIII.pais. Acesso em: 20 dez 2021.

FRAZÃO, Ana. Transparência de algoritmos x
GIBSON, William. **Neuromancer**. Aleph, 1984.

GIBSON, Willian. **Neuromancer.** Nova York: Ace Books, 1984.

GLOBO. **Fintechs recorrem a dados**. Rio de Janeiro, 2021. Disponível em: https://valorinveste.globo.com/google/amp/produtos/servicos-financeiros/noticia/2021/01/25/fintechs-recorrem-a-dados-de-celular-e-redes-sociais-para-analisar-credito.ghtml. Acesso em: 14 maio 2021.

GONZÁLEZ, Mariana. **Conheça o cenário das leis de proteçao de dados pessoais ao redor do mundo**. 2020. Disponível em: https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/ . Acesso em: 2 ago. 2021.

GREENLEAF, G. **Global Data Privacy Laws**. 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International. 2017. Disponível em: https://ssrn.com/abstract=2993035. Acesso em: 03 abr. 2022.

GUIA orientativo para definições dos agentes de tratamento de dados pessoais do encarregado. Brasília: ANPD, maio 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 30 nov. 2022.

GUIMARÃES, Arthur. **Responsabilidade civil na LGPD**: não há consenso entre especialistas. JOTA. 2022. Disponível em: https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402 Acesso em: 09 nov. 2022.

HABERMAS, J. **Between Facts and Norms**: Contributions to a Discourse Theory of Law and Democracy. Cambridge: Polity Press, 1996.

HABERMAS, Jürgen. **Between facts and norms**: Contributions to a discourse theory of law and democracy. Cambridge: Polity Press, 1996.

HANS, JONAS. **O princípio responsabilidade**: ensaio de uma ética para a civilização tecnológica Hans Jonas. Rio de Janeiro: Contraponto, 2006.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das letras. 2018.

HARARI, Yuval Noah. **21 lições para o século** 21. São Paulo: Companhia das letras. 2018.

HARVARD, Law Revew. **O direito a privacidade**. 1890. Disponível em: https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 2 ago. 2021.

HILDEBRANDT, M. Defining Profiling. **A New Type of Knowledge**? *In*.: Hildebrandt, M.; Gutwirth, S. (Org.) Profiling the European Citizen: Cross-Disciplinary Perspectives.Cham/SWI: Springer ScienceICO, 2022. O que sao dados pessoais. Ico, 2022. Disponível em: https://ico.org.uk/for- organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation- gdpr/what-is-personal-data/what-is-personal-data/#pd2. Acesso em: 3 ago. 2022.

HURLEY, Mikella; ADEBAYO, Julius. Credit Scoring in the Era of Big Data. **Yale Journal of Law & Technology**, n. 148, v. 18, pp. 53-54, 2016.

I ASKED an online tracking company for all of my data and here's what I found. [s.l.], 7 nov. 2018. Disponível em: https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found. Acesso em: 30 nov. 2022.

IDEC. **Após pressão da sociedade, Senado aprova Lei de Dados Pessoais**. 2018Disponível em: https://idec.org.br/noticia/apos-pressao-da-sociedade-senado-aprova-lei-de-dados-pessoais. Acesso em: 10 nov. 2020.

IDEC. **Guia de educação financeira**: como organizar finanças. 2015. São Paulo: Idec, 2015. Disponível em: http:// www.idec.org.br/pdf/guia_educacao_financeira.pdf. Acesso em: 9 dez. 2022

IMPO, Centro de Informação Oficial. **Ley De Proteccion De Datos Personales**. Uruguai, 2008. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 2 ago. 2021.

INSTITUTO DE DEFESA DO CONSUMIDOR. **Por Trás da pontuação de crédito**: conheça seus direitos. São paulo: 2017.Disponível em: https://idec.org.br/system/files/ferramentas/manual-pontuacao-creditos.pdf. Acesso em: 9 dez. 2022

INSTITUTO DE PESQUISAS ECONÔMICAS APLICADAS. **Risco de Crédito**: desenvolvimento do modelo credit scoring para a gestão da inadimplência de uma instituição de microcrédito. Brasília: Ipea, 2006. Disponível em: http://www.ipea.gov.br/ipeacaixa/ premio2006/docs/trabpremiados/IpeaCaixa2006_Profissional_02lugar_tema03.pdf. Acesso em: 9 dez. 2022

INTER-AMERICAN COMMISSION ON HUMAN RIGHTS. **National jurisprudence on freedon of expression. And access to information**. 2013. Disponível em: https://www.oas.org/en/iachr/expression/docs/publications/2013%2005%2020%20national % 20jurisprudence%20on%20freedom%20of%20expression.pdf. Acesso em: 28 set. 2021.

JONAS, Hans. **O princípio responsabilidade**: ensaio de uma ética para a civilização tecnológica. 2011. Rio de Janeiro: Ed. PUC-Rio, 2006. Disponível em:

https://edps.europa.eu/system/files/2021-08/opinion_consumercredit-final_en.pdf. Acesso em: 09 de abr. de 2022.

JUNQUEIRA, Thiago. **Seguros para os riscos impostos pelo uso da inteligência artificial**. Consultor Jurídico. 2022. Disponível em: https://www.conjur.com.br/2022-out-13/seguros-contemporaneos-seguros-riscos-impostos-uso-inteligencia-artificial. Acesso em: 9 dez. 2022

JUSBRASIL. **Ação Civil pública**. 2021Disponível em: https://www.jusbrasil.com.br/processos/381389479/peca-peticao-trf03-acao-responsabilidade- do-fornecedor-acao-civil-publica-civel-de-instituto-brasileiro-de-defesa-da-protecao-de- dados-pessoais-compliance-e-seguranca-da-informacao-sigilo-contra-serasa-e-uniao-federal- 1338582684 Acesso em: 14 maio 2021.

JUSBRASIL. **Painel LGPD nos Tribunais**. 2021. Disponível em: https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html. Acesso em: 16 nov. 2021.

KISSINGER, Henry; LLC , Delphin; HUTTENLOCHER, Daniel. **The Age of A.I.** Dom Quixote, 2021.

KISSINGER, Henry; SCHMIDT, Eric; HUTTENLOCHER, Daniel. **A era da inteligência artificial.** São Paulo: Don Quixote, 2021.

LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial**: entre categorias e conceitos, a busca por marcos regulatórios. Indaiatuba, SP : Foco, 2022.

LACERDA, Bruno; TORQUATO, Zampier. **Estatuto jurídico da Inteligência Artificial**: entre categorias e conceitos, a busca por marcos regulatórios. São Paulo: Editora Foco, 2022.

LEITÃO, Miriam. **O passado é incerto**. 2022. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/510284/noticia.html?sequence=1. Acesso em: 19 abr. 2022.

LENK, Hans. **O que é responsabilidade?** 2006. Disponível em: https://philosophynow.org/issues/56/What_is_Responsibility. Acesso em: 04 nov. 2022.

LENK, Hans. **O que é responsabilidade?** Philosophy now. 2022. Disponível em: https://philosophynow.org/issues/56/What_is_Responsibility. Acesso em: 9 dez. 2022
LEWIS, E. ***An Introduction to Credit scoring***. Fair Isaac: San Rafael, California. 1992.

LIABILITY. *In:* CAMBRIDGE Dictionary, 2022. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/*liability*. Acesso em: 02 nov. 2022.

LIMA, Cíntia Rosa Pereira; PEROLI, Kelvin. Aplicação da Lei Geral de Proteção de Dados do Brasil no Tempo e no Espaço. *In:* **Comentários à lei geral de proteção de dados**. (Cood.) Cítia Rosa Pereira de Lima. São Paulo: Almedina, 2020.

LINDOSO, Maria Cristine Branco. **Discriminação de gênero em processos decisórios automatizados**. Dissertação - Faculdade de Direito, Universidade de Brasília. Brasília. 2019. Disponível em:

https://repositorio.unb.br/bitstream/10482/38524/1/2019_MariaCristineBrancoLin doso.pdf. Acesso em: 08 mar. 2021.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janciro: FGV Editora, 2018.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. Porto Alegre: 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MARRAFON, Marco; Medon, Filipe. **Importância da revisão humana das decisões automatizadas na lei geral de proteção de dados**. Consultor jurídico. 2019. https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd

MARTINS, Guilherme Magalhães. Responsabilidade civil, acidente de consumo e a proteção do titular de dados na Internet. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo. **Proteção de dados pessoais na sociedade da informação**: entre dados e danos. Indaiatuba: Foco, 2021.
MARTINS, Guilherme magalhaes; LONGHI , João victor rozatti. **Responsabilidade civil nas relações de consumo**. Indaiatuba, SP: Editora Foco, 2022

MARTINS, Guilherme Magalhaes; LONGHI, João Victor Rozatti. **Responsabilidade civil nas relações de consumo.** Indaiatuba, SP: Editora Foco, 2022.

MEDON, Filipe. **Inteligência artificial e responsabilidade civil**: autonomia, riscos e solidariedade. São Paulo: JusPodivm, 2022.

MEDON, Filipe. **Inteligência Artificial e Responsabilidade Civil**: autonomia, riscos e solidariedade. São Paulo: Editora JusPodivm, 2022.
MEDON, Filipe. Inteligência artificial e responsabilidade civil: autonomia, riscos e solidariedade. Salvador: JusPodivm, 2020
MEDON, Filipe. **Inteligência artificial e responsabilidade civil**: autonomia, riscos e solidariedade, 2 ed. Salvador: Juspodivm, 2022.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar**. 2020.

MENDES, Laura Schertel Ferreira. O direito fundamental a proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, p. 45-81 jul./set. 2011.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Migalhas. 2020. Disponível em:https://www.migalhas.com.br/coluna/migalhas-de-protecao-

de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acesso em: 10 nov. 2020.

MIRAGEM, Bruno et al. (org.). **Direito do consumidor**: 30 anos CDC: da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2021.

MMA. **Sobre o MMA**. 2022. Disponível em: https://www.mmaglobal.com/files/documents/copia_de_mma-playbook-privacy_2018_pt-3.pdf. Acesso em: 10 nov. 2020.

MONIER, Jean Claude**. personne humaine et responsabilité civile, Droit et cultures**. Paris: L´Harmattan, 1996.

MONIER, Jean Claude. **Personne humaine et responsabilité civile**. Paris: L´Harmattan, 1996. (Droit et cultures, n. 31).

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Instituto Igarapé, 2018.

MORAES, Maria Celina Bodin de. Prefacio. *In*: SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação a diluição dos danos. São Paulo: Atlas, 2007.

MORAES, Maria Celina Bodin de. Prefacio. *In*: SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação a diluição dos danos. São Paulo: Atlas, 2007

MULHOLLAND, caitlin; NASSER, rafael; CARVALHO, gustavo robichez. **A LGPD e o novo marco normativo no Brasil / organização Caitlin Mulholland**. Porto Alegre: Arquipélago, 2020.

NEGRINI, Sergio; Carolina, GIOVANINI. Dados nao pessoais: a retórica da anonimização no enfrentamento à covid-19 e o privawashing. **Internet & sociedade**. 2020. Disponpivel em: https://revista.internetlab.org.br/dados-nao-pessoais-a-retorica-da-anonimizacao-no-enfrentamento-a-covid-19-e-o-privacywashing/ . Acesso em: 15 jan. 2022.

NIC.BR. **Como robôs influenciaram as eleições de 2014 no Brasil**. 2018. Disponível em: https://nic.br/noticia/na-midia/como-robos-influenciaram-as- eleicoes-de-2014-no-brasil/. Acesso em: 10 nov. 2020.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). L**ei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thonson Reuters Brasil, 2019

OLIVEIRA, João José. Novas regras podem te deixar sem crédito por seu trabalho, endereço e idade. **UOL Economia**. São Paulo. 2020. Disponível em: ht-tps://economia.uol.com.br/noticias/redacao/2020/06/27/biros-criam-indices- que-di-ficultam-vida-de-quem-precisa-de-credito.htm. Acesso em: 29 jan. 2021.

OLIVEIRA; Marco AURÉLIO BELIZZE; PEREIRA LOPES, Isabela Maria. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

ORWELL, George. **1984.** New York: Penguin/Signet Classics, 1984. *E-book.*

ORWELL, George. **1984**. Nova lorque: Penguin/Signet Classics, 1961.

PADUA, Cleusa. **O sistema scoring e a dignidade da pessoa humana**. 2015. Disponível em: https://cleusanect.jusbrasil.com.br/artigos/223769925/o-sistema- scoring-e-a-dignidade-da-pessoa-humana?ref=serp. Acesso em: 10 out. 2022.

PAGALLO, Ugo. **The laws of robots**: crimes, contracts, and torts. Dordrecht: Springer, 2003.

PAGALLO, Ugo. **The laws of robots**: crimes, contracts, and torts. Dordrecht: Springer,

PAIVA, Letícia. **LGPD**: 77% das decisões que citam lei não resultaram em condenação em 2021. 2022. Disponível em: www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao-27012022. Acesso em: 19 abr. 2022.

PALHARES, Felipe. **Temas atuais de proteção de dados**. São Paulo: Revista dos Tribunais, 2020.

PASQUALE, Frank. **The Black Box Society**. Cambridge (EUA): Harvard University Press, 2015.

PASQUALE, Frank. **The Black Box Society**. Cambridge (EUA): Harvard University Press, 2015

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015

PASQUALOTTO, Adalberto *et al*. **Responsabilidade civil**: novos riscos. Indaiatuba, SP: Editora Foco, 2019.

PECK, Patrícia. **Proteção de Dados Pessoais**: Comentários à Lei nº 13.709/2018 LGPD. São Paulo: Saraiva, 2018.

PECK, Patrícia. **Proteção de Dados Pessoais**: comentários à Lei nº 13.709/2018 LGPD. São Paulo: Saraiva, 2018.

PEREIRA, Laudelina; SILVA, Tarcísio. **O consumidor na era da pontuação de crédito**. 2022.

PÉRON, Evita. **Donde hay uma necesidad nace um derecho**. Arsat, 2022. Disponível em: https://www.casarosada.gob.ar/pdf/Contexto%20-%20Arsat%20en%20la%20Argentina.pdf. Acesso em: 23 jul. 2022

PORTAL DA PRIVACIDADE. Atoridade britanica aponta falhas no tratamento de dados feitos por biros de crédito. 2020. Dispoível em: https://www.portaldaprivacidade.com.br/autoridade-britanica-aponta-falhas-no-tratamento-de- dados-feito-por-biros-de-credito/ Acesso em: 16 ago. 2022.

PROIBIÇÃO ao Alibaba é mais uma etapa da guerra das plataformas digitais EUA x China. *In:* BRASIL247, [s.l.], 2011. Disponível em: https://www.brasil247.com/blog/proibicao–ao–alibaba– e–mais–uma–etapa–da–guerra–das–plataformas–digitais–eua–x–china–8cjgrz5u ). Acesso em: 3 set. 2022

PROJETO fixa regras para uso de dados pessoais do consumidor por empresas de proteção ao crédito. Brasília, 2020 Disponível em: https://www.camara.leg.br/noticias/692295-projeto-fixa-regras-para-uso-de-dados-pessoais- do-consumidor-por-empresas-de-protecao-ao-credito/. Acesso em: 15 out. 2022

PROTEÇÃO de dados pessoais completa quatro anos. Brasília, 2012. Disponível em: https://www.camara.leg.br/noticias/904176-lei-geral-de-protecao-de- dados-pessoais-completa-quatro-anos-com-avancos-e-desafios/. Acesso em: 14 maio. 2021

PROVOST, Foster. **Data Science para negócios**. Rio de Janeiro: Alta Books, 2016.

PROVOST, Foster; FAWCETT, Tom. Data Science para negócios. Rio de Janeiro: Alta Books, 2016.

QUIJANO, Aníbal. Colonialidade do poder e classificação social. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula (Orgs.). **Epistemologias do Sul**. Coimbra: Almedina, 2009.

QUIJANO, Aníbal. Colonialidade do poder e classificação social. *In*: Santos, Boaventura de Sousa; Meneses, Maria Paula (Org.). **Epistemologias do Sul**. Coimbra: Edições Almedina, 2009.

QUINTILIANO, Leonardo. Posso vender meus dados pessoais? O resgate da doutrina da privacidade como propriedade. **Migalhas,** São Paulo, 25 nov. 2022. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/377587/posso-vender-meus-dados-pessoais. Acesso em: 30 nov. 2022.

RAAB C. **Networks for Regulation**: Privacy Commissioners in a Changing World. Journal of Comparative Policy Anal-ysis: Research and Practice. 2011.

RAMOS, Carmem Lúcia Silveira. **Diálogos sobre Direito Civil**: Construindo a Racionalidade Contemporânea. Rio de Janeiro: Renovar, 2002

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD. **template guia**. 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx

RENDA, Andrea; SIPICZKI, Agnes; YEUNG, Timothy. **Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe**. 2020. Disponível em: https://artificialintelligenceact.eu/wp- content/uploads/2022/06/AIA-COM-Impact-Assessment-3-21-April.pdf. Acesso em: 09 abr. 2022.

RODOTA, Stefano. **Palestra no Rio de Janeiro**. 2003. Disponível em: http://www.rio.rjg0v.br/dIstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf. Acesso em: 25 nov. 2022.

RODOTÀ, Stefano. Palestra no Rio de Janeiro. 2003. Disponível em: http://www.rio.rjg0v.br/dIstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf. Acesso em: 25 nov. 2022.

ROSENVALD, Nelson. 4 Conceitos de Responsabilidade Civil para a 4. Revolução Industrial e o Capitalismo de Vigilância. In: EHRHARDT JÚNIOR, Marcos (coord.). **Direito civil**: futuros possíveis. Forum, 2021.

ROSENVALD, Nelson. A LGPD e a despersonalização da personalidade. **Migalhas**, São Paulo, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350374/a-lgpd-e-a-despersonalizacao-da-personalidade. Acesso em: 5 mai. 2022.

ROSENVALD, Nelson. A polissemia da responsabilidade civil na LGPD. **Migalhas,** São Paulo, 6 nov. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336002/a-polissemia-da-responsabilidade-civil-na-lgpd. Acesso em: 3 nov. 2022.

ROSENVALD, Nelson. Quatro conceitos de responsabilidade civil para a 4ª revolução industrial e o capitalismo de vigilância. *In:* EHRHARDT JÚNIOR, Marco. **Direito civil:** futuros possíveis. Belo Horizonte: Forum, 2022.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. **Tecnologias emergentes**: seguros e fundos de compensação. Disponível em: https://www.conjur.com.br/2021-jul-22/seguros-contemporaneos-tecnologias-emergentes-seguros-fundos-compensacao. Acesso em: 04 nov. 2022

ROSSNAGEL, A. Einleitung. **Handbuch Datenschutzrecht**: Die neuen Grundlagen für Wirtschaft und Verwaltung. Munique: Beck Verlag, 2003.

ROUSSEAU, Jean-Jacques**. Discurso sobre a origem e os fundamentos da desigualdade entre os homens**. São Paulo: Nova Cultural, 1991.

RUZYK, Carlos Eduardo Pianovski. A responsabilidade civil por danos produzidos no curso de atividade econômica e a tutela da dignidade da pessoa humana: o critério do dano ineficiente. *In*: RAMOS, Carmem Lucia Silveira *et al.* (orgs.). **Diálogos sobre direito civil**: construindo uma racionalidade contemporânea. Rio de Janeiro: Renovar, 2002.

SANTOS, Romualdo Baptista dos. **Responsabilidade civil por dano enorme**. Curitiba: Juruá, 2018

SÃO PAULO. Tribunal de Justiça. **Processo nº 0081878-31.2020.8.05.0001.** Trata do golpe do motoboy, em que um criminoso se utiliza de fraude (se passando por funcionário de banco) para obter dados pessoais da vítima e efetuar transações subtraindo dinheiro de contas bancárias, constatada a fraude, os Tribunais aplicaram o Código de Defesa do Consumidor, destacando a responsabilidade civil por defeito do serviço e utilizando a LGPD como argumento complementar. Jurisprudência. 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1237604277/inteiro-teor-1237604297. Acesso em: 10 set. 2022.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**. Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/download/875/985/3804. Acesso em: 7 fev. 2022.

SARMENTO, Daniel. **A vinculação dos particulares aos direitos fundamentais**: o debate teórico e a jurisprudência do STF. *In*: LEITE, George Salomão; SALERT, Ingo Wolfgang; CARBONELL, Miguel (Coord.). Direitos, deveres e garantias fundamentais. Salvador, 2011.

SCARLET, Gabrielle Bezerra Sales. Notas sobre a proteção de dados pessoais na sociedade informacional na perspectiva do atual sistema normativo brasileiro. *In:* **Comentários à lei geral de proteção de dados**. (Cood.) Cítia Rosa Pereira de Lima. São Paulo: Almedina, 2020.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação diluição dos danos. 6. ed. São Paulo: Atlas, 2015

SCHWARTZ, Paul; SOLOVE, Daniel. The PII problem: privacy and a new concept of personally identifiable information. **Law Review**. 2011. Disponível em: https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-86-6-Schwartz-Solove.pdf . Acesso em: 7 fev. 2022.

segredo de empresa. **Jota**. 2021. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2021-06-09-Transparencia_de_algoritmos_x_segredo_de_empresa_As_controversias_a_respeito_das_decisoes_judiciais_trabalhistas_que_determinam_a_realizacao_de_pericia_no_algoritmo_da_Uber.pdf. Acesso em: 9 dez. 2022

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data privacy Law**, [s. l.], v. 7, n. 4, p. 233-242, 2017.

SENADO NOTÍCIAS. **Lei Geral de Proteção de Dados entra em vigor**. Agência Senado. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei- geral-de-protecao-de-dados-entra-em-vigor. Acesso em: 10 nov. 2020.

SERASA EXPERIAN. **Cadastro Positivo**. 2020. Disponível em: https://www.serasaexperian.com.br/lgpd/#:~:text=Por%20se%20tratar%20de%20uma,o%20tr atamento%20dos %20dados%20positivos. Acesso em: 14 de maio. 2021.

SERASA SCORE. **Uma nova versão do Serasa Score 2.0 para você**. 2022. Disponível em: https://www.serasaconsumidor.com.br/score/. Acesso em: 1 de outubro de 2017.

SICSÚ, Abraham Laredo. ***Credit Scoring***: desenvolvimento, implantação, acompanhamento. São Paulo: Blucher, 2010.

SILVA, Filipe Carreira da. **Espaço Público em Habermas**. United Kingdom: Universidade de Cambridge, 2001. Disponível em: https://repositorio.ul.pt/bitstream/10451/22584/1/ICS_FCSilva_Espaco_LAN.pdf. Acesso em: 02 nov. 2022.

SILVA, Filipe Carreira da. Espaço público em Habermas. Universidade de Cambridge: 2021. Disponível em: https://repositorio.ul.pt/bitstream/10451/22584/1/ICS_FCSilva_Espaco_LAN.pdf Acesso em: 9 dez. 2022

SILVA, João Calvão da. **Cumprimento e sanção pecuniária compulsória**, 2. ed. Coimbra: Coimbra Editora, 1995.

SILVA, José Afonso da. **Comentário Contextual à Constituição**. São Paulo: Malheiros, 2006.

SILVA, José Afonso. **Curso de direito constitucional positivo**. 37. ed. São Paulo: Malheiros, 2013.

SILVA, Thayse de Oliveira; SILVA, Lebiam Tamar Gomes. Os impactos sociais, cognitivos e afetivos sobre a geração de adolescentes conectados a tecnologia. **Pepsic**. v. 34, n. 103. 2017. Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S0103-84862017000100009. Acesso em: 4 maio 2022.

SILVA, João Calvão da. **Cumprimento e Sanção Pecuniária Compulsória**. 2. ed. Coimbra: Coimbra Editora, 1995

SILVEIRA, Victor doering da. **o consumidor na era da pontuação de crédito**. Letramento: 2022.

SIMÃO, Bárbara Prado. **O consumidor na era da pontuação de crédito**. Belo Horizonte, MG: Casa do Direito, 2022.

SOUSA, Samuel Brandão de. bancos de dados, escore de crédito e o direito do consumidor. **Núcleo de Conhecimento**. Disponível em: https://www.nucleodoconhecimento.com.br/lei/bancos-de-dados. Acesso em: 20 nov. 2022.

SOUSA, Samuel. **Bancos de dados, escore de crédito e o direito do consumidor**. 2020. Disponível em: https://www.nucleodoconhecimento.com.br/lei/bancos-de-dados. Acesso em: 28 jul. 2020.

SSRN. **2020 encerra uma década de 62 novas leis de privacidade de dados**. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611. Acesso em: 10 nov. 2020.

STANFORD. **The rule of law**. 2016. Disponível em: https://plato.stanford.edu/entries/rule-of-law/. Acesso em: 9 dez. 2022

STEINMÜLLER, Wilhelm; LUTTERBECK, Bernd; MALLMANN, Christoph; HARBORT, Uwe; KOLB, Gerhard; SCHNEIDER, Jochen. Grundfragen des Datenschutzes. **Gutachten im Auftrag des Bundesministeriums des Innern.** BTdrucks: 1971.

STEINWASCHER, Aline Rodrigues e. **Cadastro positivo**: o que muda para o mercado e para os consumidores. Consultor Jurídico. 2020. Disponível em: https://www.conjur.com.br/2020-jan-22/ali-ne-steinwascher-muda-cadastro-positivo#:~text=Trazendo%20n%C3%BAmer05%2C%20segundo%20estudos%2

0do,45%25%20nos%20%C3%ADndices%20de%20inadimpl%C3%AAncia. Acesso em: 06 set. 2021.

STJ. **Inteiro Teor das súmulas**. Brasília: 2022. Disponível em: https://www.stj.jus.br/docs_internet/jurisprudencia/tematica/download/SU/Sumulas/Sumulas STJ.pdf. Acesso em: 9 dez. 2022

SUGIMOTO, Erick. **Lgpd e o código civil**. 2022. Disponível em: https://ericksugimoto65.jusbrasil.com.br/artigos/919410066/lgpd-e-sua-interacao-com-o-codigo-civil Acesso em: 14 maio 2021.

SWIRE, P. **The Second Wave of Global Privacy Protection**: Symposium Introduction, 74. Ohio State Law Journal 841. 2013.

TEPEDINO, Gustavo. Temas de Direito Civil. 1. ed. Rio de Janeiro: Renovar, 1999.

THE RULE of Law. *In:* STANFORD Encyclopedia of Philosophy, [s.l.], Jun. 22, 2016. Disponível em: https://plato.stanford.edu/entries/rule-of-law. Acesso em: 25 nov. 2022.

THIBIERGE , Catherine. Libres propôs sur l´évolution du droit de la responsabilité (vers un élargissement de la fonction de la responsabilité civile? **Revue Trimestrelle de Droit Civile**. Paris, Jul.-set./1999.

THIBIERGE, Catherine. Libres propôs sur l´évolution du droit de la responsabilité (vers un élargissement de la fonction de la responsabilité civile? **Revue Trimestrelle de Droit Civile,** Paris, v. 3, p. 561, Jul./Set. 1999.

TJDF. **Determinação do serasa**. Brasília, 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais. Acesso em: 5 out. 2022.

TJRJ. **Procedimento do juizado especial cível. Dano moral. Tribunal de Justiça do Rio de Janeiro**. Rio de Janeiro, 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj- rj/1195859965/inteiro-teor-1195859966. Acesso em: 10 set. 2022.

TOMASEVICIUS FILHO, Eduardo. **Em direção a um novo 1984**? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada. R. Fac. Dir. Univ. São Paulo v. 109 p. 129-169 jan./dez. 2014. Disponível em: https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402 Acesso em: 14 maio 2021.

UNIÃO EUROPEIA. **General data protection regulation.** 2016. Disponível em: https://gdpr- info.eu/chapter-6/. Acesso em: 09 abr. 2022.

UNIÃO EUROPEIA. **Manual da legislação europeia sobre proteção de dados**. 2014. Disponível em: https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf. Acesso em: 30 mar. 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Disponível em: https://eur- lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 09 de abr. 2022.

UNIÃO EUROPEIA. **Regulamento geral de proteção de dados**. 2016. Disponível em: https://gdpr-text.com/pt/read/article-5/?col=1&lang1=pt&lang2=en&lang3=es#. Acesso em: 2 jun. 2022.

UOL. **Cadastro positivo é institucional**. 2019. Disponível em: https://congressoemfoco.uol.com.br/blogs-e-opiniao/forum/cadastro-positivo-e-inconstitucional/ Acesso em: 14 maio 2021.

UOL. **Justiça manda serasa parar de vender dados**. 2020. Disponível em https://www1.folha.uol.com.br/mercado/2020/11/justica-manda-serasa-parar-de-vender-dados-pessoais-de-brasileiros.shtml Acesso em: 14 maio 2021.

UOL. **Notificação serasa**. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/procon-notifica-serasa-por-exigencia-de-senha-de-banco-para-pesquisa-online.htm?cmpid=copiaecola. Acesso em: 14 maio 2021.

VELLOZO, André. **Startup de brasileiro chega ao país e converte dado pessoal em dinheiro**. Folha de São Paulo: 2022. Disponível em: https://www1.folha.uol.com.br/colunas/painelsa/2022/11/startup-de-brasileiro-chega-ao-pais-e-converte-dado-pessoalemdinheiro.shtml?utm_source=whatsapp&utm_medium=social&utm_campaign=compwa. Acesso em: 9 dez. 2022

VENTURI, Thais Goveia Pascoaloto. **A proteção contra a violação dos direitos e a tutela inibitória material**. São Paulo: Malheiros, 2014.

VENTURI, Thais goveia pascoaloto. **Responsabilidade civil preventiva**: a proteção contra a violação dos direitos e a tutela inibitória material. Malheiros, 2014

VIANNA, Marcelo. **Um novo 1984?** O projeto RENAPE e as discussões tecnopoliticas no campo da informática brasileira durante os governos militares na década de 1970. 2014. Disponível em: http://revistase-letronicas.pucrs.br/ojs/index.php/oficinadohistoriador/article/view/18998/12057. Acesso em: 10 nov. 2020.

VILARINO, Ramon. **O consumidor na era da pontuação de crédito**. Rio de Janeiro: Forense, 2022.

VOGEL, D. **Trading Up**: Consumer and Environmental Regulation in a Global Economy. Cambridge, MA: Harvard, 1995.

WIDEN, Ron. **Como posso ajudar?** 2022. Disponível em: https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%200f%202019%20Bill%20Text.pdf. Acesso em: 9 dez. 2022

WINEGAR, Angela G.; SUNSTEIN, Cass R. How much is data privacy worth? A preliminary investigation. **Journal of Consumer Policy**, Cham: Springer, v. 42, p. 1-16, 2019.

WIZIACK, Julio. Startup de brasileiro chega ao país e converte dado pessoal em dinheiro. **Folha de São Paulo,** São Paulo, 19 nov. 2022. Disponível em: https://www1.folha.uol.com.br/colunas/painelsa/2022/11/startup-de-brasileiro-chega-ao-pais-e-converte-dado-pessoal-em-dinheiro.shtml&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 30 nov. 2022.

WYDEN. **Como posso ajuda-lo.** 2022. Disponível em: https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bil l%20Text.pdf. Acesso em: 2 set. 2022.

ZALNIERIUTE, Monika; MOSES, Lyria Bennett; WILLIAMS, George. The rule of law and automation of government decision-making. **Modern Law Review,** [s.l.], v. 82, n. 3, p. 1-27, 2019. Disponível em: http://www5.austlii.edu.au/au/journals/UNSWLRS/2019/14.pdf. Acesso em: 03 nov. 2022.

ZALNIERIUTE; Monika; MOSES, Lyria Bennett; WILLIAMS, George. The rule of law and automation of government decision-making. **Modern Law Review**. 2019. Disponível em: http://www5.austlii.edu.au/au/journals/UNSWLRS/2019/14.pdf. Acesso em: 9 dez. 2022

ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. **Revista dos Tribunais**, São Paulo, n.1009, supl. Caderno especial, p. 183-198, nov. 2019.

ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor**. Coletânea do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2019.

ZANATTA, Rafael. **Perfilização, Discriminação e Direitos**: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Researchgate, 2019. Disponível em: https://www.researchgate.net/profile/Rafael-Zanatta/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defe sa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/links/5c7078f8a6fdcc4715941ed7/Perfilizacao-Discriminacao-e-Direitos-do-Codigo-de-Defesa-do-Consumidor-a-Lei- Geral-de-Protecao-de-Dados-Pessoais.pdf). Acesso em: 09 abr. 2022.

ZARSKY, Tal. Unidertanding discrimination in the scored society. **Washington law review**.v. 89, n. 4, 2014. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol89/iss4/10 . Acesso em: 09 abr. 2022.