UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

CACYONE GOMES BARBOSA GONÇALVES LAVAREDA

# DIREITO À PROTEÇÃO DE DADOS PESSOAIS E DIREITOS DA PERSONALIDADE: UM ESTUDO A PARTIR DO DANO CAUSADO PELA PERFILIZAÇÃO

Recife
2023

CACYONE GOMES BARBOSA GONÇALVES LAVAREDA

# DIREITO À PROTEÇÃO DE DADOS PESSOAIS E DIREITOS DA PERSONALIDADE: UM ESTUDO A PARTIR DO DANO CAUSADO PELA PERFILIZAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestra em Direito. Área de concentração: Transformações do Direito Privado.Orientadora: Fabíola Lôbo.

Orientadora: Profa. Dra. Fabíola Albuquerque Lobo.

Recife

2023

Catalogação na fonte
Bibliotecária Karollyne Ferreira Dantas, CRB-4/2319

L396d Lavareda, Cacyone Gomes Barbosa Gonçalves.
Direito à Proteção de Dados Pessoais e Direitos da Personalidade: um estudo a partir do dano causado pela perfilização / Cacyone Gomes Barbosa Gonçalves Lavareda. -- Recife, 2023.
171 f.

Orientador: Prof. Dra. Fabíola Albuquerque Lobo.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, 2023.

Inclui referências.

1. Responsabilidade Civil - Brasil. 2. Proteção de Dados - Brasil. 3. Direito à privacidade. 4. Direitos da personalidade. I. Lobo, Fabíola Albuquerque (Orientadora). II. Título.

346.81 CDD (22. ed.) UFPE (BSCCJ 2024-23)

CACYONE GOMES BARBOSA GONÇALVES LAVAREDA

# DIREITO À PROTEÇÃO DE DADOS PESSOAIS E DIREITOS DA PERSONALIDADE: UM ESTUDO A PARTIR DO DANO CAUSADO PELA PERFILIZAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestra em Direito. Área de concentração: Transformações do Direito Privado.

Aprovado em: 31/08/2023.

**BANCA EXAMINADORA**

_____

Profa. Dra. Fabiola Albuquerque Lobo (Orientadora)
Universidade Federal de Pernambuco – UFPE

_____

Prof. Dr. Silvio Romero Beltrão (Examinador Interno)
Universidade Federal de Pernambuco – UFPE

_____

Prof. Dr. Ivanildo de Figueiredo Andrade de Oliveira Filho (Examinador Interno)
Universidade Federal de Pernambuco – UFPE

_____

Profa. Dra. Maria Antonieta Lynch de Moraes (Examinadora Externa)
Universidade Federal de Pernambuco – UFPE

Aos meus avós, Francisco e Juraci, às minhas filhas Maria Luísa e Maria Eduarda, ao meu marido Antonio Lavareda. Meus amores.

## AGRADECIMENTOS

Por chegar até aqui com perseverança e a graça de Deus, depois de superada uma pandemia e todo contexto da impossibilidade de um ensino presencial que ela causou. Foram tempos difíceis para a produção acadêmica. Os atos de estudar e escrever muitas vezes foram interrompidos para refletir sobre a dor da perda de amigos e parentes que se foram durante os dois anos de mestrado "pandêmico". A dissertação mais que do que nunca vem com a certeza de superação pessoal e da vitória da ciência.

Preciso agradecer às minhas amadas filhas Maria Eduarda e Maria Luísa as quais tento diariamente ensinar através do exemplo para que percebam que a educação pode transformar vidas, melhorar o mundo e curar dores da alma.

Ao meu marido Antonio Lavareda, mentor, amor vida, amigo e o maior incentivador que eu poderia ter.

À minha orientadora Fabiola Lôbo, tão sábia, disponível, humana, facilitadora, compreensiva, doce. Grande educadora como a gente lê em Paulo Freire.

Ao querido Ivanildo Figueiredo meu primeiro orientador desta dissertação e que tão generosamente se dispôs a tecer avaliações preciosas na banca de qualificação e pelos ensinamentos durante as aulas do mestrado. Não esquecerei.

E por falar em banca, tenho enorme gratidão ao professor Silvio Romero pelas exigências e contribuições que foram tão almejadas por esta mestranda. Eu sabia quão valiosa e singular seria sua participação neste trabalho pela sumidade que é, sobretudo quando se trata de direitos da personalidade. Obrigada pelas conversas, aos livros emprestados e as correções.

Ao admirado professor Venceslau pela consideração que não é de hoje, pelos ensinamentos, pela didática em repassar os conhecimentos e por ser um homem de fé. Isso faz diferença na docência.

Aos professores Alexandre Pimentel, Roberto Paulino e Antonieta Lynch pela generosidade, consideração e disponibilidade de conhecimentos.

Obrigada ainda à Carminha. Ou como sempre falamos por mensagem uma com a outra: gratidão! Seu carisma e prontidão mesmo sem nos conhecermos pessoalmente em meio à pandemia tocaram meu coração.

Gratidão por vitórias. Como a de um segundo mestrado concluído no IDP (Instituto Brasileiro de Ensino, desenvolvimento e Pesquisa), em Brasília, concomitante a este na faculdade de direito do recife - UFPE, do qual muito me orgulho. Pois estudar numa Universidade Federal é o sonho de muitos.

Quero homenagear (*in memoriam*), com muito carinho e orgulho por ter sido sua aluna e amiga, o professor Danilo Doneda. Eu tenho certeza de que onde quer que eu vá levarei uma parte do seu legado como o pai da proteção de dados pessoais no Brasil.

E apesar de atravessar os mestrados em período pandêmico sigo com a mesma perseverança e gratidão, por chegar ao final do meu segundo mestrado com a graça de estar caminhando, em nome do Pai celestial, na preparação para o doutorado. Pois como dizia dom Hélder Câmara, não, não pare, o importante é manter o ritmo, embora caindo aos pedaços, continuar na caminhada certa, pois graça das graças é não desistir nunca.

“Agora dispomos da tecnologia, com a qual podemos agir à distâncias tão enormes que não podem ser abarcadas por nossa imaginação ética, ainda confinada, como o tem sido por séculos, ao curto espaço do que está “à vista” e ao “alcance”” (Bauman, 2008, p. 60-61).

## RESUMO

O tratamento de dados pessoais é um dos temas mais estudados na atualidade. O motivo é a dependência da sua utilização por parte da atual economia tecnológica e globalizada, movida a dados pessoais, também chamada de "*data driven*". Os dados pessoais são hoje a projeção da personalidade dos indivíduos no ambiente virtual. O uso de técnicas de tratamento automatizado de dados pessoais para avaliar e prever comportamentos humanos vem ganhando cada vez mais escala, dada aí a preocupação refletida na literatura identifica ameaças à preservação da autonomia humana quando sujeitos são afetados por elas. Nessa linha, busca-se entender como a perfilização, representa ameaças aos direitos da personalidade, ao incorporar premissas que tornam obsoleto o agir humano e que impedem o processo de subjetivação em situações de tomada de decisão automatizada. A partir de então o objeto desse estudo é a crescente utilização da tecnologia 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, dano à direitos da personalidade, tomando como exemplo a natureza do *credit score* e sua relação com a inteligência artificial através da perfilização, sob o olhar do Código Civil e da 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 econômicos e discriminatórios na atual sociedade tecnológica resultando em danos à personalidade. A metodologia é pautada na concatenação entre pesquisa bibliográfica e documental, análise jurisprudencial e cotejamento entre as legislações nacional e estrangeira para investigar os danos e a consequente responsabilidade civil. Dessa forma, harmonizando os demais ordenamentos legais do microssistema da proteção de dados pessoais e com a Constituição Federal, por uma análise sistemática, buscou-se entender o tipo de responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor. Destaca-se a necessidade de mais transparência das decisões baseadas em dados e com ênfase no direito à explicação e de explicabilidade aos titulares de dados pessoais. Assim foram analisadas as disposições da Lei Geral de Proteção de Dados para identificar a sua dimensão de proteção e a centralidade dos interesses dos titulares, em oposição a identificabilidade como elemento normativo central, como também os pilares que regulam o *profiling* no ordenamento jurídico brasileiro. Ao final ainda pode- se constatar paralelamente, três deveres obrigacionais para agentes de tratamento que desejem se utilizar de técnicas de *profiling*: uma proteção substantiva a partir do devido processo informacional e o direito a

inferências razoáveis não discriminatórias como forma de buscar regular os resultados gerados pela perfilização.

**Palavras-chave:** *Profiling*; Direitos da personalidade; Proteção de Dados; Autodeterminação informativa; Responsabilidade civil.

**ABSTRACT**

The processing of personal data is one of the most studied topics today. The reason is the dependence of its use on the part of the current technological and globalized economy, driven by personal data, also called “data driving”. Personal data is today the projection of the personality of individuals in the virtual environment. The use of techniques for automated processing of personal data to assess and predict human behavior is gaining more and more scale, given the concern reflected in the literature to identify threats to the preservation of human autonomy when subjects are affected by them. In this line, we seek to understand how *profiling* represents threats to personality rights, by incorporating assumptions that make human action obsolete and that impede the process of subjectivation in situations of automated decision-making. From then on, the object of this study is the increasing use of technology for the processing of personal data in order to achieve maximum efficiency in processes in different areas. The main objective of this work is to examine, in the light of law, damage to personality rights, taking as an example the nature of the *credit score* and its relationship with artificial intelligence through *profiling*, from the perspective of the civil code and the General Law of Protection of Personal Data for delineating the civil liability of actors who process traditional and alternative personal data to compose a *credit* note and use it for economic and discriminatory purposes in today's technological society resulting in damage to the personality. The methodology is based on the concatenation of bibliographical and documentary research, jurisprudential analysis and comparison between national and foreign legislation to investigate the damages and consequent civil liability in sharing personal data of individuals with deviation of purpose resulting in damage to personality rights. 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. It highlights 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 transparency and with an emphasis on the right to explanation and explainability to the holders of personal data. Thus, the provisions of the General Data Protection Law were analyzed to identify their protection dimension and the centrality of the interests of the holders, as opposed to identifiability as a central normative element, as well as the pillars that regulate *profiling* in the Brazilian legal system. At the end, it can still be seen, in parallel, three obligatory duties for

treatment agents who wish to use *profiling* techniques: a substantive protection based on due informational process and the right to reasonable non-discriminatory inferences as a way of seeking to regulate the results generated by *profiling*.

**Keywords:** *Profiling*; Personality rights; Data Protection; Informative self-determination; Civil responsibility.

## LISTA DE ILUSTRAÇÕES

Figura 1 - The context & challenges ..... 50
Figura 2 - Overview: privacy and data protection instruments in Europe ..... 51
Figura 3 - Mapa de modelo que resultou em Discriminação algorítmica no Brasil..... 106
Figura 4 - Uma captura de tela do PI de solicitação de acesso do titular dos dados ..... 111

## LISTA DE TABELAS

Tabela 1 - Entenda o Marco Legal de Proteção de Dados ..... 68
Tabela 2 - Comparativo entre os textos que deram origem a LGPD 1 ..... 127
Tabela 3 - Comparativo entre os textos que deram origem a LGPD 2 ..... 128

**SUMÁRIO**


**1 INTRODUÇÃO ..... 15**
**2 DIREITOS DA PERSONALIDADE NO ORDENAMENTO BRASILEIRO ..... 18**
**2.1 Direitos da personalidade ..... 18**
**2.2 Características dos direitos da personalidade ..... 22**
**2.3 Personalidade e riscos atuais ..... 24**
**2.4 A diferença entre direito fundamental e direitos da personalidade ..... 28**
**2.5 Como reconhecer um novo direito de personalidade ..... 39**
**3 O CONTEXTO DO SURGIMENTO DO DIREITO À PROTEÇÃO DE DADOS NA EUROPA E NO ORDENAMENTO JURÍDICO BRASILEIRO ..... 44**
**3.1 Da origem do direito à proteção de dados pessoais no contexto europeu (GDPR) e o reconhecimento como direito fundamental ..... 44**
**3.2 O contexto brasileiro da Lei Geral de Proteção de Dados Pessoais ..... 57**
**3.3 Princípios da Lei Geral de Proteção de Dados Pessoais ..... 79**
**3.4 Arcabouço normativo harmônico à proteção de dados pessoais como direito da personalidade ..... 82**
**4 A PROTEÇÃO DE DADOS PESSOAIS E A PERFILIZAÇÃO ..... 95**
**4.1 A perfilização e a repercussão nos direitos da personalidade ..... 95**
**4.2 O perfil de crédito e o dano ao direito da personalidade de proteção de dados pessoais ..... 100**
**4.3 A regulação e a proteção de dados pessoais ..... 115**
**5 A RESPONSABILIDADE CIVIL PELO DANO AO DIREITO DE PERSONALIDADE DE PROTEÇÃO DE DADOS PESSOAIS ..... 119**
**5.1 A responsabilidade civil no Código Civil ..... 119**
**5.2 A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais ..... 125**
5.2.1 Responsabilidade Civil subjetiva ou objetiva ..... 126
5.2.2 Responsabilidade civil dos agentes de tratamento ..... 138
**5.3 A responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do score para fins discriminatórios ao consumidor ..... 139**
**6 CONSIDERAÇÕES FINAIS ..... 153**
**REFERÊNCIAS ..... 156**

# 1 INTRODUÇÃO

No cenário digital, o advento da tutela dos dados pessoais no ordenamento jurídico pátrio, através da Lei Geral de Proteção de Dados, representa grande avanço. Sem prejuízo de sua importância para a evolução tecnológica, social e econômica, o mau uso dos dados pessoais na formação de perfis pode estimular discriminações, causando danos ao livre desenvolvimento da personalidade - mesmo assegurada a autodeterminação informativa - ferindo garantias civis e constitucionais, especialmente quando dados são manejados pelo poder público e privado.

O domínio e uso massivo dos dados intensifica a vigilância do indivíduo numa amplitude e profundidade como nunca vista operada pelo capitalismo. Nesse sentido, há a consequente formação de perfis individuais, fragilizando e causando danos a direitos da personalidade como a discriminação, dano à privacidade e, inescapavelmente à dignidade da pessoa humana. Tais danos devem ser prevenidos e reparados socorrendo-se do ordenamento jurídico, a exemplo do Código Civil com a responsabilização civil.

A datificação da vida humana é perceptível e a Lei Geral de Proteção de Dados (LGPD) consagrou a expressão genérica “tratamento de dados” para se referir às diversas operações, como coleta, produção, armazenagem, avaliação, transferência, que envolvem dados pessoais, e são inerentes à grande maioria das atividades desempenhadas socialmente. A criação da LGPD se deu ante à necessidade de inovação do ordenamento jurídico para acompanhar as transformações sociais, visando efetivar proteção aos titulares desses dados pessoais, mas sem restringir o desenvolvimento socioeconômico que hoje possui os dados pessoais como referencial.

A partir desse cenário, a presente pesquisa tem como norte a seguinte questão: O que existe hoje no ordenamento jurídico brasileiro é capaz e suficiente para reparar danos ao direito de personalidade?

O objetivo principal é apontar o reconhecimento de um novo direito da personalidade, qual seja, o direito à proteção de dados pessoais. Este já entendido e positivado como um direito fundamental autônomo, distinto do direito à privacidade. E como direito fundamental, ele irradia por todo o ordenamento jurídico, numa visão civil- constitucional, materializando com sua tutela específica. No caso em tela, com o intuito de buscar a sua devida reparação em situações de dano através da funcionalização da responsabilização civil. Para alcançar tal objetivo, buscar-se-á, observar, verificar, os danos causados pela perfilização, já que o ser humano se tornou objeto do extrativismo de dados pessoais, buscando sua eficaz reparação.

Os objetivos específicos deste trabalho são: explicitar a natureza, as características e a diferença entre os direitos da personalidade e os fundamentais; correlacionar os direitos da personalidade na Lei Geral de Proteção de Dados brasileira, contextualizando com o Regulamento Geral de Proteção de Dados Europeu, posto que este é um diploma de referência mundial para o tema, não deixando de lado todo o arcabouço normativo brasileiro harmônico à Lei Geral de Proteção de Dados; analisar danos causados aos direitos da personalidade, considerando a proteção de dados como um direito da personalidade este direito que existe no código civil numa interpretação constitucional sistemática em consonância; por fim, determinar qual a responsabilidade civil é cabível pelo dano causado a direito de personalidade de proteção de dados pessoais.

A relevância da pesquisa, além do próprio cenário apresentado, se dá em razão da expressiva influência e utilização dos dados pessoais para fins econômicos, sendo inegável que os cidadãos são vulneráveis diante dos riscos e danos imprevisíveis com o avanço que a tecnologia e inovação podem gerar para a sociedade, seja aos indivíduos e à própria coletividade.

A proteção de dados pessoais do ponto de vista constitucional é um direito fundamental autônomo, assegurado pelo artigo 5º, inciso LXXIX da Constituição. Nesse sentido, é garantido o direito à proteção dos dados pessoais, incluindo os meios digitais, independentemente da privacidade. Esse entendimento supera a visão anterior do STF, que limitava a proteção constitucional ao sigilo das comunicações (com base no artigo 5º, inciso XII da Constituição), considerando a privacidade como uma garantia individual de abstenção do Estado na esfera privada individual (RE 418.416, Tribunal Pleno, julg. em 10/5/2006, public. em 19/12/2006 no DJU).

Insta frisar que foi superado antigo paradigma do próprio STF com o reconhecimento do direito à proteção de dados como um novo direito fundamental, destacado e autônomo em relação ao direito à privacidade, com a identificação de uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade.

A afirmação da autonomia do direito fundamental à proteção de dados deriva do direito fundamental à dignidade da pessoa humana; da proteção constitucional à intimidade (artigo 5º, inciso X, da CF/88) diante do aumento de novos riscos derivados do avanço tecnológico; e do reconhecimento do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa.

E a proteção de dados pessoais lastreada na dignidade da pessoa humana é nascedouro de um novo direito de personalidade.

Dessa forma, em um primeiro momento, conceitua-se o direito de personalidade, a formação do seu rol, a sua natureza jurídica e como se adquire status de direito da personalidade, ou seja, como nasce um novo direito desta espécie. A partir daí contextualiza-se a sociedade da informação e o alcance jurídico trazido pela Lei Geral de Proteção de Dados, asseverando a proeminência da autodeterminação informativa frente às decisões automatizadas como as baseadas na formação de perfis. Em seguida, adentra-se ao debate acerca do caráter fundamental conferido à tutela dos dados pessoais. Após, a pesquisa se dedica à análise de algumas nuances da aplicação da lei ao tratamento de dados pelo poder econômico. Por fim, reflete sobre o aumento do monitoramento dos cidadãos e os danos reflexos aos direitos da personalidade causado a partir da formação de perfis pessoais e se há resposta para essa reparação no ordenamento brasileiro.

Para o desenvolvimento da pesquisa será utilizada a metodologia hipotético-dedutiva. Além disso, o trabalho se utilizará do tipo de pesquisa bibliográfico, por consultar documentos jurídicos e legais, bem como a análise literária na área jurídica e da tecnologia da informação através de autores como Danilo Doneda, Laura Schertel Mendes e Nelson Rosenvald, Paulo Lôbo, Sílvio Romero.

# 2 DIREITOS DA PERSONALIDADE NO ORDENAMENTO BRASILEIRO

Embora haja historicamente uma margem plástica, expansiva sobre os direitos da personalidade, como projeção da personalidade de alguém, é preciso saber o quê, qual aspecto da personalidade se pretende defender. Ou seja, no caso em estudo, é importante diferenciar à luz do Código Civil de 2002 e da Doutrina, o que é a personalidade, o que é um direito de personalidade, como ele surge e é reconhecido.

De onde vem o rol, como um novo direito de personalidade pode ser reconhecido e a partir do quê. E esse novo direito precisaria ser positivado, tipificado, para a partir de então, ser reconhecido? E sendo reconhecido, como deve ser tutelado e a sua consequente responsabilização civil? É o que se pretende demonstrar nesse é que o direito à proteção de dados pessoais é um direito personalíssimo devendo ser tutelado pelo Código Civil a partir de um mandamento constitucional implícito que irradia sua essência da dignidade da pessoa humana e tem força extraída da liberdade, da vida privada, habeas data, e, apesar da relação, não se confunde com a autodeterminação informativa (Oliveira, 1977, p. 68).

## 2.1 Direitos da personalidade

Mais complexo do que definir personalidade é a tentativa de definir os direitos decorrentes dessa, posto que o que lhe dá origem não reside num conceito fechado como já demonstrado. Mas, o sentido jurídico de personalidade é ligado à ideia de pessoa, do latim persona.

Pessoa é o bem supremo da ordem jurídica, o seu fundamento e seu fim, tendo o Estado seu sentido de existir em função das pessoas e não o contrário (Beltrão, 2014). A origem dos direitos da personalidade faz-se desnecessária diante da numerosa bibliografia sobre o tema, porém é de fundamental importância seu registro pontual no trabalho para que se possa reafirmar a complexidade de sua conceituação, características e teorização ao longo da história. E como o direito está em constante mudança e expansão como será demonstrado, sua origem servirá aqui, apenas, de ponto de partida, embora não se tenha a pretensão de aqui traçar a sua evolução histórica em detalhes.

Os direitos da personalidade surgem a partir de uma interpretação dos direitos pessoais absolutos de liberdade, segurança e propriedade na Legislação criminal que até então os protegia.

Assim se introduzia por Teixeira de Freitas o conceito de direito da personalidade.

> A enumeração de taes direitos é feita ao arbítrio de cada Escriptôr, sem que haja nisso inconveniente. Em ultima analyse reduzem-se aos direitos de personalidade e de propriedade, ou antes aos de personalidade sómente. O direito de propriedade é uma realização do direito de personalidade relativamente a objetos exteriores, de que o homem tem necessidade para sua existencia e desenvolvimento. Antes dessa realização existe a simples faculdade - liberdade - de unir á personalidade os obiectos exteriores. Ainda não ha direito de propriedade. O direito de propriedade começa no momento, em que a união se verifica. Chamados direitos absolutos- liberdade, segurança e propriedade -, entrão na compreensão da Legislação Criminal, que os protege e assegura a sua penalidade. Desses direitos o de propriedade unicamente entra na Legislação Civil. É no direito de propriedade que havemos de achar os direitos reais (Freitas, 1915).

Mas apenas o direito de propriedade entrou na Legislação Civil à época (1876) e por terem sido violados os direitos pessoais (se violados) dando lugar a ações de perdas e danos (Gonçalves, 2022, p. 64).

Os direitos pessoais são aqueles que constituem o sujeito numa pretensão relativamente a alguém, por oposição às pretensões relativas a coisas (Freitas, 1915).

E apesar de autores como Espíndola e Clóvis Beviláquia, do Tratado de Direito Privado de Pontes de Miranda, até a década de 1950, as obras de direito civil com as referências aos direitos da personalidade são praticamente inexistentes. Pois, só no projeto do Código Civil de 1963, é que os direitos de personalidade surgem e com uma cláusula geral de tutela, proposta por Orlando Gomes, rezava que:

> Art. 29.º Direitos da Personalidade - O direito à vida, à liberdade e à honra, e outros reconhecidos à pessoa humana são inalienáveis e intransmissíveis, não podendo seu exercício sofrer limitação voluntária.
> Parágrafo único. Quem for atingido ilicitamente em sua personalidade pode exigir que o atentado cesse e reclamar perdas e danos, sem prejuízo de sanções de outra natureza a que fique sujeito o ofensor (Gonçalves, 2022, p. 63-71).

A ofensa à personalidade da esfera penal passou a ser um ilícito civil e sua tutela ampla e aberta. Seu rol de bens exemplificativo (vida, liberdade e honra) e alguns direitos especiais como direito à integridade física, à imagem e ao nome (Gonçalves, 2022, p. 71).

Assim, como não há valor que supere o valor da pessoa humana (Santos, 1999, p. 93) e o direito da personalidade nele se fundamenta como projeções físicas ou psíquicas da pessoa, ou suas características mais importantes. Eles protegem a essência da pessoa (Borges, 2005, p. 20). Sendo direitos próprios, autênticos, com traços irrepetíveis, exclusivos, daí derivando suas

características que os colocam como direitos, por sua natureza, originários, vitalícios, imprescritíveis e absolutos, inerentes à própria pessoa, e, à princípio, indisponíveis.

"Direitos da personalidade dizem-se as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim da sua projeção essencial no mundo exterior" (França, 1996. p. 1033).

Numa das definições, os direitos da personalidade podem ser categoria especial de direitos subjetivos que, fundada na dignidade da pessoa humana, garante o gozo e o respeito ao seu próprio ser, em todas as suas manifestações espirituais ou físicas (Beltrão, 2014, p. 12). Corroborando em mais uma conceituação que reforça o caráter amplo e protetivo dos direitos da personalidade:

> A dignidade da pessoa humana implica que a cada homem sejam atribuídos direitos, por ela justificados e impostos, que assegurem esta dignidade na vida social. Esses direitos devem representar um mínimo, que crie o espaço no qual cada homem poderá desenvolver a sua personalidade. Mas devem representar também um máximo, pela intensidade da tutela que recebem. Assim se funda a categoria dos direitos da personalidade. Mais diretamente que qualquer outro instituto jurídico, implica a projeção de pressupostos fundantes [...] (Ascensão, 1997, p. 64).

O direito de personalidade da origem, até o rol positivado no código civil de 2002, percorreu uma longa trajetória. Como marco legal para o surgimento do direito da personalidade, no Código Civil, temos a previsão de que todas as pessoas são capazes de direitos e deveres na ordem civil (art. 1º), seguido do 2º artigo que aponta um marco inicial da personalidade civil: "A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde concepção, os direitos do nascituro" (Brasil, 2002). Nesse contexto, é importante ressaltar que os direitos da personalidade são direitos essenciais à dignidade (Brasil, 2002). Entende-se que os direitos da personalidade são direitos essenciais à dignidade e à integridade e, independem da capacidade civil da pessoa. Por isso, como já dito, protegem tudo o que lhe é próprio: honra, vida, liberdade, privacidade, intimidade, entre outros.

O tema é abordado de forma mais específica e especial*, mas ainda não exaustiva,* no Código Civil brasileiro, nos artigos 11 ao 20. Dentre os tópicos abordados no Código Civil, tem-se a proteção à integridade do corpo da pessoa, da imagem, da inviolabilidade da vida privada, a proibição da divulgação de escritos, da transmissão da palavra ou a publicação, exposição e utilização da imagem da pessoa. Esse rol vem no que mais se assemelha ao tipificado no Código Civil de 1975. O regime dos direitos de personalidade previsto no Projeto

de Código Civil (1975) conheceu força de lei e corresponde, sem modificação substancial, ao atual regime do Código Civil brasileiro como se ilustra (Gonçalves, 2022, p. 75).

A consagração dos direitos de personalidade mantém-se como um desiderato irrenunciável no Projeto de Código Civil (1975):

> (...) cabe dar realce à disciplina dos chamados direitos de personalidade. Os projectos anteriores já haviam dado atenção a esta matéria, pensamos ter fixado, em alguns artigos fundamentais, as regras indispensáveis à tutela dos valores da subjetividade, a começar pelos concernentes ao direito sobre o próprio corpo, para fins de transplante, ou mesmo para pesquisas científicas. O problema da tutela da imagem e da intimidade, bem como do uso do nome da pessoa, são aspectos que a nova Codificação teve em vista reger, pondo o valor da pessoa no fulcro do ordenamento jurídico (Reale, 1978 *apud* Gonçalves, 2022).

Moreira Alves coube, a elaboração da Parte Geral do Projeto de Código Civil (1975), cujo articulado (tal como publicado a 13-jun.-1975, no Diário do Congresso Nacional):

> Capítulo II - Dos Direitos da Personalidade
> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
> Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.
> Parágrafo único. Em se tratando de morto, terá legitimação para requerê-la o cônjuge sobrevivente, ou qualquer parente da linha reta, ou da colateral até o quarto grau.
> Art. 13. Salvo exigência médica, os atos de disposição do próprio corpo são defesos quando importarem diminuição permanente da integridade física, ou contrariarem os bons costumes.
> Parágrafo único. Admitir-se-ão, porém, tais atos para fins de transplante, na forma estabelecida em lei especial.
> Art. 14. É válida, com objetivo científico, ou altruístico, a disposição gratuita do próprio corpo, no todo ou em parte, para depois da morte.
> Parágrafo único. O ato de disposição pode ser livremente revogado a qualquer tempo.
> Art. 15. Ninguém pode ser constrangido a submeter-se, com risco de vida, a tratamento médico ou a intervenção cirúrgica.
> Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o nome patronímico.
> Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.
> Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.
> Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Redação sugerida por COUTO E SILVA, como nota JOSE CARLOS MOREIRA ALVES, A Parte Geral do Projecto de Código Civil Brasileiro - Subsídios Históricos para o Novo Código Civil Brasileiro, 2.1 ed.,2003, 67 (Gonçalves, 2022, p. 73).

Mesmo dada a semelhança ao de 1975, o Código Civil 2002 trouxe a modificação axiológica da codificação brasileira, que deixou de ter um perfil essencialmente patrimonial, característico do código civil de 1916, concebido para uma sociedade agrária, tradicionalista e conservadora, para se preocupar substancialmente com o indivíduo, em perfeita sintonia com o espírito da Constituição Cidadã de 1988 (Gagliano, 2019. p. 211).

## 2.2 Características dos direitos da personalidade

Diante da premissa de que os direitos da personalidade não se restringem a um rol taxativo, mas exemplificativo, é interessante e importante entender suas características para auxiliar na pesquisa.

Direitos da personalidade preservam a individualidade de cada pessoa. São direitos não patrimoniais inerentes à pessoa, compreendidos no núcleo essencial de sua dignidade. Eles concretizam a dignidade da pessoa humana no âmbito civil (Lobo, p 137).

Eles são classificados pela doutrina de várias formas, e no dizer de José de Oliveira Ascensão, são muitos e, por isso, precisam ser sistematizados, e seus critérios de classificação são inúmeros e relativos (Ascensão, 1998, p. 96-97). E a classificação de tais bens serve ao direito e se constrói levando em consideração a capacidade dos bens de atender às necessidades humanas e coletivas (Perlingieri, 2022, p. 236).

De acordo com Hubmann, sua classificação compreende os direitos à personalidade, os direitos à individualidade em três esferas – individual, privada e secreta- e a dos Direitos ao desenvolvimento da personalidade. Tendo a personalidade como um evento dinâmico, não acabado, ao qual esse trabalho se filia (Hubmann, 1967. p. 21-39).

A forma como o indivíduo se expressa, suas principais características e como ele constrói o seu pensamento, são elementos que ajudam a definir a personalidade, a sua forma de se expressar no mundo. Assim, pode-se concluir que cada indivíduo tem a sua personalidade e características que o diferenciam dos demais.

E a essas características protegidas pelo reconhecimento dos direitos da personalidade como direitos civis que preservam a individualidade, resguardam a dignidade humana durante toda a vida e são valores, algo que não se pode abrir mão por ser um imperativo axiológico de toda a ordem jurídica (Universidade de Coimbra, 1999, p. 151).

Em consonância, as características dos direitos da personalidade são inatas ou originárias, posto que são adquiridos ao nascer independente da vontade; como vitalícios: perduram a vida toda e alguns se refletem mesmo após a morte; como imprescritíveis: perduram enquanto durar a vida e, em alguns casos, são protegidos após o falecimento; como inalienáveis: são relativamente indisponíveis, porque não possuem valor econômico imediato, exceto se houver violação desse direito, quando nascerá uma indenização como forma de compensação do direito violado e; como absolutos: podem ser opostos *erga omnes* (Brasil, 2002).

Nesse contexto, o Código Civil em seu art. 11 apresenta que estes são direitos: Intransmissíveis: não se transmite a outra pessoa, cabendo apenas àquela; Irrenunciáveis: continuam com o indivíduo; não podem sofrer limitação voluntária (Brasil, 2002).

Segundo Beltrán de Heredia pode-se classificar tais direitos em três grupos.

1º - São inatos ou originários. Quer-se significar que tais direitos pertencem ao homem pelo simples fato de ser homem, por razão de nascimento, sem que para adquiri-los seja necessário um modo ou título legal de aquisição. Não são concedidos pelo Estado, mas nascem com a pessoa e aquele se limita a reconhecê-los.

2º - São direitos muito pessoais. São direitos individuais, privados e absolutos. Individuais, porque só são próprios da pessoa física, do indivíduo. Não, das pessoas morais ou jurídicas. Voltaremos a este ponto na pergunta seguinte. Privados, porque, como já sabemos, pertencem ao indivíduo como tal, independentemente de outras qualidades jurídicas que possa ostentar, como as de cidadão ou administrado. Além disso, porque o seu disciplinamento jurídico é feito de acordo com os critérios e princípios do Direito Privado. Absolutos, porque são eficazes em relação a todos. Eles são dotados de eficácia *erga omnes*, como os direitos reais. Em relação a eles, existe um dever universal ou geral de respeito.

3º - Eles são extrapatrimoniais. Eles estão fora do comércio. Não podem ser objeto de tráfico jurídico, como não pode ser a pessoa, da qual derivam esta nota característica: todo o tratamento jurídico privilegiado ou de especial amparo que recebem estes direitos justifica-se, precisamente, por razão da dignidade da pessoa, em homenagem da qual se reconhecem. A extra patrimonialidade argumenta: Eles são irrenunciáveis pelo seu titular. Pelo menos, é assim que a doutrina é expressa. Não renuncia à vida a mãe que, em algum suposto extremo e felizmente já quase inexistente, oferece a sua vida por a dar ao nascituro? Ou o bombeiro, por

salvar um semelhante? Não há renúncia no doador de um órgão destinado a um transplante? O que, na verdade, se quer dizer não é tanto que o titular não possa renunciar, mas que a sua renúncia carece de eficácia jurídica em relação a terceiros. Ninguém pode fazer valer supostas reivindicações ou efeitos jurídicos com base numa renúncia prévia de qualquer um destes direitos por parte do seu titular. Simplesmente, porque, apesar de ter renunciado, o titular, a qualquer momento, pode voltar do seu acordo ou revogar a sua renúncia. Depende exclusivamente da sua vontade a consumação da renúncia: pode lê-la até ao fim, como nos exemplos apresentados, mas ninguém pode exigi-la juridicamente. Da mesma forma, são indisponíveis: não podem ser objeto de negócio jurídico de disposição. Não podem ser vendidos, cedidos, transmitidos ou doados. Mas a lei parece aceitar, pelo menos parcialmente, certas faculdades dispositivas sobre aqueles direitos. Finalmente, a última consequência que deriva da extrapatrimonialidade é que são imprescritíveis: não podem ser extintos por prescrição, isto é, pelo não uso prolongado no tempo. Acabam apenas com a morte do seu titular (Pueche, 2008, p. 41-44).

De maneira semelhante, Silvio Romero caracteriza os direitos da personalidade como sendo intransmissíveis, irrenunciáveis e indisponíveis, pessoais e extrapatrimoniais, imprescritíveis, inatos ou adquiridos e absolutos, mas não ilimitados (Beltrão, 2014, p. 13-20).

Não há aqui a pretensão de se estender sobre as características já tão exploradas pela doutrina, mas pontuar que elas seguem importantes, sobretudo para novas discussões que podem surgir sobre limites e finalidades que as colocam à prova diante de novas situações, riscos e danos à personalidade do mundo digital. Pois, como ensina Silvio Romero, a imposição de limites aos direitos da personalidade, diante do complexo normativo do sistema jurídico, em face da dinâmica do próprio direito, demonstra que o seu exercício deve corresponder aos interesses e fins sociais (Beltrão, 2013).

## 2.3 Personalidade e riscos atuais

Essa pergunta vem sendo feita até hoje e sempre será uma indagação constante e instigante da humanidade não só no ramo do direito, mas da psicologia, da sociologia, da medicina, e em tantas outras áreas da ciência dada a sua importância para a compreensão humana, para o seu desenvolvimento, proteção e conservação.

Cabendo aqui inclusive uma busca pela sua designação, origem no dicionário, onde é possível apreender várias e amplas conceituações atualizadas inclusive, acrescentando-se neologismos. Por ser o dicionário um apoio para a ciência no sentido de ter sido criado para

divulgar conhecimento científico, a partir do século XVIII, que fosse acessível para toda a população – Pois essa era a ideia do movimento enciclopedista – cabe aqui uma busca por sua designação, origem da palavra personalidade no dicionário, onde é possível apreender várias e amplas conceituações atualizadas, acrescentando-se neologismos. Assim foi escrita a *"Encyclopédie ou dictionnaire raisonné des sciences, des arts et des métiers"* ou Enciclopédia ou Dicionário Fundamentado nas Ciências, nas Artes e nas Profissões, *"Par une societé de gens de lettres"* ou por uma sociedade de gente letradas (Diderot; Alembert, 1993).

De acordo com o dicionário escolhido – Michaelis –, o conceito de personalidade é amplo, atual, verificável, social, jurídico, científico, mas também não exaustivo.

> 1 Qualidade ou condição de uma pessoa. 2 Tudo aquilo que determina a individualidade de uma pessoa moral, segundo a percepção alheia: Devo dizer que fiquei impressionado: era como se o rapaz estivesse mesmo vivendo a cena. Ao terminar a narrativa, agradeceu-me, magnânimo, por ter oportunizado o recuo no tempo que lhe permitirá encontrar sua verdadeira personalidade. 3 Qualidade essencial e exclusiva de uma pessoa; aquilo que a distingue de todas as outras; caráter, identidade, originalidade. 4 Imagem assumida e projetada publicamente por alguém. 5 Conjunto de atributos e características que diferenciam uma nação, uma comunidade, um grupo de pessoas: "Quando, em fins de abril ou princípios de maio de cada ano, embarcava de volta à capital federal, Tibério Vacariano, ao vestir a sua roupa de linho ou tropical, envergava também a sua 'personalidade carioca'" (EV). 6 Pessoa célebre, afamada; celebridade. 7 Alguma coisa que é o reflexo ou a semelhança de uma personalidade humana distinta. 8 Conjunto de predisposições psíquicas que diferenciam uma pessoa e que estabelecem um padrão de resposta comportamental característica, e de certa forma previsível, que cada pessoa desenvolve como estilo de vida (Michaelis, 2023).

Seguindo a mesma proposta de não taxatividade, na doutrina jurídica, a personalidade também tem inúmeras conceituações. A exemplo, tem-se que a personalidade é a faculdade reconhecida à pessoa, sujeito das relações jurídicas. Assim, pode-se dizer que toda pessoa é dotada de personalidade (Beltrão, 2014, p. 7).

> O conceito de personalidade está umbilicalmente ligado ao de pessoa. Todo aquele que nasce com vida torna-se uma pessoa, ou seja, adquire personalidade. Esta é, portanto, qualidade ou atributo do ser humano. Pode ser definida como aptidão genérica para adquirir direitos e contrair obrigações ou deveres na ordem civil. É pressuposto para a inserção e atuação da pessoa na ordem jurídica (Gonçalves, 2014, p. 107).

De maneira didática e tão claramente definida, o conceito de personalidade está relacionado sobre quem. A indagação que se segue presume a busca de um ser não igual a qualquer outro, único. À pergunta antropológica de base - o que é o Homem? - responde o

conceito de pessoa. Já ao *quis est* - à pergunta sobre quem o Homem é -, responde o conceito de personalidade (Gonçalves, 2022, p. 96).

Na doutrina, e como marco base do estudo ora em comento, considera-se que a personalidade não é exatamente um direito; é um conceito básico sobre o qual se apoiam os direitos e constituem o mínimo necessário da substância da própria personalidade (Venosa, 2003, p. 160).

Nessa linha, só a partir de novas experiências, casos concretos, pode-se conhecer mais sobre o que é personalidade apoiado no pensamento Kantiano (Kant, 1987, p. 273-274), de que fenômenos são a percepção humana do mundo, pois os seres humanos não têm como saber da essência das coisas em si, mas apenas das coisas segundo o raciocínio que permite viver a experiência.

Considera-se também uma visão ética desse conceito, posto que é o que deve importar e guiar a ciência. Por isso, nunca será demais fazê-la como agora, em um momento de transformação da sociedade denominada “de risco”, em que a própria personalidade humana através de suas experiências (Cendon, 2000, p.33) vem sendo explorada em todos os aspectos.

Essa exploração, infelizmente parece não visar a humanidade como um fim em si (mas como meio) como eticamente se deve pretender, mas é organizada para servir a um novo modelo capitalista: o baseado no extrativismo de dados pessoais com o risco de expropriação, despersonalização da própria personalidade e ameaça à autonomia humana com fins entre eles, econômicos, como alerta o professor Nelson Rosenvald, colidindo com o disposto no CC/2002 em seus artigos 11.12 e 927 por exemplo.

> (...) o intitulado "capitalismo de vigilância" não consiste em uma nova tecnologia, mas em uma nova forma de mercado que reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais que são disponibilizados no mercado como produtos de predição que antecipam e modelam comportamentos futuros. A visão kantiana do ser humano como fim em si é desvirtuada por um instrumentalismo, cuja base é a expropriação de nossa personalidade em prol de finalidades alheias, pois a própria sociedade se torna objeto de extração e controle. A realidade digital converte situações existenciais em uma nova propriedade baseada na despossessão da essência daquilo que nos define, através de uma modificação comportamental, cujo legado de danos pode custar a nossa própria humanidade. A edificação do livre-arbítrio proveniente da narrativa liberal provavelmente se desintegrará quando, mesmo em sociedades supostamente livres, depararmo-nos diariamente com instituições, corporações e agências governamentais que compreendem e manipulam o que até então era nosso inacessível reino interior (Rosenvald, 2021).

Os riscos atuais quando se fala em tecnologia, *big techs*, buscadores de conteúdo, sites, aplicativos, redes sociais, são imensuráveis dada a rapidez da inovação, da sede da economia da atenção para coletar uma infinidade de dados pessoais – atomizando o ser humano à partículas mínimas para extrair dele seus dados penetrando na mais íntima esfera de sua vida, para perfilhar, segmentar, alvejar por meio de conteúdo, discriminar, modular comportamentos, e predizer ao ponto de não deixar escolha, tolhendo seu arbítrio, seu livre desenvolvimento. Utilizando-se da experiência humana através da coleta de seus dados pessoais ininterruptamente por meio de cliques, *cookies* (arquivos de texto que rastreiam a navegação do usuário *on*-line), dispositivos móveis conectados à internet e espalhados pela casa, a exemplo da *Alexa*, dos aparelhos de televisão, aparelho celular, outros vestíveis como (relógios inteligentes) e câmeras detectoras de emoções. A chamada inteligência artificial com seus algoritmos está em tudo e evolui exponencialmente como *ChatGPT*, marco da utilização massiva da inteligência artificial generativa. Como percebe Yuval Noah Harari:

> Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso vamos perceber o universo inteiro como um fluxo de dados (Harari, 2019, p. 83).

Tal inteligência artificial possui exponenciais saltos de desenvolvimento utilizando-se de dados, inclusive pessoais, e tem sido na atualidade uma das grandes ameaças à personalidade e aos direitos. Sobre as características dessa 4. Revolução industrial:

> Velocidade: ao contrário das revoluções industriais anteriores, esta evolui em um ritmo exponencial e não linear. Esse é o resultado do mundo multifacetado e profundamente interconectado em que vivemos; além disso, as novas tecnologias geram outras mais novas e cada vez mais qualificadas. - Amplitude e profundidade: ela tem a revolução digital como base e combina várias tecnologias, levando a mudanças de paradigma sem precedentes da economia, dos negócios, da sociedade e dos indivíduos. A revolução não está modificando apenas o "o que" e o "como" fazemos as coisas, mas também "quem" somos. Impacto sistêmico: ela envolve a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda sociedade" (Schwab, 2016, p. 12).

O avanço da tecnologia com o avanço acelerado do *ChatGPT* com a inteligência artificial generativa nos primeiros meses de 2023, e a corrida da indústria da tecnologia para ver quem sai na frente no uso das ferramentas de inteligência artificial, mobilizou numa carta aberta, assinada por mais de 1300 cientistas, empresários de tecnologia e representantes do

meio acadêmico alertando e pedindo que os experimentos com IA sejam pausados diante dos riscos à humanidade.

Para proteger a personalidade nesse contexto mundial, é necessário recorrer aos direitos e às tutelas correspondentes. Pois o século XXI é uma época em que estão em evidência os direitos das pessoas e o cinzelamento de sua dogmática com os novos reptos antropológicos – pela mudança de paradigma civilizacional e os desafios decorrentes da tecnologia que ainda assim, relacionam-se com a tutela da personalidade (Gonçalves, 2022, p.22-23).

Na ótica da filosofia e do direito, chama-se atenção para as consequências repulsivas da moderna vitória da tecnologia sobre a ética.

## 2.4 A diferença entre direito fundamental e direitos da personalidade

É frequente na doutrina o debate sobre a repercussão dos direitos fundamentais nos direitos da personalidade. Quais seriam suas diferenças e conexões. E hoje acrescenta-se: como atender a necessidade do indivíduo de obter a reparação civil de um direito que é fundamental, mas não está tipificado como direito da personalidade no Código Civil?

Antes de qualquer coisa, é preciso entender a diferença entre direito fundamental e direitos da personalidade para buscar a conexão entre eles, para então se socorrer na gênese à proteção pretendida a fim de obter tal reparação civil.

Na Constituição da República Federativa do Brasil, considerada a carta de direitos brasileira, constam no art. 5º regulamentado no capítulo "Dos Direitos e Deveres Individuais e Coletivos" localizado no título "Dos Direitos e Garantias Fundamentais" (Brasil, 1988).

Porém, os direitos fundamentais vêm muito antes da Constituição Brasileira de 1988, sua característica introdutória começa a se estabelecer em 1215 com a Magna Carta Libertatum, doravante Magna Carta (considerada incompleta), e depois com as outras cartas de direitos, como a Petição de Direitos (Petition of Rights), de 1628, à lei de Habeas Corpus (Habeas Corpus Act), de 1679, e, o Bill of Rights (famigerada em meios acadêmicos de direito, a Carta de Direitos) de 1689. As duas últimas revisitam a fim de restringir prisões arbitrárias e sem julgamento prévio perante um juiz competente, ou seja, por inobservância do *due process of* law (Saleme, 2020. p. 8).

Os direitos fundamentais em caso de violação, seria da vítima contra o Estado, e este em dever proteção contra a lesão, que os tutela os consagrando legislativamente (a exemplo do Código Civil), ou através da jurisprudência, formas globalmente consideradas nas suas diversas

manifestações e no seu potencial de desenvolvimento, os direitos da personalidade. (Boletim da Faculdade de Direito da Universidade de Coimbra, 1999, p. 151).

A partir de 1916 o Brasil passa a ter uma codificação civil. Antes vigorava o direito português. Porém, frustradamente, a proteção dos bens jurídicos da personalidade ficou de fora. Esse era um código essencialmente patrimonialista e individualista.

Mas em 1954, com Pontes de Miranda (Miranda, 1955), após quase 40 anos da entrada em vigor do Código Civil, a obra Tratado de Direito Privado, do autor, traz uma lição completa sobre os direitos da personalidade não vista até a década de 50. A obra até hoje é dominante no núcleo duro da disciplina.

Já no projeto de Código Civil de 1963, com a figura de Orlando Gomes, preconizava como objetivo primeiro, preservar um dos valores fundamentais da civilização que é o respeito à pessoa humana, tendo inclusive a inserção de uma cláusula geral de tutela, uma proteção aberta, abrangendo todos os direitos reconhecidos à pessoa humana, porém com pouca previsão de direitos especiais de personalidade (Gonçalves, 2022, p.63-74).

> Art. 29.º Direitos da Personalidade - O direito à vida, a liberdade e à honra, e outros reconhecidos à pessoa humana são inalienáveis e intransmissíveis, não podendo seu exercício sofrer limitação voluntária.
> Parágrafo único. Quem for atingido ilicitamente em sua personalidade pode exigir que o atentado cesse e reclamar perdas e danos, sem prejuízo de sanções de outra natureza a que fique sujeito o ofensor (Gomes, 1985, p.17).

Apenas no Código Civil de 1975 consagraram-se os direitos da personalidade.

> (...) cabe dar realce à disciplina dos chamados direitos de personalidade. Os projectos anteriores já haviam dado atenção a esta matéria. Pensamos ter fixado, em alguns artigos fundamentais, as regras indispensáveis à tutela dos valores da subjetividade, a começar pelos concernentes ao direito sobre o próprio corpo, para fins de transplante, ou mesmo para pesquisas científicas.
> O problema da tutela da imagem e da intimidade, bem como do uso do nome da pessoa, são aspectos que a nova Codificação teve em vista reger, pondo o valor da pessoa no fulcro do ordenamento jurídico (Reale, 1978, p. 171).

Mas à Moreira Alves coube a elaboração da Parte Geral do Projeto de Código Civil (1975), como supracitado e corroborando com o entendimento a seguir:

> "Os direitos de personalidade, ausentes no Código de 1916, foram admitidos no Brasil por força de construções doutrinárias, com base em leis especiais e na Constituição da República. O Código de 2002 regula alguns direitos de personalidade (...). Duas cláusulas gerais são veiculadas nos arts. 12 e 21. O art. 12. prevê a possibilidade de cessar ameaça ou lesão a direitos de

> personalidade e o ressarcimento pelos danos causados. Nos termos do art. 21: " vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (Tepedino, 2003, p. 3-20).

Para o professor Silvio Romero, o Código Civil atribuindo aos direitos da personalidade um caráter residual preferiu disciplinar aquelas figuras que não se destacam em uma carta política, como o direito ao nome e o direito à imagem, não retomando algumas figuras significativas, como o direito à vida, ao desenvolvimento da personalidade e à liberdade. Pois segundo esse entendimento, tais direitos já se encontram disciplinados na Constituição Federal.

Ele reforça que a pessoa é o fundamento e o fim do direito, e não são todos os direitos que disciplinam aspectos pessoais que podem ser tratados como direitos da personalidade, mas que a compreensão sobre a proteção da dignidade da pessoa humana, no mínimo, dê espaço ao livre desenvolvimento da sua personalidade. E para tal, cabe o máximo da sua tutela.

E conclui afirmando ser necessário verificar em cada uma das situações em concreto a existência do fundamento ético da dignidade da pessoa humana. Assim, ele corrobora que os direitos da personalidade são uma categoria especial de direitos subjetivos que, fundada na dignidade da pessoa humana, garantem o gozo e o respeito ao seu próprio ser, em todas as suas manifestações espirituais ou físicas.

Porém, que esses direitos não devem ser confundidos com os Direitos Fundamentais que dizem respeito à qualidade de cidadão da pessoa perante o Estado (Beltrão, 2014).

Porém, considerando a corrente civil-constitucional, Doneda bem lembra que mesmo com o aperfeiçoamento de algumas dimensões da personalidade por meio do direito privado entre o século XIX e início do XX, considere-se um marco mais característico na continuidade desse processo que foi a Constituição de Weimar, de 1919.

Tal Carta repercute ainda hoje em diversos países, ao aprimorar a relação entre o direito público e o direito privado, englobando em âmbito constitucional institutos-chave do direito civil, como a família, a propriedade e o contrato (Doneda, 2006, p. 74), o que foi fundamental para a proteção de novos direitos que surgem até hoje na esfera civil inclusive diante dos acontecimentos dos últimos anos, pela forma e quantidade de uso de dados pessoais para formação de perfil dos indivíduos.

Tal Constituição alemã assumiu especial posição no panorama jurídico europeu, em detrimento da francesa. Depois disso, a relação entre direito civil e Constituição passou a ser reavaliada no mundo. A conscientização da unidade do ordenamento jurídico passa a ser baseada então na dignidade da pessoa humana.

E o instituto da personalidade, estudado no direito civil, foi o que apresentou a mais forte vocação para tornar-se o centro de irradiação no direito privado dessa nova dogmática, voltada à proteção da pessoa. Nesse sentido, Pontes de Miranda afirma que, com relação à teoria dos direitos da personalidade, é possível começar a pensar para o mundo uma nova manhã do direito (Miranda, 1983, p. 5-6). Assim, ocorreu que os direitos em torno da personalidade, bem como seus vários aspectos – como o nome, a honra, a imagem e outros –, acabaram sendo compreendidos pelo direito civil como direitos subjetivos da pessoa, que mereceriam indenização se violados. Porém, enquanto a Lei Fundamental alemã, consolidou um direito geral de personalidade, a Constituição Federal brasileira trouxe o que "pode se chamar" de uma cláusula geral de proteção. O que também possibilitou uma maleabilidade e versatilidade de aplicação diante de situações novas e complexas (Mattietto, 2017).

Para Tepedino, os arts. 12 e 21 do CC 2002, já citados anteriormente, ambos os dispositivos, lidos isoladamente no âmbito do corpo codificado, não trazem grande novidade, sendo certo que a vida privada é constitucionalmente inviolável (CF, art. 5. ° *caput*, e inciso X) e que qualquer lesão ou ameaça de lesão possibilita a correspondente tutela jurisdicional (CF, art. 5.9, XXXV). Os preceitos ganham, contudo, algum significado se interpretados como especificação analítica da implícita cláusula geral de tutela da personalidade prevista no texto constitucional que pode ser compreendida nos arts. 1, III (dignidade humana como valor fundamental da República), 3. °, III (igualdade substancial) e 5, parágrafo 2. ° (mecanismos de expansão do rol dos direitos fundamentais).

Dessa forma, entende o doutrinador que a partir daí, deverá o intérprete romper com a ótica tipificadora seguida pelo Código Civil, ampliando a tutela da pessoa humana não apenas no sentido de admitir uma ampliação de hipóteses de ressarcimento, mas, de maneira muito mais ampla, no intuito de promover a tutela da personalidade mesmo fora do rol de direitos subjetivos previstos pelo legislador codificado (Tepedino, 2003, p. 3-20, 9-19).

Ao fato de a Constituição Federal preceder o Código Civil de 2002, com o fundamento mãe do princípio da dignidade da pessoa humana, não poderia este sobrepor o avanço normativo consagrado pela reforma da Carta Magna de 1988, constitui este mais um argumento para um ambiente jurídico civil-constitucional. E embora, recebendo críticas de parte da doutrina, por carência de metodologia e banalização da dignidade da pessoa humana, e à natureza histórico-dogmática do direito (Gonçalves, 2022, p.83-85), por exemplo, é a corrente civil-constitucional que mais se adequa aos problemas que afetam a personalidade humana diante das emergentes, constantes e velozes ameaças e danos na sociedade do risco que não podem esperar um processo normativo longo e lento de tipificação e possuem respaldo de boa parte da doutrina pelo que

demonstra. Assim, na ótica civil-constitucional se encontra o direito da personalidade à proteção de dados pessoais.

Ademais, o art. 5° da LICC revela este espírito do Código Civil ao afirmar: "Na aplicação da lei, o juiz atenderá aos fins sociais a que ela se dirige e às exigências do bem comum" reconhece ao intérprete a capacidade de operar o Código de modo a melhor adequá-lo ao caso concreto. Tal princípio caminha alinhadamente ao princípio da eticidade.

Por todo o exposto entre diferenças e conexões dos direitos fundamentais em relação aos direitos da personalidade, caminha-se para a busca da proteção do direito à proteção de dados pessoais positivado na Constituição Federal como Direito fundamental autônomo, no dia 10 de fevereiro de 2022. O Congresso Nacional promulgou a Emenda Constitucional 115 (EC 115), incluindo a proteção de dados pessoais na categoria de direitos e garantias fundamentais constantes do artigo 5º da Constituição Federal. Com isso, o referido dispositivo passa a conter o inciso LXXIX, com a previsão de que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais" (Brasil, 1988).

E conforme o Supremo Tribunal Federal, a proteção de dados já não pode ser compreendida como um simples exercício negativo do Estado em relação aos indivíduos, mas como um direito/dever dos agentes sociais públicos e incluindo-se aí nas relações entre privados agora sacramentado na Constituição, que vem reclamando esforços de diversos setores, em especial dos operadores do Direito, para permear as relações jurídicas e alcançar, na prática, o *status* concedido agora pela Lei Maior.

No Título II - Dos Direitos e Garantias Fundamentais da Constituição da República Federativa do Brasil, elenca-se um rol de direitos e garantias individuais e coletivas nos aspectos sociais, econômicos e políticos considerados indispensáveis ao exercício da cidadania pelos brasileiros. E é nele, que está expresso o direito fundamental à proteção de dados pessoais, deixando claro que este é um direito autônomo, não se confundindo com o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art.5, XII).

O sigilo a que se refere o art. 5º, XII, da Constituição da República é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si. Desta forma, a obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei n. 9.296/96.

De outra forma, posteriormente, no julgamento da ADI 6387, no voto da ministra Rosa Weber, ela já reconhecia que:

> Nessa linha, afirma que se pode extrair do texto constitucional, em particular das garantias expressas de proteção à dignidade da pessoa humana, à privacidade, à intimidade e ao sigilo dos dados pessoais, uma "tutela constitucional do direito à autodeterminação informativa". Afirmando assegurada, na Constituição da República, "uma tutela autônoma aos dados pessoais e não apenas ao conteúdo das comunicações" (Corrêa, 2022, p. 82).

Vale ressaltar ainda que não há que se confundir o direito autônomo à proteção de dados pessoais, tipificado na CF, com o direito fundamental ao sigilo dos dados bancários. Primeiro, a Constituição Federal não prevê expressamente a proteção do sigilo bancário, ele é um desdobramento do direito à privacidade (art. 5º, X). Ademais, o sigilo bancário é a "obrigação que têm os bancos de não revelar, salvo justa causa, as informações que venham a obter em virtude de sua atividade profissional" (Covello, 2001). Para a jurisprudência, os dados protegidos por sigilo bancário, são os serviços típicos de conta, como aplicações financeiras, transferências e depósitos.

E esses, apesar de dados, não são considerados dados pessoais em si. Pois essa proteção do sigilo bancário é apenas aos dados referentes à movimentação financeira das contas. Não há que se confundir dados bancários com sigilo bancário.

O sigilo bancário abrange apenas as "operações ativas e passivas e os serviços prestados", conforme dispõe o art. 1º da Lei Complementar no 105/2001, desta forma não incluindo os dados cadastrais de correntistas, entendidos como o nome, endereço, telefone, RG ou CPF (ou CNPJ).

Dados pessoais como nome, endereço, telefone, RG e CPF ou CNPJ de correntistas bancários não são protegidos pelo sigilo bancário, mas pelo direito fundamental à proteção de dados, e na infraconstitucional LGPD. Assim, não há que se confundir o direito fundamental extraído da interpretação da CF (sigilo bancário), com o direito fundamental autônomo à proteção de dados pessoais. O sigilo bancário alcança as operações ativas e passivas e os serviços das instituições financeiras (aplicações, transferências, depósitos, etc.), não estando submetidos a este segredo os dados pessoais cadastrais bancários (número da conta-corrente, nome completo, documentação pessoal, número de telefone e endereços físicos e eletrônicos do respectivo titular, RG e CPF).

E enquanto o direito fundamental à proteção de dados pessoais refere-se exclusivamente à pessoa natural identificada ou identificável, o sigilo de dados pode referir-se à pessoa jurídica.

Diante da existência de indícios da prática de ilícitos penais envolvendo verbas públicas, cabe ao MP, no exercício de seus poderes investigatórios (art. 129, VIII, da CF/88), requisitar

os registros de operações financeiras relativos aos recursos movimentados a partir de conta-corrente de titularidade da Prefeitura. Essa requisição compreende, por extensão, o acesso aos registros das operações bancárias sucessivas, ainda que realizadas por particulares, e objetiva garantir o acesso ao real destino desses recursos públicos. (STJ. 5ª Turma. HC 308493-CE).

Dito de outra maneira, segundo o Ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita, não se restringe 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; Rodrigues Júnior; Fonseca, 2021, p. 67).

> LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela EC n. 115/2022)
> § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.

As normas relativas ao direito à proteção de dados são — nos termos do artigo 5º, º 1º, CF — dotadas de aplicabilidade imediata (direta) e vinculam diretamente todos os atores públicos, bem como os atores privados.

O direito fundamental à proteção de dados pessoais passa a estar submetido a uma expressa reserva legal simples, que empodera o legislador infraconstitucional para efeito de estabelecer intervenções restritivas no âmbito de proteção do direito, implicando, por outro lado, a observância das exigências da reserva de lei, pena de inconstitucionalidade da restrição.

> Como parte integrante da Constituição formal, os direitos fundamentais possuem status normativo superior em relação a todo o restante do ordenamento jurídico nacional; 2) na condição de direito fundamental, assume a condição de limite material à reforma constitucional [..]; 3) também as normas relativas ao direito à proteção de dados são - nos termos do art. 5°, $1°, CF - dotadas de aplicabilidade imediata (direta) e vinculam todos os atores públicos, bem como sopesadas as devidas ressalvas, consoante será tratado em tópico específico - os atores privados (Sarlet, 2020, p. 186).

Os estudiosos do Direito Constitucional retratam sobre a eficácia dos direitos fundamentais em dois aspectos. O aspecto vertical, no qual o titular passa a ter instrumentos capazes de se opor aos arbítrios do Estado frente a possíveis abusos. O aspecto horizontal, em que o titular pode exigir que os demais membros da sociedade respeitem o seu exercício, tendo-se a preocupação de não invadir o exercício de direitos pelos demais. Afinal, não cabe apenas a "um simples dever de ação do Estado para proteger bens ou promover fins constitucionais, mas de um dever de acção para 'segurar' direitos consagrados e protegidos por normas constitucionais" (Canotilho, 2001, p. 113).

Assim, com os olhos em uma teoria que possibilita enxergar e proteger manifestações da personalidade que sempre existiram, mas que passaram a ser exploradas ostensivamente, de maneira prejudicial à pessoa. Tamanha exploração que fere a dignidade da pessoa humana ameaçando sua condição, como já defendido por Nelson Rosenvald, resta reclamar, assim, proteção, reconhecendo a proteção de dados pessoais na categoria de "novos direitos" de personalidade é uma consequência natural, portanto um dever no ordenamento jurídico. Pois, como ensina Tartuce (2016, p. 98):

> Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral, de tutela da pessoa humana, contida no art. 1o, III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, de tutela da pessoa humana, contida no art. 1º, III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação. Em suma, existem outros direitos da personalidade tutelados no sistema, como aqueles constantes do Texto Maior. O rol do Código Civil é meramente exemplificativo (numerus apertus) e não taxativo (numerus clausus).

A lógica dada ao intérprete e legislador ordinário, qual seja, a dignidade da pessoa humana, passou a ter prioridade na compreensão dos direitos da personalidade também porque o Código Civil de 2002, passou a eleger uma visão humanista pós Segunda Guerra Mundial, conferindo unidade ao ordenamento jurídico na superação do público privado, pois os valores da Constituição de 1988 tornaram-se referência (Kelsen, 2009).

No mesmo raciocínio sobre como reconhecer um novo direito da personalidade, é necessário basear-se na teoria expansiva adotada pelo Código Civil de 2002, na qual o rol desses direitos, ratificando o raciocínio acima, não é taxativo, mas exemplificativo não abarcando assim todas as possibilidades futuras de manifestação da personalidade humana e por isso, seus aspectos não podem deixar de ser tutelados com o fundamento de que não estão simplesmente positivados, pois já são implícitos.

Ademais, o Código Civil, temos a previsão de que todas as pessoas são capazes de direitos para a doutrina, o conceito de personalidade apenas reflete a materialização, em palavras, de uma ideia abstrata sobre um rico fenômeno da evolução humana previsto constitucionalmente.

Como bem ratifica o raciocínio em face do princípio fundamental da dignidade da pessoa humana, pode-se dizer que a pessoa é o bem supremo da ordem jurídica, o seu fundamento e o seu fim. Sendo possível concluir que o Estado existe em função das pessoas e não o contrário, a pessoa é o sujeito do direito e nunca o seu objeto (Beltrão, 2014). Nesse sentido, os direitos da personalidade são direitos essenciais à dignidade da pessoa humana e à sua integridade, protegem tudo o que lhe é original, próprio, como a honra, a vida, a liberdade, a privacidade, a intimidade, entre outros.

Na sociedade hiper conectada existe um problema que gira em torno da necessidade atual de as pessoas se tornarem visíveis para existirem e, assim, têm seus dados pessoais utilizados para a formação de perfis de cunho social, político e econômico. Todos esses perfis são analisados e direcionados pelo monopólio da tecnologia digital global. Aqui ressalta-se que, mesmo que não haja legislação específica que determine como se dará o limite de tratamento de dados pessoais, pode-se recorrer à cláusula geral da proteção da personalidade e ao princípio da dignidade humana para tentar conciliar a proteção integral da pessoa humana com os interesses das grandes empresas envolvidas no fluxo de tecnologias e informações (Nascimento, 2017, p. 265-288).

Diferentemente da Lei Fundamental alemã que erigiu um direito geral de personalidade, a Constituição brasileira estabeleceu, via princípio fundamental da dignidade da pessoa humana, a sua atuação implícita como cláusula geral de tutela da personalidade. Essa técnica jurídica propicia, em sistemas jurisprudenciais valorativos, conferir maleabilidade e versatilidade de aplicação a situações novas e complexas (Sousa, 1995, p. 92-93) como reclama hodiernamente o mundo digital.

Nesse contexto, e corroborando com a narrativa trazida até então sobre a expansividade dos direitos da personalidade, faz-se necessário trazer à baila que a doutrina classifica tais direitos de diferentes maneiras, o que não os invalida, mas se propõe à finalidade científica taxonômica. Essa diversidade de classificação fortalece a percepção da inexistência de um rol taxativo, apesar de tipificado, demonstrando, na verdade, certa convergência e conexão.

Assim, não sendo a definição exaustiva, como diz Roxana Borges (2005, p. 25), “são direitos em expansão. Com a evolução legislativa e o desenvolvimento do conhecimento

científico acerca do direito, vão-se revelando novas situações que exigem proteção jurídica e, consequentemente, novos direitos vão sendo reconhecidos".

Assim, o direito à proteção de dados pessoais como novo direito da personalidade, em tese, poderia se encaixar na ideia de que dados pessoais são a projeção da pessoa na sociedade.

Os dados pessoais são informações relativas às pessoas. O conceito é deveras amplo. Inclui desde atributos da pessoa (nome, estado civil, domicílio) e circunstâncias da vida civil (vínculos associativos, nível educacional, profissão), até informações que explicitam preferência sexual, condição de saúde, caracteres genéticos, ideologias, crenças religiosas etc. Referem-se, enfim, ao modo de ser da pessoa; dizem o que ela é, revelando sua personalidade.

Estes dados podem eventualmente ser desvinculados da pessoa, tornando-se um bem "externo" circulável. Porém, é de se observar que continuam sendo informações "pessoais", mantendo vínculo específico com a pessoa, implicando na sua valoração a partir do seguinte ponto de vista: a informação deve ser entendida como uma extensão da personalidade.

Por isso, não existe exagero em afirmar que os dados formam uma espécie de "retrato" da pessoa e, logo, constituem mais uma projeção da personalidade que merece e deve ser protegida (Doneda, 2006).

> Como se observa, esses direitos referem-se, de um lado, à pessoa em si (como ente individual, com seu patrimônio físico e intelectual), e, de outro, à sua posição perante outros seres na sociedade (patrimônio moral), representando, respectivamente, o modo de ser da pessoa e suas projeções na coletividade (como ente social) (Bitta, 2015, p. 48-49)

Desta feita a decisão paradigmática e histórica que considerou a eficácia horizontal dos direitos fundamentais à proteção de dados pessoais trouxe entre outros argumentos que a afirmação da autonomia do direito fundamental à proteção de dados deriva do direito fundamental à dignidade da pessoa humana; da proteção constitucional à intimidade (artigo 5º, inciso X, da CF/88) diante do aumento de novos riscos derivados do avanço tecnológico; e do reconhecimento do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa. E que a autodeterminação informativa tem uma perspectiva subjetiva — que protege os indivíduos contra intervenções indevidas do Estado e de empresas no direito fundamental à proteção de dados — e uma dimensão objetiva, que exige do Estado obrigações positivas para a garantia desse direito, tanto nas relações com o poder público, quanto nas relações privadas.

No julgamento da MP 954/2020:

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. DIREITOS FUNDAMENTAIS. COMPARTILHAMENTO DE DADOS POR EMPRESAS DE TELECOMUNICAÇÕES PRESTADORAS DE SERVIÇO TELEFÔNICO COM A FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. SUPORTE À PRODUÇÃO ESTATÍSTICA OFICIAL DURANTE SITUAÇÃO DE EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO CORONAVIRUS COVID 19. ALEGADA VIOLAÇÃO À INVIOLABILIDADE DA INTIMIDADE, DA VIDA PRIVADA, DA HONRA DAS PESSOAS E AO SIGILO DOS DADOS. PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA. DIREITO À AUTODETERMINAÇÃO INFORMATIVA. MEDIDA PROVISÓRIA 954/2020. CF/88, ARTS. 1o, III; 2o; 5o, X E XII; E 62. 1. A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, extraídos da garantia da inviolabilidade da intimidade e da vida privada (art. 5o, X), do princípio da dignidade da pessoa humana (art. 1o, III) e da garantia processual do habeas data (art. 5o, LXXII), previstos na Constituição Federal de 1988. 2. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), que entrará em vigor em 16 de agosto de 2020, define os princípios e procedimentos para o tratamento dos dados pessoais e os critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude desse tratamento. 3. A Carta de Direitos Fundamentais da União Europeia reconhece, em seu art. 8o, que “todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito”. Também o Tribunal Constitucional Alemão, em julgamento paradigmático ocorrido em 1983, reconheceu a autonomia do "direito à autodeterminação informativa" , assentando que a atividade de processamento dos dados pessoais deve seguir “precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade” (Brasil, 2020).

A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, 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. 5o, 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.

Um direito da personalidade, como tal, deve ter sua essência na cláusula geral da dignidade da pessoa humana. Dessa forma, o julgamento da ADI já havia deixado claro tal ponto, reforçado nos ensinamentos de Laura Mendes, também citados na referida ADI.

> Para além da coincidência do léxico com os modernos instrumentos internacionais de tutela da privacidade, certo é que a proteção da dignidade humana e a inviolabilidade da intimidade e da vida privada numa sociedade da informação somente pode ser atingida hoje por meio da proteção contra os riscos do processamento de dados pessoais. Assim, quando se interpreta a norma do art. 5o, X, em conjunto com a garantia do habeas data e com o

> princípio fundamental da dignidade humana, é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais (Mendes, 2018. p. 188).

Do exposto acima, numa análise sistemática. Fica evidente que a proteção de dados pessoais irradia da Constituição Federal e deve ser tutelada pelo Código Civil de 2022, por força constitucional. E tendo em vista que aquele adotou expressamente a teoria expansionista de direitos da personalidade, como será demonstrado, o direito à proteção de dados pessoais pode ser considerado um "novo direito" da personalidade. Nesse sentido, o professor Flávio Tartuce destaca a perspectiva constitucional dos direitos de personalidade:

> (...) Os direitos de personalidade têm por objeto os modos de ser, físicos ou morais do indivíduo. O que se busca proteger com tais direitos são os atributos específicos da personalidade, sendo esta a qualidade do ente considerado pessoa. Em síntese, pode-se afirmar que os direitos da personalidade são aqueles inerentes à pessoa e à sua dignidade (art. 1.o, III, da CF/1988) (Tartuce, 2018, p. 515).

## 2.5 Como reconhecer um novo direito de personalidade

Preliminarmente, há diferenças importantes entre a privacidade e a proteção de dados pessoais. A privacidade possui caráter mais individual, enquanto a proteção de dados é mais coletiva. A privacidade é um direito negativo, enquanto a proteção de dados assume qualidade de direito positivo, que pressupõe o controle dos dados pelo próprio indivíduo, que decide onde, quando e como seus dados circulam. Por fim, o direito à privacidade oportuniza o usufruto tranquilo da propriedade, enquanto a proteção de dados está mais ligada ao direito de igualdade, ou seja, a não discriminação e ao usufruto de oportunidades sociais, como afirma Laura Schertel mencionada na decisão.

O próprio STF reconheceu o direito à proteção de dados como um novo direito fundamental, destacado e independente do direito à privacidade, com a identificação de uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade. Como bem define Bruno Bioni, o "centro gravitacional da proteção dos dados pessoais difere do direito à privacidade – i.e., a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado" (Bioni, 2019, p. 99).

E esse direito também não se confunde com o sigilo das comunicações, anteriormente já previsto na Constituição Federal.

Os incisos X e XI do art. 5º da Carta Magna tratam da inviolabilidade da intimidade, da vida privada e da casa do indivíduo, enquanto o inciso XII salvaguarda a confidencialidade dos dados. Em suma, além de tratarem da segurança do domicílio e das comunicações pessoais, os três incisos tratam também da proteção de informações pessoais, de modo que devem ser interpretados sistematicamente, pois se resguarda, além da segurança, a esfera particular do indivíduo contra a curiosidade pública e a ingerência de estranhos (Crespo; Ribeiro Filho, 2019).

E "o direito à autodeterminação informativa nasce, assim, para garantir um direito à intimidade privada no que aos tratamentos de dados pessoais diz respeito" (Castro, 2005, p.25).

Ademais, quanto ao sistema de proteção de dados pessoais que a LGPD passa a integrar, observa-se que não existe contradição ou conflito entre a LGPD e as legislações específicas. Pois, a lei 13.709/18 preceitua que os direitos e princípios expressos na norma não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais na qual a República Federativa do Brasil seja parte (art. 64). Corroborando o preceito legal, verifica-se que em capítulo atinente ao tratamento de dados pessoais pela Administração Pública, tem-se que os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes na Lei do Habeas Data, na Lei Geral do Processo Administrativo e na Lei de Acesso à Informação (art. 23, § 3º). No que tange às questões relacionadas à responsabilidade e ao ressarcimento de danos, nas hipóteses em que os direitos do titular forem violados no âmbito das relações consumeristas, aplicar-se-á o Código de Defesa do Consumidor (art. 45). Ao se analisar as práticas legais aptas a conferir segurança e o sigilo dos dados também é possível verificar o diálogo da norma com outras legislações, pois, segundo o art. 49, os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados para atender à LGPD, bem como às demais normas regulamentares.

A importância de tais direitos é tamanha que eles foram incluídos na Assembleia Geral da Organização das Nações Unidas de 1948 e na Convenção Europeia de 1950, após a segunda guerra, como forma de reação às agressões à dignidade humana e, por isso, lhe são absolutamente protetivos e necessários resguardando uma relação intrínseca do objeto (a dignidade da pessoa humana) e os direitos que ela reclama proteção (Lotufo, 2002).

Proteções que surgem tendo sido reclamadas enquanto novas situações da vida em sociedade fazem nascer, potencializar riscos, ameaças e lesões à personalidade. Por isso, do Código Civil, com base na Constituição Federal e lastreada em reflexões doutrinárias, é possível se extrair que os direitos da personalidade, apoiados no princípio basilar da dignidade humana

são direitos em expansão, enquanto novas situações se revelam e exigem proteção jurídica. “Aquele princípio é direito vigente já, pelo que já actualmente temos de encontrar para ele modo de expressão” (Ascensão, 1997, p. 76).

E esse modo de expressão (direito da personalidade) corresponde a uma circunstância histórica (Ascensão, 1997, p. 76) e sua tipificação no ordenamento infraconstitucional, pois os modos de tutela da personalidade são típicos, e que outras figuras em tese, só poderiam ser acolhidas mediante alterações da lei.

Nessa lógica, sendo o rol de tais direitos aberto, não taxativo, -exatamente para que se reconhecendo novos direitos merecedores de tutela - sejam eles positivados para a garantia efetiva da pessoa em sua totalidade, sem discussões ou dúvidas que levem a uma insegurança jurídica. Se a ideia é a possibilidade real de expansão de novos direitos, logicamente, seu reconhecimento com a respectiva positivação, corresponde à ideia que está na essência da teoria expansionista de ampliar a garantia. Aumentar o leque de proteção nomeadamente em lei. Cabe assim adequadamente a análise criteriosa, caso a caso, para ser assegurado o direito da personalidade. Sobre isso, Borges (2005, p. 25) afirma que:

> Os direitos de personalidade presentes na Constituição Federal nem a listagem contida no texto do Código Civil de 2002 são listas exaustivas ou taxativas dos direitos de personalidade, uma vez que estes não são unicamente direitos típicos. Pelo contrário, são listas apenas exemplificativas e refletem dado momento histórico que está em veloz mutação. Lembre-se da regra do art. 5°, $ 2°, do texto constitucional, que afirma que os direitos e garantias ali previstos não excluem outros que venham a ser reconhecidos posteriormente.

Ainda sobre isso, o Enunciado 274 do CJF afirma que os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral de tutela e promoção da pessoa humana, contida no art. 1°, inc. III, da Constituição (princípio da dignidade da pessoa humana).

> Com efeito, a escolha da dignidade da pessoa humana como fundamento da República, associada ao objetivo fundamental de erradicação da pobreza e da marginalização, e de redução das desigualdades sociais, juntamente com a previsão do §2º do art. 5º, no sentido de não exclusão de quaisquer direitos e garantias, mesmo que não expressos, desde que decorrentes dos princípios adotados pelo texto maior, configuram uma verdadeira cláusula geral de tutela e promoção da pessoa humana, tomada como valor máximo pelo ordenamento" (Tepedino, 1999, p. 48).

Daí nasce a observância para que, em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação. Ou seja, o Enunciado só reforça o entendimento da doutrina sobre a não taxatividade do rol dos direitos da personalidade, que traduz que novos direitos podem surgir, ser reconhecidos e serem formal e expressamente tutelados. É a ideia de não excluir, mas de aumentar as possibilidades de reconhecimento de tais manifestações, objeto de reflexão científica e jurídica e respectivo comando legal explícito.

> Uma posição flexível, como ele mesmo coloca, dada a generalização desse campo, torna possível, a nosso ver, o abrigo dos novos direitos que, naturalmente, a reflexão científica vira identificar e trazer para o posterior sancionamento no direito positivo (Bittar, 2015, p. 48-49).

Assim, sendo, não deve haver limite para reconhecimento de direito da personalidade se a manifestação é favorável ao indivíduo e é lastreada no princípio da dignidade humana. A limitação para reconhecimento de direito da personalidade está em qualquer manifestação favorável ao indivíduo, que não tenha por base o princípio da dignidade da pessoa humana e, por isso, não pode ser considerada direito da personalidade (Beltrão, 2013).

E apesar de o CC de 2002, com redação originária antecedente à Constituição, não fazer nenhuma alusão expressa ao princípio da dignidade da pessoa humana; todavia, por força da primazia constitucional, este e os demais princípios determinam o sentido fundamental das normas infraconstitucionais (Lôbo, 2022, p. 59).

Ademais, numa compreensão coerente com o mundo atual, o Professor Paulo Lobo considera que, mesmo que direitos da personalidade não sejam assim tipificados no ordenamento infraconstitucional, não importa. Para serem aceitos, basta que sejam tipos já reconhecidos socialmente e conformes com o princípio da dignidade da pessoa humana, posto que eles não se esgotam nos tipos que nos oferecem as distintas legislações (Lôbo, 2022, p. 142). Corroborando, nesta altura da história, não se pode prever quais outros direitos dessa categoria serão acolhidos e tipificados no ordenamento jurídico futuro (Sessarego, 1992, p. 40).

Inovando no sentido da “tipicidade aberta dos direitos da personalidade” (Lôbo, 2022, p. 141) o professor Paulo Lobo classifica-os como tipos mais gerais de direitos da personalidade, porém sem qualquer pretensão de exaurimento, como o direito à proteção de dados pessoais (Lôbo, 2022, p. 151).

E como método para identificação de novos tipos de direitos da personalidade, o magistrado pode tomar como base a tipicidade aberta dos direitos da personalidade diante de

uma violação onde não se possa encontrar tal direito buscado pela vítima numa tipificação já posta.

> Quando o juiz deparar-se com situação fática que não se enquadra nos tipos legais de direitos da personalidade, mas que evidencia violação a esta, deve verificar se é cabível, no caso, a tutela do princípio da dignidade da pessoa humana. Essa operação hermenêutica de reenvio ao princípio assegura a plena aplicabilidade dos direitos da personalidade (Lôbo, 2022, p. 142).

Ideia essa que, na linha dessa dissertação, percebe-se a mais eficaz diante dos desafios e riscos aos direitos da personalidade na atualidade.

Mas, como um novo direito da personalidade, a proteção de dados pessoais se encaixaria em qual tipo de classificação, tendo em vista que os dados pessoais são sobremaneira transversais e podem estar em vários direitos da personalidade já tipificados? Essa é uma indagação que carece de mais discussão, inclusive podendo-se considerar a hipótese de uma nova classificação em que todas as outras, possam deste "novo direito" ser espécie. Ou, sobre esse ponto, de maneira elucidativa, o professor Paulo Lobo esclarece que dificilmente se pode isolar qualquer dos direitos da personalidade, pois cada situação de fato poderá configurar lesão a um conjunto deles. Como exemplo, a lesão ao direito à imagem (retrato, efígie) redunda frequentemente também em lesão à honra, à vida privada e à intimidade. Por outro lado, pode-se fazer um paralelo com a proteção de dados pessoais que ora pode envolver imagem, privacidade e outros bens da personalidade conjuntamente. Então, nesse caso, o juiz deverá considerar esse fato quando fixar a reparação compensatória (Lôbo, 2022, p. 143).

Sobre sua natureza, os dados pessoais são informações relativas à pessoa que permitem a sua identificação, sendo um bem jurídico de natureza extrapatrimonial, sendo ele direito da personalidade. Posto que, diante dos desafios da tecnologia, a LGPD veio para proteger os direitos da personalidade na era da informação, os dados pessoais. A referida lei determina que todo o cidadão tem o direito de ao menos saber como seus dados pessoais são tratados.

# 3 O CONTEXTO DO SURGIMENTO DO DIREITO À PROTEÇÃO DE DADOS NA EUROPA E NO ORDENAMENTO JURÍDICO BRASILEIRO

## 3.1 Da origem do direito à proteção de dados pessoais no contexto europeu (GDPR) e o reconhecimento como direito fundamental

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 da 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. A Alemanha 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, têm-se os princípios relativos ao tratamento de dados pessoais, consagrados no artigo 5º 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 os primeiros debates em torno da promoção da 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 iniciou 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, reconheceram-se os valores de proteção da privacidade individual e familiar (Artigo 12) e a liberdade de informação, opinião e de expressão (Artigo 19) os quais são inspirações de todas as leis protetivas de 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, familiar e à informação, bem como permitiu à autoridade pública ingerência nesses direitos, estabelecendo como limites à 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 (European Commission, 2017).

Em 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 XXI, 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 (União 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 em 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” (União Europeia, 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 não requer a aprovação de leis nacionais compatíveis com suas determinações. Seu objetivo é 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 podem ser, dessa forma, pensados como um instrumento para a globalização dos padrões de privacidade e proteção de dados.

Sobre o reconhecimento do direito à proteção de dados pessoais como direito fundamental na Europa, 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 (Steinmüller *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* (Swant, 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 na figura 1 criada pela *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).

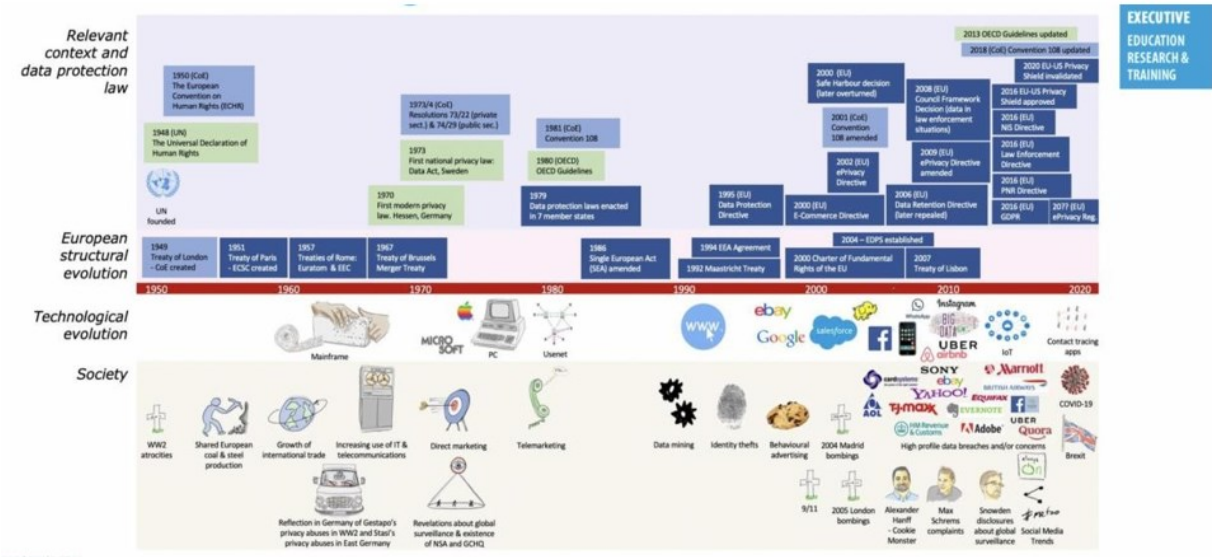


Figura 1: The context & challenges
Fonte: Maastricht University (2022).

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.

> 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 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.

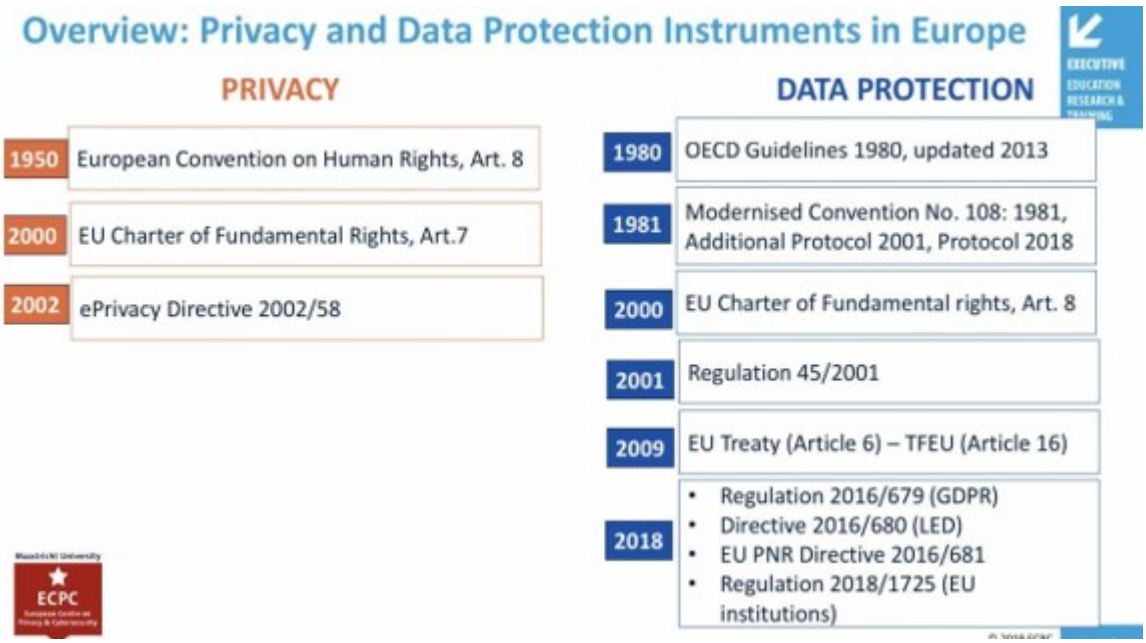


Figura 2 - Overview: privacy and data protection instruments in Europe.
Fonte: Maastricht University (2022).

A partir do exposto na figura 2 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 e que serão elencados no desenvolver do trabalho. 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 considerem 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 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. Trazendo à baila o primeiro caso, na Inglaterra, em 1818, 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. Após 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 a 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, 2019).

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 (Warren; Brandeis, 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 (Warren; Brandeis, 1890).

Na sequência cronológica, um segundo 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 (Bertoncello, 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. 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 outro cenário: o do controle, do monitoramento, da vigilância, da classificação com a perfilização, da influência e da discriminação das pessoas, que pode chegar a alterar sua própria essência (Doneda, 2017).

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. Mas 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, 2020, p. 48).

E mesmo antes do Regulamento Geral de Proteção de Dados europeu, países além da Alemanha, como França, Itália, França, já possuíam legislações nesse sentido que foram incorporadas também através da Diretiva 45/96 que precedeu o referido Regulamento Geral.

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 medidas técnicas 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.

Depois de feito 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, segue-se então o seu desenvolvimento no Brasil.

## 3.2 O contexto brasileiro da Lei Geral de Proteção de Dados Pessoais

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. Assim como fizemos com o GDPR.

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 como importante instrumento de defesa de milhões de pessoas, sobretudo do ponto de vista dos consumidores. Estes, especialmente, vítimas da perfilização e consequente discriminação. A aprovação da lei é o resultado de um longo trabalho feito por amplos setores da sociedade. Foram 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). Contudo, 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 ao fixar as mesmas exigências para companhias de diferentes portes, a lei elevaria o nível de exigência (técnica, de segurança e procedimental) a uma altura que startups e empresas menores dificilmente conseguiriam alcançar. Para o mercado, na lógica econômica e do lucro, arriscava-se desestimular a inovação e prejudicar o desenvolvimento da economia digital (MMA, 2022).

Pois bem, voltando 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 da democracia, da liberdade de expressão e na economia, ressalta-se que a ausência de um quadro normativo específico não implicava, em absoluto, que a matéria não fosse relevante. Pois 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, incisos X e XII, com menção no Código Civil, artigo 21, teve o poder 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 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 formando e utilizando-se dos seus perfis pessoais *on-line*:

> 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 dados 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 (Meyer, 2018).

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 mais140 países onde essa garantia já era uma realidade há muitos anos. (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 pretendiam 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, 2020b).

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. É possível 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, ao desmistificar 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 estava no caminho da luta pela redemocratização do país. A deputada Cristina Tavares deu corpo ao projeto que 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 aí 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 para evitar danos à personalidade (Brasil, 1980).

> § 2.º Para efeito desta lei, considera-se tratamento automatizado de informações nominativas, todo o conjunto de operações realizadas pelos meios automáticos e que permitem, sob qualquer forma, a identificação das pessoas físicas às quais elas se aplicam.

A justificativa do referido Projeto de Lei, em pleno ano de 1980, é um verdadeiro manifesto em defesa dos direitos da personalidade diante do uso dos dados pessoais dos indivíduos, que modificaria o artigo 9º do Código Civil e o art. 368 do Código Penal.

Importa que a informática respeite quatro séries de valores dois tradicionais: os direitos do homem e as liberdades individuais ou públicas e dois mais propalados atualmente: a vida privada e a identidade humana.

A noção da vida privada aparece pela primeira vez na França na lei de 1970 que visa a reforçar a garantia dos direitos individuais, numa parte intitulada “proteção à vida privada”. Essa lei modifica o art. 9º do Código Civil e o 368 do Código Penal a fim de aumentar a proteção à vida privada e à intimidade.

A noção de “identidade humana”, primeiro objetivo citado pela nova lei. é o mais novo nos textos. A expressão é hoje utilizada em sociologia, em psicologia e nos estudos sobre a cultura e o saber.

Identidade se junta à personalidade sem, entretanto, se confundirem entre si. Refere-se ao que é essencial e singular em cada ser humano de acordo com seu tipo e seu meio. Em relação à informática, a palavra significa que a máquina deve respeitar o nome de cada um e não pode reduzir seus direitos a números anônimos.

A questão da privacidade é, sem dúvida, a mais polêmica das questões, a que mais publicidade tem recebido e a que produziu maiores consequências legais em diversos países.

A era do computador possibilitou, pelo menos potencialmente, a agregação de dados sobre indivíduos, dados esses antes dispersos em arquivos manuais. O “rastro” que uma pessoa deixa hoje de sua passagem pode ser muito mais nítido e permanente com o uso de computadores. Em consequência de extensões, debates públicos e alterações nas legislações vêm sendo propostas e tornadas efetivas, notadamente nos países adiantados.

A Suécia foi pioneira na alteração de sua legislação. Nos Estados Unidos, principalmente após Watergate e outras invasões da privacidade, houve grande impulso na legislação sobre a matéria.

Uma lei de 1975 regula os bancos de dados federais ou criados com ajuda federal. A lei contém dispositivos que possibilitam o conhecimento, por parte do público, dos bancos de dados existentes.

A Inglaterra também no final de 1975 publicou um estudo sobre a regulamentação de bancos de dados computadorizados. Textualmente diz que “a existência e objetivo de sistemas de informação devem ser publicamente conhecidos, bem como a categoria de dados que manipulam, e é facultado o acesso aos mesmos, pelos interessados”.

A lei canadense, que trata da proteção da vida privada, baseia-se no seguinte princípio: "os indivíduos têm direito à vida privada e ao acesso aos registros que contêm informações sobre sua pessoa, para todos os fins, mormente para assegurar que eles sejam completos e as informações contidas exatas e compatíveis com o interesse público.

Lei da República Federal da Alemanha datada de 27 de janeiro de 1977, em seu art. 4. °, preceitua que qualquer pessoa tem acesso aos dados armazenados a seu respeito e pode corrigi-los quando não corresponderem à realidade.

Verifica-se pelas providências adotadas por vários países que o problema da proteção à privacidade do indivíduo é da maior atualidade, face ao impacto que a informação computadorizada causou no mundo moderno. Se por um lado, o desenvolvimento da informática possibilitou um grande avanço no sentido da imediata recuperação de dados, por outro, constitui ameaça à intimidade do cidadão.

Nada mais oportuno que, à semelhança de outros países, legislemos no sentido de salvaguardar o direito de cada um quanto ao sigilo e à retificação dos dados sobre sua pessoa.

Assim é que achamos por bem apresentar esta proposta e submetê-la ao arbítrio desta Casa, ciente de sua importância no resguardo dos princípios e direitos fundamentais do homem.

A Iniciativa não cogita ser a primeira e provavelmente não será a última, mas cremos que o momento é chegado de dar a nosso povo o direito de se precaver contra eventuais ofensas à sua integridade.

Submetemos, pois, à apreciação dos doutos pares este projeto de lei que, sem dúvida, sofrerá alterações de molde a aprimorá-lo no sentido de atender às justas reivindicações de todos quantos compreendem seu largo alcance.

Mas, 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 consta dos autos do processo digital de tramitação (às folhas 40) do mesmo. 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 durante aquele período:

> 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, constando 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 com finalidade diversa da coleta e a necessidade de consentimento expresso. Uma curiosidade, 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. Em 05 de junho de 1987, a Lei Estadual 5.702, no estado de São Paulo, concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa.

No ano de 1988, na Constituição Federal, pela primeira vez, surge a garantia constitucional do *Habeas Data* em meio ao trauma dos brasileiros durante o período da ditadura. Um direito de buscar suas informações pessoais em relação ao Estado (órgãos públicos). “Pode-se afirmar que o habeas data foi criado no Brasil durante a elaboração da Constituição de 1988, tendo sido inspirado na recente utilização, por autoridades públicas, de dados inteiramente falsos ou contendo erros, visando a fins políticos e com grave prejuízo de direitos individuais” (Dallari, 2002).

Em 1988, também houve o estabelecimento da defesa do consumidor. Passa-se a receber as demandas relacionadas a dados pessoais e dois anos depois, em 1990, o Código de Defesa do Consumidor, que foi inspirado, de acordo com o responsável 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 nesta normativa 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.

Em 2002, o Código Civil (Lei 10.406/2002), em seus artigos 12 e 21, considerando a proteção de dados pessoais 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). Já 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 (Doneda, 2020)

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 à época, que tinha consciência desse direito fundamental à proteção de dados pessoais, esse acordo, 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 após 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 aos titulares dos dados 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, 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 Lei 12.737/12 (Lei Carolina Dickmann) sobre a invasão de dispositivos, comentada Tomasevicius Filho (Tomasevicius Filho, 2014). A atriz teve fotos íntimas obtidas de seu computador pessoal e divulgadas na Internet pelo fato de

ela não ter se 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 à invasão de privacidade a deixarem de praticar essas condutas. 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, organizada 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.º 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 dos indivíduos através dos seus perfis pessoais, orquestrado pelo Governo Americano depois dos atentados das torres gêmeas, no histórico 11 de setembro. Francisco Brito Cruz descreve, conforme enxerto baixo, 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, 2019).

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 aprovada 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).

Tabela 1 - Entenda o Marco Legal de Proteção de Dados.

| | |
|---|---|
| **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, obtidos 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;<br>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. |

Fonte: Agência Senado Federal (2020).

Após 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 (Mulholland, 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 Exterior, que dele derivou um documento chamado de "Medidas para a Proteção de dados pessoais e sua livre circulação", incorporado em 2010 ao Mercosul. Foi quando a matéria teria sido discutida, segundo Doneda, pela primeira vez pelo Poder Executivo Brasileiro. O texto que serviu de marco a partir do debate público, com devidas contribuições posteriores, fomentou a consolidação de texto-base para o Anteprojeto de Lei de Proteção de Dados pelo Ministério da Justiça. Até 2015, tal texto 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 por sua vez encaminhou o Anteprojeto para um debate público. O resultado foi de cerca de 1200 contribuições para enfim ser consolidado o texto em 2016 e enviado ao Congresso Nacional (Projeto de Lei nº 5.726/2016, aprovada 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 de fato adiada por forças políticas e econômicas. Mas havia a necessidade de o Brasil integrar a Organização para a Coordenação e Desenvolvimento Econômico (OCDE). Tal Organização 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 ainda da entrada em vigor do já citado

Regulamento Geral Europeu de Proteção de Dados, fatos complementares tornaram o cenário mais propenso 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; iii) 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 supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia 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 o Estado - conseguirem cumprir com a LGPD a tempo” (Gimene, 2020).

Se por um lado, fatores a princípio poderiam levar ao adiamento da vigência da Lei Geral de Proteção de Dados Pessoais, forçaram a sua aprovação. A pandemia da COVID-19, por outro lado, 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 perfilhados e monitorados 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 vem 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, Ehrhardt Junior, 2022, p. 167).

Pela urgência da situação, as normas tenderam a ser flexibilizadas e as decisões governamentais foram, muitas vezes, tomadas sem as devidas reflexões acerca do impacto na vida privada e 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, esse foi um dos motivos para que a entrada em vigor da Lei Geral de Proteção de Dados no Brasil não significasse sua plena eficácia. Ou seja, até hoje, nos idos de 2023, 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, têm alma bandeirante. É liberal, capitalista, tendo seu maior ativo extraído do ser humano. Este em condição variável, crescente e permanente de vulnerabilidade na relação assimétrica de poder e 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, coletados, perfilizados a partir de situações consumeristas. Nessas relações, os direitos da personalidade dos titulares de dados no contexto de avanço da tecnologia e da inovação, os quais são na essência a alma da Lei Geral de Proteção de Dados Pessoais, são infringidos.

Na resumida análise histórica e normativa da sequência dos acontecimentos, segue-se análise do contexto da 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 que 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 mais danosas que o Estado na coleta de dados pessoais. Elas desenvolveram o método de commoditificação 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, (Srnicek, 2016), 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, movimentados, perfilizados 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 crescendo há décadas.

É necessário avivar aqui alguns fatos, por serem fundantes e fortes argumentos baseados em necessidades crescentes da sociedade em transformação que sempre está clamando soluções. No caso da privacidade, foi preciso ampliar essa proteção de alguma forma, ao ponto de ser imprescindível um novo direito. Pois, a constitucional tutela da privacidade já não satisfazia, sozinha, a proteção de dados pessoais. Reafirmando, pois, segundo Doneda, que "tal operação, se bastaria para abarcar a disciplina sob a égide constitucional, acaba por simplificar demasiadamente os fundamentos da tutela de dados pessoais, o que pode eventualmente 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 artigo 2º. 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 por meio de uma Proposta de Emenda Constitucional analisada a seguir antes de sua aprovação.

O projeto de emenda à constituição 17/19 foi aprovado 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 época, era a de que fosse competência da União a função de legislar sobre o tema. Ou seja, pelo projeto de emenda à 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.

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 à 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 (Brasil, 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 à 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 um direito fundamental autônomo. Como um dos efeitos, essa decisão da Suprema Corte acabou por determinar urgência à tramitação da anteriormente ao projeto de emenda à 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, pessoas físicas ou jurídicas a fim de realizar pesquisa estatística não presencial diante do isolamento populacional imposto pela pandemia (Brasil, 2020a).

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 vista realizar-se de pesquisa que precisaria apenas de amostra; além da falta de transparência para com 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 grande capacidade 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 considerado 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") (Scherte; Rodrigues 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. Ela 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 mecanismos 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; Rodrigues 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. E 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. 5º 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 do novo direito que já vinha sendo acolhido pela doutrina, sob o manto de outras proteções constitucionais como o direito à privacidade, à intimidade e ao sigilo das comunicações, do habeas data e do princípio da dignidade humana (Guerreiro; 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.º 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, 2020, 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, cabe 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, 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 Agência 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. Todas dependem de solução a partir das decisões 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 traz uma expectativa de

alterações e interpretações benéficas no cenário da rede de proteção dos titulares.

### 3.3 Princípios da Lei Geral de Proteção de Dados Pessoais

A LGPD é uma lei considerada principiológica pela doutrina e com um núcleo comum e convergente aos países que tutelam a proteção de dados (Bennet, 2006, p. 131). Dessa maneira, inicialmente, aproximando as legislações que tratam sobre o tema em diversos países do mundo, pelo conteúdo e pela forma, é possível destacar que a ideia básica é a de controle, ou seja, a garantia de controle dos dados pessoais pelo próprio titular, diante da autodeterminação informativa. Essa autodeterminação, uma verdadeira expansão da autonomia privada, tem como base a liberdade do titular, não só de acesso aos bancos de dados, mas também de determinar como as informações a seu respeito poderão ser utilizadas, respeitados sempre os princípios (Basan, 2022, p. 54).

O Art. 6º da referida legislação reza que as atividades de tratamento de dados pessoais deverão observar a boa-fé, citada nomeadamente e em seguida, demais princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Chama-se a atenção para o princípio da boa-fé, que também tem destaque nos artigos 187 e 422 do Código Civil, além de dispositivos do Código de Defesa do Consumidor, entre os quais os artigos. 4º, III e 51, IV.

Em se tratando de dados pessoais, a boa-fé é fundamental no equilíbrio dos interesses envolvidos, porque há o temor produzido por não se conhecer quem os solicita, tampouco se tem como avaliar os riscos advindos do que se fará com os dados coletados, uma vez que podem ser usados de forma lícita, mas também de forma ilícita. Daí se pode interpretar que os outros princípios a seguir elencados são, na realidade, desdobramentos da boa-fé. Seriam então critérios, hipóteses de comportamentos corretos, coerentes com a boa-fé e que também figuram no Regulamento Europeu de Privacidade e Proteção de Dados numa lógica de regulação semelhante. Nesse sentido, o GDPR tem como princípios a licitude, lealdade e transparência; a limitação das finalidades; a minimização dos dados e a limitação da conservação; a exatidão; e a integridade, bem como no ordenamento brasileiro detalhado a seguir: “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” (GDPR, 2016).

Nota-se, portanto, que a finalidade trata do respeito ao motivo pelo qual o dado pessoal foi coletado e pelo qual passa por tratamento. Evidentemente, uma das grandes funções deste princípio é limitar o tratamento, evitando os riscos decorrentes do uso secundário dos dados, feito de forma desconhecida e não autorizada pelo seu titular (Bassan, 2022, p. 60). Assim, em regra, esse princípio exige que o propósito do tratamento seja conhecido antes mesmo da coleta de dados, possuindo grande relevância prática. Afinal, ele é o fundamento para impor restrições, como a de transferência de dados a terceiros, ou mesmo servir como base para valorar a razoabilidade do uso de determinados dados para certas finalidades, "fora da qual haveria abusividade" (Doneda, 2019, p. 182).

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (GDPR, 2016).

Em resumo, o que a LGPD determina é que o uso de dados pessoais deve se restringir às informações adequadas para a finalidade almejada, promovendo o tratamento do mínimo de dados necessários para o alcance do objetivo pretendido. Esse raciocínio também encontra amparo no GDPR, que prevê a minimização dos dados e a limitação da conservação, restringindo o tratamento somente dos dados pertinentes e efetivamente necessários para os propósitos definidos, tornando a prática empresarial de coletar todas as informações possíveis, para depois definir o uso, evidentemente ilícita.

> Por que tantas informações são coletadas sobre as compras diárias de todos? Porque, como notou um observador, as leis sobre privacidade podem variar de país para país, mas as leis da economia não. As leis da economia da era da informação dizem que a informação tem valor - é um produto que pode ser vendido, como meias, carros e pasta de dente (Henderson, 2006, p. 27 *apud* Basan, 2022, tradução do autor).

> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (GDPR, 2016).

O que se busca por meio da transparência, portanto, é proporcionar que o titular consiga identificar, de maneira cristalina, a legalidade, a legitimidade e a segurança do tratamento de dados pessoais, garantindo a confiança e a compreensão das pessoas a respeito dos procedimentos realizados e, consequentemente, possibilitando o exercício dos direitos dos titulares de dados (Vainzof, 2019, p. 152). “VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (GDPR, 2016).

A segurança da informação é um dos fundamentos primordiais da Lei Geral de Proteção de Dados, afinal, a norma estabelece mecanismos concretos para atender ao imperativo de proteção de dados, que, em última análise, tutela os atributos personalíssimos do titular, como desdobramento do direito fundamental à proteção de dados pessoais.

A definição pormenorizada do tema é mais bem definida no Capítulo VII da Lei Geral de Proteção de Dados, que descreve a segurança e as boas práticas no tratamento de dados, conforme previsão dos artigos 46 ao 51:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei. § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados

> pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. 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.§ 1º 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.§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º 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: I - 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 estejam sob 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; f) 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; eh) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - 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.§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional. Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais. (Brasil, 2020). [B]

## 3.4 Arcabouço normativo harmônico à proteção de dados pessoais como direito da personalidade

Neste tópico se faz necessário reforçar os conceitos e os direitos de personalidade no Código Civil de 2002 a fim de realçar sistematicamente a relação entre as duas normas, quer

seja Código Civil de 2002 e a Lei Geral de Proteção de Dados Pessoais, no que diz respeito ao tema buscando encontrar consonância e harmonia ratificando o reforço da proteção trazida pela LGPD com o chamado "novo direito": o da proteção de dados pessoais. Dados pessoais esses que refletem e representam em sua essência todos os direitos da personalidade.

O surgimento da Lei Geral de Proteção de Dados reverberou e trouxe reflexões ao Código Civil 2002 e, como o ordenamento brasileiro é uno, se faz necessário determinar, de forma sistemática, que possíveis interpretações e alterações ocorreram. A importância de se aprofundar os estudos entre o Código Civil 2002 e a Lei Geral de Proteção de Dados Pessoais na seção de direitos de personalidade é entender a relevância desta correlação para a devida aplicação da novel, principalmente quanto ao livre desenvolvimento da personalidade e à dignidade da pessoa humana, princípios estes diretamente relacionados a um direito fundamental autônomo, descolado da privacidade, e recentemente reconhecido que é o direito à proteção de dados pessoais. Conforme explicitado anteriormente, ratificamos nossa compreensão acerca da autonomia dos dados pessoais frente aos direitos da personalidade.

Nesse ponto, diferencia-se essencialmente do direito à privacidade, sendo um equívoco dogmático indicar a proteção de dados pessoais como uma mera evolução do direito à privacidade (Bioni, 2018, p. 98-99). Em uma sociedade digital, o tratamento de dados tem se tornado cada vez mais expansivo e impacta cada vez mais pessoas e realidades sociais. Nesse contexto, portanto, a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana", por existir um leque vasto de liberdades individuais relacionadas com a proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade, pois este é atrelado a uma divisão das esferas pública e privada de seus titulares (Bioni, 2018, p. 99).

De fato, afirmar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma "construção dogmática falha" que dificulta sua compreensão (Bioni, 2019, p. 99).

Considerando o direito fundamental à proteção de dados pessoais como um direito autônomo e da personalidade, é importante buscar estabelecer a correlação entre o código civil de 2002 e a Lei geral de Proteção de Dados relacionando conceitos e os direitos de personalidade realçando sistematicamente a relação entre as duas normas, quer seja, Código Civil de 2002 e a Lei Geral de Proteção de Dados Pessoais de maneira dedutiva com pesquisas bibliográficas.

A respeito do que é personalidade, reforçando que fora abordado no primeiro capítulo, norte-americano Gordon Allport, (Allport, G. W., 1937) psicólogo que entrou para a história

por estabelecer as bases da psicologia da personalidade, possui uma teoria que é considerada uma das primeiras teorias humanistas por sua concepção do ser humano como um ente autônomo com livre arbítrio. Nela, se definiu a personalidade como sendo a organização dinâmica dos sistemas psicofísicos que determina uma forma de pensar e de agir. Esta organização é única em cada sujeito no seu processo de adaptação ao ambiente.

Ainda sobre a teoria, é possível pensar que o aspecto dinâmico da personalidade se reflete na medida em que cada pessoa está constantemente em interação com o meio envolvente, sendo esta apenas interrompida com a morte.

Relativamente às formas de pensar e de agir, estas mostram que a personalidade tem uma vertente interna (o pensamento) e uma vertente externa (o comportamento). A certeza de que somos únicos e com particularidades que nos traduzem a uma originalidade tão exclusiva e pessoal que não faltam conceitos diante da necessidade de informar essa realidade e a importância deles para se entender, respeitar, proteger e fomentar o livre desenvolvimento das personalidades. Por isso, não é demais trazer aqui também esse raciocínio reforçado por grandes psicólogos que metaforizam a personalidade, como a estrutura ou a silhueta psíquica individual, ou ainda, o modo de ser peculiar do eu. Então, nada mais justo do que tutelar, proteger essa singularidade, também tão importante para as teorias de direito da personalidade.

O Direito Civil sobrepõe-se à personalidade, sobre a singularidade psíquica, física, que faz ser quem se é, o que se é, o manto da personalidade jurídica:

> A personalidade jurídica tem por base a personalidade psíquica, somente no sentido de que, sem essa última não se poderia o homem ter elevado até a concepção da primeira. Mas o conceito jurídico e o psicológico não se confundem. Certamente o indivíduo vê na sua personalidade jurídica a projeção de sua personalidade psíquica, ou, antes, um outro campo em que ela se afirmar, dilatando-se ou adquirindo novas qualidades (Beviláqua, 1999, p. 81).

Assim, é o conjunto das qualidades e atributos singularmente individuais, protegidos por lei. Essas características, que são atributos da personalidade, são, objetivamente falando, informações, dados, que, agrupados ou separados, continuam sendo a base para a projeção psíquica de cada indivíduo. Se a personalidade jurídica é a projeção da personalidade, os dados de cada um são o átomo desse sistema de proteção. Quanto mais atomizado se é, maior, mais ampliada e profunda deve ser essa tutela para abarcar e dar conta de um mundo que está indo cada vez mais fundo para extrair de cada pessoa humana, partículas mínimas: dados para obter informações e gerar conhecimento capaz de conhecer ser humano mais do que ele mesmo. A

finalidade é influenciar, moldar, ensinar, tangenciar, dividir, manipular para, no mínimo, alterar a essência da personalidade até nos despersonalizar cada indivíduo por completo, atendendo ao que vem sendo chamado de economia de dados (Rosenvald, 2021).

A vinculação do código civil no que diz respeito aos direitos da personalidade é tão patente que tais direitos figuram tal qual nos seus fundamentos.

Em seu artigo 17, a Lei Geral de Proteção de Dados Pessoais diz: “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei” (Brasil, 2019). Ou seja, esse texto legal traz a base necessária para a compreensão e a interpretação de que dados pessoais são sim projeções da personalidade, mesmo que não expressamente na Lei Geral de Proteção de Dados e implicitamente no Código Civil, como veremos adiante. Antes, convém deixar claro o que são dados.

Conforme o art. 5º da Lei Geral de Proteção de Dados, o dado pessoal é toda informação relacionada à pessoa natural identificada ou que possa, através “de”, ser identificável. É a partir disto que estão dispostos os direitos dos titulares de dados pessoais. (Brasil, 2019). Dados são códigos (Devlin, 1999). A matéria-prima da informação. De uma maneira simplista, podemos dizer que sozinho ele transmite mensagem e titularidade, afinal, todo dado vem de alguém, de algum lugar a que pertence, embora esteja a ele apenas relacionado, ele transmite a informação e produz conhecimento. Nesse raciocínio, as informações são dados tratados. Pois, quando dados são processados e agrupados, tornam-se informações. Nesse ponto, há um significado, e é possível afirmar ou decidir algo com base nesse agrupamento que não tem limite. Pode ser feito inúmeras vezes, de diversas maneiras, obtendo conhecimentos de toda ordem a respeito de um indivíduo.

Podemos dizer, então, que informação é o conjunto de dados já processados e tratados. Se a informação é um dado trabalhado, conhecimento é a informação trabalhada. Esse é o ponto onde toda informação relevante deve chegar. Por sua definição, conhecimento é o ato de abstrair ideia ou noção de alguma coisa.

> Tomando de empréstimo uma metáfora famosa de outro antropólogo, Claude Lévi-Strauss, poderíamos pensar na informação como o cru, enquanto o conhecimento seria o cozido. É claro que a informação é apenas relativamente crua, visto que os "dados" não são de maneira nenhuma "dados" objetivamente, e sim percebidos pelas mentes humanas, repletas de suposições e preconceitos. Mas o conhecimento é "cozido", no sentido de ser processado. Os processos, discutidos longamente no Capítulo 2, incluem a verificação, a crítica, a medição, a comparação e a sistematização (Burke, Peter, 1937, p. 14).

Tal explanação é importante para voltar à ideia de que dados são átomos, fragmentos, características dos atributos de nossa personalidade, ou seja, de cada um de nós, que reunidos refletem, traduzem a nossa personalidade, podendo deles serem extraídas e informações e ser produzidos conhecimento e a ele atribuído valor no mundo capitalista do extrativismo de dados. Assim, fica mais claro concluir que dados são a essência, o miolo da própria personalidade. E é importante que se entenda que eles, os dados, sempre estiveram ali, sempre existiram e indiretamente já eram protegidos pelo Código Civil, especificamente no capítulo direitos da personalidade. Mas o que mudou é que o ser humano passou a ser explorado de maneira tão profunda, detalhada e demasiada, tão ostensiva, minuciosamente, e até inconsciente, a ponto de uma máquina, ter o potencial de conhecer, reconhecer uma pessoa, e diante de informações atuais, extrair seu passado, influenciar seu presente e poder predizer, categorizá-la e moldar seu futuro, não só em prejuízo do livre desenvolvimento da personalidade individual, mas também coletiva. É o que diz Shoshana Zuboff ao definir capitalismo de vigilância como uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; e ela vai além ao diagnosticar uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento (Zuboff, 2020).

No que implica essa modificação de comportamento, qual dano, fica evidente também nos dizeres dela uma expropriação de direitos humanos críticos, destituindo a soberania do indivíduo, culminando na sua despersonalização. E essa ideia da importância de uma livre personalidade, da proteção desse direito, vem sendo reclamada desde outros períodos da nossa história, como no sistema feudal.

> Esta mencionada promoção do status jurídico da pessoa humana é decorrência imediata de duas tradições, em especial: a do cristianismo, que ao exaltar o indivíduo como ente único, de valor absoluto sejam quais forem suas condições, distinguia este da coletividade e ainda reconhecia seu livre arbítrio; e a das declarações de direitos surgidas em fins do século XVIII, como substrato para realizar a libertação do homem das várias limitações que lhe eram apostas pelo sistema feudal (Doneda, 2005, p. 4-5)

E se sistematicamente o poder econômico do modelo capitalista reivindica liberdades humanas, a proteção dos direitos da personalidade da pessoa humana deve ser revisada, ampliada, alterada, como busca esta pesquisa, a fim de garantir sua tutela efetiva.

Com o regramento do direito à proteção de dados pessoais, hoje há um reforço aplicado e específico da tutela já existente dos direitos da personalidade na perspectiva de ser adequado ao nosso tempo. Faz-se necessário ressaltar essa proteção de maneira cirúrgica contra a ideia capitalista fragmentar da personalidade, encarando os dados pessoais como "átomos pessoais". Porém, o pressuposto sempre existiu. Dessa forma, fica clara a harmonia e o sentido de complementariedade da novel Lei Geral de Proteção de Dados Pessoais em consonância com os direitos da personalidade no Código Civil em vigor.

Mais detidamente, o reconhecimento de proteção à personalidade, o surgimento de um novo direito, deriva de uma composição da psicologia (existencial, psíquico), da sociologia (interação social que traz sentido à criação, reforço de direitos) chancelado pelo direito (civil e proteção de dados pessoais).

O ser humano, visto como indivíduo vivendo sozinho, não teria, em tese, a necessidade de tutelar direitos, mas a partir do momento em que ele se torna um ser gregário, vivendo em sociedade, isso se faz imperioso (Duguit, 1996, p. 25-26.) Assim, há o surgimento da personalidade jurídica, oriunda da necessidade de proteção de características individuais originais, reconhecidas pelas teorias da personalidade. Tais como: imagem, nome, corpo, honra que, em qualquer dimensão, é dado pessoal.

Fazendo uma retrospectiva, há 50 anos, por exemplo, não havia a necessidade de uma lei específica e geral para a proteção de dados pessoais. O que existia era um gatilho para tal norma que expandiu o escopo da personalidade jurídica, ou seja, o leque de direitos, "novos direitos", foi o desenvolvimento tecnológico associado à exploração econômica de informações pessoais. De maneira exemplificativa e comparativa de aspectos relevantes, temos o avanço cultural (sociologia) com o consequente reconhecimento de novos direitos (ex.: casamento gay), que já existia, mas não era reconhecido. De outra forma, a complexificação do tecido da prática social (ex: desenvolvimento tecnológico, gerando novos padrões de interação social como redes sociais, motores de busca, internet das coisas, perfilização com uso da inteligência artificial).

Décadas atrás, pelo menos no Brasil, não havia por parte da sociedade a consciência ou o despertar da necessidade de se reforçar ou estabelecer novos direitos correntes relacionados à tecnologia. As características nomeadamente protegidas pelo código civil, reconhecidas como direitos da personalidade, como nome, corpo, imagem, honra, eram exploradas, utilizadas de maneira até então, se comparado aos tempos atuais, "limitada", mínima e minimizada. Hoje, o que existe é a extração de dados através do avanço da tecnologia que fragmentou, a porções tão mínimas, e aprofundou de tal maneira o conhecimento sobre o indivíduo como se o colocasse

sob as lentes de um microscópio. Alcançando o que antes era invisível ou desconhecido dele mesmo. Mas o indivíduo não mudou. A tecnologia é que hoje existe e que explora ostensivamente, profundamente, ininterruptamente a privacidade, a intimidade, tendo acesso a porções mínimas do ser humano para experiências que não o visam como fim. Mas como meio, instrumento.

> Em junho de 2006, o grupo Telefônica, controlador da operadora Vivo no Brasil, comemorava o lançamento do Vivo Dados Patrocinados, uma troca comercial parecida com promoção. O cliente assistia a um comercial de trinta segundos da Unilever, a patrocinadora da ação, e depois respondia a uma breve pesquisa. Ao final, resgatava a recompensa, um pacote de dados para navegar na internet. Parecia um bom negócio. O que custava, para um adolescente, por exemplo, ver um anúncio de desodorante ou xampu? O problema é que custava. Nos próximos anos, a barganha poderá significar a privacidade desse adolescente. Mas, em 2017, o custo estava estimado em pouco mais de 4.5 dólares. De acordo com a revista inglesa The Economist, esse era o preço médio cobrado pelo Facebook ao anunciante que quisesse entrar na *timeline* de um usuário. Empresas de tecnologia pagam suas próprias contas com os dados que coletam dos internautas - mesmo que eles não saibam - ao vendê-los no pregão do mercado publicitário (Fucuta, 2018, p. 186-191).

A vida se tornou um ambiente *on-life*, onde não é possível coletar e tratar dados pessoais a todo momento, esteja o indivíduo on-line ou offline. Sendo múltiplas as violações a direitos fundamentais, que "acabam por se propagar instantaneamente, em tempo real, geometricamente, na rede mundial de computadores" merecendo atenção pela Ciência Jurídica. (Colombo, 2022, p. 4). Assim, influencia-se a liberdade de pensamento, o direito de ir e vir, a saúde, o comportamento, a própria vida a partir da formação de perfis. A exemplo do uso da biometria para uso de reconhecimento facial, a formação de perfis pessoais, os algoritmos de predição de comportamento, são hoje ditam o que se é, o que se foi e o que o indivíduo deve ser.

> Tudo isso junto pode revelar muito mais sobre sua vida e intimidade do que você gostaria. Um documento publicado pela Unesco, chamado *Global Survey on Internet Privacy and Freedom of Expression*, revela o potencial de devastação do cruzamento dos nossos dados. Existe uma empresa norte-americana que presta serviços de marketing na área da saúde, diz o documento. magine que ela venda listas de pessoas que sofram de doenças como câncer de mama, diabetes ou problemas cardíacos. Combinadas com outros dados - idade. gênero, renda, estado civil. nome e sobrenome -, essas listas seriam puro ouro nas mãos das seguradoras de saúde. Se a moeda desse sistema da pretensa economia de graça é o dado pessoal, todos irão querer obtê-lo (Fucuta, 2018, p. 189).

Como bem deve ser relembrado, computadores, sistemas de comunicação e programação genética são todos amplificadores e extensões da mente humana. O que pensamos e como pensamos é expresso em bens, serviços, produção material e intelectual (Castells, 2020, p. 89). São, então, manifestações de nossa personalidade, bens tutelados juridicamente e ameaçados.

A partir de então, é perceptível a relação direta entre a LGPD e o Código Civil, de forma que essa ligação se dá pela necessidade de reforçar e estender formalmente o manto do guarda-chuva protetor dos direitos da personalidade. A LGPD figura como mais uma camada de proteção para evitar "a despersonalização da personalidade. Que é a expropriação da personalidade, uma ameaça à autonomia humana mediante um ataque à consciência e a conversão do ser humano em um projeto de personalização." (Rosenvald, 2021). E, como bem captura Rosenvald (2021), a visão kantiana do homem como fim em si está sendo desvirtuada por um instrumentalismo cuja base é a expropriação de nossa personalidade em prol de finalidades alheias, pois a própria sociedade se torna objeto de extração e controle. A realidade digital converte situações existenciais em uma nova propriedade baseada na despossessão da essência daquilo que nos define, por meio de uma modificação comportamental cujo legado de danos pode custar a nossa própria humanidade (Rosenvald, 2021). A expropriação da personalidade não é uma nova tecnologia, mas em uma nova forma de mercado que reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais disponibilizados no mercado como produtos de predição que antecipam e modelam comportamentos futuros (Zuboff, 2020).

Voltando ao cerne do estudo, é possível ver de três formas este diálogo de fontes entre o Código Civil e a Lei Geral de Proteção de Dados: ambos zelam praticamente pelos mesmos direitos (da personalidade). A LGPD traz uma ideia de proteção específica e procedimentalizada. Esse diálogo de fontes também está demonstrado na cumulação de sanções em relação à reparação administrativa, na LGPD, e cível, no Código Civil 2002.

O reforço aos direitos da personalidade fica explícito na LGPD, pelo princípio da especialidade e pelo caráter preventivo em ambos os regramentos. Pois, no artigo 12 do código civil, está positivado que "Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei" (Brasil, 2002). E como ressalta Danilo Doneda quanto aos direitos da personalidade, a disciplina não se pretende exaustiva, portanto, podemos vislumbrar o reconhecimento da proteção de dados pessoais. A primeira observação sobre a introdução dos direitos da personalidade no novo Código Civil é a de que o legislador optou por reconhecer

especificamente o que entendeu como o atual estado de evolução jurisprudencial. Ademais, é possível fazer várias outras correlações entre o Código Civil e a Lei Geral de Proteção de Dados no quesito direitos da personalidade, quais sejam, a título de exemplos: imagem, nome, honra, privacidade, intimidade, próprio corpo. Pois todos esses atributos traduzem, refletem dados, logo, o direito à proteção de dados está neles também. Ou melhor, é intrínseco a eles.

Seguindo nessa correlação, ratifica-se a harmonia entre os seguintes artigos das referidas leis.

a) Artigos 1,16,17,18,19 do Código Civil c/c artigo 17, da LGPD;

> Art.1. Toda pessoa (natural) é capaz de direitos e deveres na ordem civil. [...]Art. 16. Toda pessoa (natural) tem direito ao nome, nele compreendidos o prenome e o sobrenome. Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória. Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial. Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome (Brasil, 2002).

Já no artigo 17 da Lei Geral de Proteção de Dados, "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos desta Lei" (Brasil, 2018). Como dados pessoais, leia-se aqui, há direitos subjetivos, inerentes, implícitos e protegidos pelos direitos da personalidade, além do que, o rol de direitos da personalidade no código civil não é taxativo, logo, não há impedimento para seu reconhecimento dessa forma também. E nome, sobrenome, prenome também são dados pessoais.

b) Artigos 20 e 21 do Código Civil c/c artigos 2 e 17 (parte final), da Lei Geral de Proteção de Dados Pessoais.

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes. Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (Brasil, 2002).

Já a Lei Geral de Proteção de Dados Pessoais dispõe em seu art. 2º:

> Art. 2. A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; IV - a inviolabilidade da intimidade, da honra e da imagem; VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Enquanto a parte final do Artigo 17 da Lei Geral de Proteção de Dados Pessoais aborda que "[...] e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos desta Lei." (Brasil, 2018).

c) Art.11 do Código Civil c/c art. 7, I da Lei Geral de Proteção de Dados:

No Art. 11 se delimitam os aspectos inerentes aos direitos da personalidade: "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária." (Brasil, 2002). Mas, pelas exceções dos casos previstos em lei, como diz o Código Civil, e dada a especialidade da Lei Geral de Proteção de Dados Pessoais, temos que podemos tratar dados nas seguintes hipóteses:

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

d) Artigo 12, Código Civil, c/c seção III c/c art. Artigo 52, § 2º, Lei Geral de Proteção de Dados Pessoais que tratam da responsabilidade civil.

Conforme o artigo 12 do Código Civil, "Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei" (Brasil, 2002).

> Art. 42. LGPD 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 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 se equipara 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.§ 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. 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 terceiros. 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 de segurança previstas no art. 46 desta Lei, der causa ao dano. 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. [...] Art. 52, § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica (Brasil, 2018).

e) Art.13 e 14, Código Civil, c/c art. 11, inciso II, alínea f da Lei Geral de Proteção de Dados Pessoais.

> Art. 13. Salvo por exigência médica (física ou psicológica), é defeso o ato de disposição do próprio corpo, quando importar diminuição permanente da integridade física, ou contrariar os bons costumes. Art. 14. É válida, com objetivo científico, ou altruístico, a disposição gratuita do próprio corpo, no todo ou em parte, para depois da morte. Parágrafo único. O ato de disposição pode ser livremente revogado a qualquer tempo (Brasil, 2002).

Complementarmente, o artigo 11, II, f da Lei Geral de Proteção de Dados Pessoais aborda "a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (Brasil, 2018).

f) Artigo 15, Código Civil, c/c artigo 7, da LGPD:

O Art. 15 do Código Civil aborda que "Ninguém pode ser constrangido a submeter-se, com risco de vida, a tratamento médico ou a intervenção cirúrgica." (BRASIL, 2002). Podemos ter, por exemplo, exames de coleta genética para tratamento de câncer. Nesse sentido, o artigo 7º da Lei Geral de Proteção de Dados se coaduna, pois "o tratamento de dados pessoais somente, inclusive relacionados à saúde, só poderá ser realizado nas hipóteses estabelecidas por lei" (Brasil, 2018).

Recapitulando, as pessoas e suas individualidades, as características da sua personalidade, como honra, nome, corpo e imagem, se hoje estão fragmentadas ao máximo, atomizadas e, portanto, indivíduos estão mais expostos e explorados pela economia de dados, por empresas. A ponto desses atributos inatos, antes vistos através de uma lente macro, agora estão sendo vistos por uma lente micro e precisam de mais uma camada de proteção, porque foram alcançados, passaram a ser vistos e explorados.

Porque essa proteção aos direitos se tornou insuficiente. Muitas destas informações pessoais estavam ali, encobertas, embutidas, escondidas, brutas e inexploradas, quiçá inconscientes, e estão vindo à tona à luz de um chamamento por vezes involuntário, sem transparência ou ética, imposto pela interação social que se desenvolve no ambiente da tecnologia. Esta, que apesar de não ser completamente danosa, invadiu, fragmentou e atomizou o ser humano, extraindo dados, que cruzados geram informação e a informação gera conhecimento. O ser humano está exposto e não é sequer solicitado seu consentimento.

Assim, fazer uma correlação dos direitos da personalidade com o direito à proteção de dados, sistematizadamente demonstra que não só a essência dessa proteção, mas de todos os direitos positivados no código civil a respeito dos direitos da personalidade ecoam e

permanecem mais protegidos posto que qualquer atributo da personalidade pode ser traduzido em dados pessoais agora tutelados por lei específica como um novo direito.

# 4 A PROTEÇÃO DE DADOS PESSOAIS E A PERFILIZAÇÃO

## 4.1 A perfilização e a repercussão nos direitos da personalidade

Os avanços tecnológicos nos aproximam cada vez mais do público, tudo é exposto e muitas vezes involuntariamente por parte do indivíduo. É a morte do anonimato com as novas tecnologias capazes de agir a distância e de modo autônomo, transformando seres humanos num "tsunami de dados". Pouco tem restado para a esfera do privado. Com isso, as redes sociais, por exemplo, tornaram-se vitrines da vida particular e tudo o que acontece na Internet permite que o conteúdo exposto seja veiculado para o mundo, em questão de segundos, perpetuando-se independente do caráter do conteúdo. Nesse sentido, se faz relevante e justificável abarcar no direito à proteção de dados pessoais, em especial a figura do *Profiling* (ou perfilização).

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 processo de perfilização envolve o registro dos dados, agregar e monitorar esses dados, identificar padrões, interpretar os resultados e monitorar para checar resultados e aplicar os perfis (Zanatta, 2019).

De maneira mais didática, quando se "alimenta" um banco de dados, que gerencia as contas a receber de uma empresa, os dados pessoais devem ser inseridos corretamente como o nome do cliente, o valor do serviço, da linha de crédito e o endereço. Esses dados são chamados de atributos (Bioni, 2019, p. 55).

Esses dados também são utilizados para tomada de decisão.

> Tal sistema de gerenciamento permite, por exemplo, identificar um fator que será determinante para adoção ou não de uma ação de marketing, como a classificação daqueles clientes que têm maior probabilidade de ser seduzidos por uma "mala direta", ou, por outro tipo de abordagem publicitária. Ou, ainda, no exemplo antes mencionado, se a linha de crédito deverá ser expandida de acordo com a inadimplência acumulada dos clientes devedores (Bioni, 2019, p. 55).

Nessa linha, o perfil de crédito ou *credit scoring* pode ser definido como o processo de atribuição de pontos às variáveis de decisão mediante técnicas estatísticas. Trata-se de

processo que estima a probabilidade de que um cliente com certas características, pertença ou não a um grupo possuidor de outras determinadas características consideradas desejáveis, hipótese em que se aprova um limite de crédito. Essa técnica estabelece uma regra de discriminação de um determinado cliente solicitante de crédito (Vicente, 2001, p.49). Os sistemas de pontuação de crédito estimam a probabilidade de um cliente ser ―bom pagador ou ―mau pagador com base em suas características: ―Existem vários fatores associados à possibilidade de inadimplência. Um modelo de escoragem de crédito combina os fatores mais importantes associados à possibilidade de inadimplência, determina o inter-relacionamento entre eles e atribui números para gerar o e*score* final. A prática tem por objetivo produzir um modelo de escoragem de crédito no qual, em tese, quanto maior for o e*score*, menor será o risco de perda com devedores duvidosos (Gherardi; Ghielmetti, 1997).

O que ocorre é que com a perfilhação de dados pessoais na perspectiva de vida cada vez mais *on-line*, é certo que se pode esperar um prolongamento da pessoa através da utilização maciça dos seus dados ininterruptamente por tecnologias cada vez mais inovadoras.

> O ser humano terá um prolongamento e projeção completa no ambiente digital, sendo todas as suas individualidades datificadas. Problematiza-se, mais ainda, o desafio da tutela dos dados pessoais como um novo direito da personalidade, já que muitos aspectos da vida de uma pessoa poderão ser decididos a partir dessa sua extensão eletrônica (Bioni, 2019, p. 121).

O *Profiling* é uma ferramenta de tratamento de dados pessoais que figura entre as que ostentam o maior potencial lesivo. Desta forma, para fins desse estudo, é importante demonstrar quais são os riscos decorrentes da perfilização, bem como a tutela da privacidade dos dados pessoais nos processos de geração de perfil digital dos usuários da Internet. (Silva, Santos, Jesus, 2021). Pois,

> [...] 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).

Como já mencionado 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 outras palavras: O *score* de crédito é a manifestação quantitativamente sumarizada de resultados de modelos de análises preditivas quanto ao comportamento financeiro do consumidor. O resumo numérico em *score* 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 *score*s, 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 datificado e o consumo de informações produzidas por birôs, veículos, organizações e pessoas comuns".

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". (Doneda, 2019).

Sendo assim,

> [...] 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 (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) (União Europeia, 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 na totalidade é mais utilizado na 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).

A coleta, processamento e compartilhamento de dados acontece sem que se tenha noção do alcance desse monitoramento de cada indivíduo. E essas informações são objeto das empresas que fazem escoragens de crédito que vão além do estabelecido em lei, pois coletam dados indiscriminadamente no mundo on-line partindo para precificações personalizadas, por exemplo, mais conhecidas pelas práticas de *geo-pricing* e *geo-blocking*. Essas duas espécies juntas, consideram a localização geográfica do consumidor, para com base nesses dados pessoais, propiciar precificação algorítmica. No Brasil, à época dos Jogos Olímpicos de 2016, uma empresa formulava preços diversos a partir da localização de onde o potencial consumidor acessava a plataforma. O caso foi alvo de ação civil pública e resultou em multa de R$ 7,5 milhões de reais.

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 segregar 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, 2006). 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 o 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 considera 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 *score*s 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 e*score* 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).

Segundo Doneda, a perfilização consiste na elaboração de perfis de comportamento de uma pessoa (ou de um grupo de pessoas) a partir de suas informações pessoais, que podem ser disponibilizadas por ela mesma ou que são colhidas.

Sendo a única representação de indivíduos para terceiros – inclusive para o próprio Estado –, essas técnicas de previsão de comportamentos, ou de padrões de comportamento, podem significar a diminuição da esfera de liberdade de inúmeros indivíduos (Mendes, 2014).

Por isso, o *Profiling* denota um poder de dano muito severo aos direitos da personalidade se não utilizado com a devida cautela.

O próprio modo de operacionalização do *Profiling* evidencia não só o caráter impessoal dessa ferramenta, mas a fragilidade das regulações existentes. Por isso, é preciso encarar o mecanismo do *Profiling* com franqueza, uma vez que o cerne dele é a discriminação, pois identifica padrões de comportamento e classifica o indivíduo a partir de categorias pré-estabelecidas no contexto de uma economia alimentada por dados pessoais.

Pelo demonstrado, fica patente a potencialidade lesiva aos direitos da personalidade a partir do uso inadequado de dados pessoais. A partir de então passa-se ao estudo mais detalhado do perfil de crédito, posto que é nesse contexto que mais dados são coletados dos indivíduos, alimentando bancos de dados de empresas privadas pelo mundo, muitas vezes compartilhados, transferidos livremente e sem fronteiras.

## 4.2 O perfil de crédito e o dano ao direito da personalidade de proteção de dados pessoais

Dados pessoais podem ser minerados, explorados para obter informações, conhecimento e valor. “Dados pessoais podem ser minerados, explorados para obter informações, conhecimento e valor. Mineração de dados e o tratamento de conjuntos de dados extremamente grandes parecem ser essenciais para quase todas as disciplinas empíricas no século XXI” (Stanford Business, 2022).

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

> Há, no entanto, uma diferença crucial entre o debate jurídico sobre automação da década de 1890 e as discussões atuais sobre o processamento automatizado. O salto tecnológico diz respeito à “lógica envolvida” nesse processamento automatizado. Este último considera cada vez mais uma classe específica de algoritmos que aumentam ou substituem a análise e a tomada de decisões por humanos, como ocorre com a disciplina de aprendizado de máquina, ou seja, algoritmos capazes de definir ou modificar regras de tomada de decisão autonomamente. O segundo passo de nossa fenomenologia está, portanto, relacionado ao campo da IA e, mais especificamente, à mudança crucial da automação para a autonomia artificial (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 como 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, reclamando 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, como diz Bodin:

> [...] uma vez munidas de tais informações (dados pessoais), entidades privadas e governamentais tornam-se capazes de "rotular" e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis. [...] um acervo suficientemente amplo de informações permite a elaboração de perfis de consumo, o que se, de um lado, pode ser utilizado para incrementar e personalizar a venda de produtos e serviços, de outro, pode aumentar o controle sobre a pessoa, desconsiderando sua autonomia e dificultando a participação do indivíduo no processo decisório relativo ao tratamento de seus dados pessoais, de seu patrimônio informativo (Bodin, 2016, p.21).

Considerando, para efeito deste trabalho, o *score* de crédito e esse tratamento de dados para formação de perfis sendo automatizado, termina este por oferecer riscos aos direitos de personalidade através do uso dos dados pessoais. Com os danos decorrentes do uso de dados

pessoais e da discriminação, há desrespeito à dignidade da pessoa humana, à autodeterminação informativa, do consumidor, à privacidade, ao livre desenvolvimento da personalidade.

Estas formas de discriminação podem se materializar na demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado (Rodotà, 2008, p. 70).

Ainda sobre o tratamento inadequado de dados sensíveis que geram discriminação e segregação abusiva no âmbito das relações de consumo.

> Os dados do consumidor podem ser usados para muitos propósitos com os quais os consumidores talvez não concordem tão facilmente, decisões de emprego e classificações por provedores de seguro saúde que excluem ou prejudicam os "desfavorecidos" geneticamente ou medicamente; decisões de emprego ou moradia baseadas em riscos de personalidade percebidos; decisões de emprego ou moradia baseadas em preferências sexuais ou religiosas; e assim por diante (Cohen, 2000, p. 27)[1]

Nessa toada, a formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação "[...] seja porque dados pessoais, aparentemente não "sensíveis", podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas" (Rodotà; 2008, p. 56).

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). Cabe ao Direito regular e promover a responsabilização.

Caso não consideremos a internet um espaço "constitucional", que respeite o ordenamento jurídico infra, podem prevalecer apenas as razões da segurança e do controle, conforme se arrisca acontecer na atualidade. E, de toda forma, prevaleceriam as lógicas de mercado, que já estão impondo regras, visto que a maioria das atividades *on-line* é de tipo comercial e que a Web é considerada uma gigantesca mina de dados pessoais, fatores graças aos quais nasceu uma sociedade da vigilância e da classificação (Rodotà, 2008).

---

[1] Texto original: "*Consumer data can be used for many purposes to which consumers might not so blithely agree, employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have-nots*; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences; and so on*".

Dados pessoais como projeção da personalidade traduzem uma nova identidade. Relembrando personalidade como as características ou o conjunto de características que distingue uma pessoa da outra. Os direitos da personalidade seriam os caracteres incorpóreos e corpóreos que conformam a projeção da pessoa humana. A exemplo, nome, honra, integridade física e psíquica seriam apenas alguns dentre uma série de outros atributos que dão forma a esse prolongamento. E a ciência jurídica o protege das agressões que afetem a sua individualidade. Nessa lógica trata-se de conferir tutela jurídica aos elementos que emprestam conteúdo ao valor-fonte do ordenamento jurídico, aos bens (da personalidade) que individualizam o sujeito perante a sociedade.

Analisando sob a perspectiva do dado relacionado à esfera de uma pessoa, pode-se inserir dentre os direitos da personalidade. Dado como "pessoal" é uma projeção, extensão ou dimensão do seu titular. E cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. A ponto de poder se dizer que circula no mundo *on-line* um avatar pessoal. O seu perfil. A sociedade e a economia se orientam e movimentam a partir desses signos identificadores do cidadão. E na maioria das vezes isso não é uma escolha pessoal pela datificação do humano e sua impossibilidade de ter inclusive acesso a direitos e serviços se não estiver no mundo on-line.

> Os dados pessoais refletem um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações. Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação de seus dados pessoais para que a sua projeção seja precisa. Por isso, os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade. Tal construção dogmática é útil, pois é tal ampliação normativa que assegura o direito à retificação e de acesso aos dados e outras posições jurídicas próprias do direito à proteção dos dados pessoais (e.g. direito de revisão de decisões automatizadas) (Bioni, 2019, p. 99-100).

Na técnica de perfilhamento dados são algoritmicamente processados produzindo um provável perfil e a obscuridade dos processos decisórios dificulta ainda mais a transparência do processo para que o indivíduo vulnerável possa se defender. Afinal, se esses dados pessoais não estão corretos, as chances de erro e de dados manipulados refletem o potencial discriminatório que eles podem ter. Mas para exemplificar há casos emblemáticos de perfilhamento de cidadãos que lhe causaram danos.

O caso Kyle Behm. O cidadão teve problemas para encontrar um emprego após ser diagnosticado com transtorno bipolar. Porém, apesar de resultados quase perfeitos na prova SAT, a qual é uma versão americana do chamado vestibular no Brasil. Behm entrou com um processo contra sete companhias pelo uso de um teste de personalidade desenvolvido pela Kronos, uma empresa de gerenciamento de força de trabalho, por entender que o responsável por sua dificuldade de ser recolocado no mercado era o algoritmo (Mendes; Mattiuzzo, 2019).

O caso Loomis no COMPAS. A *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS). É uma ferramenta pensada para o gerenciamento de penitenciárias a partir de "informações sobre gestão de detentos críticos", que avalia a saúde mental dos detentos até o rastreamento de gangues. Conforme a *Equivant,* empresa que desenvolveu o COMPAS, a ferramenta funciona a partir de uma árvore decisória, técnica de inteligência artificial, onde os algoritmos classificam os detentos em um grau de risco que varia de um a nove, sendo nove o mais alto e um o mais baixo. Porém, o algoritmo passou a ser utilizado também para avaliação do risco de reincidência. Em 2013, Loomis foi acusado de fugir da polícia na Cidade de La Crosse ao dirigir um carro anteriormente utilizado em um tiroteio e como Loomis tinha sido condenado previamente por agressão sexual e, após uma avaliação do COMPAS, considerou-se com base nessa probabilidade de reincidência, que ele possuía alto risco de cometer outro crime. Assi, Loomis foi condenado a uma sentença de seis anos. O caso não foi revertido nem na Suprema Corte, mesmo a defesa alegando que não houve acesso à defesa da avaliação de risco realizada pelo COMPAS.

Outros dois casos relatam os malefícios do perfilamento (*profiling)* com uso de dados pessoais que geraram tratamento discriminatório. Os casos ocorreram nos EUA e se referiram a contratação de serviços médicos e de seguridade (consumidor).

No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez. Em outro caso, relacionado a dados de saúde, "quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados" (Mulholland, 2018).

O caso de racismo algorítmico no e*score* de crédito brasileiro. O Ramon Vilarino, pesquisador que se preocupa em usar computação para desenhar políticas públicas que construam justiça social, trabalhou construindo modelos de inteligência artificial na Serasa e no Nubank (Vilarino, 2022). Ele testemunhou que para explorar as possibilidades de produzir

aplicações acessíveis aos consumidores seria necessário utilizar o *SHAP values. Ou seja,* 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 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 utilizando 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.

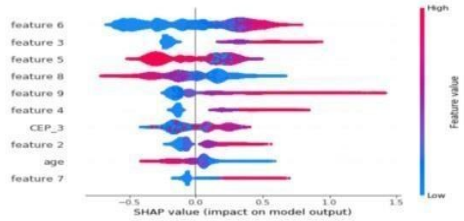


Figure 6: Summary of feature impacts over the dataset. For example, typically, high values of "age" drive the probability of default down (and the credit score up), while low values of "age" do the opposite.


Figure 7: Empirically estimated $E[\phi_{\text{CEP-3}}(f, \mathbf{x})|\text{CEP-3}]$


Figure 8: Self-declared not-white proportion by CEP-3

Figura 3: Mapa de modelo que resultou em Discriminação algorítmica no Brasil
Fonte: Ramon Vilarino (2022).

Corroborando com o 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).

Em 1995, 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 (Brasil, 1995).

Por outro lado, no julgamento do Recurso Especial 1.457.199-RS, além de definido o que é o *score* de crédito, a jurisprudência define a natureza da relação de consumo do *score* de crédito 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 (Brasil, 2014).

Esse risco de perfil de crédito é maior atualmente, inclusive, porque se pode usar os chamados dados alternativos para a perfilização. 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 *score*s 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).

Esses dados oferecerem riscos de discriminação, de quebra de equidade no tratamento de consumidores pertencentes a grupos desprotegidos pela descontextualização de determinadas informações, como, por exemplo, um perfil de "moradores de áreas subvalorizadas" (carentes). Há também riscos de transparência, pois o consumidor não sabe como essa informação compôs a base de dados, gerando prejuízos de acesso ao crédito e ao direito da personalidade. Outro fator é 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, aumenta a hipótese de vazamentos de dados (Silveira, 2022, p. 280).

Na proposta de regulamento de inteligência artificial da União Europeia, o sistema de cumprimento para a qualidade dos dados propostos 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 (União Europeia, 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 c 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 assistência social, dentre 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).

O caso de perfilhamento *Quanticast,* a seguir, ilustra como o ser humano consumidor virou um objeto, uma fonte inesgotável de dados pessoais, diz *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 sociedade civil em geral a responsabilizar ainda mais essas indústrias (Carriere-Swallon; Haksar, 2019, tradução nossa).

Segundo Carriere-Swallon e Haksar (2019), é grande 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) (Calçado, 2015). A ideia era que através do design seria possível prover experiências mais ricas, mas isso iria requerer dados ricos, o que significaria 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 a que o indivíduo não tem acesso e nem tem consciência do tanto de informações a seu respeito são coletadas. 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 estão todos os produtos (dados), fornecedores (fontes). Porém, o consumidor só tem acesso ao pouco que está em exposição pela loja, após passar por um filtro de seleção.

A captura de tela (deliberadamente) feita pelo Frederike (borrada abaixo) mostra como isso traz tantas informações pessoais sobre 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 (Privacy International, 2018).


Figura 4 - Uma captura de tela do PI de solicitação de acesso do titular dos dados
Fonte: Privacy International (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) (Privacy International, 2018).

A situação relatada demonstra um caso concreto de como a coleta de dados pessoais em rede é onipresente pelo fluxo contínuo, tendo sido desenvolvidos algoritmos que podem conectar conjuntos de dados para permitir análises muito mais amplas e profundas do que antes (Provost; Fawcett, 2016, p. 2).

E essas análises podem inclusive ser feitas 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 visa 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 (artefatos como refrigeradores inteligentes, relógios, aparelhos celulares) interagem uns com os outros e processam as informações/dados em um contexto de hiper conectividade. O atual cenário de hiper conectividade 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 no qual 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).

O caso de perfilhação e monitoramento *Amazon Echo*. Outro exemplo é o sistema da *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; Fawcet, 2016, p. 2).

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 *score* 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).

Refletir sobre a possibilidade de o uso desses dados pessoais serem usados para discriminar alguém a partir da criação de perfis automatizados, com base na utilização de algoritmos é prevenir danos e proteger pessoas. “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; Fawcet, 2016, p. 298). Ou seja, os fins passam a justificar os meios levando à perda de uma visão ética.

No caso do *Score* de Crédito, em que se aprofunda esse trabalho, é possível compará-lo com um método de formação de perfil, posto que é uma função estatística matemática (algorítmica) que atende às variáveis (parâmetros) com a meta para atender o objetivo de formular uma nota de pontuação de crédito relativa a alguém com base em informações pessoais a partir de fontes de dados. O que tem base na jurisprudência “A utilização de score 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 afirmar também, de que o *score* de crédito é um algoritmo de inteligência artificial utilizado para minerar dados no sentido de que minerar é: “a busca de

correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados (no caso, dados pessoais), com o auxílio de instrumentos estatísticos e matemáticos" (Doneda, 2006, p. 176). Ademais, a escoragem de crédito depende da qualidade dos dados pessoais coletados a respeito do seu titular. Dados incorretos produzirão efeitos potencialmente danosos.

Tendo como exemplo a captura dos dados de navegação dos consumidores pode ser robustecida por metadados (a partir dos chamados *cookies*), em conjugação, ainda, com dados pessoais usualmente cadastrais, coletados para o fim de, traçando o perfil do potencial consumidor, viabilizar a elevação ou redução do preço final do produto, ou serviço que lhe é apresentado, maximizando lucros. O potencial de discriminação de preços, condições negociais, qualidade e quantidade e outras informações relevantes, nessas práticas, depende de variáveis complexas e dos substratos valorados (com maior ou menor 'peso') pelos algoritmos que operacionalizam a coleta e o processamento de dados (Araújo; Santos, 2022, p. 83).

Ressalta-se que não se pode o titular de dados ficar submisso a esses dilemas do consumidor na era da tecnologia. Pois ela 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 que se apropria da vida humana numa exploração lucrativa, levando ao novo eu-colonizado, alterando sua essência, modulando seu comportamento, expropriando-o (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 maneira ética o avanço da tecnologia e da inovação frente aos desafios impostos aos direitos da personalidade.

Lembre-se de que a função dos direitos da personalidade é promover e assegurar o valor-fonte do ordenamento jurídico, a pessoa humana que se encontra respaldada por um sistema ou uma cláusula geral de proteção e que está ameaçada em sua essência. Essa orientação da pessoa como valor -fonte é energizada pela concepção de um direito privado despatrimonializado ou repersonalizado (Bioni, 2019, p. 99).

As novas tecnologias trazem novos desafios a esse respeito. Por isso, necessário se faz revisitar constantemente os direitos da personalidade para se aperfeiçoar a busca incessante e mutável da tutela da pessoa humana.

## 4.3 A regulação e a proteção de dados pessoais

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).

Para 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 até 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 qual todo o tipo de informação circula sem a necessidade de interação física do ser humano (Gibson, 1984).

Há quem defenda que 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, sobretudo na Europa, dados os altos riscos à personalidade humana. Pois, nessa lógica, a inteligência artificial se utiliza de algoritmos alimentados por bases de dados pessoais. Como vem sendo dito desde o primeiro capítulo dessa pesquisa, esses dados são coletados de inúmeras fontes conhecidas e desconhecidas no grande mundo interconectado do ciberespaço: Internet das coisas, redes sociais, sites, cookies (arquivos de texto que perseguem o usuário num rastreamento on-line) o que torna isso um problema. Uma forma de governança de algoritmos está na regulação dos dados que o alimentam e no 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).

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 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 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). Mas isso não quer dizer que essa falta de alternativa seja fatal. Posto que cada Estado e seu ordenamento infra, há que operacionalizar seu sistema de proteção para prevenir e combater danos a direitos.

A prática de *score* 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 foi aprovada em 2023. Nesse caso, o *score* baseado em coleta de dados comportamentais para classificação de credibilidade pelas autoridades públicas ou por organizações em seu nome (concessão de crédito como política pública) fica expressamente proibido.

No Brasil, continua pendente de regulamentação o Marco Regulatório da Inteligência Artificial. O Projeto de Lei 2.338/23 está em fase de tramitação. Ele 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 como a centralidade da pessoa humana, igualdade, não discriminação, livre desenvolvimento da personalidade, privacidade, proteção de dados, autodeterminação informativa e defesa do consumidor, além de princípios e diretrizes e conceito de inteligência artificial que também se aplicam

logicamente, ao *score* de crédito. Sendo a atividade, pela técnica de inteligência artificial aplicada, taxada como de alto risco.

> Art. 17. São considerados sistemas de inteligência artificial de alto risco aqueles utilizados para as seguintes finalidades:
> V - avaliação da capacidade de endividamento das pessoas naturais ou estabelecimento de sua classificação de crédito.

E há interconexão do Projeto de Lei em comento com a 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. 1º 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).

# 5 A RESPONSABILIDADE CIVIL PELO DANO AO DIREITO DE PERSONALIDADE DE PROTEÇÃO DE DADOS PESSOAIS

## 5.1 A responsabilidade civil no Código Civil

A Lei Geral de Proteção de Dados Pessoais, o Código de Defesa do Consumidor, estabeleceram 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 estudado no capítulo anterior, refletido no perfil de crédito, demonstra-se a caracterização, em grande medida, de danos extrapatrimoniais.

Entre os desafios atuais no ordenamento jurídico brasileiro para a proteção da pessoais no uso de algoritmo de inteligência artificial para formulação do perfil 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 danos como a discriminação.

Verificaremos se 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 socorram a sociedade antes de criar 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, reestabelecendo o "*status quo*" para os novos tempos. A era da chamada Quarta Revolução industrial se socorre da instrumentalização do ser humano e exposição a riscos indetectáveis em sua totalidade através do uso de seus dados pessoais (no sentido da projeção da personalidade) ininterruptamente e de maneira onipresente para ampliar o lucro (Schwab, 2016).

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 que há posto para, em um segundo momento, sendo necessário, buscar a regulação complementar. Pois, como diz Medon (2022, p.522), "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.

A regra geral estabelecida pelo Código Civil brasileiro – art. 927 - reza que "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).

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 (Rosenvald, 2021), 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 haver o pleno desenvolvimento onde a responsabilidade civil pode e deve operar. É ter que responder à emergência de novos danos para a responsabilidade jurídica poder 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 à *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. Um direito de cláusulas gerais que rejuvenesçam constantemente o sistema. A própria realidade tratou disso, como exemplifica Rosenvald, com propriedade, nas seguintes observações a partir do Código Civil:

> 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 extraem novas interpretações e 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).

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).

Tendo em conta que os direitos fundamentais possuem uma categoria específica de direitos que dizem respeito aos valores essenciais da pessoa humana, sendo 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. Silva (1995, p.466) entende que:

> 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 passa pela prevenção do acto ilícito lesivo, e não pela repressão e remedeio da violação.

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 *responsibility* é o sentido moral da responsabilidade. Independe de convenções ou lei. Há a aceitação voluntária como um guia pessoal para a 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 (2022, p.26), 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. 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, CC/02) 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 que na *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 ao nível de demonstração das medidas adotadas para o cumprimento das normas (Bioni, 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. Ressalta-se que 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 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 por meio 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 r*esponsibility* 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.

## 5.2 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 para a 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, 2021, p. 3)

Esses riscos e consequentes danos aos direitos da personalidade recaem no maior repositório das mazelas do ordenamento jurídico, qual seja, a responsabilização civil.

> No direito privado, central é o conceito de responsabilidade civil. A rigor, o direito das obrigações, no qual se situa a disciplina da responsabilidade civil, estrutura-se sobre a relação entre dever/débito e responsabilidade. [...] O objeto da relação obrigacional de responsabilidade civil será sempre o de dever de indenizar, aí entendido como o dever de responder com seu patrimônio pela reparação do vitimado dano ao qual se lhe imputa responsável (Miragem *et al*., 2021, p. 3-4).

E no caso da proteção de dados pessoais, 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 com seu sistema de responsabilidade civil pelo tratamento irregular dos dados pessoais, a socorrer a sociedade.

"Sistema de alarme com sensores que, apesar de não especializados, funcionam por toda a sociedade." (Habermas, 1992, p. 359 *apud* Silva, 2001). A esfera pública enquanto um sistema de detecção de problemas sociais, segundo Habermas, tem uma concepção de que é igualmente capaz de problematizar questões por si detectadas e identificadas. Mas para que se desempenhe corretamente esta função, a esfera pública deverá tematizar os problemas sociais, apresentar possíveis soluções e dramatizá-los de modo 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, conforme 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, poder 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 devido a 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.

### 5.2.1 Responsabilidade Civil subjetiva ou objetiva

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 xeque 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 (2022) 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, conforme quadro abaixo, a responsabilidade é objetiva; na segunda versão 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 Câmara dos Deputados. E na redação final da Lei Geral de Proteção de Dados Pessoais eliminaram-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:

Tabela 2 - Comparativo entre os textos que deram origem a LGPD 1

| 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 | 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-sea 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. | a efetiva indenização 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. |

Fonte: Bioni (2022).

Tabela 3 - Comparativo entre os textos que deram origem a LGPD 2

| 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 | Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer | 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 | § 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 |

| | | | |
|---|---|---|---|
| dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei. | hipótese, independente de culpa. | alegação, houver hipossuficiência para fins de produção de prova ou quando a 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 | hipossuficiência para fins de produção de prova ou quando a 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, 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. |

| | | | |
|---|---|---|---|
| | | responsáveis, na medida de sua participação no evento danoso. | |

Fonte: Bioni (2022).

Analisando os quadros, a retirada desses elementos textuais pode significar que o legislador preferiu deixar a lei com possibilidades de interpretação da responsabilidade civil, considerando as transformações sociais advindas da Internet, por exemplo, e seus riscos de danos digitais. O que, aparentemente, demonstra uma prudência legislativa. Pois, "o estágio atual da responsabilidade civil pode justamente ser descrito como um momento de erosão 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).

Sobre a desnecessidade ou perda de importância da prova do nexo causal, para Mulholland basta a presunção da causalidade em determinadas situações que envolvem atividade de risco, por exemplo (Mulholland, 2018).

A "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 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 de 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 no 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 *responsibility* é um norte *ex ante* para a Lei Geral de Proteção de Dados enquanto 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 na totalidade.

> 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 princípio 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). A partir, então, de um contexto de hiperconexão 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 estejam sob 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 possuir um caráter prescritivo sobre como se deve proceder, da conduta aos mecanismos de lançar mão para cumprir a lei, o princípio ainda carrega consigo uma alta carga retórica. Especialmente quando ele é interpretado 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 conforme a lei. Em vez de enxergar *accountability* apenas como um fim em si, 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, conforme prescreve a lei. Ou seja, É garantia aos titulares a obtenção de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, conforme o art. 6º, 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 renunciar a 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, independe da classificação binária da responsabilidade subjetiva ou objetiva. Isto porque, é a extensão do dano e o quanto se concorreu para esse resultado que definirá 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 de 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 pressupõe 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.

Assim, tem-se 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 trata de espécies diferentes. E, sendo a Lei Geral de Proteção de Dados Pessoais uma norma nos quais 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 para 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*. Ela 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, 2023).

> 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 hípervulnerável (Bioni, 2019, p. 165).

No mais, o microssistema da Lei Geral de Proteção de Dados, com normas também previstas em outras leis, 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).

Também se extrai do parágrafo 2 do artigo 42, a noção de risco-proveito. O ônus da prova em eventos decorrentes do ilegal tratamento dos dados pessoais chama a atenção para a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais que 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-proveito ainda dá pistas 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 constatação 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 o elemento do dever de reparar com a inversão do ônus da prova rompe os diques do modelo subjetivo. Sobre isso, algumas leis podem 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). Todas elas em harmonia com a Lei Geral de Proteção de Dados Pessoais, conforme previsto no §3º do art. XX.

> § 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 parágrafo terceiro, que 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 lido 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 3º e 4º, 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 deixar claro tais excludentes caso sejam demandados. Para isso, é necessário cumprir o prescrito nos artigos 50 e 51 da Lei Geral de Proteção de Dados Pessoais, utilizando-se os agentes do exercício regular de direito (art.188, inc. 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 a serem exploradas: fato exclusivo do titular dos dados (vítima) e fato exclusivo de terceiro. Sendo esta última, uma excludente que abarca qualquer terceiro, como clientes, colaboradores, fornecedores, prestadores de serviço que porventura tenha acesso (art.5, inc. 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, seja ele pessoa física ou jurídica (ANPD, 2021). Dessa forma, o terceiro sendo ele o encarregado de dados ou não, em consonância com a 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, 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 de segurança 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).

### 5.2.2 Responsabilidade civil dos agentes de tratamento

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; Faleiros Júnior, 2019, p. 85).

## 5.3 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, principalmente no Brasil e na Europa. 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 a proteção de dados pessoais como direito da personalidade, 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. Ainda, a conexão e 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 perfilhamento, assim caracterizado o *score* de crédito como

uma de suas modalidades, para ratificar o direcionamento do estudo e trazer mais elementos argumentativos, conectando-o ainda mais com o ordenamento e com a sua natureza dentro do conceito gênero de inteligência artificial. A partir de então, de maneira conjugada e harmônica, contribuir para a designação da responsabilidade civil na formação e compartilhamento de dados dos consumidores por desvio de finalidade da proteção ao crédito no uso do *score* para fins discriminatórios ao consumidor.

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; Oms 202, p. 88).

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, 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 ocorre 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, crese 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 (Mendes; Mattiuzzo, 2019, 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 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 determinante. 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. Então, vejamos, a partir da *responsibility, accoutability, answerability* e como última ratio, a *liability* no intuito de se alcançar uma responsabilidade civil mais lastreada na ética, na prevenção do que no dano em si (União Europeia, 2021). Assim, a partir da Lei Geral de Proteção de Dados Pessoais, que em seus fundamentos protege a pessoa em seis, dos seus sete incisos no artigo 2º.

> 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. (Brasil, 2018).

Uma das formas de proteção é o agir de boa-fé (uma manifestação moral, *responsibility* 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 não pode ser 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). 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 – como falta de transparência, negativa de acesso, opacidade das decisões automatizadas, coleta de dados sensíveis, falta de qualidade dos dados, resultando em práticas discriminatórias expressam clara falta de conformidade (*compliance*) com a Lei Geral de Proteção de Dados Pessoais.

Como exemplo, resgate-se o caso já mencionado 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. Sem conformidade. Considerando 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*. Alegou-se ainda 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 mediante 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 proteção de 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 o cumprimento 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 de o 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 outra forma, 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 pela IA, 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 como no caso do PL 2338/23, em seu artigo 10, que prevê a possibilidade de intervenção ou revisão humana por meio, por exemplo, da geração de perfis. A revisão humana também 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 propositalmente 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 aos sistemas 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 ação ou 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 de 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 relacionam-se claramente 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. Trata-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).

Como estratégia para minimizar e mitigar danos, a risquificação é utilizada no bloco europeu e no AI Act., projeto de inteligência artificial do bloco econômico, há uma proposta de classificação ainda mais detalhada de risco de tecnologias. O risco varia de altíssimo a 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, conforme 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) [B] 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.

Segundo 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).

No Brasil, como a Lei Geral de Proteção de dados Pessoais não estabelece claramente a exigência do relatório de impacto, os quatro maiores birôs de crédito que atuam no país – Serasa Experian, Boa Vista, SPC Brasil e Quod, 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 pessoais (sensíveis, 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*.

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 usados 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 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 2338/2023, em trâmite, que trata da regulação de inteligência artificial no Brasil. Em nove capítulos, o projeto prevê avaliação de riscos, responsabilização dos agentes envolvidos e direitos de pessoas eventualmente afetadas pela Inteligência Artificial. Ainda descreve as obrigações da autoridade

competente para fiscalizar, e sugere, em caso de infração às regras, multa de até R$ 50 milhões para pessoas físicas e de até 2% do faturamento de empresas. O PL considera a atividade de perfil de crédito de alto risco em seu artigo 17. Dessa forma, a responsabilidade correspondente será a objetiva.

> Art. 29. As hipóteses de responsabilização civil decorrentes de danos causados por sistemas de inteligência artificial no âmbito das relações de consumo permanecem sujeitas às regras previstas na Lei n° 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), sem prejuízo da aplicação das demais normas desta Lei.
> Art. 27. O fornecedor ou operador de sistema de inteligência artificial que cause dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema.
> § 1° Quando se tratar de sistema de inteligência artificial de alto risco ou de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano.
> §2° Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

Por fim, através da *responsibility*, há formas de conceber uma abordagem ética e de boa-fé que contamine todo o sistema de gestão de dados. Laudelina Pereira e Tarcízio Silva, demonstram por meio de pesquisa feita no site reclame aqui e na rede social Twitter, como a falta de transparência e opacidade algorítmica refletida mediante reclamações nesses ambientes por parte dos consumidores, revelam os sentimentos de discriminação e injustiça diante da falta de ensinamentos, de discussões que promovam 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, não apenas com foco na reparação pecuniária, mas na perspectiva de se agir também preventivamente, e com precaução para evitar o dano, vem a ser essa proposta a que mais se mostrou adequada ao atual cenário de riscos e danos.

# 6 CONSIDERAÇÕES FINAIS

A crescente e onipresente utilização de dados pessoais somada ao argumento da necessidade destes para o 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 por meio do compartilhamento entre as empresas restou configurado 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 e as decisões automatizadas ficam demonstradas que são a base da estratégia para o desenvolvimento econômico mundial. Como exposto no presente trabalho mediante 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-os em tempo real, mínimos detalhes dos comportamentos humanos nas diversas áreas. Nada fica de fora da vigilância onipresente: educação, da saúde, ambiente profissional, de consumo para uso financeiro - como apontado nos sistemas de perfilização de crédito. O uso de dados alternativos ensejando inferências discriminatórias, equivocadas ou desatualizadas, afetando o acesso ao crédito, é patente. A utilização do perfil de crédito, ou *score* de crédito, numa relação de causa-consequência trouxe à baila das discussões legais e reivindicações da sociedade, principalmente acerca da natureza dessa técnica de inteligência artificial, do vício do consentimento (sem transparência) como ferramenta ineficaz diante da incapacidade de gerir, apenas através dele, a autodeterminação informativa. Dessa maneira, carece o consumidor de ter o direito a tratamentos mais transparentes com respeito aos dados pessoais utilizados nos novos métodos de avaliação do crédito. Este supostamente 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 um 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 permitido 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 *Responsibility, 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 a 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 de 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 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 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 objetiva.

Conclui-se 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


ABRAFI. **Carta aberta às Autoridades: Pela imediata segurança jurídica no tratamento de dados pessoais**. [*S. l.*]: ABRAFI, 2018. Disponível em: http://www.abrafi.org.br/js/ckeditor/foto_internas/CartaabertaasautoridadesLGPDeSegurancaJuridica_VF15.pdf. Acesso em: 09 abr.2022.

ALLPORT, G. W. **Personality**: a psychological interpretation. New York: Holt, 1937.

ARAÚJO, Lourenço Ribeiro Grossi; SANTOS, Yuri Alexandre dos. The Role Of Error In Machine Learning And The Law: Challenges And Perspectives. *In*: PARENTONI, Leonardo; CARDOSO, Renato César. **Law, technology and innovation**. Belo Horizonte: Expert Editora Digital, 2021.

ARNAUD, André-Jean. **la gouvernance**: un outil de participation. [*S. l.*]: Lgdj, 2014.

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

ASCENSÃO, Jose Oliveira. **Direito Civil**: teoria geral 1. Saraiva: São Paulo, 1997.

ASIA-PACIFIC ECONOMIC COOPERATION. **Privacy Framework**. [*S. l.*]: CTI Sub-Fora & Industry Dialogues Groups, 2005. Disponível: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework. Acesso em: 20 mar. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**. Rio de Janeiro: ABNT, 2021.

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

BASAN, Arthur Pinheiro. Disposições preliminares: Art. 6. *In*: MARTINS, Guilherme Magalhães, LONGHI, João Victor Rozatti, FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados Pessoais**: Lei 13.709/2018. Indaiatuba: Editora Foco, 2022.

BASAN, Arthur Pinheiro; BONNA, Alexandre Pereira. **Comentários à lei geral de proteção de dados pessoais**. Indaiatuba: Editora Foco, 2022.

BAUMAN, Zygmunt. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2008.

BELTRÃO, Silvio Romero. Direito da personalidade: natureza juridica, delimitação do objeto e relações com o direito constitucional. **Revista do Instituto do Direito Brasileiro**, [*s. l.*], ano 2, n. 1, 2013. Disponível em: https://www.cidp.pt/revistas/ridb/2013/01/2013_01_00203_00228.pdf. Acesso em: 13 mar. 2023.

BELTRÃO, Silvio Romero. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2014

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

BENNETT, C.J. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, *In*: AGRE, Philip; ROTENBERG, Marc. **Technology and Privacy**: The New Landscape. Cambridge: MIT, 1997. p. 99-124.

BENNETT, Colin; RAAB, Charles. **The governance of privacy: policy instruments in global perspective**. Cambridge: MIT, 2006.

BERTONCELLO, Franciellen. **Direitos da personalidade**: uma nova categoria de direitos a ser tutelada. 2006. Dissertação (Mestrado em Direito) - Centro Universitário de Maringá, Maringá, 2006.

BEVILÁQUA, Clóvis. **Teoria Geral do Direito Civil**. São Paulo: RED Livros, 1999.

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

BIONI, Bruno; SILVA, Paula; Pedro, Martins. 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. **Cadernos Técnicos da CGU**, Brasília, DF, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504/284. Acesso em: 16 nov. 2022.

BITTAR, C. A. **Os Direitos da Personalidade**. 8. ed. São Paulo: Saraiva, 2015.

BITTAR, C. A. **Os Direitos da Personalidade**. 8. ed. São Paulo: Saraiva, 2015.

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

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

BORGES, Roxana Cardoso Brasileiro. **Disponibilidade dos direitos da personalidade e autonomia privada**. São Paulo: Saraiva, 2005.

BRAGA, Jeffeson Oliveira; FERREIRA, Rafael Freire. **Direito, economia e tecnologia: ensaios interdisciplinares**. Goiânia: Editora Espaço Acadêmico, 2019.

BRASIL 2021. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas**. Brasília, DF: Agência Câmara de Notícias, 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.

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

BRASIL. **Ação Direta de Inconstitucionalidade 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. Câmara dos Deputados. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados**. Brasília, DF: Câmara dos Deputados. 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: 19 abr. 2022.

BRASIL. Câmara dos Deputados. **Lei Geral de Proteção de Dados Pessoais completa quatro anos com avanços e desafios**. Brasília, DF: Câmara dos Deputados, 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.

BRASIL. Câmara dos Deputados. **PL 4374 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. Brasília, DF: Câmara dos Deputados, 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2261130 Acesso em: 3 set. 2022.

BRASIL. Câmara dos Deputados. **Projeto de lei PL 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. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao-2052488. Acesso em: 21 mar.2021.

BRASIL. Congresso Nacional. **Medida Provisória n° 954, de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística… Brasília, DF: Presidência da República, 2020. https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619/pdf. Acesso em: 20 ago. 2022.

BRASIL. **Decreto n. 6659**. Brasília, DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6659.htm. Acesso em: 14 de maio. 2021.

BRASIL. Lei nº 10.406 de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 20 out. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. 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 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 abr. 2022.

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

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Brasília, DF: Presidência da República, 2020.

BRASIL. **Projeto de Lei 2.796 de 1980**. Brasília, DF: Diário do Congresso Nacional, 1980. Disponível em: https://imagem.camara.gov.br/Imagem/d/pdf/DCD23ABR1980.pdf#page=19. Acesso em: 10 nov. 2020.

BRASIL. **Projeto de Lei 4.365 de 1977**. Brasília, DF: Diário do Congresso Nacional, 1977. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 10 nov. 2020.

BRASIL. **Projeto de Lei nº 3.514, de 2015**. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1414594&filename=Avulso%20PL%203541/2015. Acesso em 10 set. 2021.

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. **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. **Recurso Especial nº 1.457.199 - RS (2014/0126130-2)**. Recurso Especial Representativo de Controvérsia (Art. 543-C do CPC). Tema 710/STJ. Direito do Consumidor. Arquivos de Crédito. Sistema "Credit Scoring". Relator: Ministro Paulo de Tarso Sanseverino, Brasília, DF: STJ, 2014.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **TJDFT determina suspensão de venda de dados pessoais pelo Serasa**. Brasília, DF: TJDFT, 2020. https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/novembro/tjdft-determina-a-suspensao-de-venda-de-dados-pessoais-pelo-serasa.

BUCHINER, Benedikt. **Informationelle Selbstbestimmung im Prioatrecht**. 2006.

BURKE, Peter. **Uma história social do conhecimento II**: da Enciclopédia à Wikipédia. Tradução Denise Bottmann. Rio de Janeiro: Zahar, 2012.

BYGRAVE, l. **Data Protection Law**: Approaching its Rationale, Logic and Limits. Toronto: Information and Privacy Commission, 2002.

CALÇADO, Phil. **The back-end for front-end pattern (BFF)**. [*S. l.*: *s. n.*], 2015. Disponível em: http://philcalcado.com/2015/09/18/the_back_end_for_front_end_pattern_bff.html

CANOTILHO, José Gomes. Omissões normativas e deveres de proteção. *In*: DIAS, Jorge de Figueiredo (coord.). **Estudos em homenagem a Cunha Rodrigues Coimbra**: Coimbra Editora, 2001.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p.163-170, jan.-mar. 2020.

CARRIÈRE-SWALLOW, Yan; HAKSAR, Vikram. The economics and implications of data: an integrated perspective. **International Monetary Fund**. Washington, n. 19, Sep. 2019.

CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.) . **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021.

CASTELLS, Manuel. **A sociedade em rede**. 22. ed. São Paulo: Paz e Terra, 2020.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CATALAN, Marcos. **A morte da culpa na responsabilidade contratual**. 2. ed. Indaiatuba: Editora Foco, 2019.

CENDON, Paolo. **Le persone: diritti della personalita**. Turim: Utet, 2000.

CHINELLATO, Silmara Juny de Abreu e MORATO, Antonio Carlos. **Direitos básicos de proteção de dados pessoais, o princípio da transparência e a proteção dos direitos intelectuais**: Tratado de proteção de dados pessoais. Tradução . Rio de Janeiro: Forense, 2023.

COHEN, Julie E. **Examined Lives**: Informational Privacy and the Subject as Object. Washington: Georgetown University Law Center, 2000. Disponível em: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?params=/context/facpub/article/1819/&path_info=examined.pdf. Acesso em: 19 abr. 2022.

COLOMBO, Cristiano. **Comentários à lei geral de proteção de dados pessoais**. Indaiatuba: Editora Foco, 2022.

CORDEIRO, A. Barreto Menezes (coord.). **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Coimbra: Almedina, 2021.

CORRÊA, Fernanda Alves. Os desafios da administração pública na adequação da LGPD: uma análise acerca de sua compatibilidade com a LAI e o amplo compartilhamento de dados. In: TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio. **Proteção de dados e tecnologia**: estudos da pós-graduação em Direito Digital. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq, 2022.

CORTAZIO, Renan Soares. Bancos de dados no Brasil: uma análise do Sistema Credit Scoring à luz da Lei n. 13.709/2018 (LGPD). **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro**, Rio de Janeiro, v. 2 n. 3, set./dez., p. 1-28, 2019. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/download/99/72/126. Acesso em: 19 abr. 2022.

COULDRY, Nick; MEJIAS, Ulises. Data colonialism: rethinking big data's relation to the contemporary subject. **Television and New Media**, [*s*. *l*.], 2018. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf. Acesso em: 19 abr. 2022.

COVELLO, Sergio Carlos. O sigilo bancário como proteção à intimidade. **Revista de direito bancário e de mercado de capitais**, [*s*. *l*.], v. 1, n. 3, p. 89-90, set./dez. 1998.

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da lei geral de proteção de dados pessoais. **Revista de Direito Privado**, São Paulo, v. 98, p. 161-186, mar./abr., 2019.

CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital**: a experiência de elaboração legislativa do Marco Civil da Internet. 2015. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: www.dataprivacybr.org/wp-content/uploads/2020/04/Os-dados-e-o-vi%CC%81rus.pdfhttps://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 3 ago. 2022.

DALLARI, Dalmo de Abreu. O Habeas Data no sistema jurídico brasileiro. **Revista da Faculdade de Direito**, São Paulo, v. 93, p. 239-253, 2002. Disponível em: https://www.revistas.usp.br/rfdusp/article/download/67544/70154/88966. Acesso em: 3 ago. 2022.

DATA PRIVACY, 2020. **Dados e o vírus**. São Paulo: Data Privacy, 2020 Disponível em: https:// Acesso em: 14 de maio. 2021.

DEVLIN, K. **Infoscience**: Turning Information into Knowledge. New York: W.H. Freeman, 1999.

DIDEROT, Denis; D'ALEMBERT, Jean Le Rond d'. **Encyclopédie 1, ou dictionnaire raisonné des sciences, des arts et des métiers Poche**. [*S*. *l*.]: Flammarion, 1993.

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. **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. Os direitos de personalidade no código civil. R**evista da Faculdade de Direito dos Campos**, Goytacazes, n. 6, 2005.

DONEDA, Danilo. **Privacy in the digital age**. Brasília, DF: ITU 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; MENDES, Laura Shertel. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DOSHI-VELEZ, Finale; KORTZ, Mason. Accountability of al under the law: the role of explanation. Cambridge: DASH Harvard, 2017.

DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In*: PASQUALOTTO, Adalberto *et al*. **Responsabilidade civil**: novos riscos. Indaiatuba: Editora Foco, 2019.

DUGUIT, Léon. **Fundamentos do Direito**. São Paulo: Ícone, 1996.

EUROPEAN COMMISSION. **Article 29 Data Protection Working Party**. Bruxelas: European Commission, 2017. Disponível em: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827. Acesso em: 05 de abr. de 2022.

EUROPEAN COMMISSION. **Data Protection Rules Fit for a digital and globalized age, Press Statement**. [*S. l.*]: European Commission, 2015.

FRAZÃO, Ana. **Discriminação algoritmica**: por que os algoritmos preocupam quando acertam e quando erram? Parte VIII. [*S. l.*: *s. n.*] Disponível em: https://www.professoraanafrazao.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.pdf. Acesso em 20 dez 2021.

FREITAS, Augusto Teixeira de. **Consolidação das leis civis**. Rio de Janeiro: J.R. dos Santos, 1915.

FUCUTA, Brenda. **Hipnotizados**: O que os nossos filhos fazem na internet e o que a internet faz com eles. Rio de Janeiro: Objetiva, 2018.

GAGLIANO, P. S.; PAMPLONA FILHO, R. **Novo curso de direito civil**: parte geral. 18. ed. rev. e atual. São Paulo: Saraiva, 2016.

GDPR. **Regulamento Geral de Proteção de Dados**. [*S. l.*]: União Europeia, 2016.

GHERARDI, Carlo; GHIELMETTI, Sílvia. Escoragem de Crédito: Metodologia que identifica Estatisticamente o Risco de Crédito. **Tecnologia do Crédito**, São Paulo, Ano 1, n. 2, set. 1997.

GIBSON, Willian. **Neuromancer**. Nova York: Ace Books, 1984.

GOMES, Orlando. **Código Civil**: Projeto Orlando Gomes. [*S. l.*; *s. n.*], 1985.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. 12 ed. São Paulo: Saraiva, 2014.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**. São Paulo: Saraiva, 2022.

GONÇALVES, Diogo Costa. **Lições de Direitos de Personalidade**: Dogmática Geral e Tutela Nuclear. São Paulo: Principia, 2022.

GREENLEAF, Graham; COTTIER, Bertil. 2020 Ends a Decade of 62 New Data Privacy Laws. **SSRN**, [s. l.], 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611. Acesso em: 3 ago. 2022.

GUERREIRO, Ruth ; TEIXEIRA, Tarcisio. **Lei Geral de Proteção de Dados Pessoais**: Comentada artigo por artigo: 4. ed. São Paulo: Saraiva, 2022.

GUIMARÃES, Graziely Rodrigues. Critérios e limites para o tratamento de dados realizado no enfrentamento da Covid- 19. **Revista dos Estudantes de Direito da Universidade de Brasília**, Brasília, DF, 19. ed., 2021https://periodicos.unb.br/index.php/redunb/article/view/37324/30321. Acesso em: 3 ago. 2022.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HUBMANN, **Heinrich. Das Persönlichkeitsrecht**. 2. ed. Köln: Böhlau, 1967.

HURLEY, Mikella; ADEBAYO, Julius. Credit scoring in the era of big data. **The Yale Journal of Law & Technology**, v. 18, 2016.

IDEC. **Após pressão da sociedade, Senado aprova Lei de Dados Pessoais**. São Paulo: IDEC, 2018. Disponível 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.

INSTITUTO DE PESQUISAS ECONÔMICAS APLICADAS. **Risco de Crédito**: desenvolvimento do modelo credit scoring para a gestão da inadimplência de uma instituição de microcrédito. Brasília, DF: Ipea, 2006. Disponível em: http://www.ipea.gov.br/ipeacaixa/premio2006/docs/trabpremiados/IpeaCaixa2006_Profissional_02lugar_tema03.pdf. Acesso em: 9 dez. 2022.

JUNQUEIRA, Thiago. **Seguros para os riscos impostos pelo uso da inteligência artificial**. [*S. l.*]: Consultor Jurídico. 2022.

KANT, Immanuel. **Crítica da razão pura**. São Paulo: Nova Cultural, 1987.

KELSEN, Hans. **Teoria pura do Direito**. [*S. l.*]: Forense Universitária, 2009.

KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. **The age of AI**: and our human future. [*S. l.*]: Little Brown and Company, 2021.

LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial**: entre categorias e conceitos, a busca por marcos regulatórios. São Paulo: Editora Foco, 2022.

LENK, Hans. **What is responsability?**. [*S. l.*]: Philosophy now, 2006. Disponível em: https://philosophynow.org/issues/56/What_is_Responsibility.

LEWIS, E. M. **An introduction to credit scoring**. San Rafael: Fair, Isaac and Co., Inc. 1992.

Liability . In: CAMBRIDGE Dictionary. Cambridge: Cambridge University Press & Assessment, c2022. https://dictionary.cambridge.org/pt/dicionario/ingles/liability. Acesso em: 3 ago. 2022.

LIMA, Cíntia Rosa Pereira; PEROLI, Kelvin. Aplicação da Lei Geral de Proteção de Dados do Brasil no Tempo e no Espaço. *In*: LIMA, Cíntia Rosa Pereira(coord.). **Comentários à lei geral de proteção de dados**. São Paulo: Almedina, 2020.

LÔBO, Paulo. **Direito Civil**: Parte Geral: Volume 1. São Paulo: Saraiva, 2022.

LÔBO, Paulo. **Direito Civil**: Volume 1: Parte Geral. 11. ed. São Paulo: Saraiva, 2022.

LOTUFO, Renan. **Curso avançado de direito civil: parte geral**. São Paulo: RT, 2002.

MAGRANI, Eduardo. Entre dados e robôs. **Ética e Privacidade na Era da Hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

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 Magalhães; LONGHI, João Victor Rozatti. Responsabilidade civil na Lei Geral de Proteção de Dados,consumo e a intensificação da proteção da pessoa humana na internet. **Revista de Direito do Consumidor**, São Paulo, n. 139, jan./fev. 2022.

MATTIETTO, Leonardo. Dos direitos da personalidade à cláusula geral de proteção da pessoa. **Revista de Direito da Procuradoria Geral**, Rio de Janeiro, edição especial, 2017. Disponível em: https://pge.rj.gov.br/comum/code/MostrarArquivo.php?C=MTM1ODc%2C. Acesso em: 13 mar. 2023.

MEDON, Filipe. **Inteligência artificial e responsabilidade civil**: autonomia, riscos e solidariedade. Salvador: JusPodivm, 2020.

MEDON, Filipe; FALEIROS JÚNIOR, José Luiz de Moura. Discriminação algorítmica de preços, Perfilização e Responsabilidade civil nas relações de consumo. *Revista Direito e Responsabilidade*, Coimbra, a. 3, p. 94-969, 2021.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: https://ojs.unifor.br/rpen/article/download/10828/pdf/44878. Acesso em: 3 ago. 2022.

MENDES, Laura Schertel Ferreira. Habeas Data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/download/655/905/2765. Acesso em: 20 ago. 2022.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, ano 28, p. 157-180, jul.-ago. 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista de Direito Público**, [*s. l.*], 2019.

MENDES, Laura Schertel; RODRIGUES JÚNIOR. Otavio Luiz; FONSECA, Gabriel Campos Soares da. Fundamentos constitucionais: o Direito Fundamental à Proteção De Dados *In*: MENDES, Laura Schertel *et al*. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 61-72.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB**, ano 5, n. 1, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. Acesso em: 3 ago. 2022.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. [*S. l.*]: Migalhas, 2020. https://menkeadvogados.com.br/wp-content/uploads/2020/11/MenkeAudoterminac%CC%A7a%CC%83oInformativa.pdf.

MEYER, Maximiliano. **Como robôs influenciaram as eleições de 2014 no Brasil**. [*S. l.*]: NIC.BR, 2018 Disponível em: https://nic.br/noticia/na-midia/como-robos-influenciaram-as-eleicoes-de-2014-no-brasil/. Acesso em: 10 nov. 2020.

MICHAELIS, 2023. **Personalidade**. [*S. l.*]: Editora Melhoramentos, c2023. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/personalidade. Acesso em: 28 jan. 2023.

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**. [*S. l.*]: 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.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. **Instituto Igarapé**, [*s. l.*], n. 39, 2018.

MORAES, Maria Celina Bodin de. Prefácio. In: SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Atlas, 2007.

MORAES, Maria Celina Bodin. LGPD: um novo regime de responsabilização civil dito "proativo". **Editorial a Civilistica.com**, Rio de Janeiro, a. 8, n. 3, 2019. Disponivel em: https://civilistica.com/wp-content/uploads1/2020/04/Editorial-civilistica.com-a.8.n.3.2019-2.pdf. Acesso em: 29 ago. 2021.

MULHOLLAND, Caitlin**. A LGPD e o novo marco normativo no Brasil**.Porto Alegre: Arquipélago, 2020.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de Direitos Fundamentais. Uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18). **R. Dir. Gar. Fund.**, Vitória, 2018, v. 19, n. 3, p. 159-180.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. **Revista de Informação Legislativa**, Brasília, DF, v. 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: https://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265.pdf. 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 (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

ORWELL, George. **1984**. New York: Penguin/Signet Classics, 2021.

PAGALLO, Ugo. **The laws of robots**: crimes, contracts, and torts. Dordrecht: Springer, 2013.

PASQUALE, Frank. **The Black Box Society**. Cambridge: Harvard University Press, 2015.

PECK, Patrícia. **Proteção de Dados Pessoais**: comentários à Lei nº 13.709/2018 LGPD. São Paulo: Saraiva, 2018.

PEREIRA, Laudelina; SILVA, Tarcísio. Laudelina. Literacia midiática e algorítmica em prol de engajamento cidadão sobre escores de crédito. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Casa do Direito, 2022.

PERLINGIERI, Pietro. P**erfis do Direito Civil**: introdução ao Direito Civil Constitucional. [*S. l.*]: Editora Renovar, 2022.

PRIVACY INTERNATIONAL. **Asked an online tracking company for all of my data and here's what I found**. [*S. l.*]: PI, 2018.

PROVOST, Foster; FAWCETT, Tom. **Data Science para negócios**. Rio de Janeiro: Alta Books, 2016.

PUECHE, José Enrique. **Manual sobre bienes y derechos de la personalidad**. 2. ed.i Madrid: Dykinson, 2008.

QUIJANO, Aníbal. Colonialidade do poder e classificação social. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula (org.). **Epistemologias do Sul**, Coimbra: Almedina, 2009.

RAMOS, Carmem Lúcia Silveira. **Diálogos sobre Direito Civil**: Construindo a Racionalidade Contemporânea. Rio de Janeiro: Renovar, 2002.

RIO DE JANEIRO (Estado). **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. Rio de Janeiro: Assembléia Legislativa do Estado do Rio de Janeiro, 1984. http://alerjln1.alerj.rj.gov.br/contlei.nsf/f25571cac4a61011032564fe0052c89c/664ba2b6d609873803256560005880 55?OpenDocument&ExpandSection=-2. Acesso em: 3 ago. 2022.

RIO DE JANEIRO. **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, DF: Governo do Estado do Rio de Janeiro, 1984. Disponível em: https://gov-rj.jusbrasil.com.br/legislacao/149858/lei-824-84. Acesso em: 10 ago. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. A LGPD e a despersonalização da personalidade. [*S. l.*]:. Migalhas. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350374/a-lgpd-e-a-despersonalizacao-da-personalidade. Acesso em: 15 set. 2021.

ROSSNAGEL, A. Einleitung. *In*: ROSSNAGEL, A. (org.). **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.

SALEME, Edson Ricardo. **Direito Constituciona**l. 3. ed. Barueri: Manole, 2020.

SANTOS, Fernando Ferreira. **Princípio Constitucional da Dignidade da pessoa humana**. Fortaleza: Celso Bastos, 1999.

SANTOS, Romualdo Baptista dos. **Responsabilidade civil por dano enorme**. Curitiba: Juruá, 2018.

SARLET, Ingo. Proteção de dados pessoais como direito fundamental na Constituição Federal de 1988: contributo para uma construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, v. 14, n. 42, jan./jun. 2020, p. 179-218. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 20 ago. 2022.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

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, nov. 2017.

SESSAREGO, Carlos Fernández. **Protección jurídica de la persona**. Lima: Uni-versidad de Lima, 1992.

SICSÚ, Abraham Laredo. **Credit Scoring**: desenvolvimento, implantação, acompanhamento. São Paulo: Blucher, 2010.

SILVA, Filipe Carreira da. **Espaço Público em Habermas**. Cambridge: Universidade de Cambridge, 2001. Disponível em: https://repositorio.ul.pt/bitstream/10451/22584/1/ICS_FCSilva_Espaco_LAN.pdf. Acesso em: 3 ago. 2022.

SILVA, João Calvão da. **Cumprimento e sanção pecuniária compulsória**. 2. ed. Coimbra: Coimbra Editora, 1995.

SILVA, José Afonso. **Curso de direito constitucional positivo**. 37 ed. São Paulo: Malheiros, 2013.

SILVA, Luciana Ferreira da; SANTOS, Pedro Otto Souza; JESUS, Tâmara Silene Moura de. Novos contornos do direito à privacidade: *Profiling* e a proteção de dados pessoais. **Brazilian Journal of Development**, Curitiba, v. 7, n. 11, p.104173-104185 nov. 2021. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/issue/view/149. Acesso em: 10 mar. 2023.

SILVA; Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos . O tratamento de dados pessoais no combate à COVID-19: entre soluções e danos colaterais. *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo. **Direito Civil e tecnologia**. 2020.

SILVEIRA, Victor doering da. **O consumidor na era da pontuação de crédito**. Letramento: 2022.

SIMÃO, Bárbara; OMS, Juliana. Pontuação de crédito e cadastro positivo: diferenças, complementaridades e assimetrias regulatórias. *In*: SIMÃO, Bárbara Prado *et al*. **O consumidor na era da pontuação de crédito**. Belo Horizonte: Casa de Direito, 2022.

SOUSA, R. V. A. Capelo de. **O Direito Geral de Personalidade**. Coimbra: Almedina, 1995.

SRNICEK, Nick. **Capitalismo de Plataformas**. Caja Negra: Buenos Aires, 2018.

STANFORD. **The rule of law**. Califórnia: Stanford University, 2016. Disponível em: https://plato.stanford.edu/entries/ruleof-law/. Acesso em: 9 dez. 2022.

STEINMÜLLER, Wilhelm *et al*. **Grundfragen des Datenschutzes**. [*S. l.*]Bundesministerium des Innern: 1971.

SWANT, Marty. **As marcas mais valiosas do mundo**. [*S. l.*]: Forbes, 2020. Disponível em: https://forbes.com.br/listas/2020/07/as-marcas-mais-valiosas-do-mundo-em-2020/. Acesso em: 1 ago. 2020.

TARTUCE, Flavio. **Manual de Direito Civil**. 8. ed. rev., atual. e ampl. São Paulo: Método, 2018.

TARTUCE, Flávio. **Manual de Direito Civil**: Volume único. 6 ed. São Paulo: Editora Forense, 2016.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais, privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, 2017. Disponível em: https://ojs.unifor.br/rpen/article/view/6272/pdf. Acesso em: 9 dez. 2022.

TEPEDINO, Gustavo. Contornos constitucionais da propriedade privada. *In*: TEPEDINO, Gustavo. **Temas de Direito Civil**. Rio de Janeiro: Renovar, 1999.

TEPEDINO, Gustavo. **Crise de fontes normativas e técnica legislativa na parte geral do Código Civil de 2002**. In: TEPEDINO, Gustavo. A parte geral do novo código civil: estudos na perspectiva civil constitucional. Rio de Janeiro: Renovar, 2003.

TEPEDINO, Gustavo. **Temas de direito civil**. Editora Renovar: Rio de Janeiro, 1999.

THE ECONOMIST. **The end of privacy**. [*S. l.*]: The Economist, 1999. Disponível em: https://www.economist.com/leaders/1999/04/29/the-end-of-privacy. Acesso em: 2 ago. 2020.

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.

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 de maio. 2021.

UNIÃO EUROPEIA. **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**. Bruxelas: Jornal Oficial da União Europeia, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046. Acesso em: 09 de abril de 2022.

UNIÃO EUROPEIA. **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial**. Bruxelas: Jornal Oficial da União Europeia, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em: 09 de abr. 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 09 de abr. 2022.

UNIVERSIDADE DE COIMBRA. **Boletim da Faculdade de Direito**. Coimbra: Universidade de Coimbra, 1999.

VAINZOF Rony. Disposições preliminares. *In*: BLUM, Renato Opice; MALDONADO, Viviane Nobrega (Coord.), **LGPD: lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters Brasil, 2019.

VENOSA, Sílvio de Salvo. **Curso de direito civil brasileiro**. 3. ed. São Paulo: Atlas, 2003.

VENTURI, Thais Goveia Pascoaloto. **Responsabilidade civil preventiva**: a proteção contra a violação dos direitos e a tutela inibitória material. São Paulo: 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. **Oficina do Historiador**, Porto Alegre, Suplemento especial, 2014, p.1448-1471. Disponível em**:** http://revistaseletronicas.pucrs.br/ojs/index.php/oficinadohistoriador/article/view/18998/12057. Acesso em: 10 nov. 2020.

VICENTE, E. F. R. **A estimativa do risco na constituição da PDD**. 2001. Dissertação (Mestrado em Administração) - Universidade de São Paulo, São Paulo, 2001.

VILARINO, Ramon. **O consumidor na era da pontuação de crédito**. Forense: 2022.

WALD, Arnoldo; FONSECA, Rodrigo Garcia da. O Habeas Data na Lei nº 9.507/97. **Rev. Minist. Público**, Rio de Janeiro, v. 7, 1998. Disponível em: https://www.mprj.mp.br/documents/20184/2845503/Arnoldo_Wald___Rodrigo_Garcia_da_Fonseca.pdf. Acesso em: 3 ago. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Boston v. 4, 15 dec. 1890. Disponível em: https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 2 ago. 2021.

WEINRIB, Ernest J. The disintegration of duty. *In*: MADDEN, M. Stuart (Ed.). **Exploring tort law**. Cambridge: Cambridge University Press, 2005

WINEGAR, Angela G.; SUNSTEIN, Cass R. How much is data privacy worth? A preliminary investigation. **Journal of Consumer Policy**, [*s*. *l*.], v. 42, p. 1-16, 2019.

WYDEN. **Como posso ajuda-lo**. [*S*. *l*.]: United States Senate, 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.

ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor**. São Paulo: Revista dos Tribunais, 2019.

ZUBOFF, Shoshana. **Era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.